University of Mississippi

eGrove

Guides, Handbooks and Manuals

American Institute of Certified Public Accountants (AICPA) Historical Collection

6-1-2005

AICPA Technical Practice Aids, as of June 1, 2005, Volume 2

American Institute of Certified Public Accountants (AICPA)

Follow this and additional works at: https://egrove.olemiss.edu/aicpa_guides

Part of the Accounting Commons

AICPA Technical Practice Aids

As of June 1, 2005

Volume 2

AICPA

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

AICPA Technical Practice Aids

Volume 2

Statements of Position
Auditing and Attestation

Practice Alerts

Suitable Trust Services Criteria and Illustrations

As of June 1, 2005

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

AICPA Technical Practice Aids

Volume 2

Statements of Position
Auditing and Attestation

Practice Alerts

Suitable Trust Services Criteria and Illustrations

As of June 1, 2005

Copyright © 2005 by
the American Institute of Certified Public Accountants, Inc.,
New York, NY 10036-8775

All rights reserved. For information about the procedure for requesting permission to make copies of any part of this work, please visit www.aicpa.org. A Permissions Request Form for e-mailing requests and information on fees are available there by clicking on the copyright notice at the foot of the AICPA homepage.

1 2 3 4 5 6 7 8 9 0 AAP 0 9 8 7 6 5

ISBN 0-87051-543-8

CHANGES AFFECTING VOLUME 2

Statements of Position—Auditing and Attestation Recently Added

Statement	Title	Addition Date	Section
SOP 04-1	*Auditing the Statement of Social Insurance*	November 2004	14,410

Practice Alerts Recently Added

Statement	Title	Addition Date	Section
PA 04-1	*Illegal Acts*	November 2004	16,270

Practice Alerts Recently Deleted

Statement	Title	Deleted By	Section
PA 02-1	*Communications With the Securities and Exchange Commission*	SEC Document, *Guidance for Consulting on Accounting Matters with the Office of the Chief Accountant*	[16,210]

TABLE OF CONTENTS

VOLUME 2

.... How to Use Volume 2 1

STATEMENTS OF POSITION
AUDITING AND ATTESTATION

.... Introduction 30,201

14,000 Statements of Position—Auditing and Attestation 30,211

[14,010] Revision of Form of Auditor's Report (7/74)

[14,020] Audits of Brokers and Dealers in Securities (12/76)

[14,030] Clarification of Accounting, Auditing, and Reporting Practices Relating to Hospital Malpractice Loss Contingencies (3/78)

14,040 Confirmation of Insurance Policies in Force (8/78)

[14,050] Report on a Financial Feasibility Study (10/82)

14,060 Auditing Property and Liability Reinsurance (10/82)

14,070 Auditing Life Reinsurance (11/84)

[14,080] Illustrative Auditor's Reports on Financial Statements of Employee Benefit Plans Comporting With Statement on Auditing Standards No. 58, *Reports on Audited Financial Statements* (SOP 88-2)

[14,090] Reports on Audited Financial Statements of Brokers and Dealers in Securities (SOP 89-1)

14,100 Reports on Audited Financial Statements of Investment Companies (SOP 89-2)

14,110 Questions Concerning Accountants' Services on Prospective Financial Statements (SOP 89-3)

[14,120] Reports on the Internal Control Structure in Audits of Brokers and Dealers in Securities (SOP 89-4)

[14,130] Auditors' Reports in Audits of State and Local Governmental Units (SOP 89-6)

14,140 Report on the Internal Control Structure in Audits of Investment Companies (SOP 89-7)

14,150 Accountants' Services on Prospective Financial Statements for Internal Use Only and Partial Presentations (SOP 90-1)

14,160 Report on the Internal Control Structure in Audits of Futures Commission Merchants (SOP 90-2)

[14,170] Auditors' Reports Under U.S. Department of Housing and Urban Development's Audit Guide for Mortgagors Having HUD Insured or Secretary Held Multifamily Mortgages (SOP 90-4)

VOLUME 2—continued

Section *Page*

14,000 Statements of Position—Auditing and Attestation—continued

[14,180] Inquiries of Representatives of Financial Institution Regulatory Agencies (SOP 90-5)

[14,190] Directors' Examinations of Banks (SOP 90-6)

[14,200] The Auditor's Consideration of the Internal Control Structure Used in Administering Federal Financial Assistance Programs Under the Single Audit Act (SOP 90-9)

[14,210] Reports on Audited Financial Statements of Property and Liability Insurance Companies (SOP 90-10)

14,220 Questions and Answers on the Term *Reasonably Objective Basis* and Other Issues Affecting Prospective Financial Statements (SOP 92-2)

14,230 Auditing Insurance Entities' Loss Reserves (SOP 92-4)

[14,240] Audits of State and Local Governmental Entities Receiving Federal Financial Assistance (SOP 92-7)

14,250 Auditing Property/Casualty Insurance Entities' Statutory Financial Statements—Applying Certain Requirements of the NAIC Annual Statement Instructions (SOP 92-8)

[14,260] Audits of Not-for-Profit Organizations Receiving Federal Awards (SOP 92-9)

14,270 Reporting on Required Supplementary Information Accompanying Compiled or Reviewed Financial Statements of Common Interest Realty Associations (SOP 93-5)

14,280 The Auditor's Consideration of Regulatory Risk-Based Capital for Life Insurance Enterprises (SOP 93-8)

14,290 Inquiries of State Insurance Regulators (SOP 94-1)

14,300 Letters for State Insurance Regulators to Comply With the NAIC Model Audit Rule (SOP 95-4)

14,310 Auditor's Reporting on Statutory Financial Statements of Insurance Enterprises (SOP 95-5)

[14,320] Audits of States, Local Governments, and Not-for-Profit Organizations Receiving Federal Awards (SOP 98-3)

14,330 Reporting on Management's Assessment Pursuant to the Life Insurance Ethical Market Conduct Program of the Insurance Marketplace Standards Association (SOP 98-6)

[14,340] Engagements to Perform Year 2000 Agreed-Upon Procedures Attestation Engagements Pursuant to Rule 17a-5 of the Securities Exchange Act of 1934, Rule 17Ad-18 of the Securities Exchange Act of 1934, and Advisories No. 17-98 and No. 42-98 of the Commodity Futures Trading Commission (SOP 98-8)

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

VOLUME 2—continued

Section *Page*

14,000 Statements of Position—Auditing and Attestation—continued
- 14,350 Guidance to Practitioners in Conducting and Reporting on an Agreed-Upon Procedures Engagement to Assist Management in Evaluating the Effectiveness of Its Corporate Compliance Program (SOP 99-1)
- 14,360 Auditing Health Care Third-Party Revenues and Related Receivables (SOP 00-1)
- 14,370 Performing Agreed-Upon Procedures Engagements That Address Internal Control Derivative Transactions as Required by the New York State Insurance Law (SOP 01-3)
- 14,380 Reporting Pursuant to the Association for Investment Management and Research Performance Presentation Standards (SOP 01-4)
- 14,390 Performing Agreed-Upon Procedures Engagements That Address Annual Claims Prompt Payment Reports as Required by the New Jersey Administrative Code (SOP 02-1)
- 14,400 Attest Engagements on Greenhouse Gas Emissions Information (SOP 03-2)
- 14,410 Auditing the Statement of Social Insurance (SOP 04-1)

PRACTICE ALERTS

16,000 Practice Alerts 50,741
- 16,010 Dealing With Audit Differences
- 16,020 Auditing Inventories—Physical Observations
- [16,030] Acceptance and Continuance of Audit Clients
- [16,040] Revenue Recognition Issues
- [16,050] Auditing Related Parties and Related-Party Transactions
- 16,060 The Private Securities Litigation Reform Act of 1995
- 16,070 Members in Public Accounting Firms
- 16,080 Audits of Employee Benefit Plans
- 16,090 Changes in Auditors and Related Topics
- 16,100 The Auditor's Use of Analytical Procedures
- 16,110 Professional Skepticism and Related Topics
- 16,120 Responding to the Risk of Improper Revenue Recognition
- 16,130 Guidance for Independence Discussions With Audit Committees
- 16,140 How the Use of a Service Organization Affects Internal Control Considerations
- 16,150 Accounting for Certain Equity Transactions
- 16,160 Guidance for Communication With Audit Committees Regarding Alternative Treatments of Financial Information Within Generally Accepted Accounting Principles
- 16,170 Auditing Construction Contracts

VOLUME 2—continued

Section *Page*

16,000 Practice Alerts—continued
- [16,180] Quarterly Review Procedures for Public Companies
- 16,190 Common Peer Review Recommendations
- 16,200 Audit Considerations in Times of Economic Uncertainty
- [16,210] Communications With the Securities and Exchange Commission
- 16,220 Use of Specialists
- 16,230 Reauditing Financial Statements
- 16,240 Audit Confirmations
- 16,250 Journal Entries and Other Adjustments
- 16,260 Acceptance and Continuance of Clients and Engagements
- 16,270 Illegal Acts

SUITABLE TRUST SERVICES CRITERIA AND ILLUSTRATIONS

17,000 Suitable Trust Services Criteria and Illustrations 52,001
- 17,100 Suitable Trust Services Criteria and Illustrations for Security, Availability, Processing Integrity, Online Privacy, and Confidentiality (Including WebTrust® and SysTrust®)
- 17,200 Suitable Trust Services Criteria and Illustrations for WebTrust® for Certification Authorities

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

HOW TO USE VOLUME 2

Scope of Volume 2 . . .

This volume, which is a reprint of a portion of volume 2 of the looseleaf edition of *Technical Practice Aids*, includes Statements of Position—Auditing and Attestation of the Audit and Attest Standards Division of the American Institute of Certified Public Accountants (AICPA), Practice Alerts of the AICPA SEC Practice Section Professional Issues Task Force, and Suitable Trust Services Criteria and Illustrations of the AICPA Assurance Services Executive Committee.

How This Volume Is Arranged . . .

The contents of this volume are arranged as follows:

Statements of Position—Auditing and Attestation

Practice Alerts

Suitable Trust Services Criteria and Illustrations

How to Use This Volume . . .

The arrangement of material is indicated in the general table of contents at the front of the volume. There is a detailed table of contents covering the material within each major division.

STATEMENTS OF POSITION—AUDITING AND ATTESTATION

Statements of Position—Auditing and Attestation are assigned section numbers in chronological order as they are issued. Each paragraph or equivalent is decimally numbered for reference purposes.

PRACTICE ALERTS

Practice Alerts are assigned section numbers in chronological order as they are issued. Each paragraph or equivalent is decimally numbered for reference purposes.

SUITABLE TRUST SERVICES CRITERIA AND ILLUSTRATIONS

The Suitable Trust Services Criteria and Illustrations are assigned section numbers in chronological order as they are issued. Each paragraph or equivalent is decimally numbered for reference purposes.

[The next page is 30,201.]

STATEMENTS OF POSITION AUDITING AND ATTESTATION

Introduction

Auditing and Attestation Statements of Position are issued to achieve one or more of several objectives: to revise, clarify, or supplement guidance in previously issued Audit and Accounting Guides; to describe and provide implementation guidance for specific types of audit and attestation engagements; or to provide guidance on specialized areas in audit and attestation engagements. The auditing and attestation guidance in a Statement of Position has the same authority as auditing and attestation guidance in an Audit and Accounting Guide, and members should be aware that they may be asked to justify departures from such guidance if the quality of their work is questioned.

[The next page is 30,211.]

AUD Section 14,000

STATEMENTS OF POSITION AUDITING AND ATTESTATION

TABLE OF CONTENTS

Section		*Paragraph*
[14,010]	Revision of Form of Auditor's Report (7/74) [Superseded by the AICPA Audit and Accounting Guide *Audits of Property and Liability Insurance Companies*, 1990]	
[14,020]	Audits of Brokers and Dealers in Securities (12/76) [Withdrawn by inclusion in the AICPA Audit and Accounting Guide *Audits of Brokers and Dealers in Securities*, 1985]	
[14,030]	Clarification of Accounting, Auditing, and Reporting Practices Relating to Hospital Malpractice Loss Contingencies (3/78) [Superseded by the AICPA Audit and Accounting Guide, *Audits of Providers of Health Care Services*, 1990]	
14,040	Confirmation of Insurance Policies in Force (8/78)	.01-.05
	Effective Date	.05
[14,050]	Report on a Financial Feasibility Study (10/82) [Superseded by the AICPA *Guide for Prospective Financial Statements*, 1986]	
14,060	Auditing Property and Liability Reinsurance (10/82)	.01-.23
	Introduction	.01-.08
	Applicability and Scope	.08
	Ceded Reinsurance	.09-.13
	Internal Controls of the Ceding Company	.09-.10
	Auditing Procedures	.11-.13
	Assumed Reinsurance	.14-.19
	Internal Controls of the Assuming Company	.14-.15
	Auditing Procedures	.16-.18
	Pools, Associations, and Syndicates	.19
	Reinsurance Intermediaries	.20-.22
	Effective Date	.23
14,070	Auditing Life Reinsurance (11/84)	.01-.25
	Applicability	.01
	Introduction	.02-.13
	Generally Accepted Accounting Principles	.11-.12
	Scope	.13

Section		*Paragraph*
14,070	Auditing Life Reinsurance (11/84)—continued	
	Ceded Reinsurance	.14-.19
	Internal Controls of the Ceding Company	.14-.15
	Auditing Procedures	.16-.19
	Assumed Reinsurance	.20-.24
	Internal Controls of the Assuming Company	.20-.21
	Auditing Procedures	.22-.24
	Effective Date	.25
[14,080]	Illustrative Auditor's Reports on Financial Statements of Employee Benefit Plans Comporting With Statement on Auditing Standards No. 58, *Reports on Audited Financial Statements* (SOP 88-2) [Superseded by the AICPA Audit and Accounting Guide *Audits of Employee Benefit Plans*, 1991]	
[14,090]	Reports on Audited Financial Statements of Brokers and Dealers in Securities (SOP 89-1) [Superseded by and incorporated into the AICPA Audit and Accounting Guide *Brokers and Dealers in Securities*, 1997]	
14,100	Reports on Audited Financial Statements of Investment Companies (SOP 89-2)	.01-.02
	Introduction	.01
	Effective Date	.02
14,110	Questions Concerning Accountants' Services on Prospective Financial Statements (SOP 89-3)	.01-.23
	Reporting on Financial Forecasts That Include a Projected Sale of an Entity's Real Estate Investment	.01-.04
	Question	.01
	Answer	.02-.04
	Sales Prices Assumed When a Financial Forecast Includes a Projected Sale of an Entity's Real Estate Investment	.05-.09
	Question	.05-.06
	Answer	.07-.09
	Reporting on Information Accompanying a Financial Forecast in an Accountant-Submitted Document	.10-.13
	Question	.10
	Answer	.11-.13

Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section		Paragraph
14,110	Questions Concerning Accountants' Services on Prospective Financial Statements (SOP 89-3)—continued	
	Financial Projections Included in General-Use Documents	.14-.17
	Question	.14
	Answer	.15
	Question	.16
	Answer	.17
	Support for Tax Assumptions	.18-.20
	Question	.18
	Answer	.19-.20
	Periods Covered by an Accountant's Report on Prospective Financial Statements	.21-.23
	Question	.21
	Answer	.22-.23
[14,120]	Reports on the Internal Control Structure in Audits of Brokers and Dealers in Securities (SOP 89-4) [Superseded by and incorporated into the AICPA Audit and Accounting Guide *Brokers and Dealers in Securities*, 1997]	
[14,130]	Auditors' Reports in Audits of State and Local Governmental Units (SOP 89-6) [Superseded by and incorporated into SOP 92-7, *Audits of State and Local Governmental Entities Receiving Federal Financial Assistance*]	
14,140	Report on the Internal Control Structure in Audits of Investment Companies (SOP 89-7)	.01-.04
	Introduction	.01-.02
	Report on Internal Control Required by the SEC	.03
	Effective Date	.04
14,150	Accountants' Services on Prospective Financial Statements for Internal Use Only and Partial Presentations (SOP 90-1)	.01-.34
	Part I—Guidance on the Accountant's Services and Reports on Prospective Financial Statements for Internal Use Only	.01-.09
	Procedures	.03-.04
	Reporting	.05-.09
	Part II—Partial Presentations of Prospective Financial Information	.10-.32
	Introduction	.10-.13

Section		*Paragraph*
14,150	Accountants' Services on Prospective Financial Statements for Internal Use Only and Partial Presentations (SOP 90-1)—continued	
	Uses of Partial Presentations	.12-.13
	Preparation and Presentation of Partial Presentations	.14-.24
	Accountant's Involvement With Partial Presentations	.25-.32
	Compilation and Examination Procedures	.29
	Applying Agreed-Upon Procedures to Partial Presentations	.30
	Standard Accountant's Compilation, Examination, and Agreed-Upon Procedures Reports	.31-.32
	Effective Date	.33
	Appendix—Illustrations of Partial Presentations	.34
14,160	Report on the Internal Control Structure in Audits of Futures Commission Merchants (SOP 90-2)	.01-.04
	Introduction	.01-.02
	Report on Internal Control Required by CFTC Regulation 1.16	.03
	Effective Date	.04
[14,170]	Auditors' Reports Under U.S. Department of Housing and Urban Development's Audit Guide for Mortgagors Having HUD Insured or Secretary Held Multifamily Mortgages (SOP 90-4) [Superseded by the AICPA Auditing Standards Division, November 1992]	
[14,180]	Inquiries of Representatives of Financial Institutions (SOP 90-5) [Superseded by and incorporated into the AICPA Audit and Accounting Guide *Banks and Savings Institutions*, 1996]	
[14,190]	Directors' Examinations of Banks (SOP 90-6) [Superseded by and incorporated into the AICPA Audit and Accounting Guide *Banks and Savings Institutions*, 1996]	
[14,200]	The Auditor's Consideration of the Internal Control Structure Used in Administering Federal Financial Assistance Programs Under the Single Audit Act (SOP 90-9) [Superseded by and incorporated into SOP 92-7, *Audits of State and Local Governmental Entities Receiving Federal Financial Assistance*]	
[14,210]	Reports on Audited Financial Statements of Property and Liability Insurance Companies (SOP 90-10) [Superseded by SOP 95-5, *Auditor's Reporting on Statutory Financial Statements of Insurance Enterprises*]	

Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section		Paragraph
14,220	Questions and Answers on the Term *Reasonably Objective Basis* and Other Issues Affecting Prospective Financial Statements (SOP 92-2)	.01-.59
	Responsible Party's Basis for Presenting a Financial Forecast	.01-.43
	Consideration of the Length of the Forecast Period	.44-.46
	Disclosure of Long-Term Results	.47-.56
	The Accountant's Consideration of Whether the Responsible Party Has a Reasonably Objective Basis for Presenting a Financial Forecast	.57-.58
	Effective Date	.59
14,230	Auditing Insurance Entities' Loss Reserves (SOP 92-4)	.01-.107
	Introduction	.01
	Scope	.02-.03
	Effective Date	.04
	Chapter 1—Accounting for Loss Reserves	.05
	Chapter 2—The Loss Reserving Process	.06-.47
	Types of Business and Their Effect on the Estimation Process	.06-.10
	Policy Duration	.07
	Type of Coverage	.08
	Kind of Insurance Underwritten, Lines of Business, or Type of Risk	.09-.10
	Components of Loss Reserves	.11-.12
	Estimating Methods	.13-.31
	Illustrative Projection Data	.22-.31
	Loss Adjustment Expense Reserves	.32-.39
	ALAE Reserve Calculation Approaches	.33-.36
	ULAE Reserve Calculation Approaches	.37-.39
	Changes in the Environment	.40-.43
	Use of Specialists by Management in Determining Loss Reserves	.44-.47
	Chapter 3—Audit Planning	.48-.60
	Audit Objectives	.48-.49
	Audit Planning	.50-.54
	Audit Risk and Materiality	.55-.60
	Audit Risk	.56-.63
	Materiality	.64
	Chapter 4—Auditing Loss Reserves	.65-.106
	Auditing the Claims Data Base	.65-.66

Section		*Paragraph*
14,230	Auditing Insurance Entities' Loss Reserves (SOP 92-4)—continued	
	Evaluating the Reasonableness of the Estimate	.67-.75
	Selecting an Audit Approach	.67-.69
	Reviewing and Testing the Process Used by Management to Develop the Estimate	.70-.73
	Developing an Independent Expectation of the Estimate	.74-.75
	Analytical Procedures	.76-.77
	Loss Reserve Ranges	.78-.97
	Risk Factors and Developing a Range	.83-.90
	Evaluating the Financial Effect of a Reserve Range	.91-.96
	Auditor Uncertainty About the Reasonableness of Management's Estimate and Reporting Implications	.97
	Use of Specialists by Auditors in Evaluating Loss Reserves	.98-.100
	Evaluating the Reasonableness of Loss Adjustment Expense Reserves	.101-.102
	Ceded Reinsurance	.103-.106
	Understanding an Insurance Company's Reinsurance Program	.104-.106
	Appendix—Inherent and Control Risk Factors Affecting Loss Reserves	.107
[14,240]	Audits of State and Local Governmental Entities Receiving Federal Financial Assistance (SOP 92-7) [Superseded by the Audit and Accounting Guide *Audits of State and Local Governmental Units*, 1994]	
14,250	Auditing Property/Casualty Insurance Entities' Statutory Financial Statements—Applying Certain Requirements of the NAIC Annual Statement Instructions (SOP 92-8)	.01-.09
	Applicability	.01
	Introduction	.02-.03
	Auditing Procedures	.04-.08
	Effective Date	.09
[14,260]	Audits of Not-for-Profit Organizations Receiving Federal Awards (SOP 92-9) [Superseded by SOP 98-3, *Audits of States, Local Governments, and Not-for-Profit Organizations Receiving Federal Awards*. See section 14,320.]	

Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section		Paragraph
14,270	Reporting on Required Supplementary Information Accompanying Compiled or Reviewed Financial Statements of Common Interest Realty Associations (SOP 93-5)	.01-.08
14,280	The Auditor's Consideration of Regulatory Risk-Based Capital for Life Insurance Enterprises (SOP 93-8)	.01-.29
	Introduction and Scope	.01-.02
	Overview of Risk-Based Capital	.03-.05
	Audit Planning	.06
	Going-Concern Considerations	.07-.19
	Substantial Doubt Remains	.14-.18
	Independent Auditor's Reports	.15-.18
	Substantial Doubt Alleviated	.19
	Other Reporting Considerations	.20-.28
	Uncertainties	.20-.26
	Emphasis of a Matter	.27-.28
	Effective Date	.29
14,290	Inquiries of State Insurance Regulators (SOP 94-1)	.01-.12
	Introduction	.01
	Applicability	.02–.03
	Auditor's Consideration of State Regulatory Examinations	.04-.06
	Auditor's Consideration of Permitted Statutory Accounting Practices	.07-.11
	Effective Dates	.12
14,300	Letters for State Insurance Regulators to Comply With the NAIC Model Audit Rule (SOP 95-4)	.01-.13
	Introduction	.01-.02
	Scope	.03
	Conclusions—Form and Content	.04-.12
	Awareness	.04-.05
	Change in Auditor	.06-.07
	Qualifications	.08-.09
	Notification of Adverse Financial Condition	.10-.11
	Report on Internal Controls	.12
	Effective Date	.13
14,310	Auditor's Reporting on Statutory Financial Statements of Insurance Enterprises (SOP 95-5)	
	Introduction and Background	.01-.07
	Prescribed-or-Permitted Statutory Accounting Practices	04-.05
	NAIC-Codified Statutory Accounting	[.06]
	Other Relevant AICPA Pronouncements	.07

Section		*Paragraph*
14,310	Auditor's Reporting on Statutory Financial Statements of Insurance Enterprises (SOP 95-5)—continued	
	Applicability	.08-.09
	Conclusions	.10-.26
	Superseding Statement of Position 90-10, *Reports on Audited Financial Statements of Property and Liability Insurance Companies*	.10
	General Distribution Reports	.11-.15
	Limited Distribution Reports	.16-[.19]
	General and Limited Distribution Reports	.20-.25
	Mutual Life Insurance Enterprises	.26
	Effective Dates	.27
[14,320]	Audits of States, Local Governments, and Not-for-Profit Organizations Receiving Federal Awards (SOP 98-3) [Deleted by the AICPA Audit Guide *Audits of States, Local Governments, and Not-for-Profit Organizations Receiving Federal Awards*]	
14,330	Reporting on Management's Assessment Pursuant to the Life Insurance Ethical Market Conduct Program of the Insurance Marketplace Standards Association (SOP 98-6)	.01-.39
	Summary	
	Introduction and Background	.01-.02
	Scope	.03
	Overview of the IMSA Life Insurance Ethical Market Conduct Program	.04-.11
	Principles of Ethical Market Conduct	.04-.06
	IMSA Assessment Questionnaire	.07
	Insurance Marketplace Standards Association Membership and Certification Process	.08-.09
	IMSA Independent Assessor Application Process and Required Training	.10
	IMSA Assessment Handbook	.11
	Conclusions	.12-.23
	Planning the Engagement	.12-.16
	Establishing an Understanding With the Client	.17
	Assessments of Attestation Risk	.18-.20
	Evidential Matter	.21-.23
	Reporting Considerations	.24-.35
	Elements of the Report	.27-.35
	Effective Date	.36
	Appendix A—Assessment of Attestation Risk	.37
	Appendix B—Illustrative Procedures	.38
	Appendix C—Sample Engagement Letter	.39

Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section		Paragraph
[14,340]	Engagements to Perform Year 2000 Agreed-Upon Procedures Attestation Engagements Pursuant to Rule 17a-5 of the Securities Exchange Act of 1934, Rule 17Ad-18 of the Securities Exchange Act of 1934, and Advisories No. 17-98 and No. 42-98 of the Commodity Futures Trading Commission (SOP 98-8) (11/98) [Withdrawn due to the expiration of year 2000 readiness assertions of CTFC Advisory No. 17-98]	
14,350	Guidance to Practitioners in Conducting and Reporting on an Agreed-Upon Procedures Engagement to Assist Management in Evaluating the Effectiveness of Its Corporate Compliance Program (SOP 99-1)	.01-.36
	Summary	
	Introduction and Background	.01-.03
	Overview of a Typical Corporate Integrity Agreement	.04-.05
	Conditions for Engagement Performance	.06-.20
	Establishing an Understanding With the Client	.08
	Users' Responsibilities	.09-.10
	Practitioner's Responsibilities	.11-.14
	Involvement of a Specialist	.15-.17
	Internal Auditors and Other Personnel	.18-.20
	Planning the Engagement	.21
	Working Papers	.22-.23
	Management's Representations	.24
	Reporting Considerations	.25-.31
	Appendix A—Sample Corporate Integrity Agreement	.32
	Appendix B—Sample Statement of Management's Assertions	.33
	Appendix C—Sample Engagement Letter	.34
	Appendix D—Sample Procedures	.35
	Appendix E—Sample Report	.36
14,360	Auditing Health Care Third-Party Revenues and Related Receivables (SOP 00-1)	.01-.38
	Summary	
	Introduction and Background	.01-.04
	Scope and Applicability	.05
	Third-Party Revenues and Related Receivables—Inherent Uncertainties	.06-.08
	Management's Responsibilities	.09-.11
	The Auditor's Responsibilities	.12-.15
	Evidential Matter	.16-.21
	Potential Departures From GAAP Related to Estimates and Uncertainties	.22-.37
	Unreasonable Accounting Estimates	.24-.30
	Inappropriate Accounting Principles	.31-.33
	Inadequate Disclosure	.34-.37
	Appendix—Other Considerations Related to Government Investigations	.38

Section		Paragraph
14,370	Performing Agreed-Upon Procedures Engagements That Address Internal Control Over Derivative Transactions as Required by the New York State Insurance Law (SOP 01-3)	.01-.38
	Introduction and Background	.01-.06
	Applicability	.07-.08
	The Law	.09-.12
	Definition of a Derivative	.09-.11
	Derivative Use Plan	.12
	Related Professional Standards	.13-.19
	AT Section 201, "Agreed-Upon Procedures Engagements," Statement on Standards for Attestation Engagements No. 10	.13-.16
	Statement on Auditing Standards No. 92, *Auditing Derivative Instruments, Hedging Activities, and Investments in Securities*	.17-.19
	Procedures to Be Performed	.20-.27
	Establishing an Understanding With the Client	.28
	Management Representations	.29-.31
	Restriction on the Performance of Procedures	.32-.33
	Dating the Report	.34
	Effective Date	.35
	Appendix A—Illustrative Agreed-Upon Procedures Report	.36
	Appendix B—Agreed-Upon Procedures for Testing Internal Control Over Derivative Transactions	.37
	Appendix C—Illustrative Management Representation Letter	.38
14,380	Reporting Pursuant to the Association for Investment Management and Research Performance Presentation Standards (SOP 01-4)	.01-.44
	Introduction and Background	.01-.06
	Scope	.07-.08
	Overview of the AIMR-PPS Standards	.09-.17
	Firmwide Compliance With the AIMR-PPS Standards	.09-.13
	Firmwide Verification and Performance Examination	.14-.17
	Examination Engagement	.18-.37
	Engagement Objectives	.18-.19
	Planning the Engagement	.20-.21
	Establishing an Understanding With the Client	.22-.23
	Obtaining Sufficient Evidence	.24-.29
	Representation Letter	.30
	Reporting	.31-.37
	SOP Effective Date	.38

Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section		Paragraph
14,380	Reporting Pursuant to the Association for Investment Management and Research Performance Presentation Standards (SOP 01-4)—continued	
	Appendix A—AIMR-PPS Guidance for a Level I Verification	.39
	Appendix B—AIMR-PPS Guidance for a Performance Examination (Level II)	.40
	Appendix C—Sample Engagement Letter: Level I Verification and Performance Examination (Level II)	.41
	Appendix D—Sample Management Representation Letter: Level I Verification and Performance Examination (Level II)	.42
	Appendix E—Illustrative Attest Reports: Level I Verification	.43
	Appendix F—Illustrative Attest Reports: Level I Verification and Performance Examination (Level II)	.44
14,390	Performing Agreed-Upon Procedures Engagements That Address Annual Claims Prompt Payment Reports as Required by the New Jersey Administrative Code (SOP 02-1)	.01-.29
	Introduction and Background	.01-.04
	Applicability	.05
	The Code	.06-.10
	Definitions	.06
	Reporting Requirements	.07-.10
	Related Professional Standards	.11-.13
	Chapter 2, "Agreed-Upon Procedures Engagements," of Statement on Standards for Attestation Engagements No. 10 (AT Sec. 201)	.11-.13
	Procedures to Be Performed	.14-.19
	Establishing an Understanding With the Client	.20
	Management Representations	.21-.23
	Restriction on the Performance of Procedures	.24
	Dating the Report	.25
	Effective Date	.26
	Appendix A—Illustrative Agreed-Upon Procedures Report	.27
	Appendix B—Agreed-Upon Procedures That Address Annual Claims Prompt Payment Reports as Required by the New Jersey Administrative Code	.28
	Appendix C—Illustrative Management Representation Letter	.29

Section		*Paragraph*
14,400	Attest Engagements on Greenhouse Gas Emissions Information (SOP 03-2)	.01-.84
	Background and Introduction	.01-.14
	Climate Change and Greenhouse Gases	.01-.03
	The Kyoto Protocol	.04-.06
	GHGs to Be Regulated by the Kyoto Protocol	.07
	Why U.S. Companies Are Considering Strategies to Address Their GHG Emissions	.08-.09
	GHG Emissions Trading Programs and GHG Registries in the United States	.10-.13
	Terms and Definitions Used by Registries and Regulatory Frameworks	.14
	Scope of SOP	.15-.16
	Engagement Acceptance Considerations	.17
	Independence	.18-.20
	Adequate Knowledge of Subject Matter and Use of a Specialist	.21-.29
	Criteria	.30-.36
	Attributes to Be Met by GHG Emission Reductions	.35-.36
	Materiality	.37
	Uncertainty in the Measurement of GHG Emissions	.38
	Consistency	.39
	Boundaries	.40
	Scopes for Reporting GHG Emissions: Direct and Indirect Emissions	.41-.44
	Baselines	.45
	Examination Engagement: GHG Inventory	.46-.48
	Objective of the Engagement	.46-.47
	Written Assertion by the Responsible Party	.48
	Examination Engagement: GHG Emission Reduction Information	.49-.54
	Objective of the Engagement	.49
	Written Assertion by the Responsible Party	.50
	Examples of GHG Emission Reduction Projects	.51
	Prerequisite for an Examination of GHG Emission Reduction Information	.52-.54
	Engagement Performance	.55-.63
	Planning the Examination Engagement	.55-.57
	Part of Attest Engagement Performed by Other Practitioners	.58
	Attestation Risk	.59-.60
	Obtaining Sufficient Evidence	.61-.63
	Consideration of Subsequent Events	.64
	Adequacy of Disclosure	.65
	Representation Letter	.66-.68

Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section		Paragraph
14,400	Attest Engagements on Greenhouse Gas Emissions Information (SOP 03-2)—continued	
	Reporting	.69-.77
	Attest Documentation	.78
	Effective Date	.79
	Appendix A—Glossary	.80
	Appendix B—Sources for GHG Emission Protocols and Calculation Tools	.81
	Appendix C—Illustrative Management Representation Letter	.82
	Appendix D—Illustrative Examination Reports on GHG Emissions Information	.83
	Appendix E—Illustrative Examination Reports on GHG Emission Reduction Information	.84
14,410	Auditing the Statement of Social Insurance (SOP 04-1)	.01-.23
	Introduction	.01-.03
	Applicability	.04
	Management's Responsibilities	.05-.08
	Preparing Social Insurance Estimates	.06
	Conceptual Model	.07
	Designing and Implementing Internal Control Related to Estimates	.08
	The Auditor's Responsibility	.09-.40
	Planning the Audit	.11-.31
	Performing Audit Procedures	.32-.36
	Reporting	.37-.40
	Effective Date and Transition	.41
	Appendix—Illustrative Controls and Audit Procedures	.42

[The next page is 30,291.]

Section 14,040

Confirmation of Insurance Policies in Force

August 1978

NOTICE TO READERS

The American Institute of Certified Public Accountants has issued a series of industry-oriented audit guides that present recommendations on auditing procedures and auditors' reports and in some instances on accounting principles, and a series of accounting guides that present recommendations on accounting principles. Based on experience in the application of those guides, AICPA committees may from time to time conclude that it is desirable to change a guide. A statement of position is used to revise or clarify certain of the recommendations in the guide to which it relates. A statement of position represents the considered judgment of the responsible AICPA committee.

To the extent that a statement of position is concerned with auditing procedures and auditors' reports, its degree of authority is the same as that of the audit guide to which it relates. As to those matters, members should be aware that they may be called on to justify departures from the recommendations of the committee.

To the extent that a statement of position relates to standards of financial accounting or reporting (accounting principles), the recommendations of the committee are subject to ultimate disposition by the Financial Accounting Standards Board. The recommendations are made for the purpose of urging the FASB to promulgate standards that the committee believes would be in the public interest.

.01 In February 1975, the AICPA Special Committee on Equity Funding stated ". . . except for certain observations relating to confirmation of insurance in force and auditing related party transactions, generally accepted auditing standards are adequate and . . . no changes are called for in the procedures commonly used by auditors." The AICPA industry audit guide, *Audits of Stock Life Insurance Companies* (paragraph 3.78), states: "It may also be appropriate to select in-force policies for confirmation directly with policyholders of premium amounts, date to which premiums are paid, policy loans, accumulated dividends, etc." The special committee recommended "that the Institute's auditing standards executive committee consider whether the Life Insurance Audit Guide requires clarification with regard to the confirmation of policies with policyholders."

.02 The special committee further stated:

> Another auditing procedure, which heretofore has not been considered particularly useful, is verification of the authenticity of a selected number of policies included in the in-force inventory by direct confirmation with the policyholders. Such a procedure has not generally been considered necessary because it would be unusual for companies to overstate liabilities. Inflation of the inventory of life insurance in force by a company that follows statutory accounting would result in an overstatement of the liability for future policyholder benefits and a reduction in current earnings. However, when companies report on the basis of generally accepted accounting principles (GAAP) there could be motivation for overstating insurance in force because it could result in an addition to current earnings.

There could be an additional motivation for overstating insurance in force when reinsurance of policies has the effect of materially increasing current earnings, which can occur when a company reports on the basis of either GAAP or statutory accounting. Reinsurance of life insurance policies permits the elimination of the related liability for future policyholder benefits. Under certain circumstances, reinsurance may also result in increasing current earnings to the extent that the proceeds received from reinsurance exceed expenses incurred in connection with the sale and servicing of the reinsured policies.

.03 As stated above, the audit guide suggests confirmation of insurance policies in force directly with policyholders; however, the audit guide does not discuss circumstances when confirmation would be appropriate and, as a result, practice has varied. The purpose of this statement of position is to identify those circumstances in which the independent auditor ordinarily should confirm insurance policies in force. This statement of position is applicable to both stock and mutual life insurance companies.

.04 Satisfactory results of the comparison of insurance policies in force with premium collections along with other ordinary auditing procedures (see paragraphs 3.70 through 3.90, 6.08 through 6.14, and 9.02 through 9.07 of the audit guide) will normally provide the auditor with sufficient competent evidential matter as to the validity of those policies included in the inventory of insurance policies in force. However, the auditor ordinarily should confirm insurance policies in force with policyholders in the following circumstances:

a. Proper maintenance of the inventory of insurance in force may be materially deficient due to an absence of segregation of duties or other controls.

b. Trend analyses or ratios that measure insurance in force indicate erratic or unusual results that have not been satisfactorily explained.

c. Additions to insurance in force cannot be related to the collection of premiums.

d. Significant amounts of insurance in force result from related party transactions, and the related party's financial statements are not audited by the auditor.

e. The company markets insurance products, such as those with immediate cash value features or with unusual commissions arrangements, that could motivate the agent to submit fictitious policies.

f. Ceded reinsurance activities can materially increase earnings or investable funds.

[Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Effective Date

.05 This statement of position provides for practices that may differ in certain respects from present acceptable practices. Accordingly, this statement of position will be effective for audits performed in accordance with generally accepted auditing standards for periods ending on or after December 31, 1978. [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Insurance Companies Committee

JOHN E. HART, *Chairman*
EDWARD F. BADER
CORMICK L. BRESLIN
FRANK A. BRUNI
JAMES L. GEORGE
WAYNE KAUTH
LOREN B. KRAMER
R. LAWRENCE SOARES
MICHAEL M. SONDERBY
RICHARD D. WAMPLER II

AICPA Staff

D.R. CARMICHAEL, *Vice President*
Auditing Standards

DAVID V. ROSCETTI, *Manager*
Auditing Standards

[The next page is 30,321.]

Section 14,060

Auditing Property and Liability Reinsurance

Supplements *Audits of Property and Liability Insurance Companies*

October 1982

NOTICE TO READERS

This Statement of Position presents recommendations of the Reinsurance Auditing and Accounting Task Force of the AICPA Insurance Companies Committee regarding the application of generally accepted auditing standards in auditing property and liability reinsurance. This Statement of Position supplements the audit and accounting guide *Audits of Property and Liability Insurance Companies*. It represents the considered opinion of the AICPA Reinsurance Auditing and Accounting Task Force on the best auditing practice in the industry and has been reviewed by members of the AICPA Auditing Standards Board for consistency with existing auditing standards. AICPA members may have to justify departures from the recommendations in this statement if their work is challenged.

Introduction

.01 Reinsurance is the assumption by one insurer of all or part of a risk originally undertaken by another insurer. Reinsurance is not transacted directly with the general public, but, instead, between insurance companies. In the United States there are basically three types of reinsurance entities: professional reinsurers, reinsurance departments of primary insurance companies, and various groups or syndicates of insurers referred to as reinsurance pools or associations.

- *Professional reinsurers*, while likely permitted by their charters and licenses to operate as primary insurance companies, engage almost exclusively in reinsurance.
- *Reinsurance departments* of primary insurance companies function as units of primary insurers and engage in the reinsurance business.
- *Reinsurance pools* (also referred to as associations or syndicates) may be organized to provide their members with reinsurance protection and management for certain specialized, high-risk coverage or with general access to the reinsurance market for traditional lines of business.

In addition, reinsurance intermediaries (including brokers, agents, managing general agents, and similar entities) facilitate the business of reinsurance by bringing together reinsurance purchasers and sellers. The functions of reinsurance entities may include underwriting, designing and negotiating the terms of reinsurance, placing reinsurance, accumulating and reporting transactions, distributing premiums, and collecting and settling claims.

.02 Major reasons for insurance companies to enter reinsurance contracts are to—

a. Reduce their exposure on particular risks or classes of risks.

b. Protect against accumulations of losses arising from catastrophes.

c. Reduce their total liabilities to a level appropriate to their premium volumes and amounts of capital.

d. Provide financial capacity to accept risks and policies involving amounts larger than could otherwise be accepted.

e. Help stabilize operating results.

f. Obtain assistance with new products and lines of insurance.

For similar reasons, reinsurers may at times reinsure their own risks with other insurance and reinsurance companies, a practice known as retrocession.

.03 Reinsurance may be transacted under broad, automatic contracts called "treaties," which are usually of long duration and which cover some portion of a particular class of business underwritten by the insurers. Reinsurance may also be transacted under "facultative" agreements, which cover specific individual risks and require the insurer and reinsurer to agree on terms and conditions of reinsuring each risk. Reinsurance may either be "pro rata," in which the reinsurer and the insurer share proportionately in the premiums and losses, or "excess," in which only the insurer's losses above a fixed point, known as the "retention," are reinsured. (For a description of the various types of reinsurance transactions, see the AICPA Audit and Accounting Guide *Audits of Property and Liability Insurance Companies*, chapter 6.) [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.04 In ceding all or part of a risk the "ceding company" does not discharge its primary liability to its insureds. The ceding company remains fully liable for the face amount of the policy issued. Through reinsurance, the ceding company reduces its maximum exposure in the event of loss by obtaining the right to reimbursement from the "assuming company" for the reinsured portion of the loss.

.05 The accounting entries for reinsurance ceded transactions are the opposite of the entries that arise from direct business. The amounts for reinsurance transactions are usually netted against the related accounts in financial statements. FASB Statement No. 60,* *Accounting and Reporting by Insurance Enterprises*, describes in paragraph 38 the accounting for ceded reinsurance:

> Amounts that are recoverable from reinsurers and that relate to paid claims and claim adjustment expenses shall be classified as assets, with an allowance for estimated uncollectible amounts. Estimated amounts recoverable from reinsurers that relate to the liabilities for unpaid claims and claim adjustment expenses shall be deducted from those liabilities. Ceded unearned premiums shall be netted with related unearned premiums. Receivables and payables from the same reinsurer, including amounts withheld, also shall be netted. Reinsurance premiums ceded and reinsurance recoveries on claims may be netted against related earned premiums and incurred claim costs in the income statement.[1]

---

* FASB Statement No. 113, *Accounting and Reporting for Reinsurance of Short-Duration and Long-Duration Contracts*, supersedes paragraphs 38–40 and 60(f) of FASB Statement No. 60 and amends paragraph 44 of FASB Statement No 5. The provisions of paragraphs 39 and 40 are incorporated in paragraph 18 of FASB Statement No. 113. FASB Statement No. 113 applies to financial statements for fiscal years beginning after December 15, 1992. [Footnote added, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

[1] FASB Statement No. 60,* paragraph 60*f* also specifies the following disclosures regarding reinsurance: "The nature and significance of reinsurance transactions to the insurance enterprise's operations, including reinsurance premiums assumed and ceded, and estimated amounts that are recoverable from reinsurers and that reduce the liabilities for unpaid claims and claim adjustment expenses."

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.06 The accounting entries for reinsurance assumed normally parallel those for direct insurance. However, the extent of the detail in the information provided to the assuming company by the ceding company or the reinsurance intermediary can vary significantly regarding—

a. Timeliness of the information submitted.

b. Detail of information relating to policies, claims, unearned premiums, and loss reserves.

c. Annual statement line-of-business classification.

d. Foreign currency translation information on business assumed from companies domiciled in foreign countries ("alien companies").

Information on losses incurred but not reported (IBNR) and bulk reserves also may be provided by ceding companies under pro rata reinsurance arrangements. Generally no IBNR will be provided on nonproportional (excess) reinsurance arrangements. Based on the quality and comprehensiveness of the detail presented, the information provided may or may not be used by the assuming company.

.07 FASB Statement No. 60† describes reporting in conformity with generally accepted accounting principles for "payments to insurance companies that may not involve transfer of risk." Similar guidance is provided in FASB Statement No. 5,† *Accounting for Contingencies*, paragraph 44. Paragraph 40 of FASB Statement No. 60† states—

> To the extent that a reinsurance contract does not, despite its form, provide for indemnification of the ceding enterprise by the reinsurer against loss or liability, the premium paid less the premium to be retained by the reinsurer shall be accounted for as a deposit by the ceding enterprise. Those contracts may be structured in various ways, but if, regardless of form, their substance is that all or part of the premium paid by the ceding enterprise is a deposit, the amount paid shall be accounted for as such. A net credit resulting from the contract shall be reported as a liability by the ceding enterprise. A net charge resulting from the contract shall be reported as an asset by the reinsurer.

Applicability and Scope

.08 This statement provides guidance on auditing property and liability reinsurance, including accident and health reinsurance. The following sections describe certain significant aspects of internal control structure policies and procedures regarding ceded reinsurance and assumed reinsurance and describe the related auditing procedures. SAS No. 55, *Consideration of the Internal Control Structure in a Financial Statement Audit*, states, "establishing and maintaining an internal control structure is an important management responsibility." The concept of materiality is inherent in the work of the independent auditor, and the elements of materiality and relative risk underlie the application of generally accepted auditing standards. [Revised, April 1996,

† FASB Statement No. 113, *Accounting and Reporting for Reinsurance of Short-Duration and Long-Duration Contracts*, supersedes paragraphs 38—40 and 60(f) of FASB Statement No. 60 and amends paragraph 44 of FASB Statement No 5. The provisions of paragraphs 39 and 40 are incorporated in paragraph 18 of FASB Statement No. 113. FASB Statement No. 113 applies to financial statements for fiscal years beginning after December 15, 1992. [Footnote added, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Ceded Reinsurance

Internal Controls of the Ceding Company

.09 The ceding company should have those internal control structure policies and procedures that it considers necessary to (*a*) evaluate the financial responsibility and stability of the assuming company (whether the assuming company is domiciled in the United States or in a foreign country) and (*b*) provide reasonable assurance of the accuracy and reliability of information reported to the assuming company and amounts due to or from the assuming company. The ceding company's control procedures to evaluate the financial responsibility and stability of the assuming company may include—

a. Obtaining and analyzing recent financial information of the assuming company, such as—

- Financial statements and, if audited, the independent auditor's report.
- Financial reports filed with the Securities and Exchange Commission (U.S.), Department of Trade (U.K.), or similar authorities in other countries.
- Financial statements filed with insurance regulatory authorities, with particular consideration of loss reserve development and the quality and liquidity of the company's invested assets.

b. Obtaining and reviewing available sources of information relating to the assuming company, such as—

- Insurance industry reporting and rating services.
- Insurance department examination reports.
- Loss reserve certifications filed with regulatory authorities.
- Letters relating to the design and operation of internal control structure policies and procedures filed with regulatory authorities.
- Insurance Regulatory Information System results filed with regulatory authorities.

c. Inquiring about the assuming company's retrocessional practices and experience.

d. Inquiring about the general business reputation of the assuming company and the background of its owners and management.

e. Ascertaining whether the assuming company is authorized to transact reinsurance within the ceding company's state of domicile or whether letters of credit or other means of security are provided if the assuming company is not so authorized.

f. Considering the need for and evaluating the adequacy of collateral from the assuming company on certain reinsurance contracts.

[Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

.10 The ceding company's control procedures relating to the accuracy and reliability of information reported to the assuming company and amounts due to or from the assuming company are generally similar in nature to other control procedures for the recording of insurance transactions. Those control procedures are not addressed in this statement.

Auditing Procedures

.11 In obtaining an understanding of the internal control structure, the ceding company's independent auditor should review the ceding company's procedures for determining the assuming company's ability to honor its commitments under the reinsurance contract. If the auditor intends to rely on the prescribed procedures, he should perform tests of the ceding company's procedures to obtain reasonable assurance that they are in use and operating as planned. [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.12 The absence of adequate procedures by the ceding company to determine the assuming company's ability to honor its contractual commitments, or the lack of reasonable assurance that such procedures are in use and operating as planned, may constitute a material weakness in the ceding company's internal control structure.[2] If the auditor assesses control risk at the maximum level, whether because of a material weakness or other reasons, he should extend his procedures to evaluate the collectibility of amounts recorded in the financial statements as recoverable from the assuming company. The auditor's extended procedures may include certain of the procedures specified in paragraph .09, but they are not necessarily limited to those procedures. The auditor's inability to perform the procedures he considers necessary, whether as a result of restrictions imposed by the client or by circumstances such as the timing of the work, the inability to obtain sufficient competent evidential matter, or an inadequacy in the accounting records, constitutes a scope limitation that may require the auditor to qualify his opinion or disclaim an opinion (see SAS No. 58, paragraphs 40 through 48 and 70 through 72). In such circumstances, the reasons for the auditor's qualification of opinion or disclaimer of opinion should be described in his report. [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.13 To obtain reasonable assurance that reinsurance contracts are appropriately accounted for, the independent auditor of the ceding company should perform procedures for selected contracts, selected transactions, and related balances, which include the following:

a. Read the reinsurance contract and related correspondence to—

- Obtain an understanding of the business objective of the reinsurance contract, and

---

[2] SAS No. 60, *Communication of Internal Control Structure Related Matters Noted in an Audit*, states, "A material weakness in the internal control structure is a reportable condition in which the design or operation of one or more of the internal control structure elements does not reduce to a relatively low level the risk that errors or irregularities in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions." SAS No. 60 requires the auditor to communicate to the audit committee or to individuals with a level of authority and responsibility equivalent to an audit committee in organizations that do not have one, reportable conditions, including material weaknesses in the internal control structure that come to his or her attention during an audit. [Footnote added, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

- Determine whether the contract should be accounted for according to the provisions of FASB Statement No. 60,‡ paragraph 40 (see paragraph .07, above).

b. Trace entries arising from selected reinsurance contracts to the appropriate records.

c. Trace the selected transactions to supporting documents and test the related receivables and payables.

d. Obtain written confirmation of selected balances. In certain circumstances, confirmation of contract terms may be appropriate.

Assumed Reinsurance

Internal Controls of the Assuming Company

.14 A significant element of the assuming company's internal control structure related to assumed reinsurance is appropriate control procedures that the company considers necessary for assessing the accuracy and reliability of data received from the ceding company (whether the ceding company is domiciled in the United States or in a foreign country). Principal control procedures of the assuming company may include—

a. Maintaining an underwriting file with information relating to the business reasons for entering the reinsurance contract and anticipated results of the contract. The underwriting file may include—

- Historical loss ratios and combined ratios of the ceding company.
- Anticipated loss ratios under the contract.
- An indication of the frequency and content of reports from the ceding company.
- Prior business experience with the ceding company.
- The assuming company's experience on similar risks.
- Information regarding pricing and ceding commissions.

b. Monitoring the actual results reported by the ceding company and investigating the reasons for and the effects of significant deviations from anticipated results.

c. Visiting the ceding company and reviewing and evaluating its underwriting, claims processing, loss reserving, and loss reserve development monitoring procedures.

d. Obtaining from the ceding company a special-purpose report by their independent accountant regarding the ceding company's internal

‡ FASB Statement No. 113, *Accounting and Reporting for Reinsurance of Short-Duration and Long-Duration Contracts*, supersedes paragraphs 38—40 and 60(f) of FASB Statement No. 60 and amends paragraph 44 of FASB Statement No 5. The provisions of paragraphs 39 and 40 are incorporated in paragraph 18 of FASB Statement No. 113. FASB Statement No. 113 applies to financial statements for fiscal years beginning after December 15, 1992. [Footnote added, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

accounting controls relating to ceded reinsurance (see SAS No. 30,[11] *Reporting on Internal Accounting Control*, paragraphs 60–61).

[Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.15 Additional control procedures of the assuming company may include—

a. Obtaining and analyzing recent financial information of the ceding company, such as—

- Financial statements and, if audited, the independent auditor's report.
- Financial reports filed with the Securities and Exchange Commission (U.S.), Department of Trade (U.K.), or similar authorities in other countries.
- Financial statements filed with insurance regulatory authorities, with particular consideration of loss reserve development.

b. Obtaining and reviewing available sources of information on the ceding company, such as—

- Insurance industry reporting and rating services.
- Insurance department examination reports.
- Loss reserve certifications filed with regulatory authorities.
- Letters relating to the design and operation of internal control structure policies and procedures filed with regulatory authorities.
- Insurance Regulatory Information System results filed with regulatory authorities.

c. Inquiring about the general business reputation of the ceding company and the background of its owners and management.

[Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Auditing Procedures

.16 In obtaining an understanding of the internal control structure, the assuming company's independent auditor should review the assuming company's procedures for assessing the accuracy and reliability of data received from the ceding company. If the auditor intends to rely on the prescribed procedures, he should perform tests of the company's procedures to obtain reasonable assurance that they are in use and operating as planned. [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.17 The absence of adequate procedures by the assuming company to obtain assurance regarding the accuracy and reliability of data received from

---

[11] On April 20, 1992, the AICPA's Auditing Standards Board issued an exposure draft of a proposed Statement on Standards for Attestation Engagements, *Reporting on an Entity's Internal Control Structure Over Financial Reporting*. The Statement would supersede SAS No. 30. A final statement is expected to be issued in 1993. [Footnote added, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

the ceding company, or the lack of reasonable assurance that such procedures are in use and operating as planned, may constitute a material weakness in the assuming company's internal control structure.[3] If the auditor assesses control risk at the maximum level, whether because of a material weakness or other reasons, he should extend his procedures to obtain assurance regarding the accuracy and reliability of the data received from the ceding company. The auditor's extended procedures should ordinarily include, but would not necessarily be limited to, one or more of the following:

a. Performing certain of the principal control procedures specified in paragraph .14

b. Visiting the ceding company's independent auditor and reviewing his working papers (see SAS No. 1, section 543.12.)

c. Performing auditing procedures at the ceding company or requesting the independent auditor of the ceding company to perform agreed-upon procedures

d. Obtaining the report of the ceding company's independent auditor on policies and procedures (relating to ceded reinsurance) placed in operation and tests of operating effectiveness (see SAS No. 70, *Service Organizations*.)

The auditor's inability to perform the procedures he considers necessary, whether as a result of restrictions imposed by the client or by circumstances such as the timing of the work, the inability to obtain sufficient competent evidential matter, or an inadequacy in the accounting records, constitutes a scope limitation that may require the auditor to qualify his opinion or disclaim an opinion (see SAS No. 58, paragraphs 40 through 48 and 70 through 72). In such circumstances, the reasons for the auditor's qualification of opinion or disclaimer of opinion should be described in his report. [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.18 To obtain reasonable assurance that reinsurance contracts are appropriately accounted for, the independent auditor of the assuming company should perform procedures for selected contracts, selected transactions, and related balances, which include the following:

a. Read the reinsurance contract and related correspondence to—

- Obtain an understanding of the business objective of the reinsurance contract.
- Determine whether the contract should be accounted for according to the provisions of FASB Statement No. 60,[#] paragraph 40 (see paragraph .07, above).

b. Trace entries arising from selected reinsurance contracts to the appropriate records.

---

[3] See footnote 2.

[#] FASB Statement No. 113, *Accounting and Reporting for Reinsurance of Short-Duration and Long-Duration Contracts*, supersedes paragraphs 38–40 and 60(f) of FASB Statement No. 60 and amends paragraph 44 of FASB Statement No 5. The provisions of paragraphs 39 and 40 are incorporated in paragraph 18 of FASB Statement No. 113. FASB Statement No. 113 applies to financial statements for fiscal years beginning after December 15, 1992. [Footnote added, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

c. Trace the selected transactions to supporting documents and test the related receivables and payables.

d. Obtain written confirmation of selected balances. In certain circumstances, confirmation of contract terms may be appropriate.

Pools, Associations, and Syndicates

.19 Participation in reinsurance pools, associations, and syndicates is in some respects similar to reinsurance, and the guidance in paragraphs .14–.18 is generally applicable in the audit of an assuming company (participating company). Pools, associations, and syndicates often issue audited financial statements to participating companies, and the auditor of a participating company may use the report of the independent auditor of the pool, association, or syndicate in his audit. Guidance on the auditor's considerations in those circumstances is provided in SAS No. 1, section 543, *Part of Audit Performed by Other Independent Auditors*. [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Reinsurance Intermediaries

.20 Reinsurance may be transacted and serviced directly between the ceding and assuming companies or through reinsurance intermediaries (including brokers, agents, managing general agents, or similar entities). When a reinsurance intermediary is involved, the control procedures of the reinsurance intermediary are an integral part of the reinsurance transaction. The assuming and ceding companies should coordinate their control procedures with those of the reinsurance intermediary.

.21 A company may delegate to a reinsurance intermediary the performance of the procedures described in paragraphs .09 and in .14 and .15. The company, however, should have procedures to satisfy itself that the reinsurance intermediary is adequately performing those procedures. The guidance provided the independent auditor in paragraphs .11 and .12 and in .16 and .17 is applicable.

.22 In addition to the functions discussed in paragraphs .09 and in .14 and .15, a reinsurance intermediary may be authorized to collect, hold, disburse, and remit funds on behalf of the insurance company. The insurance company should have controls to provide reasonable assurance that the reinsurance intermediary is—

a. Adequately performing those functions.

b. Safeguarding the funds and, if required, appropriately segregating the funds.

c. Settling accounts on a timely basis.

The insurance company may accomplish this by obtaining a special report from the independent auditor of the reinsurance intermediary or by visiting the reinsurance intermediary and reviewing its controls relating to those functions. The auditor of the insurance company should review the company's internal control procedures, and, if he intends to rely on them, he should test the operation of those control procedures. If the auditor decides not to rely on those controls, he should extend his procedures to obtain assurance that the objectives described in *a–c* above are met.

Effective Date

.23 This statement of position provides for practices that may differ in certain respects from present practices. Accordingly, this statement of position

will be effective for audits performed in accordance with generally accepted auditing standards for periods ending on or after December 31, 1983. Earlier application is encouraged. [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Reinsurance Auditing and Accounting Task Force

JOHN E. HART, *Chairman*
DAVID HOLMAN
C. DONALD HOWELL
RICHARD A. LINDROOTH
SCOTT MALMGREN
RICHARD P. MEYEROWICH
COLEMAN D. ROSS
CHARLES L. WARNER

Insurance Companies Committee

JOHN L. MCDONOUGH, JR., *Chairman*
JOHN T. BAILY
JOHN R. BERTHOUD
PERRY G. BLOCKER
PETER S. BURGESS
DENNIS H. CHOOKASZIAN
DONALD E. DANNER
RONALD P. FRERES
PAUL W. HIGGINS
DEAN W. JONES
JOHN W. POPP
RICHARD D. WAMPLER II

D.R. CARMICHAEL
Vice President, Auditing
BRIAN ZELL
Manager, Auditing Standards

[The next page is 30,341.]

Section 14,070

Auditing Life Reinsurance

Supplements *Audits of Stock Life Insurance Companies*

November 1984

NOTICE TO READERS

This statement of position presents the recommendations of the Reinsurance Auditing and Accounting Task Force of the AICPA Insurance Companies Committee regarding the application of generally accepted auditing standards in auditing life reinsurance. This statement of position supplements the industry audit guide, *Audits of Stock Life Insurance Companies*. It represents the considered opinion of the Reinsurance Auditing and Accounting Task Force on the best auditing practice in the industry and has been reviewed by members of the AICPA Auditing Standards Board for consistency with existing auditing standards. AICPA members may have to justify departures from the recommendations in this statement if their work is challenged.

Applicability

.01 This statement provides guidance on auditing life reinsurance. Guidance on auditing property and liability reinsurance, including accident and health reinsurance, is provided in the statement of position entitled, *Auditing Property and Liability Reinsurance*, issued by the AICPA Auditing Standards Division in October 1982.

Introduction

.02 When an insurance company issues life insurance policies, it undertakes a number of risks relating to the ultimate profitability of the policies, such as adverse experience regarding mortality or terminations, inadequate investment earnings, and unanticipated costs. Reinsurance is the assumption by one insurer (the assuming company) of all or part of the risks originally undertaken by another insurer (the ceding company).

.03 Each life insurance company determines its *retention limit*, which represents the maximum loss exposure acceptable to the company that could result from the death of any individual insured by the company. The retention limit will vary depending on the age of the insured at issuance of the policy, the type of insurance plan involved, and whether the insured is classified as a standard or substandard risk. If the policy exceeds the retention limit, the company will reinsure the excess portion of the risk. A company may also reinsure part or all of a policy within its retention limit if the company sees a need to limit its risk.

.04 Reinsurance also provides a means for the company to meet certain other objectives such as to avoid "surplus strain" resulting from the statutory accounting treatment of expenses and reserves, to reduce fluctuations in claim experience or to stabilize mortality cost, to provide additional capacity to accept business that would otherwise have to be declined, to protect solvency, to obtain underwriting assistance regarding risk classification, or to assist in financial and tax planning strategies.

.05 By ceding all or part of the risk, the ceding company does not discharge its primary obligations to its insureds. Therefore, the ceding company is concerned with the ability of the assuming company to honor its commitments under the reinsurance contract. The assuming company, on the other hand, is concerned with the accuracy and reliability of the information received from the ceding company regarding the risks it has assumed and, in some circumstances, the ability of the ceding company to honor commitments to the assuming company. Factors that are pertinent to the auditor's evaluation of reinsurance contracts include the types of reinsurance agreements and the consequent nature of the risks transferred, contractual safeguards in the reinsurance agreements, and internal control structure regarding reinsurance maintained by the ceding company or by the assuming company. [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.06 Reinsurance may be transacted through—

a. *Facultative agreements*, whereby each risk or portion of a risk is reinsured individually, the assuming company having the option to accept or reject it.

b. *Automatic agreements*, whereby an agreed portion of business written is automatically reinsured, thus eliminating the need to submit each risk to the assuming company for acceptance or rejection.

.07 Life reinsurance contracts generally take one of three forms: yearly renewable term, coinsurance, or modified coinsurance.

a. *Yearly renewable term* (*YRT*) reinsurance involves the purchase of reinsurance on the policyholder's life on a year-by-year basis. Typically the amount of reinsurance provided and the reinsurance premium charged for a particular contract will change from year to year on a scheduled basis. The reinsurance premium will depend on factors such as the age and sex of the insured, the duration of the policy, and the underwriting classification (standard or substandard risks). Yearly renewable term reinsurance generally transfers only the mortality risk to the assuming company.

b. *Coinsurance* differs from yearly renewable term reinsurance in that the assuming company participates in substantially all aspects of the original policy and in that the contract generally covers a longer period of time. The assuming company will receive its share of the policy premiums and pay its share of the face amount of claims and cash values on terminations. The assuming company will establish its share of the statutory policy reserves, and the ceding company will reduce its reserves for the portion reinsured. If the policy is participating, the assuming company will generally reimburse the ceding company for its share of the policyholder dividend. The assuming company also generally reimburses the ceding company for its commission outlay and usually pays an additional amount toward the ceding company's expenses. The assuming company ordinarily participates in the risks regarding investment, mortality, terminations, and other risks of the policy.

c. *Modified coinsurance* differs from coinsurance only in that the reserves and the assets supporting the reserves remain with the ceding company. In addition to the transactions required by coinsurance, a "reserve adjustment" payment between the assuming and ceding

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

companies is made each year. The assuming company will be paid interest on the assets supporting the reserves according to a specified formula, which may involve a fixed rate or may be related to the interest earnings of the ceding company. Depending on the formula, the investment risk may be borne by the ceding company or the assuming company, or it may be shared. As with coinsurance, the assuming company ordinarily participates in the mortality, termination, and other risks.

.08 Life insurance companies may also purchase *nonproportional reinsurance* on all or part of their insurance. One form of nonproportional reinsurance is stop-loss, under which the assuming company agrees to reimburse the ceding company for aggregate losses that exceed a specified amount. Another form is catastrophe reinsurance, under which the assuming company agrees to reimburse the ceding company for losses in excess of a specified amount that result from a single accident.

.09 Reinsurance agreements often provide for participation by the ceding company in the profits generated under the reinsurance. The reinsurance agreement will specify the method of computing the profit and the formula for sharing it.

.10 Typically, reinsurance agreements are individually negotiated and tailored to the needs and objectives of the ceding and assuming companies. The foregoing descriptions of life reinsurance agreements are not exhaustive, and variations from the described approaches are common.

Generally Accepted Accounting Principles

.11 The accounting entries for reinsurance ceded transactions are the opposite of the entries that arise from direct business. With certain exceptions, the amounts for reinsurance transactions are netted against the related accounts in financial statements. The accounting entries for reinsurance assumed normally parallel those for direct insurance.[1]

.12 FASB Statement No. 60* describes reporting in conformity with generally accepted accounting principles for "payments to insurance companies that may not involve transfer of risk." Similar guidance is provided in FASB Statement No. 5, *Accounting for Contingencies*, paragraph 44. Paragraph 40 of FASB Statement No. 60* states—

> To the extent that a reinsurance contract does not, despite its form, provide for indemnification of the ceding enterprise by the reinsurer against loss or liability, the premium paid less the premium to be retained by the reinsurer shall be accounted for as a deposit by the ceding enterprise. Those contracts may be structured in various ways, but if, regardless of form, their substance is that all or part of the premium paid by the ceding enterprise is a deposit, the amount paid shall be accounted for as such. A net credit resulting from the contract shall be reported as a liability by the ceding enterprise. A net charge resulting from the contract shall be reported as an asset by the reinsurer.

---

[1] FASB Statement No. 60,* *Accounting and Reporting by Insurance Enterprises*, specifies certain accounting and disclosure requirements for reinsurance.

* FASB Statement No. 113, *Accounting and Reporting for Reinsurance of Short-Duration and Long-Duration Contracts*, supersedes paragraphs 38 through 40 and 60(f) of FASB Statement No. 60 and amends paragraph 44 of FASB Statement No 5. The provisions of paragraphs 39 and 40 are incorporated in paragraph 18 of FASB Statement No. 113. FASB Statement No. 113 applies to financial statements for fiscal years beginning after December 15, 1992. [Footnote added, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Scope

.13 The following sections describe certain significant aspects of internal control structure regarding ceded reinsurance and assumed reinsurance and describe the related auditing procedures. SAS No. 55, *Consideration of the Internal Control Structure in a Financial Statement Audit*, states "establishing and maintaining an internal controling structure is an important management responsibility." The concept of reasonable assurance is inherent in management's determination of the nature and extent of internal control structure, and the elements of audit risk and materiality underlie the application of generally accepted auditing standards by the independent auditor. [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Ceded Reinsurance

Internal Control Structure of the Ceding Company

.14 The ceding company should have those internal control structure policies and procedures that it considers necessary to (*a*) evaluate the financial responsibility and stability of the assuming company (whether the assuming company is domiciled in the United States or in a foreign country) and (*b*) provide reasonable assurance of the accuracy and reliability of information reported to the assuming company and amounts due to or from the assuming company. The ceding company's control procedures to evaluate the financial responsibility and stability of the assuming company may vary, depending on the type of contracts (such as yearly renewable term and coinsurance) and other factors, and may include[2]

a. Obtaining and analyzing recent financial information of the assuming company, such as—

- Financial statements and, if the statements are audited, the independent auditor's report.
- Financial reports filed with the Securities and Exchange Commission (United States), Department of Trade (United Kingdom), or similar authorities in other countries.
- Financial statements, including the actuary's opinion, filed with insurance regulatory authorities, with particular consideration of the quality and liquidity of the company's invested assets.

b. Obtaining and reviewing available sources of information relating to the assuming company, such as—

- Insurance industry reporting and rating services.
- Insurance department examination reports.
- Letters relating to the design and operation of internal control structure policies and procedures filed with regulatory authorities.
- Insurance Regulatory Information System results filed with regulatory authorities.

---

[2] The absence of one or more specific control procedures does not necessarily indicate a weakness in the internal control structure. [Footnote revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

c. Inquiring about the assuming company's retrocessional practices and experience.

d. Inquiring about the general business reputation of the assuming company and the background of its owners and management.

e. Ascertaining whether the assuming company is authorized to transact reinsurance within the ceding company's state of domicile or whether letters of credit or other means of security are provided if the assuming company is not so authorized.

f. Considering the need for and evaluating the adequacy of collateral from the assuming company on certain reinsurance contracts.

[Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.15 The ceding company's control procedures relating to the accuracy and reliability of information reported to the assuming company and amounts due to or from the assuming company are generally similar in nature to other control procedures for the recording of insurance transactions. Those control procedures are not addressed in this statement.

Auditing Procedures

.16 The independent auditor's consideration of the ceding company's internal control structure ordinarily should include a review of the ceding company's procedures for determining the assuming company's ability to honor its commitments under the reinsurance contract. If the auditor intends to rely on the prescribed procedures, he should perform tests of the ceding company's procedures to obtain reasonable assurance that they are in use and operating as planned. [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.17 The absence of adequate procedures by the ceding company to determine the assuming company's ability to honor its contractual commitments, or the lack of reasonable assurance that such procedures are in use and operating as planned, may constitute a material weakness in the ceding company's internal control structure.[3] If the auditor assesses control risk at the maximum level, whether because of a material weakness or other reasons, he should extend his procedures to evaluate the collectibility of amounts recorded in the financial statements as receivables or reductions of liabilities that are recoverable from the assuming company. The auditor's extended procedures may include certain of the procedures specified in paragraph .14, but they are not necessarily limited to those procedures. The auditor's inability to perform the procedures he considers necessary, whether as a result of restrictions imposed by the client or by circumstances such as the timing of work, the inability to obtain sufficient competent evidential matter, or an inadequacy in the account-

[3] SAS No. 60, *Communication of Internal Control Structure Related Matters Noted in an Audit*, states, "A material weakness in the internal control structure is a reportable condition in which the design or operation of one or more of the internal control structure elements does not reduce to a relatively low level the risk that errors or irregularities in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions." SAS No. 60 requires the auditor to communicate to the audit committee or to individuals with a level of authority and responsibility equivalent to an audit committee in organizations that do not have one, reportable conditions, including material weaknesses in the internal control structure that come to his or her attention during an audit. [Footnote revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

ing records, constitutes a scope limitation that may require the auditor to qualify his opinion or disclaim an opinion (see SAS No. 58, *Reports on Audited Financial Statements*, paragraphs 38 through 66, and 70 through 72). In such circumstances, the reasons for the auditor's qualification of opinion or disclaimer of opinion should be described in his report. [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.18 Reinsurance of life insurance permits the elimination of the reinsured portion of the related liability for future policy benefits from the ceding company's financial statements. Under certain circumstances, reinsurance may also result in increasing current earnings or investable funds to the extent that the proceeds received from the assuming company exceed expenses incurred in connection with the sale and servicing of the reinsured policies. The auditor of the ceding company ordinarily should confirm insurance policies in force with policyholders when ceded reinsurance activities can materially increase current earnings or investable funds. (See the statement of position entitled *Confirmation of Insurance Policies in Force*, issued by the AICPA Auditing Standards Division, August 1978.)

.19 To obtain reasonable assurance that reinsurance contracts are appropriately accounted for, the independent auditor of the ceding company ordinarily should perform procedures for selected contracts, selected transactions, and related balances, which include the following:

a. Read the reinsurance contract and related correspondence to—

- Obtain an understanding of the business objective of the reinsurance contract.
- Determine whether the contract should be accounted for according to the provisions of FASB Statement No. 60,† paragraph 40 (see paragraph .12 above).

b. Trace entries arising from selected reinsurance contracts to the appropriate records.

c. Trace the selected transactions to supporting documents and test related receivables and payables.

d. Obtain written confirmation of selected balances. In certain circumstances, confirmation of contract terms may be appropriate.

Assumed Reinsurance

Internal Control Structure of the Assuming Company

.20 A significant element of the assuming company's internal control structure related to assumed reinsurance is appropriate control procedures that the company considers necessary for assessing the accuracy and reliability of data received from the ceding company (whether the ceding company is domiciled in the United States or in a foreign country). The appropriate control

† FASB Statement No. 113, *Accounting and Reporting for Reinsurance of Short-Duration and Long-Duration Contracts*, supersedes paragraphs 38 through 40 and 60(f) of FASB Statement No. 60 and amends paragraph 44 of FASB Statement No. 5. The provisions of paragraphs 39 and 40 are incorporated in paragraph 18 of FASB Statement No. 113. FASB Statement No. 113 applies to financial statements for fiscal years beginning after December 15, 1992. [Footnote added, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

procedures may vary depending on the type of contracts (such as yearly renewable term and coinsurance) and other factors. Principal control procedures of the assuming company may include[4]—

a. Maintaining information relating to the business reasons for entering the reinsurance contract and anticipated results of the contract, such as—

- Actuarial studies of the business assumed.
- Anticipated profitability.
- Anticipated termination rates.
- Prior business experience with the ceding company.
- The assuming company's experience on similar business.
- Information regarding pricing and ceding commissions.
- An indication of the frequency and content of reports from the ceding company.

b. Monitoring the actual results reported by the ceding company and investigating the reasons for and the effects of significant deviations from anticipated results.

c. Visiting the ceding company and reviewing and evaluating its sales, underwriting, benefits processing, and actuarial policies and procedures.

d. Obtaining from the ceding company a special-purpose report by their independent accountant regarding the ceding company's internal accounting controls relating to ceded reinsurance (see SAS No. 30,[‡] *Reporting on Internal Accounting Control*, paragraphs 60 and 61). If the ceding company's independent auditor confirmed life insurance policies in force (see paragraph .18), the assuming company might also consider obtaining a special report from the ceding company's independent auditor regarding the results of those confirmation procedures.

[Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.21 Additional control procedures of the assuming company may include—

a. Obtaining and analyzing recent financial information of the ceding company, such as—

- Financial statements and, if audited, the independent auditor's report.
- Financial reports filed with the Securities and Exchange Commission (United States), Department of Trade (United Kingdom), or similar authorities in other countries.

---

[4] See footnote 2.

[‡] On April 20, 1992, the AICPA's Auditing Standards Board issued an exposure draft of a proposed Statement on Standards for Attestation Engagements, *Reporting on an Entity's Internal Control Structure Over Financial Reporting*. The Statement would supersede SAS No. 30. A final Statement is expected to be issued in 1993. [Footnote added, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

- Financial statements, including the actuary's opinion, filed with regulatory authorities.

b. Obtaining and reviewing available sources of information on the ceding company, such as—

- Insurance industry reporting and rating services.
- Insurance department examination reports.
- Letters relating to the adequacy of internal control structure filed with regulatory authorities.
- Insurance Regulatory Information System results filed with regulatory authorities.

c. Inquiring about the general business reputation of the ceding company and the background of its owners and management.

[Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Auditing Procedures

.22 The independent auditor's consideration of the assuming company's internal control structure ordinarily should include a review of the assuming company's procedures for assessing the accuracy and reliability of data received from the ceding company. If the auditor intends to rely on the prescribed procedures, he should perform tests of the company's procedures to obtain reasonable assurance that they are in use and operating as planned. [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.23 The absence of adequate procedures by the assuming company to obtain assurance regarding the accuracy and reliability of data received from the ceding company, or the lack of reasonable assurance that such procedures are in use and operating as planned, may constitute a material weakness in the assuming company's internal control structure.[5] If the auditor assesses control risk at the maximum level, whether because of a material weakness or other reasons, he should extend his procedures to obtain assurance regarding the accuracy and reliability of the data received from the ceding company. The auditor's extended procedures should ordinarily include, but would not necessarily be limited to, one or more of the following:

a. Performing procedures such as certain of the procedures specified in paragraph .20

b. Visiting the ceding company's independent auditor and reviewing his working papers (see SAS No. 1, section 543.12, *Part of Audit Performed by Other Independent Auditors*)

c. Performing auditing procedures at the ceding company or requesting the independent auditor of the ceding company to perform agreed-upon procedures

d. Obtaining the report of the ceding company's independent auditor on policies and procedures (related to ceded reinsurance) placed in operation and tests of operating effectiveness (see SAS No. 70, *Service Organizations*)

---

[5] See footnote 3.

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

The auditor's inability to perform the procedures he considers necessary, whether as a result of restrictions imposed by the client or by circumstances such as the timing of the work, the inability to obtain sufficient competent evidential matter, or an inadequacy in the accounting records, constitutes a scope limitation that may require the auditor to qualify his opinion or disclaim an opinion (see SAS No. 58, paragraphs 40 through 48 and 70 through 72). In such circumstances, the reasons for the auditor's qualification of opinion or disclaimer of opinion should be described in his report. [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.24 To obtain reasonable assurance that reinsurance contracts are appropriately accounted for, the independent auditor of the assuming company ordinarily should perform procedures for selected contracts, selected transactions, and related balances, which include the following:

a. Read the reinsurance contract and related correspondence to—

- Obtain an understanding of the business objective of the reinsurance contract.
- Determine whether the contract should be accounted for according to the provisions of FASB Statement No. 60,[11] paragraph 40 (see paragraph .12 above).

b. Trace entries arising from selected reinsurance contracts to the appropriate records.

c. Trace selected transactions to supporting documents and test the related receivables and payables.

d. Obtain written confirmation of selected balances. In certain circumstances, confirmation of contract terms may be appropriate.

Effective Date

.25 This statement of position provides for practices that may differ in certain respects from present practices. Accordingly, this statement of position will be effective for audits performed in accordance with generally accepted auditing standards for periods ending on or after December 31, 1985. Earlier application is encouraged. [Revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

---

[11] FASB Statement No. 113, *Accounting and Reporting for Reinsurance of Short-Duration and Long-Duration Contracts*, supersedes paragraphs 38 through 40 and 60(f) of FASB Statement No. 60 and amends paragraph 44 of FASB Statement No. 5. The provisions of paragraphs 39 and 40 are incorporated in paragraph 18 of FASB Statement No. 113. FASB Statement No. 113 applies to financial statements for fiscal years beginning after December 15, 1992. [Footnote added, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Reinsurance Auditing and Accounting Task Force

JOHN E. HART, *Chairman*
DAVID HOLMAN
RICHARD A. LINDROOTH
SCOTT MALMGREN
RICHARD P. MEYEROWICH
COLEMAN D. ROSS
CHARLES L. WARNER
PAUL J. ZUCCONI

Insurance Companies Committee

FRANK A. BRUNI, *Chairman*
JOHN T. BAILY
PERRY G. BLOCKER
PETER S. BURGESS
DENNIS H. CHOOKASZIAN
JEFFREY D. CROPSEY
BOBBY R. CURTIS
JOHN F. EPPICH
HEATH FITZSIMMONS
RONALD P. FRERES
ROBERT J. HILLY
C. DONALD HOWELL
RICHARD PLUSCHAU
R. LAWRENCE SOARES

DAN M. GUY
Vice President, Auditing
BRIAN ZELL
Manager, Auditing Standards

[The next page is 30,401.]

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Section 14,100

Statement of Position 89-2 Reports on Audited Financial Statements of Investment Companies

January 1989

NOTE

This statement of position presents the recommendations of the AICPA Investment Companies Committee regarding the application of generally accepted auditing standards to reports on audited financial statements of investment companies. It represents the considered opinion of the committee on the best auditing practice in the industry and has been reviewed by members of the AICPA Auditing Standards Board for consistency with existing auditing standards. AICPA members may have to justify departures from the recommendations in this statement if their work is challenged.

Introduction

.01 In 1987, the Audit and Accounting Guide, *Audits of Investment Companies*, was issued. Chapter 9 of that guide illustrates reports on audited financial statements. In April 1988, the AICPA's Auditing Standards Board issued Statement on Auditing Standards (SAS) No. 58, *Reports on Audited Financial Statements*, which changes the auditor's standard report on financial statements. This statement of position amends *Audits of Investment Companies* in response to the changes required by SAS No. 58; it replaces paragraphs 9.03 through 9.09 of the guide with new paragraphs 9.03 through 9.09*

9.03. The following form of auditor's report may be used to express an unqualified opinion on the financial statements:

Independent Auditor's Report

To the Shareholders and
Board of Directors
XYZ Investment Companies

We have audited the accompanying statement of assets and liabilities of XYZ Investment Company, including the schedule of portfolio investments, as of December 31, 19X4, and the related statements of operations and cash flows[1] for the year then ended, the statement of changes in net assets for each of the two years in the period then ended, and the selected per share data and ratios for each of the five years in the period then ended. These financial statements and per share data and ratios are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements and per share data and ratios based on our audits.

---

* Paragraph 9.08 of the Guide was deleted and subsequent paragraphs were renumbered in October 1996 to reflect the new guidance set forth in SAS No. 79, *Amendment to Statement on Auditing Standards No. 58*, Reports on Audited Financial Statements. [Footnote added, June 1997.]

[1] FASB Statement No. 102, *Statement of Cash Flows—Exemption of Certain Enterprises and Classification of Cash Flows From Certain Securities Held for Resale*, amends FASB Statement No. 95, *Statement of Cash Flows*, to exempt highly liquid companies that meet specified conditions from the requirement to provide a statement of cash flows. [Footnote revised, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

We conducted our audits in accordance with generally accepted auditing standards. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements and per share data and ratios are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. Our procedures included confirmation of securities owned as of December 31, 19X4, by correspondence with the custodian and brokers. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements and selected per share data and ratios referred to above present fairly, in all material respects, the financial position of XYZ Investment Company as of December 31, 19X4, the results of its operations and its cash flows[2] for the year then ended, the changes in its net assets for each of the two years in the period then ended, and the selected per share data and ratios for each of the five years in the period then ended, in conformity with generally accepted accounting principles.

Independent Auditor

Anytown, USA
January 21, 19X5

9.04 The reference to "and brokers" in the fourth sentence of the scope paragraph is not normally required if the investment company's financial statements do not show an amount payable for securities purchased. Also, if securities were "verified by examination," the report should be modified to state that.

9.05 The accountant's report for a fund referred to as a "series fund" needs to be modified because of the uniqueness of the financial statements that have evolved to present its financial position, results of operations, and cash flows. The financial position, results of operations, and cash flows of the portfolios or other entities constituting the series are frequently presented in separate columns. The financial statements of the series may also be presented as if the series were a separate entity. In both cases, the scope of the audit should be sufficient to enable the auditor to report on the individual financial statements of the various entities constituting the series fund.

9.06 The following illustration is for a multicolumnar presentation of the portfolios constituting the series:

Independent Auditor's Report

To the Shareholders and
Board of Directors
XYZ Series Investment Company:

We have audited the accompanying statement of assets and liabilities, including the schedules of investments, of XYZ Series Investment Company (comprising, respectively, the Foreign, Domestic Common Stock, Long-Term Bond, and Convertible Preferred Portfolios) as of December 31, 19X4, and the related statements of operations and cash flows[3] for the year then ended, the statements of changes in net assets for each of the two years in the period then ended,

[2] See footnote 1.

[3] See footnote 1

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

and the selected per share data and ratios for each of the five years in the period then ended. These financial statements and per share data and ratios are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements and per share data and ratios based on our audits.

[*Same second paragraph as in the report illustrated in paragraph 9.03.*]

In our opinion, the financial statements and selected per share data and ratios referred to above present fairly, in all material respects, the financial position of each of the respective portfolios constituting the XYZ Series Investment Company as of December 31, 19X4, the results of their operations and their cash flows[4] for the year then ended, the changes in their net assets for each of the two years in the period then ended, and the selected per share data and ratios for each of the five years in the period then ended, in conformity with generally accepted accounting principles.

Independent Auditor

Anytown, USA
January 21, 19X5

9.07 The following illustration is for a presentation of one of the portfolios or entities constituting the series:

Independent Auditor's Report

To the Shareholders and
Board of Directors
XYZ Series Investment Company:

We have audited the accompanying statement of assets and liabilities, including the schedule of portfolio investments, of the Convertible Preferred Portfolio (one of the portfolios constituting the XYZ Series Investment Company) as of December 31, 19X4, and the related statements of operations and cash flows[5] for the year then ended, the statements of changes in net assets for each of the two years in the period then ended, and the selected per share data and ratios for each of the five years in the period then ended. These financial statements and per share data and ratios are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements and per share data and ratios based on our audits.

[*Same second paragraph as in the report illustrated in paragraph 9.03.*]

In our opinion, the financial statements and selected per share data and ratios referred to above present fairly, in all material respects, the financial position of the Convertible Preferred Portfolio of the XYZ Series Investment Company as of December 31, 19X4, and the results of its operations and cash flows[6] for the year then ended, the changes in its net assets for each of the two years in the period then ended, and the selected per share data and ratios for each of the five years in the period then ended, in conformity with generally accepted accounting principles.

Independent Auditor

Anytown, USA
January 21, 19X5

[4] See footnote 1.

[5] See footnote 1.

[6] See footnote 1.

The auditor's reports illustrated in this paragraph and in paragraph 9.06 are not intended to be all-encompassing or necessarily illustrative of all situations that may be encountered in practice.

9.08† The auditor's report should include an explanatory paragraph when the financial statements contain securities whose values were estimated by the Board of Directors in the absence of readily ascertainable market values, and the range of possible values of those securities is significant. That report, as illustrated below, should be used only if the auditor concludes that, after examining the underlying documentation supporting the board's good-faith estimate of value, the valuation principles are acceptable, are being consistently applied, are reasonably supported by the documentation, and the range of possible values is significant. If the range of possible values is not significant, a report such as that illustrated in paragraph 9.03 may be issued.

Independent Auditor's Report

To the Shareholders and
Board of Directors
XYZ Investment Company:

[*Same first, second, and third paragraphs as in the report illustrated in paragraph 9.03.*]

As explained in Note 2, the financial statements include securities valued at $_____ (_____% of net assets), whose values have been estimated by the Board of Directors in the absence of readily ascertainable market values. We have reviewed the procedures used by the Board of Directors in arriving at its estimate of value of such securities and have inspected underlying documentation, and, in the circumstances, we believe the procedures are reasonable and the documentation appropriate. However, because of the inherent uncertainty of valuation, those estimated values may differ significantly from the values that would have been used had a ready market for the securities existed, and the differences could be material.

Independent Auditor

Anytown, USA
January 21, 19X5

9.09 If the auditor concludes that the valuation procedures are inadequate or unreasonable, or that the underlying documentation does not support the valuation, the auditor should express a qualified opinion as follows:

Independent Auditor's Report

To the Shareholders and
Board of Directors
XYZ Investment Company:

[*Same first and second paragraphs as in the report illustrated in paragraph 9.03.*]

As explained in Note 2, the financial statements include securities valued at $_____ (_____% of net assets), whose values have been estimated by the Board of Directors in the absence of readily ascertainable market values. We have reviewed the procedures used by the Board of Directors in arriving at its estimate of value of such securities and have inspected underlying documentation. In our opinion, those procedures are not reasonable, and the documen-

† Paragraph 9.08 of the Guide was deleted and subsequent paragraphs were renumbered in October 1996 to reflect the new guidance set forth in SAS No. 79, *Amendment to Statement on Auditing Standards No. 58*, Reports on Audited Financial Statements. [Footnote added, June 1997.]

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

tation is not appropriate to determine the value of the securities in conformity with generally accepted accounting principles. The effect on the financial statements of not applying adequate valuation procedures is not readily determinable.

In our opinion, except for the effects on the financial statements and selected per share data and ratios of the valuation of investment securities determined by the Board of Directors, as described in the preceding paragraph, the financial statements and selected per share data and ratios referred to above present fairly, in all material respects, the financial position of XYZ Investment Company as of December 31, 19X4, the results of its operations and its cash flows[7] for the year then ended, the changes in its net assets for each of the two years in the period then ended, and the selected per share data and ratios for each of the five years in the period then ended, in conformity with generally accepted accounting principles.

Independent Auditor

Anytown, USA
January 21, 19X5

Effective Date

.02 This statement is effective at the time of its issuance.

[7] See footnote 1.

Investment Companies Committee (1988-1989)

JERRY A. DAVIS, *Chairman*
STEVEN E. BULLER
M. CHRISTOPHER CANAVAN, JR.
NICHOLAS P. CONSTANTAKIS
ROBERT F. GUNIA
PAUL A. KELLER
JAMES F. MAHONEY
RICHARD P. MEYEROWICH
PAUL R. NEVIERA
DAVID M. TAYLOR
FREDERICK M. WERBLOW
JONATHAN F. ZESCHIN

DAN M. GUY, *Vice President Auditing*
PATRICK L. MCNAMEE, *Director Audit and Accounting Guides*
DIONNE D. MCNAMEE, *Technical Manager Accounting Standards*

[The next page is 30,421.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 14,110

Statement of Position 89-3 Questions Concerning Accountants' Services on Prospective Financial Statements

April 1989

NOTE

This statement of position presents the recommendations of the Forecasts and Projections Audit Issues Task Force regarding accountants' services on prospective financial statements. It represents the considered opinion of the task force on the best practice for such engagements and has been reviewed by members of the AICPA Auditing Standards Board for consistency with existing standards. AICPA members may have to justify departures from the recommendations in this statement if their work is challenged.

Reporting on Financial Forecasts That Include a Projected Sale of an Entity's Real Estate Investment

Question:

.01 The AICPA *Guide for Prospective Financial Information* ("the Guide") states that "short-term financial forecasts may not be meaningful in (*a*) industries with a lengthy operating cycle or (*b*) situations where long-term results are necessary to evaluate the investment consequences involved. It may not be practical in all situations to present financial forecasts for enough future periods to demonstrate the long-term results. In those circumstances, the presentation should include a description of the potential effects of such results. For example, if a real estate entity's forecast does not extend to the period in which the entity's investment is expected to be liquidated, the disclosures would include a discussion of the effects of a liquidation at the end of the forecast period. Exhibit 9.08 of the Guide illustrates such a disclosure."[1] The information in exhibit 9.08 is presented in a note to a financial forecast. How should the practitioner report on a financial forecast that includes a hypothetical sale of an entity's real estate investment at the end of the forecast period?

Answer:

.02 The hypothetical sale of an entity's real estate, presented to demonstrate the potential effects of long-term results, may appear in the notes to the financial forecast or in a separate statement presented as part of the financial forecast. Such presentations should be appropriately labeled and accompanied by applicable disclosures, including significant assumptions and an indication of the purpose of the presentation.

---

[1] See paragraph 8.34 of the Guide.

.03 When the effects of a hypothetical sale of an entity's real estate are included in a note to the financial forecast, the disclosure is part of the financial forecast and it is covered by the accountant's standard report. If the hypothetical sale is presented as a projection in a separate statement, the accountant's report should be modified to report specifically on the statement. Examples of appropriate forms of reports follow:

Examination

We have examined the accompanying forecasted balance sheet of XYZ Company as of December 31, 19X8, and the related forecasted statements of income, retained earnings, and cash flows for the year then ending (the forecast), and the accompanying statement of the effect on limited partners of the projected sale of property at December 31, 19X8 (the projection). Our examination was made in accordance with standards for an examination of prospective financial statements established by the American Institute of Certified Public Accountants and, accordingly, included such procedures as we considered necessary to evaluate both the assumptions used by management and the preparation and presentation of the statements.

The accompanying projection was prepared by management to provide potential investors with information to analyze the effect of a hypothetical sale of the properties as of December 31, 19X8, and should not be considered a presentation of expected future results.

In our opinion, the accompanying forecast is presented in conformity with guidelines for presentation of a forecast established by the American Institute of Certified Public Accountants, and the underlying assumptions provide a reasonable basis for management's forecast. Also, in our opinion, the accompanying projection is presented in conformity with guidelines for presentation of a projection established by the American Institute of Certified Public Accountants, and the underlying assumptions provide a reasonable basis for management's projection, assuming the hypothetical sale of properties on the date and for the sales prices indicated. However, because events and circumstances frequently do not occur as expected, there will usually be differences between the forecasted and actual results, and even if the properties are sold on the date and for the prices indicated, there will usually be differences between the projected and actual results, and those differences may be material. We have no responsibility to update this report for events and circumstances occurring after the date of this report.

Compilation

We have compiled the accompanying forecasted balance sheet of XYZ Company as of December 31, 19X8, and the related forecasted statements of income, retained earnings, and cash flows for the year then ending (the forecast), and the accompanying statement of the effect on limited partners of the projected sale of property at December 31, 19X8 (the projection). Our compilation was made in accordance with standards established by the American Institute of Certified Public Accountants.

The accompanying projection was prepared by management to provide potential investors with information to analyze the effect of a hypothetical sale of the properties as of December 31, 19X8, and should not be considered a presentation of expected future results.

A compilation is limited to presenting, in the form of a forecast or projection, information that is the representation of management, and does not include evaluation of the support for the assumptions underlying the forecast or projection. We have not examined the forecast or projection and, accordingly, do not express an opinion or any other form of assurance on the accompanying

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

statements or assumptions. Furthermore, because events and circumstances frequently do not occur as expected, there will usually be differences between the forecasted and actual results, and even if the properties are sold on the date and for the prices indicated, there will usually be differences between the projected and actual results, and those differences may be material. We have no responsibility to update this report for events and circumstances occurring after the date of this report.

.04 In rare cases, management may forecast the sale of its investment in real estate during the forecast period. In such circumstances, the sale would not be hypothetical and should be included in the financial forecast with other operating results and significant changes in financial position. Furthermore, the sale would be covered by the accountant's standard report.[2]

Sales Prices Assumed When a Financial Forecast Includes a Projected Sale of an Entity's Real Estate Investment

Question:

.05 Paragraph 8.34 of the Guide indicates that short-term forecasts may not be meaningful in certain situations and that it may not be practical in those situations to present financial forecasts for enough future periods to demonstrate the long-term results of investment decisions. In those circumstances, the presentation should include a description of the potential effect of such results. For example, the Guide indicates that if a real estate entity's forecast does not extend to the period in which the entity's investment is expected to be liquidated, the forecast would include a discussion of the effects of a liquidation at the end of the forecast period, as shown in exhibit 9.08 of the Guide.[3]

.06 When disclosing the effects of a hypothetical liquidation (sale) of the entity's real estate investment at the end of the forecast period, what are appropriate assumptions for the sales price?

Answer:

.07 The Guide states (paragraph 7.01P) that although the responsible party need not have a reasonably objective basis for the hypothetical assumptions used in a projection, those assumptions should be consistent with the purpose of the projection. The purpose of disclosing the effects of a hypothetical sale of an entity's real estate investment at the end of the forecast period is to provide users with meaningful information about the long-term results of their investment decisions.

---

[2] In such rare circumstances, the accountant should treat the sale the same as any other significant assumption. For example, when examining the forecast, the accountant should consider whether the assumptions related to the sale are appropriate and suitably supported (for example, with respect to the timing of the sale and sales price). The accountant should also consider whether the assumptions should be identified by the responsible party as being particularly sensitive. Paragraph 8.25 of the Guide discusses the identification and disclosure of particularly sensitive assumptions.

[3] This disclosure can be presented as a footnote to a financial forecast or as a separate schedule (see "Reporting on Financial Forecasts That Include a Projected Sale of an Entity's Real Estate Investment" [paragraphs .01–.04]).

.08 Typically, the sales price is based on a specified capitalization rate of forecasted cash flows. To be consistent with the purpose of disclosing the hypothetical sale of the entity's real estate investment, the capitalization rate assumed should be consistent with the assumptions used in the forecast as well as with the entity's and the industry's experience. If the capitalization rate assumed is not consistent with the entity's or the industry's experience, the responsible party should consider whether the resulting projected sales price is appropriate, since it may result in a presentation that is inconsistent with the objective of providing users with meaningful information about the long-term results of their investment decisions.[4]

.09 Other sales prices may also be consistent with the purpose of the projection. For example, when significant nonrecourse debt is involved, the sales price assumed is often the existing mortgage balance or the existing mortgage balance plus original capital contributions.[5] Such assumed sales prices provide meaningful information that helps investors analyze their investment risk.

Reporting on Information Accompanying a Financial Forecast in an Accountant-Submitted Document

Question:

.10 An entity may request that additional details or explanations of items in a financial forecast (for example, details of sales or forecasted product line information) be included in an accountant-submitted document that contains a financial forecast and the accountant's report thereon. An entity may also request that certain nonaccounting information or other information not directly related to the basic forecast be included in such a document. The accompanying information is presented outside the financial forecast and is not considered necessary for the presentation of the forecast to be in conformity with guidelines for presentation of a financial forecast established by the American Institute of Certified Public Accountants. How should the accountant report on accompanying information presented outside the financial forecast in an accountant-submitted document when he or she has not been engaged to examine the information separately?

Answer:

.11 An accountant's report on information accompanying a financial forecast in an accountant-submitted document has the same objective as an accountant's report on the financial forecast: to describe clearly the character of the accountant's work and the degree of responsibility taken. When an accountant has examined a financial forecast included in an accountant-submitted document, the accountant's report on the accompanying information would ordinarily include the following:

- A statement that the examination has been made for the purpose of forming an opinion on whether (1) the financial forecast is presented

[4] Paragraph 8.22 states that "the basis or rationale for the assumptions should preferably be disclosed to assist the user of the financial forecast (projection) to understand the forecast (projection) and make an informed judgment about it."

[5] Paragraph 8.23P of the Guide states that "The responsible party should identify which assumptions in the projection are hypothetical."

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

in conformity with AICPA guidelines for the presentation of a forecast and (2) the underlying assumptions provide a reasonable basis for the forecast.

- Identification of the accompanying information.
- A statement that the accompanying information is presented for purposes of additional analysis and is not a required part of the financial forecast.
- An opinion on whether the accompanying information is fairly stated in all material respects in relation to the financial forecast taken as a whole or a disclaimer of opinion, depending on whether the information has been subjected to procedures applied in the examination of the financial forecast. The accountant may express an opinion on a portion of the accompanying information and disclaim an opinion on the remainder.[6]
- A caveat that the prospective results may not be achieved.

.12 Following are examples of reports that may be issued.[7]

Accompanying information has been subjected to procedures applied in the examination

Our examination of the financial forecast presented in the preceding section of this document was made for the purpose of forming an opinion on whether the financial forecast is presented in conformity with AICPA guidelines for the presentation of a forecast and whether the underlying assumptions provide a reasonable basis for the forecast. The [*identify accompanying information*] is presented for purposes of additional analysis and is not a required part of the financial forecast. Such information has been subjected to procedures applied in the examination of the financial forecast and, in our opinion, is fairly stated in all material respects in relation to the financial forecast taken as a whole. However, there will usually be differences between the forecasted and actual results, because events and circumstances frequently do not occur as expected, and those differences may be material. We have no responsibility to update this report for events and circumstances occurring after the date of this report.

Accompanying information has not been subjected to procedures applied in the examination

Our examination of the financial forecast presented in the preceding section of this document was made for the purpose of forming an opinion on whether the financial forecast is presented in conformity with AICPA guidelines for the presentation of a forecast and whether the underlying assumptions provide a reasonable basis for the forecast. The [*identify accompanying information*] is presented for purposes of additional analysis and is not a required part of the financial forecast. Such information has not been subjected to procedures applied in the examination of the financial forecast and, accordingly, we express no opinion or any other form of assurance on it. Furthermore, there will usually be differences between the forecasted and actual results, because events and circumstances frequently do not occur as expected, and those differences may

---

[6] If the accountant concludes, on the basis of known facts, that any accompanying information is materially misstated in relation to the financial forecast taken as a whole, he or she should discuss the matter with the responsible party and propose appropriate revision of the accompanying information or related disclosures. If the responsible party will not agree to revision of the accompanying information, the accountant should either modify the report on the accompanying information and describe his or her reservations regarding the information or refuse to include the information in the document.

[7] The report may be added to the report on the financial forecast or may be presented with the information accompanying the financial forecast.

be material. We have no responsibility to update this report for events and circumstances occurring after the date of this report.

.13 If accompanying information is included in an accountant-submitted document that includes a financial forecast and the accountant's compilation report thereon, the accountant's compilation report should also cover the other data. For example, the following paragraph may be added to the accountant's standard compilation report on a financial forecast if the accountant compiled the accompanying information.

> We also compiled [*identify accompanying information*] and, accordingly, do not express an opinion or any other form of assurance on such information.

Financial Projections Included in General-Use Documents

Question:

.14 The Guide indicates that, if a client expects to include a financial projection (as defined in paragraph 3.05 of the Guide) in a general-use document, an accountant should not submit the projection to the client or provide the client with any type of report thereon unless the projection is used to supplement a financial forecast for a period covered by the forecast.[8] What is an accountant's responsibility for a projection (not used to supplement a financial forecast for the period covered by the forecast) included in a client-prepared general-use document when historical financial statements and the accountant's report thereon are included in the same document?

Answer:

.15 If an accountant consents to the use of his or her report on historical financial statements in a client-prepared general-use document that contains a financial projection for a period not covered by the forecast, such projection should be accompanied by an indication by the responsible party or the accountant that the accountant provides no assurance on the financial projection.[9, 10] If the accountant has audited the historical financial statements, he or she should refer to SAS No. 8, *Other Information in Documents Containing Audited Financial Statements*. Although the accountant should consider informing the responsible party that the presentation of a financial projection for a period not covered by the forecast in a general-use document is not in conformity with the Guide, the use of such a projection in a general-use document is not presumed to be a material misstatement of fact.

Question:

.16 What is the accountant's responsibility for a financial projection (not used to supplement a financial forecast for the period covered by the forecast) included in a client-prepared general-use document when a financial forecast and the accountant's report thereon are included in the same document?

---

[8] Paragraph 10.12P of the Guide states that "an accountant . . . should not submit or report on or consent to the use of his name in conjunction with a financial projection that he believes will be distributed to those who are unable to negotiate directly with the responsible party . . ." Also, see paragraph 4.05 of the Guide.

[9] See paragraph 10.20 of the Guide.

[10] In documents filed with the Securities and Exchange Commission (SEC), the responsible party should make this statement. In addition, the presentation of the financial projection should be labeled "supplemental and unaudited."

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Answer:

.17 If an accountant consents to the use of his or her report on a financial forecast in a client-prepared general-use document that contains a financial projection for a period not covered by the forecast, such projection should be accompanied by an indication by the responsible party or the accountant that the accountant provides no assurance on the financial projection.[11] In addition, the accountant should refer to the guidance in paragraphs 10.24–10.30 of the Guide and consider informing the responsible party that the presentation of a projection for a period not covered by the forecast in a general-use document is not in conformity with the Guide.

Support for Tax Assumptions

Question:

.18 Sometimes, one of the most sensitive assumptions underlying a financial forecast relates to the income tax treatment of prospective transactions. To obtain a reasonably objective basis for such tax assumptions, the responsible party may obtain a "tax opinion" from another practitioner, such as the entity's tax counsel or another accountant. What responsibility does an accountant examining a financial forecast have in considering whether the tax opinion provides suitable support for tax assumptions underlying the financial forecast?

Answer:

.19 Technical training and experience, as well as knowledge of the client and its industry, enable the accountant to be knowledgeable about income tax matters and competent in assessing their presentation in prospective financial statements. Therefore, when carrying out procedures to determine whether another practitioner's tax opinion provides suitable support for tax assumptions, the accountant is viewed as being one who is knowledgeable in income tax matters related to the entity's forecast.[12]

.20 In determining whether another practitioner's tax opinion provides suitable support for tax assumptions[13] underlying a financial forecast, the accountant should[14]—

a. Obtain a copy of the tax opinion expected to be issued.

b. Apply the following procedures from SAS No. 73, *Using the Work of a Specialist:*

- Evaluate the professional qualifications of the other practitioner including consideration of his or her (*a*) professional certification, license, or other recognition of professional competence, (*b*)

---

[11] See footnote 10.

[12] The tax opinion provided by the other practitioner may address matters of a legal nature not directly related to amounts included in the forecast—for example, matters related to the legal form of the entity. Accountants are not expected to have the technical training and experience necessary to form an opinion on legal matters.

[13] Paragraph 15.21 of the Guide states that "the accountant should evaluate whether assumptions have been developed for all key factors upon which the entity's financial results appear to depend." When evaluating a tax opinion, the accountant should take into account whether all material tax issues have been considered.

[14] See paragraph 15.32 of the Guide. Also, if an accountant is relying on the opinion of another practitioner in connection with a tax shelter offering, reference should be made to Internal Revenue Service regulations regarding tax shelter opinions (see appendix D to the Guide).

reputation and standing in the view of peers or others, and (*c*) experience in the type of work under consideration.

- Obtain an understanding of the nature of the work to be performed by the other practitioner including the (*a*) objectives and scope of the practitioner's work, (*b*) the relationship of the other practitioner to the responsible party, (*c*) methods or assumptions used by the other practitioner, (*d*) the appropriateness of using the other practitioner's work for the intended purpose, and (*e*) the form and content of the other practitioner's findings that will enable the practitioner to make an evaluation described in SAS No. 73, paragraph 12.
- Make appropriate tests of data provided to the other practitioner.
- Evaluate whether the other practitioner's findings support the related representations in the prospective financial statements. In doing this, the accountant should read the tax opinion and consider whether (*a*) the facts used in the tax opinion are consistent with the information obtained during the examination of the forecast, (*b*) the assumptions and arguments used in the tax opinion are reasonable,[15]— and (*c*) the assumptions, facts, and arguments used in the tax opinion support the conclusions reached.

Periods Covered by an Accountant's Report on Prospective Financial Statements

Question:

.21 The Guide includes an example of an accountant's examination report on a financial forecast "for the annual periods ending December 31, 19X2 through 19X6."[16] The examination report states that the forecast was examined and concludes that (*a*) the forecast is presented in conformity with the presentation guidelines established by the American Institute of Certified Public Accountants, and (*b*) the underlying assumptions provide a reasonable basis for management's forecast. Does the accountant's examination report on a financial forecast apply to the forecast taken as a whole or to each of the discrete periods presented in the forecast?

Answer:

.22 The accountant's report on a financial forecast should correspond to the form of the forecast. Accordingly, if the forecast is presented in a columnar format in which each column represents a specific period, the accountant's report on the forecast applies to each period presented in the forecast. Conversely, an accountant's report would pertain to the entire period covered by the forecast (taken as a whole) if the presentation included a single column labeled "for the five years ending December 31, 19X6."

.23 When an accountant examines a financial forecast that presents individual discrete periods, he or she should evaluate the support for the underlying assumptions used in the preparation of the forecast for each period presented.[17]

---

[15] See footnote 12.

[16] See the illustrative report for a financial feasibility study in paragraph 17.27 of the Guide.

[17] Paragraph 15.05 of the Guide states: "Materiality is a concept that is judged in light of the expected range of reasonableness of the information, and therefore users should not expect prospective information . . . to be as precise as historical information."

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Forecasts and Projections Audit Issues Task Force (1988)

KENNETH J. DIRKES, *Chairman*
RICHARD DIETER
GEORGE J. DUVA
ROBERT W. BERLINER
ERNEST L. TEN EYCK
RICHARD M. STEINBERG
DON PALLAIS
DAVID KUTSCHER
BRUCE BALTIN
GERALD N. TUCH

DAN M. GUY
Vice President, Auditing
MIMI BLANCO-BEST
Technical Manager
Auditing Standards

[The next page is 30,461.]

Section 14,140

Statement of Position 89-7 Report on the Internal Control Structure in Audits of Investment Companies*

December, 1989

NOTE

This statement of position presents the recommendations of the AICPA Investment Companies Committee regarding the application of generally accepted auditing standards to reports on the internal control structure in audits of investment companies. It represents the considered opinion of the committee on the best auditing practice in the industry and has been reviewed by members of the AICPA Auditing Standards Board for consistency with existing auditing standards. AICPA members may have to justify departures from the recommendations in this statement if their work is challenged.

Introduction

[.01–.02] [Paragraphs deleted, June 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Report on Internal Control Required by the SEC

.03 The following is an illustration of the independent auditor's report on a management investment company's internal control structure based on the results of procedures performed in obtaining an understanding of the internal control structure and assessing control risk. These procedures should include the review, study, and evaluation of the accounting system, internal accounting controls, and procedures for safeguarding securities required by the instructions to Form N-SAR.

Board of Directors
XYZ Investment Company

In planning and performing our audit of the financial statements of XYZ Investment Company for the year ended December 31, 19X1, we considered its internal control structure, including procedures for safeguarding securities, in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements and to comply with the requirements of Form N-SAR, not to provide assurance on the internal control structure.

The management of XYZ Investment Company is responsible for establishing and maintaining an internal control structure. In fulfilling this responsibility,

* Statement on Auditing Standards (SAS) No. 78, *Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS No. 55*, revises the definition and description of internal control and makes conforming changes to relevant terminology. This SOP will be amended to conform to SAS No. 78 in a future edition of *Technical Practice Aids*.

estimates and judgments by management are required to assess the expected benefits and related costs of internal control structure policies and procedures. Two of the objectives of an internal control structure are to provide management with reasonable, but not absolute, assurance that assets are safeguarded against loss from unauthorized use or disposition and that transactions are executed in accordance with management's authorization and recorded properly to permit preparation of financial statements in conformity with generally accepted accounting principles.

Because of inherent limitations in any internal control structure, errors or irregularities may occur and not be detected. Also, projection of any evaluation of the structure to future periods is subject to the risk that it may become inadequate because of changes in conditions or that the effectiveness of the design and operation may deteriorate.

Our consideration of the internal control structure would not necessarily disclose all matters in the internal control structure that might be material weaknesses under standards established by the American Institute of Certified Public Accountants. A material weakness is a condition in which the design or operation of the specific internal control structure elements does not reduce to a relatively low level the risk that errors or irregularities in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. However, we noted no matters involving the internal control structure, including procedures for safeguarding securities, that we consider to be material weaknesses as defined above as of December 31, 19X1.†

This report is intended solely for the information and use of management and the Securities and Exchange Commission.

Accounting Firm

New York, New York
February 15, 19X2

Effective Date

.04 This statement is effective for audits of financial statements for periods beginning on or after January 1, 1989, with early application permissible.

† If conditions believed to be material weaknesses are disclosed, the report should describe the weaknesses that have come to the auditor's attention and may state that these weaknesses do not affect the report on the financial statements. The last sentence of the fourth paragraph of the report should be modified as follows:

> However, we noted the following matters involving the (control environment, accounting system, control procedures, or procedures for safeguarding securities) and its (their) operation that we consider to be material weaknesses as defined above. These conditions were considered in determining the nature, timing, and extent of the procedures to be performed in our audit of the financial statements of XYZ Investment Company for the year ended December 31, 19X1, and this report does not affect our report thereon dated February 15, 19X2. [*A description of the material weaknesses that have come to the auditor's attention would follow. Also, Sub-item 77B of the instructions to Form N-SAR says "(d)isclosure of a material weakness should include an indication of any corrective action taken or proposed."*]

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Investment Companies Committee (1988-1989)

JERRY A. DAVIS, *Chairman*
STEVEN E. BULLER
M. CHRISTOPHER CANAVAN, JR.
NICHOLAS P. CONSTANTAKIS
ROBERT F. GUNIA
PAUL A. KELLER
JAMES F. MAHONEY
RICHARD P. MEYEROWICH
PAUL R. NEVIERA
DAVID M. TAYLOR
FREDERICK M. WERBLOW
JONATHAN F. ZESCHIN

DAN M. GUY,
Vice President, Auditing
PATRICK L. MCNAMEE,
Director
Audit and Accounting Guides
DIONNE D. MCNAMEE,
Technical Manager
Accounting Standards

[The next page is 30,471.]

Section 14,150

Statement of Position 90-1 Accountants' Services on Prospective Financial Statements for Internal Use Only and Partial Presentations

January, 1990

NOTE

This statement of position presents the recommendations of the Forecasts and Projections Task Force regarding accountants' services on prospective financial statements for internal use only and partial presentations. It represents the considered opinion of the task force on the best practice for such engagements and has been reviewed by members of the AICPA Auditing Standards Board for consistency with existing standards. AICPA members may have to justify departures from the recommendations in this statement if their work is challenged.

Part I

Guidance on the Accountant's Services and Reports on Prospective Financial Statements for Internal Use Only*

.01 An accountant may be engaged to provide services on financial forecasts that are restricted to internal use in a variety of circumstances. For example, he or she may assemble a financial forecast in connection with an evaluation of the tax consequences of future actions or in connection with advice and assistance to a client evaluating whether to buy or lease an asset. When the forecast is to be restricted to internal use,[1] an accountant may perform a compilation, examination, or application of agreed-upon procedures in accordance with AICPA standards[2] or any of a spectrum of "other services" on it. The accountant need not report on such other services unless requested

* *Note:* Because financial forecasts and projections are similar in many respects, separate guidance for projections is provided only to the extent that it differs from that for forecasts. Italicized paragraphs in this section show how the guidance presented for forecasts should be modified for projections. Any plain-text paragraph not followed by an italicized paragraph applies to both forecasts and projections even though it uses only the term *forecast*.

[1] In deciding whether a potential use is *internal use*, the accountant should consider the degree of consistency of interest between the responsible party and the user regarding the forecast. If their interests are substantially consistent (for example, both the responsible party and the user are employees of the entity about which the forecast is made), the use would be deemed internal use. On the other hand, where the interest of the responsible party and the user are potentially inconsistent (for example, the responsible party is a nonowner manager and the user is an absentee owner), the use would not be deemed internal use. In some cases, this determination will require the exercise of considerable professional judgment.

[2] See chapters 12, 13, and 14 of the Guide for guidance on compilations, chapters 15, 16, and 17 of the Guide for examinations, and chapters 19, 20, and 21 of the Guide for application of agreed-upon procedures.

to by the client.[3] This section also suggests procedural and reporting guidance that an accountant might use in providing such other services on a financial forecast for internal use only.

.02 In satisfying himself or herself that the forecast will be restricted to internal use, the accountant may rely on either the written or oral representation of the responsible party, unless information comes to his or her attention that contradicts the responsible party's representation. If the accountant is not satisfied that the financial forecast will be restricted to internal use only, he or she should follow the guidance in paragraph 10.02 of the Guide.

Procedures

.03 The accountant's procedures should be consistent with the nature of the engagement. Other chapters of the Guide provide useful guidance on the type of procedures an accountant would apply when the nature of the engagement is similar to either a compilation, examination, or application of agreed-upon procedures.

.04 When an accountant provides other services on a financial forecast for internal use, he or she should establish an understanding with the client, preferably in writing, regarding the services to be performed and should specify in this understanding that the financial forecast and the report, if any, are not to be distributed to outside users.

Reporting

.05 The Statement on Standards for Accountants' Services on Prospective Financial Information, *Financial Forecasts and Projections*, does not require the accountant to report on other services performed on a financial forecast for internal use only. Accordingly, an accountant can submit a computer-generated or manually prepared financial forecast to a client without reporting on it when the forecast is for internal use only.

.06 If an accountant decides to issue a report and he or she purports to have compiled, examined, or applied agreed-upon procedures to a financial forecast for internal use only in conformity with AICPA standards, the accountant should follow the reporting guidance in other sections of the Guide.[4] If the accountant decides to issue a report on other services performed with respect to a financial forecast for internal use only, the report's form and content are flexible. However, the accountant should not report on financial forecasts that exclude a summary of significant assumptions.[5] The report preferably would—

a. Be addressed to the responsible party.

b. Identify the statements being reported on.

c. Describe the character of the work performed and the degree of responsibility taken[6] with respect to the financial forecast.

d. Include a caveat that the prospective results may not be achieved.

---

[3] However, see paragraph .09.

[4] See chapters 14, 17, and 21 of the Guide for guidance on reporting on a compilation, examination, or application of agreed-upon procedures, respectively.

[5] See paragraph 9.05 of the Guide for guidance on presentation formats for disclosure of significant assumptions.

[6] The accountant's assurance on the financial forecast should not be similar to that given for an examination unless he or she complies with the procedures for an examination as described in chapter 15 of the Guide.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

e. Indicate the restrictions as to the distribution of the financial forecast and report.

f. Be dated as of the date of the completion of his or her procedures.

.06P *In addition to the elements listed above, the accountant's report on a financial projection for internal use only preferably would include a description of the limitations on the usefulness of the presentation.*

.07 In addition to the above, the accountant's report would, where applicable, preferably—

a. Indicate if the accountant is not independent with respect to an entity on whose financial forecast he or she is providing services. An accountant should not provide any assurance on a financial forecast of an entity with respect to which he or she is not independent.

b. Describe omitted disclosures that come to his or her attention (for example, the omission of the summary of significant accounting policies discussed in paragraph 8.06 of the Guide), or simply state that there are omissions of disclosures required under the guidelines for presentation of a financial forecast. For example, when a financial forecast is included in a personal financial plan, the description may be worded as follows:

> This financial forecast was prepared solely to help you develop your personal financial plan. Accordingly, it does not include all disclosures required by the guidelines established by the American Institute of Certified Public Accountants for the presentation of a financial forecast.

.08 The following is an example report, for cases in which the accountant chooses to issue a report, when he or she has assembled a financial forecast for which distribution is limited to internal use:

> We have assembled, from information provided by management, the accompanying forecasted balance sheet and the related forecasted statements of income, retained earnings, and cash flows of XYZ Company as of December 31, 19XX, and for the year then ending.
>
> (This financial forecast omits the summary of significant accounting policies.)[7] We have not compiled or examined the financial forecast and express no assurance of any kind on it. Further, there will usually be differences between the forecasted and actual results, because events and circumstances frequently do not occur as expected, and those differences may be material. In accordance with the terms of our engagement, this report and the accompanying forecast are restricted to internal use and may not be shown to any third party for any purpose.

.08P *The following is an example report, for cases in which the accountant chooses to issue a report, when an accountant has assembled a financial projection for which distribution is limited to internal use:*

> *We have assembled, from information provided by management, the accompanying projected balance sheet and the related projected statements of income, retained earnings, and cash flows of XYZ Company as of December 31, 19XX, and for the year then ending. (This financial projection omits the summary of significant accounting policies.)*[8] *The accompanying projection and this report were prepared for* [state special purpose, for example, "presentation to the Board of Directors of XYZ Company for its consideration as to whether to add

---

[7] This sentence would be included, if applicable.

[8] This sentence would be included, if applicable.

a third operating shift"] *and should not be used for any other purpose. We have not compiled or examined the financial projection and express no assurance of any kind on it. Further, even if* [state hypothetical assumption, for example, "the third operating shift is added"] *there will usually be differences between the projected and actual results, because events and circumstances frequently do not occur as expected, and those differences may be material. In accordance with the terms of our engagement, this report and the accompanying projection are restricted to internal use and may not be shown to any third party for any purpose.*

.09 When a financial forecast for internal use only is included with an accountant's written communication (for example, with a transmittal letter or report), a caveat that the prospective results may not be achieved and a statement that the financial forecast is for internal use only should be communicated in writing. Such caveat and statement should be included in the communication on or in the prospective financial statements.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Part II

Partial Presentations of Prospective Financial Information†

Introduction

.10 Much of the guidance in the AICPA's *Guide for Prospective Financial Statements* (the "Guide") can be applied to partial presentations of prospective financial information. This section—

- Describes how that guidance applies to the unique aspects of partial presentations.
- Discusses the accountant's responsibility for partial presentations when he or she is engaged to issue or does issue a written communication that expresses a conclusion about the reliability of a written partial presentation that is the responsibility of another party (see paragraph .25).

.11 A partial presentation is a presentation of prospective financial information that excludes one or more of the items required for prospective financial statements as described in paragraph 8.06 of the Guide.[9] A partial presentation may include either forecasted or projected information and may either be extracted from a presentation of prospective financial statements or may be prepared to meet a specific need.[10] Examples of partial presentations include—

- Sales forecasts.
- Presentations of forecasted or projected capital expenditure programs.

---

† *Note:* Because forecasted and projected information is similar in many respects, separate guidance for projected information is provided only to the extent that it differs from that for forecasted information. Italicized paragraphs show how the guidance presented for forecasted information should be modified for projected information. Any plain-text paragraph not followed by an italicized paragraph applies to both forecasted and projected information even though it uses only the term *forecasted*.

[9] Paragraph 8.06 of the Guide indicates that a financial forecast may take the form of complete basic financial statements or may be limited to the following items (where such items would be presented for historical financial statements for the period):

a. Sales or gross revenues
b. Gross profit or cost of sales
c. Unusual or infrequently occurring items
d. Provision for income taxes
e. Discontinued operations or extraordinary items
f. Income from continuing operations
g. Net income
h. Primary and fully diluted earnings per share
i. Significant changes in financial position

When the financial forecast takes the form of basic financial statements, the requirement to disclose significant changes in financial position in *i* above is accomplished by presenting a statement of cash flows and its related note disclosures in accordance with FASB Statement No. 95, *Statement of Cash Flows*.

If the omitted applicable item is derivable from the information presented, the presentation would not be deemed to be a partial presentation. Paragraph 8.08 of the Guide states that a summary of significant assumptions and accounting policies and an appropriate introduction should always accompany the forecast.

[10] Partial presentations do not include estimates in historical financial statements and related notes required by generally accepted accounting principles or an other comprehensive basis of accounting. Guidance on auditing accounting estimates is contained in SAS No 57, *Auditing Accounting Estimates*.

- Projections of financing needs.
- Other presentations of specified elements, accounts, or items of prospective financial statements (for example, projected production costs) that might be part of the development of a full presentation of prospective financial statements.
- Forecasts that present operating income but not net income.
- Forecasts or projections of taxable income that do not show significant changes in financial position.
- Presentations that provide enough information to be translated into elements, accounts, or items of a financial forecast or projection. Examples include a forecast of sales units and unit selling prices and a forecast of occupancy percentage, number of rooms, and average room rates for a hotel. In contrast, if the prospective information only presents units expected to be sold but excludes unit selling prices, it would not be considered a partial presentation.

Uses of Partial Presentations

.12 Partial presentations may be appropriate in many "limited use" circumstances.[11] For example, a responsible party may prepare a partial presentation to analyze whether to lease or buy a piece of equipment or to evaluate the income tax implications of a given election, since it may only be necessary to assess the impact on one aspect of financial results rather than on the financial statements taken as a whole. However partial presentations are not ordinarily appropriate for general use. Accordingly, a partial presentation ordinarily should not be distributed to third parties who will not be negotiating directly with the responsible party (for example, in an offering document for an entity's debt or equity interests). In this context, *negotiating directly* is defined as a third-party user's ability to ask questions of and negotiate the terms or structure of a transaction directly with the responsible party.

.13 The responsible party should consider whether a presentation omitting one or more items required for prospective financial statements will adequately present the information given its special purpose. Unless there is agreement between the responsible party and potential users specifying the content of the partial presentation, a partial presentation is inappropriate if it is incomplete for what it purports to present. Examples of partial presentations that might be inappropriate include a statement of forecasted receipts and disbursements that does not include certain existing commitments of the entity or a forecast of net income that does not include disclosure of changes in financial position, when such disclosures would indicate the need for additional capital to sustain operations. A presentation of prospective sales, however, is an example of a presentation that would be appropriate in circumstances where its intended use is to negotiate the terms of a royalty agreement based on sales.

Preparation and Presentation of Partial Presentations

.14 Partial presentations omit one or more of the minimum items required in paragraph 8.06 of the Guide for prospective financial statements.[12] The guidance

[11] See paragraphs 3.13 and 4.04 of the Guide.

[12] As used here, prospective financial statements include complete basic financial statements or the minimum items described in paragraph 8.06 of the Guide (see footnote 1).

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

below describes matters to be considered in the preparation and presentation of partial presentations.

.15 *Key Factors.* If the responsible party prepares a partial presentation without preparing prospective financial statements, the responsible party should consider key factors affecting elements, accounts, or items of prospective financial statements that are interrelated with those presented. In a sales forecast, for example, a key factor to be considered is whether productive capacity is sufficient to support forecasted sales. When the prospective information included in the partial presentation is extracted from the prospective financial statements, the effects of interrelationships among elements of the prospective financial statements should have been previously determined.

.16 *Titles.* Titles of partial presentations should be descriptive of the presentation and state whether the presentation is of forecasted or projected information. In addition, titles should disclose the limited nature of the presentation and should not state that it is a "financial forecast" or a "financial projection." Examples of appropriate titles are "forecast of production capacity" and "projected operating income assuming a new plant facility."

.17 *Accounting Principles and Policies.* Significant accounting policies relevant to the information presented and its intended purpose should be disclosed.

.18 Occasionally, a different basis of accounting is used for preparing a partial presentation than that expected to be used in preparing the historical financial statements covering the same period as the partial presentation. In such circumstances, the presentation should disclose the basis of accounting to be used to prepare the historical financial statements covering the prospective period. Differences resulting from the use of the different basis to prepare the partial presentation should be described but need not be quantified.

.19 *Materiality.* The concept of materiality should be related to the partial presentation taken as a whole.

.20 *Assumptions.* Assumptions that are significant to a partial presentation include those assumptions having a reasonable possibility of a variation that may significantly affect the prospective results. Such assumptions may be either directly or indirectly related to the presentation. The selling price of a product, for example, is an assumption that could directly affect a sales forecast, whereas a company's productive capacity is an example of an assumption that could indirectly affect the sales forecast. Frequently, the more indirectly related an assumption is to the partial presentation, the greater the potential variation would have to be to have a material impact on the prospective results presented.

.21 In some situations, the disclosure of assumptions deemed to be significant to the partial presentation of prospective financial information would be virtually the same as those disclosures that would be necessary if a full presentation of prospective financial statements were to be made. For example, in a partial presentation of forecasted operating results, it is likely that most assumptions that would be significant with respect to a full presentation would also be significant with respect to the presentation of forecasted operating results. Thus, those assumptions should be disclosed.

.22 In other, more limited partial presentations of prospective financial information, however, there may be few assumptions having a reasonable pos-

sibility of a variation that would significantly affect the presentation. In a presentation of forecasted sales, for example, it would only be necessary to disclose those assumptions relating directly to the sales forecast, such as future demand and pricing, unless other assumptions—such as marketing and advertising programs, productive capacity and production costs, financial stability or working capital sufficiency—have a reasonable possibility of a variation significant enough to have a material impact on the sales forecast.

.23 The introduction preceding the summary of assumptions for a partial presentation should include a description of the purpose of the presentation and any limitations on the usefulness of the presentation.

.24 The following is an example of the introduction for a partial presentation of forecasted sales:

> This sales forecast presents, to the best of management's[13] knowledge and belief, expected sales during the forecast period. Accordingly, the sales forecast reflects its judgment as of (date), the date of this forecast, of the expected conditions and its expected course of action. The sales forecast is for use in negotiating the Company's lease override provisions and should not be used for any other purpose. The assumptions disclosed herein are those that management believes are significant to the sales forecast. There will usually be differences between the forecasted and actual results because events and circumstances frequently do not occur as expected, and those differences may be material.

.24P *The following is an example of the introduction preceding the summary of assumptions for a schedule of projected production at a maximum productive capacity:*

> *This projection of production by product line presents, to the best of management's[14] knowledge and belief, the Company's expected production for the period if management chooses to operate its plant at maximum capacity. Accordingly, the projection of production by product line reflects its judgment as of (date), the date of this projection, of the expected conditions and its expected course of action if the plant were operated at maximum capacity. The projected statement is designed to provide information to the Company's board of directors concerning the maximum production that might be achieved and related costs if current capacity were expanded through the addition of a third production shift. Accordingly, this projected statement should not be used for any other purpose. The assumptions disclosed herein are those that management believes are significant to the projected statement; however, management has not decided to operate the plant at maximum capacity. Even if the plant were operated at maximum capacity, there will usually be differences between projected and actual results because events and circumstances frequently do not occur as expected, and those differences may be material.*

Accountant's Involvement With Partial Presentations

.25 An accountant who is engaged to issue or does issue a written communication[15] that expresses a conclusion about the reliability[16] of a written par-

---

[13] If the responsible party is other than management, this reference should be to the party who assumes responsibility for the assumptions.

[14] See footnote 5.

[15] An accountant should not report on a partial presentation that excludes disclosure of the summary of significant assumptions or, for a projection, excludes identification of the hypothetical assumptions.

[16] Reliability, as it applies to a partial presentation, does not relate to the achievability of the prospective results.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

tial presentation[17] that is the responsibility of another party should examine or apply agreed-upon procedures to the presentation.[18] An accountant may also be engaged to compile a partial presentation. When an accountant compiles, examines, or applies agreed-upon procedures to a partial presentation, he or she should perform the engagement in accordance with the guidance in paragraphs .29 and .30.[19]

.26 This section does not provide standards or procedures for engagements involving partial presentations used solely in connection with litigation services, although it provides helpful guidance for many aspects of such engagements and may be referred to as useful guidance in such engagements. *Litigation services* are engagements involving pending or potential formal legal or regulatory proceedings before a "trier of fact" in connection with the resolution of a dispute between two or more parties, for example, in circumstances where an accountant acts as an expert witness. This exception is provided because, among other things, the accountant's work in such proceedings is ordinarily subject to detailed analysis and challenge by each party to the dispute.[20]

.27 The accountant should consider whether it is appropriate to report on a partial presentation.[21]

.28 Occasionally, an accountant may be engaged to prepare a financial analysis of a potential project where the engagement includes obtaining the information, making appropriate assumptions, and assembling the presentation. In such circumstances, the accountant is the asserter and the analysis is not, and should not be characterized as, forecasted or projected information as defined in paragraph .11. Such analysis would not be appropriate for general use.[22]

Compilation and Examination Procedures

.29 The procedures for compilations and examinations of prospective financial statements are generally applicable to partial presentations.[23] However, the accountant's procedures may be affected by the nature of the information presented. As described in paragraph .15, many elements of prospective financial statements are interrelated. The accountant should give appropriate consideration to whether key factors affecting elements, accounts, or items that are interrelated with those in the partial presentation he or she has been engaged to examine or compile have been considered, including key factors that may not necessarily be obvious from the partial presentation (for

---

[17] This statement covers only a partial presentation presented in written form by the party responsible for it. Consistent with the attestation standards, oral assertions about prospective results are not addressed by this statement.

[18] Examples of professional standards that may involve partial presentations not covered by this section are included in paragraph 2 of the Statements on Standards for Attestation Engagements (AICPA, *Professional Standards*, vol. 1, AT sec. 100). In addition, paragraphs 76–81 of that section contain guidance that an accountant should follow when he or she provides an attest service as part of an MAS engagement.

[19] If the accountant provides services on a partial presentation restricted to internal use only, he or she may apply the guidance in paragraphs .01–.09 of Part I of this section.

[20] See paragraph 10.03 of the Guide.

[21] See paragraphs .12 and .13.

[22] If the responsible party reviews and adopts the assumptions and presentation, the presentation might be a partial presentation. See paragraphs .11 and .12 for the definition and uses of partial presentations.

[23] See chapters 12 and 15 of the Guide.

example, productive capacity relative to a sales forecast), and whether all significant assumptions have been disclosed. The accountant may find it necessary for the scope of his or her examination or compilation of some partial presentations to be similar to that for his or her examination or compilation of a presentation of prospective financial statements. For example, the scope of an accountant's procedures when he or she examines forecasted results of operations would likely be similar to those for his or her examination of prospective financial statements since the accountant would likely need to consider the interrelationships of all accounts in the examination of results of operations.

Applying Agreed-Upon Procedures to Partial Presentations

.30 An accountant may accept an engagement to apply agreed-upon procedures to a partial presentation provided (*a*) the specified users involved have participated in establishing the nature and scope of the engagement and take responsibility for the adequacy of the procedures to be performed, (*b*) distribution of the report is to be restricted to the specified users involved, and (*c*) the partial presentation includes a summary of significant assumptions. The guidance in chapter 19 of the Guide is generally applicable to such engagements.

Standard Accountant's Compilation, Examination, and Agreed-Upon Procedures Reports

.31 The accountant's standard report on a partial presentation should include—

- An identification of the partial presentation reported on.
- A caveat that the forecasted results may not be achieved.
- A statement that the accountant assumes no responsibility to update the report for events and circumstances occurring after the date of the report.
- A description of any limitations on the usefulness of the presentation.
- For a compilation
  - — A statement that the accountant has compiled the partial presentation in accordance with guidelines established by the American Institute of Certified Public Accountants.
  - — A statement that a compilation is limited in scope and does not enable the accountant to express an opinion or any other form of assurance on the partial presentation of the assumptions.
- For an examination
  - — A statement that the examination of the partial presentation was made in accordance with AICPA standards and a brief description of the nature of such an examination.
  - — For forecasted information, the accountant's opinion that the partial presentation is presented in conformity with AICPA presentation guidelines and that the underlying assumptions provide a reasonable basis for the forecast.
  - — *For projected information, the accountant's opinion that the partial presentation is presented in conformity with AICPA presenta-*

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

tion guidelines and that the underlying assumptions provide a reasonable basis for the projection given the hypothetical assumptions.

- For an agreed-upon procedures engagement
  - — A statement that the report is intended solely for the specified users, and should not be used by others.
  - — An enumeration of the procedures performed and a reference to conformity with the arrangements made with the specified users.
  - — If the agreed-upon procedures are less than those performed in an examination, a statement that the work performed was less in scope than an examination of a partial presentation in accordance with AICPA standards, and
    - For forecasted information, a disclaimer of opinion on whether the presentation is in conformity with AICPA presentation guidelines and on whether the underlying assumptions provide a reasonable basis for the forecast.
    - *For projected information, a disclaimer of opinion on whether the presentation is in conformity with AICPA presentation guidelines and on whether the underlying assumptions provide a reasonable basis for the projection given the hypothetical assumptions.*
  - — A statement of the accountant's findings.[24]

.32 Chapters 14, 17, and 21 of the Guide describe circumstances where the accountant's standard report on a financial forecast may require modification. The guidance for modifying the accountant's standard reports included in those sections is generally applicable to partial presentations. Also, depending on the nature of the presentation, the accountant may decide to disclose that the partial presentation is not intended to be a forecast of financial position, results of operations, or cash flows. The following are the forms of the accountant's standard report when he or she has compiled, examined, or applied agreed-upon procedures to a partial presentation.[25]

Compilation Report on a Partial Presentation of Forecasted Information

We have compiled the accompanying forecasted statement of net operating income before debt service, depreciation, and income taxes of ÅAA Hotel for the year ending December 31, 19X1 (the forecasted statement) in accordance with guidelines established by the American Institute of Certified Public Accountants.

The accompanying forecasted statement presents, to the best of management's knowledge and belief, the net operating income before debt service, depreciation, and income taxes of AAA Hotel for the forecast period. It is not intended to be a forecast of financial position, results of operations, or cash flows. The

[24] The accountant may wish to state in his or her report that he or she makes no representation about the sufficiency of the procedures for the specified users' purposes.

[25] These report forms are appropriate whether the presentations are based on generally accepted accounting principles or on an other comprehensive basis of accounting.

accompanying forecasted statement and this report were prepared for the ABC Bank for the purpose of negotiating a proposed construction loan to be used to finance expansion of the hotel and should not be used for any other purpose.

A compilation is limited to presenting forecasted information that is the representation of management and does not include evaluation of the support for the assumptions underlying such information. We have not examined the forecasted statement and, accordingly, do not express an opinion or any other form of assurance on the accompanying statement or assumptions. Furthermore, there will usually be differences between forecasted and actual results because events and circumstances frequently do not occur as expected, and those differences may be material. We have no responsibility to update this report for events and circumstances occurring after the date of this report.

Compilation Report on a Partial Presentation of Projected Information

We have compiled the accompanying sales projection of XYZ Company for each of the years in the three-year period ending December 31, 19X1 in accordance with guidelines established by the American Institute of Certified Public Accountants.

The accompanying sales projection presents, to the best of management's knowledge and belief, the Company's expected sales during the projection period that would result if the Company achieved a 15 percent market share of the electric toaster market, as disclosed in items b and c of the summary of significant assumptions. The sales projection and this report were prepared for presentation to the Board of Directors of XYZ Company for its consideration of a new marketing program and should not be used for any other purpose.

A compilation is limited to presenting projected information that is the representation of management and does not include evaluation of the support for the assumptions underlying such information. We have not examined the sales projection and, accordingly, do not express an opinion or any other form of assurance on the accompanying sales projection or assumptions. Furthermore, even if the Company attained the 15 percent market share of the electric toaster market, there will usually be differences between projected and actual results because events and circumstances frequently do not occur as expected, and those differences may be material. We have no responsibility to update this report for events and circumstances occurring after the date of this report.

Examination Report on a Partial Presentation of Forecasted Information

We have examined the accompanying forecasted statement of net operating income before debt service, depreciation, and income taxes of the AAA Hotel for the year ending December 31, 19X1 (the forecasted statement). Our examination was made in accordance with standards established by the American Institute of Certified Public Accountants and, accordingly, included such procedures as we considered necessary to evaluate both the assumptions used by management and the preparation and presentation of the forecasted statement.

The accompanying forecasted statement presents, to the best of management's knowledge and belief, the expected net operating income before debt service, depreciation, and income taxes of AAA Hotel for the forecast period. It is not

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

intended to be a forecast of financial position, results of operations, or cash flows. The accompanying forecasted statement and this report were prepared for ABC Bank for the purpose of negotiating a proposed construction loan to be used to finance expansion of the hotel and should not be used for any other purpose.

In our opinion, the forecasted statement referred to above is presented in conformity with the guidelines for presentation of forecasted information established by the American Institute of Certified Public Accountants, and the underlying assumptions provide a reasonable basis for management's forecasted statement. However, there will usually be differences between forecasted and actual results because events and circumstances frequently do not occur as expected, and those differences may be material. We have no responsibility to update this report for events and circumstances occurring after the date of this report.

Examination Report on a Partial Presentation of Projected Information

We have examined the accompanying sales projection of XYZ Company for each of the years in the three-year period ending December 31, 19X1. Our examination was made in accordance with standards established by the American Institute of Certified Public Accountants and, accordingly, included such procedures as we considered necessary to evaluate both the assumptions used by management and the preparation and presentation of the sales projection.

The accompanying sales projection presents, to the best of management's knowledge and belief, the Company's expected sales during the projection period that would result if the Company achieved a 15 percent market share of the electric toaster market, as disclosed in items b and c of the summary of significant assumptions. The sales projection and this report were prepared for presentation to the Board of Directors of XYZ Company for its consideration of a new marketing program and should not be used for any other purpose.

In our opinion, the sales projection referred to above is presented in conformity with the guidelines for presentation of projected information established by the American Institute of Certified Public Accountants, and the underlying assumptions provide a reasonable basis for management's projection of expected sales during the period assuming the Company were to achieve a 15 percent market share of the electric toaster market. However, even if the Company achieves a 15 percent market share, there will usually be differences between projected and actual results because events and circumstances frequently do not occur as expected, and those differences may be material. We have no responsibility to update this report for events and circumstances occurring after the date of this report.

Agreed-Upon Procedures Report on a Partial Presentation of Forecasted Information

At your request, we have performed certain agreed-upon procedures, as enumerated below, with respect to the sales forecast of XYZ Company for the year ending December 31, 19X1. These procedures, which were specified by the Boards of Directors of XYZ Company and ABC Corporation, were performed solely to assist you, and this report is solely for your information and should not be used by those who did not participate in determining the procedures.

a. We assisted the management of XYZ Company in assembling the sales forecast.

b. We read the sales forecast for compliance in regard to format with the AICPA presentation guidelines for a partial presentation of forecasted information.

c. We tested the sales forecast for mathematical accuracy.

Because the procedures described above do not constitute an examination of a presentation of forecasted information in accordance with standards established by the American Institute of Certified Public Accountants, we do not express an opinion on whether the sales forecast is presented in conformity with AICPA presentation guidelines or on whether the underlying assumptions provide a reasonable basis for the presentation.

In connection with the procedures referred to above, no matters came to our attention that caused us to believe that the format of the sales forecast should be modified or that the presentation is mathematically inaccurate. Had we performed additional procedures or had we made an examination of the sales forecast in accordance with standards established by the American Institute of Certified Public Accountants, matters might have come to our attention that would have been reported to you. Furthermore, there will usually be differences between forecasted and actual results because events and circumstances frequently do not occur as expected, and those differences may be material. We have no responsibility to update this report for events and circumstances occurring after the date of this report.[26]

Effective Date

.33 The provisions of this statement are effective for engagements to provide services on prospective financial statements for internal use only and partial presentations beginning on or after July 1, 1990.

[26] See footnote 13.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.34

Appendix

Illustrations of Partial Presentations

A1. The illustrative partial presentations of prospective financial information included in the following pages are presented in conformity with the presentation guidelines of the Guide, although other presentation formats could also be consistent with the Guide. For example, it may be appropriate to present the summary of significant assumptions and accounting policies in a less formal manner than that illustrated, such as computer-printed output (indicating data and relationships) from "electronic worksheets" and general purpose financial modeling software, as long as the responsible party believes that the disclosures and assumptions presented can be understood by users.

A2. The following is a brief summary of the illustrative partial presentations presented below:

a. Example 1 illustrates a sales forecast prepared for the purpose of negotiating a retail company's lease override provisions.

b. Example 2 illustrates a forecasted statement of net operating income before debt service and depreciation in connection with the contemplated construction of a new sports arena.

Example 1

ABC Retail Company
Statement of Forecasted Sales for Each of the Three Years Ending December 31, 19X3‡

	Years Ending December 31,		
	19X1	*19X2*	*19X3*
Forecasted sales	$629,000	$679,000	$726,000

This sales forecast presents, to the best of management's knowledge and belief, expected sales during the forecast period. Accordingly, the sales forecast reflects its judgment as of February 14, 19X1, the date of this forecast, of the expected conditions and its expected course of action. The sales forecast is for use in negotiating the Company's lease override provisions and should not be used for any other purpose. The assumptions disclosed herein are those that management believes are significant to the sales forecast. There will usually be differences between the forecasted and actual results because events and circumstances frequently do not occur as expected, and those differences may be material.

This sales forecast is based upon an expected average rate of overall increase in market demand for the Company's products, sporting goods equipment, of 3 percent per year. During the past five years, market demand for sporting goods equipment has increased approximately 3 percent per year and the Company expects this rate of industry growth to remain steady throughout the forecast period. The sales forecast is also based upon an expected increase in the Company's market share in its geographical selling region to 23 percent by

‡ *Note:* The summary of significant accounting policies is not illustrated.

19X3, which represents a 6 to 7 percent increase in market share over the forecast period. The Company's market share during the past three years has increased one to two percentage points each year and the Company expects this rate of increase to continue during the forecast period. The sales forecast is also based upon an expected 4 to 5 percent increase in the rate of inflation for each of the next three years. The Company expects that it will be able to increase the prices of its products to cover increased costs due to inflation.

The Company plans to maintain its advertising and marketing programs at current levels and has retail-floor space available to provide for the increase in the number of products it expects to sell.

Example 2

MARS Arena
Forecasted Statement of Net Operating Income
Before Debt Service and Depreciation for
Years Ending December 31, 19X1 and 19X2
(In thousands)

	Reference	*19X1*	*19X2*
Operating revenues	C	$2,700	$2,600
Operating expenses			
Salaries and wages	D	1,050	1,100
Office and general	E	700	650
Utilities	F	500	510
Operations and maintenance	G	150	160
Total operating expenses		2,400	2,420
Net operating income before debt service and depreciation		$ 300	$ 180

See Accompanying Summary of Significant Forecast Assumptions and Accounting Policies.

MARS Arena
Summary of Significant Forecast
Assumptions and Accounting Policies
for Years Ending December 31, 19X1 and 19X2

The accompanying forecasted statement presents, to the best of management's knowledge and belief, MARS Arena's expected net operating income before debt service and depreciation for the two-year period ending December 31, 19X2. Accordingly, the forecasted statement reflects management's judgment as of August 29, 19X0, the date of this forecasted statement, of the expected conditions and its expected course of action. This presentation is intended for use by the City of MARS in evaluating financing alternatives in connection with the contemplated construction of the new arena and should not be used for any other purpose. The assumptions disclosed herein are those that management believes are significant to the forecasted statement. There will usually be differences between the forecasted and actual results because events and circumstances frequently do not occur as expected, and those differences may be material.

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

The forecasted statement presents net operating income before debt service and depreciation. Accordingly, it is not intended to be a forecast of financial position, results of operations, or cash flows.

A. Description of the Project

The City of MARS plans to build a new 10,000-seat arena at the southeast intersection of Maxwell Road and Rugby Road to replace their existing 8,000-seat arena (the City's existing arena). MARS Arena will have 3,000 available parking spaces.

B. Summary of Significant Accounting Policies

[*not illustrated*]

C. Operating Revenues

There are four basic types of events forecasted to generate operating income: sporting events, family shows (for example, circus, ice shows), concerts, and exhibitions. The significant sources of revenue for each type of event include arena rental, parking fees, food and beverage concessions, novelty and souvenir income, and advertising. Attendance during the initial year of operations is forecasted to be greater than the second year based on the "bonus" a new arena can enjoy as patrons come to see the new facility as well as to see the event. A summary of operating revenue by type of event follows.

Year 1	*Event Days*	*Average Attendance*	*Total Attendance*	*Total Revenue*
Sporting events	70	4,000	280,000	$ 860,000
Family shows	45	4,500	202,500	515,000
Concerts	30	8,500	255,000	1,025,000
Exhibitions	25	2,500	62,500	180,000
Advertising				120,000
Totals	170		800,000	$2,700,000

Year 2	*Event Days*	*Average Attendance*	*Total Attendance*	*Total Revenue*
Sporting events	70	3,900	273,000	$ 835,000
Family shows	45	4,300	193,500	490,000
Concerts	30	8,200	246,000	990,000
Exhibitions	25	2,200	55,500	160,000
Advertising				125,000
Totals	170		767,500	$2,600,000

The bases for the significant income assumptions are discussed below.

Arena Rental. Management estimates that the new arena will schedule approximately 170 event days in a representative year consisting of seventy sporting events, forty-five family shows, thirty concerts, and twenty-five exhibitions. Event days were forecasted based on discussions with users (such as sporting teams and event sponsors) and market research and analysis performed by an independent consultant. Also, the City of MARS recently obtained a commitment from the local minor league hockey team to play their home games in MARS Arena.

MARS Arena will be rented out on the basis of a percentage of the dollars generated by ticket sales (called a "percentage of gross receipts") or a fixed rent (called a "flat rate"). The percentage of gross gate receipts accruing to the facility are based on current average percentages retained by the City's existing arena. These percentages range from 10 to 50 percent depending on the type of event. Management expects ticket prices to increase between 5 and 15 percent over prices at the City's existing arena, depending on the type of event, as a result of the new modernized facility. Ticket prices forecasted for each type of event have been compared with those received by other facilities for similar events. Flat rate rentals are usually negotiated by users who do not charge an admission price or have a series of events. The flat rate rental for MARS Arena is forecasted to be between $1,000 and $4,000 and is based on an analysis of rates charged by other comparable arenas for the types of events forecasted. Management does not anticipate an increase in ticket prices or flat rate rentals during the second year of operations.

Parking Fees. Management will operate and maintain the parking facility and, accordingly, all revenues accrue to MARS Arena. Consistent with experience at the City's existing arena, management estimates that 75 percent of all patrons will arrive by car for each event. The forecasted information assumes each car will carry an average of 2.7 persons and average parking rates will be $3.50 per car.

Food and Beverage Concessions. Management has negotiated a contract with ABC Company to supply and manage the food and beverage concessions. Concession income is forecasted to be 30 percent of gross concession revenue generated at each event, based on the contractual agreement with ABC Company. MARS Arena will provide all equipment and personnel necessary to operate the concessions. Patron's forecasted average expenditure per type of event ranges from $0.75 to $3.00 and is based on an analysis of data for comparable events and facilities, including the City's existing arena.

Novelty and Souvenir Income. Similar to food and beverage concessions, management has negotiated a contract with ABC Company to supply and manage the novelty and souvenir concessions. Novelty and souvenir income is forecasted to be 30 percent of gross novelty revenue based on the contractual agreement. MARS Arena will provide all equipment and personnel necessary to operate the novelty and souvenir stands. Patron's forecasted average expenditure per type of event ranges from $0.00 to $5.25 and is based on an analysis of data for comparable events and facilities.

Advertising. Advertising income will be generated primarily from signage on the interior and exterior of MARS Arena. Revenues included in the forecasted information are based on the signage capacity of MARS Arena, contract negotiations to date, and advertising revenues at the City's existing arena.

D. Salaries and Wages

The forecasted information assumes that management will make maximum use of full-time staff rather than subcontract out services, such as facility management and security. Personnel requirements are based on staffing organizations at similar sports arenas and public assembly facilities. Pay for hourly workers is based on local wage levels and wage rates being paid to employees of the City's existing arena. Wage levels are expected to increase approximately 4 percent in the second year.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Salaries are forecasted on an individual by individual basis using expected salary rates during the forecast period. Part-time salaries and wages are assumed to be event-related expenses and passed through to tenants, except for 15 percent, which is absorbed by MARS Arena.

E. Office and General Expenses

Office and general expenses consist of insurance, advertising, fees for services, and other office and general expenses. Insurance expense is based on costs at the City's existing arena and a review of insurance coverage proposals that include estimates of general liability, fire, workers' compensation, auto-business, liquor liability and boiler-machinery coverage. Advertising expenses are based on costs incurred by the City's existing arena, the number and type of forecasted events, and expected price increases from advertising agencies. Advertising expenses are expected to be higher in the first year of operations in order to promote the new facility. Fees for services include, but are not limited to, consulting fees, legal fees, and accounting and auditing fees. These fees are estimated based on expenses of the City's existing arena and plans by management to engage consultants to assist in starting up operations. Other office and general expenses are based on experience at comparable facilities and on costs incurred by the City's existing arena.

F. Utilities

Utility expense has been estimated by the project team architects and engineers. Utilities expense includes fuel and gas, electricity, water, and sewer costs.

G. Operations and Maintenance Expenses

Operations and maintenance expenses were estimated based on the requirements of facilities similar in construction and design, age, and intended use.

Forecasts and Projections Task Force (1989)

KENNETH J. DIRKES, *Chairman*
RICHARD DIETER
HARVEY J. GITEL
ROBERT W. BERLINER
ERNEST L. TEN EYCK
RICHARD M. STEINBERG
DON PALLAIS
DAVID KUTSCHER
BRUCE BALTIN
GERALD N. TUCH

DAN M. GUY, *Vice President*
Auditing Standards
MIMI BLANCO-BEST, *Manager*
Auditing Standards

[The next page is 30,501.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 14,160

Statement of Position 90-2 Report on the Internal Control Structure in Audits of Futures Commission Merchants*

February, 1990

NOTE

This statement of position presents the recommendations of the AICPA Stockbrokerage and Investment Banking Committee regarding the application of generally accepted auditing standards to reporting on the internal control structure in audits of futures commission merchants. It represents the considered opinion of the committee on the best auditing practice in the industry and has been reviewed by members of the AICPA Auditing Standards Board for consistency with existing auditing standards. AICPA members may have to justify departures from the recommendations in this statement if their work is challenged.

Introduction

[.01–.02] [Paragraphs deleted, June 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Report on Internal Control Required by CFTC Regulation 1.16

.03 The following is an illustration of the independent auditor's report on the internal control structure required by CFTC Regulation 1.16:

> Board of Directors
> ABC Commodities Corporation
>
> In planning and performing our audit of the consolidated financial statements of ABC Commodities Corporation (the "Corporation") for the year ended December 31, 19X1, we considered its internal control structure, including procedures for safeguarding customer and firm assets, in order to determine our auditing procedures for the purpose of expressing our opinion on the consolidated financial statements and not to provide assurance on the internal control structure.
>
> Also, as required by Regulation 1.16 of the Commodity Futures Trading Commission, we have made a study of the practices and procedures (including tests of compliance with such practices and procedures) followed by the Corporation that we considered relevant to the objectives stated in Regulation 1.16

* Statement on Auditing Standards (SAS) No. 78, *Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS No. 55*, revises the definition and description of internal control and makes conforming changes to relevant terminology. This SOP will be amended to conform to SAS No. 78 in a future edition of *Technical Practice Aids*.

in making (1) the periodic computations of minimum financial requirements pursuant to Regulation 1.17, (2) the daily computations of the segregation requirements of section 4d(2) of the Commodity Exchange Act and the regulations thereunder, and the segregation of funds based on such computations, and (3) the daily computations of the foreign futures and foreign options secured amount requirements pursuant to Regulation 30.7 of the Commission.

The management of the Corporation is responsible for establishing and maintaining an internal control structure and the practices and procedures referred to in the preceding paragraph. In fulfilling this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs of internal control structure policies and procedures and of the practices and procedures referred to in the preceding paragraph and to assess whether those practices and procedures can be expected to achieve the Commission's above mentioned objectives. Two of the objectives of an internal control structure and the practices and procedures are to provide management with reasonable, but not absolute, assurance that assets for which the Corporation has responsibility are safeguarded against loss from unauthorized use or disposition and that transactions are executed in accordance with management's authorization and recorded properly to permit preparation of financial statements in conformity with generally accepted accounting principles. Regulation 1.16 lists additional objectives of the practices and procedures listed in the preceding paragraph.

Because of inherent limitations in any internal control structure or the practices and procedures referred to above, errors or irregularities may occur and not be detected. Also, projection of any evaluation of them to future periods is subject to the risk that they may become inadequate because of changes in conditions or that the effectiveness of their design and operation may deteriorate.

Our consideration of the internal control structure would not necessarily disclose all matters in the internal control structure that might be material weaknesses under standards established by the American Institute of Certified Public Accountants. A material weakness is a condition in which the design or operation of the specific internal control structure elements does not reduce to a relatively low level the risk that errors or irregularities in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. However, we noted no matters involving the internal control structure, including procedures for safeguarding customer and firm assets, that we consider to be material weaknesses as defined above.[1]

We understand that practices and procedures that accomplish the objectives referred to in the second paragraph of this report are considered by the Commission to be adequate for its purposes in accordance with the Commodity Exchange Act and related regulations, and that practices and procedures that

---

[1] If conditions believed to be material weaknesses are disclosed, the report should describe the weaknesses that have come to the auditor's attention and may state that these weakness do not affect the report on the financial statements. The last sentence of the fifth paragraph of the report should be modified as follows:

> However, we noted the following matters involving the [(control environment, accounting system, control procedures, or procedures for safeguarding customer and firm assets)] and its [(their)] operation that we consider to be material weaknesses as defined above. These conditions were considered in determining the nature, timing, and extent of the procedures to be performed in our audit of the consolidated financial statements of the Corporation for the year ended December 31, 19X1, and this report does not affect our report thereon dated February 15, 19X2. [*A description of the material weaknesses that have come to the auditor's attention and corrective action would follow.*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

do not accomplish such objectives in all material respects indicate a material inadequacy for such purposes. Based on this understanding and on our study, we believe that the Corporation's practices and procedures were adequate at December 31, 19X1, to meet the Commission's objectives.[2]

This report is intended solely for the use of management, the Commodity Futures Trading Commission, and other regulatory agencies that rely on Regulation 1.16 of the Commodity Futures Trading Commission and should not be used for any other purpose.

Accounting Firm

New York, New York
February 15, 19X2

Effective Date

.04 This statement is effective for reports issued on or after March 1, 1990, with early application permissible.

[2] Whenever inadequacies are described, the report should include the last sentence of the fifth paragraph as modified in the note above. The report should also describe material inadequacies the auditor becomes aware of that existed during the period but were corrected prior to the end of the period unless management already has reported them to the CFTC.

Stockbrokerage and Investment Banking Committee (1989-1990)

EDWARD H. JONES, *Chairman*
J. KING BOURLAND
REGINA A. DOLAN
DENNIS E. FEENEY
G. VICTOR JOHNSON
MARTIN M. LILIENTHAL
THOMAS C. LOCKBURNER
DONALD H. MACNEAL
CARLOS ONIS
STUART STECKLER
LAWRENCE A. STOLER
CHARLES M. TRUNZ III
BARRY N. WINOGRAD
MARK S. ZEIDMAN

DAN M. GUY,
Vice President, Auditing
PATRICK L. MCNAMEE, *Director*
Audit and Accounting Guides
ALBERT GOLL,
Technical Manager
Accounting Standards

[The next page is 30,521.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 14,220

Statement of Position 92-2 Questions and Answers on the Term Reasonably Objective Basis *and Other Issues Affecting Prospective Financial Statements*

February, 1992

NOTE

This Statement of Position presents the recommendations of the Forecasts and Projections Task Force regarding accountants' services on prospective financial information. It also includes recommendations regarding presentation and disclosure of prospective financial information. AICPA members may have to justify departures from the recommendations in this Statement of Position if their work is challenged.

Responsible Party's Basis for Presenting a Financial Forecast

Question

.01 Paragraph 7.03 of the AICPA *Guide for Prospective Financial Statements* (the Guide) requires a responsible party to have a reasonably objective basis for presenting a financial forecast.[1] What is the purpose of the term *reasonably objective basis*?

Answer

.02 Financial forecasts are presentations of information about the future and are inherently less precise than information reporting past events. That "softness" of forecasted data is communicated to users of financial forecasts in the introduction to the summary of significant assumptions by including a caveat that the forecasted results may not be achieved.[2] Nevertheless, financial forecasts present, to the best of the responsible party's knowledge and belief, the entity's expected financial position, results of operations, and changes in financial position (cash flows).

.03 Because users expect financial forecasts to present the responsible party's "best estimate," the term *reasonably objective basis* was included in the Guide to communicate to responsible parties a measure of the quality of information necessary to present a forecast.

---

[1] This guidance applies only to financial forecasts. As discussed in paragraph 7.01P of the Guide, the responsible party does not need a reasonably objective basis for hypothetical assumptions used in a financial projection. However, this guidance should be useful in evaluating whether other assumptions used provide a reasonable basis for a projection, given the hypothetical assumptions.

[2] Paragraph 8.29 of the Guide illustrates the type of caveat to be included: "There will usually be differences between the forecasted and actual results, because events and circumstances frequently do not occur as expected, and those differences may be material."

Question

.04 In addition to establishing the term *reasonably objective basis*, the Guide indicates that the responsible party should develop appropriate assumptions to present a financial forecast (see paragraphs 6.30 through 6.36 of the Guide). How does a responsible party evaluate whether a reasonably objective basis exists for a financial forecast and whether the assumptions underlying a particular forecast are appropriate?

Answer

.05 Considerable judgment is required to evaluate whether a reasonably objective basis exists to present a financial forecast. Accordingly, the responsible party should possess or obtain a sufficient knowledge of the reporting entity's business and industry to make the evaluation.

.06 Paragraph 4.07 of the Guide states that the responsible party has a reasonably objective basis for presenting a financial forecast if sufficiently objective assumptions can be developed for each key factor. (Paragraph 3.11 of the Guide defines *key factors* as the significant matters on which the entity's future results are expected to depend. Such factors are basic to the entity's operations and, thus, encompass matters that affect, among other things, its sales, production, service, and financing activities.) The following matters should be considered when evaluating whether such assumptions can be developed:

- Can facts be obtained and informed judgments be made about past and future events or circumstances in support of the underlying assumptions?
- Are any of the significant assumptions so subjective that no reasonably objective basis could exist to present a financial forecast?[3]
- Would people knowledgeable in the entity's business and industry select materially similar assumptions?
- Is the length of the forecast period appropriate?[4]

Other matters that responsible parties should consider when evaluating whether sufficiently objective assumptions can be developed are shown in the exhibit [paragraph .08].

.07 The evaluation of whether sufficiently objective assumptions can be developed for each key factor should be made within the following context:

- A factor is evaluated by considering its significance to the entity's plans as well as the dollar magnitude and pervasiveness of the related assumption's potential effect on forecasted results (for example, whether assumptions developed would materially affect the amounts and presentation of numerous forecasted amounts).
- The responsible party's consideration of which key factors have the greatest potential impact on forecasted results is a matter of judg-

[3] For example, the responsible party might have no reasonably objective basis for presenting a forecast that includes royalty income from products not yet invented or revenue from a thoroughbred being reared to race. In such cases, it would be inappropriate to present a forecast because of the lack of a reasonably objective basis.

[4] See paragraphs .44 through .46 of this Statement of Position (SOP).

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

ment, and is influenced by his or her perception of the needs of a reasonable person relying on the financial forecast. A key factor having the greatest potential impact on forecasted results is one in which an omission or misstatement of the related assumption would probably, in light of surrounding circumstances, change or influence the judgment of a reasonable person relying on the financial forecast.[5]

- The responsible party should seek out the best information that is reasonably available to develop the assumptions. Cost alone is an insufficient reason not to acquire needed information. However, the cost of incremental information should be commensurate with the anticipated benefit.
- A conclusion that a reasonably objective basis exists for a forecast may be easier to support if the forecast were presented as a range.

[5] The more likely it is that an assumption will have a significant effect on the overall forecasted results and that the factors relating to the assumption indicate a less objective basis, the more likely it is that the forecast should be judged as not having a reasonably objective basis.

.08

Exhibit

Sufficiently Objective Assumptions—Matters to Consider

Basis	*Less Objective*	*More Objective*
Economy	Subject to uncertainty	Relatively stable
Industry	Emerging or unstable; high rate of business failure	Mature or relatively stable
Entity:		
• Operating history	Little or no operating history	Seasoned company; relatively stable operating history
• Customer base	Diverse, changing customer group	Relatively stable customer group
• Financial condition	Weak financial position; poor operating results	Strong financial position; good operating results
Management's experience with:		
• Industry	Inexperienced management	Experienced management
• The business and its products	Inexperienced management; high turnover of key personnel	Experienced management
Products or services:		
• Market	New or uncertain market	Existing or relatively stable market
• Technology	Rapidly changing technology	Relatively stable technology
• Experience	New products or expanding product line	Relatively stable products
Competing assumptions	Wide range of possible outcomes	Relatively narrow range of possible outcomes
Dependency of assumptions on the outcome of the forecasted results*	More dependency	Less dependency

* Assumptions may depend on the achievement of other forecasted results. For example, the sales price of a real estate property in a forecast might be estimated by applying a capitalization rate to forecasted cash flows.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.09 As stated earlier, in addition to requiring a reasonably objective basis, the Guide requires a responsible party to develop appropriate assumptions to present a financial forecast. When evaluating whether assumptions underlying the financial forecast are appropriate, the responsible party should consider numerous factors, including whether—

- There appears to be a rational relationship between the assumptions and the underlying facts and circumstances (that is, the assumptions are consistent with past or current conditions).
- The assumptions are complete (that is, assumptions have been developed for each key factor).
- It appears that the assumptions were developed without undue optimism or pessimism.
- The assumptions are consistent with the entity's plans and expectations.
- The assumptions are consistent with each other.
- The assumptions, in the aggregate, make sense in the context of the forecast taken as a whole.

Assumptions that have no material impact on the presentation may not have to be evaluated individually; however, the aggregate impact of individually insignificant assumptions should be considered in making an overall evaluation of whether the assumptions underlying the forecast are appropriate.

.10 The following examples illustrate the facts and circumstances considered by the responsible party when evaluating whether there was a reasonably objective basis to present a financial forecast.

Example 1

Company Profile

.11 An established builder of single-family homes has built two garden-apartment complexes in the last three years. This developer plans to build another garden-apartment complex and wishes to syndicate the project. Both of the existing garden-apartment complexes are approaching full occupancy. The local economy is strong and has a diversified base. Furthermore, real estate in the area generally appreciates in value. There has been significant development in the area and, if it continues, supply will exceed demand within four years. The developer has appropriately considered this factor, as well as the associated cost of maintaining the proposed facility, in planning the project and developing the forecast.

.12 In the past, the developer had financed each of his projects for five years at the maximum amount allowed by local financial institutions. Forecasts for the previous two projects assumed a five-year financing period and a hypothetical sale of the property at the end of the forecast period. For the proposed development, the developer has obtained a commitment for a three-year interest-only loan for an amount equal to 70 percent of the project's estimated cost. Current discussions with bankers have indicated their willingness to convert that loan to long-term financing for the project after rental stabilization, which is consistent with normal lending practices. The developer

has indicated that he plans to refinance the committed loan after three years for an amount that exceeds the loan by approximately 76 percent. Such additional amounts (net of refinancing costs) are to be returned to the investors as a cash distribution. The developer's other resources are not sufficient to provide a meaningful guarantee of the refinancing. The forecast will be for five years, and will include a projection illustrating a hypothetical sale at the end of the forecast period. The details can be summarized as follows:

	(In thousands)
• Estimated cost of the development to the partnership	$10,000
• Committed financing (interest-only loans) at 70 percent of the estimated cost	$ 7,000
• Proposed limited partnership investment	$ 3,000
• Amount of proposed refinancing:	
— Long-term refinancing of the three-year committed loan	$ 7,000
— Additional financing for payments to limited partners	5,000
— Cost of refinancing	300
	$12,300
• Forecasted cash flow before debt service for the fourth year	$ 1,500
• Capitalization rate (considered in this example to be acceptable under the circumstances)	9%
• Capitalized value at the end of the third year	$16,700

Question

.13 Does the developer (the responsible party) have a reasonably objective basis for forecasting the proposed refinancing?[6]

Answer[7]

.14 This question can be divided into two further questions:

a. Can the developer forecast a refinancing?

b. Are the assumptions about the amount and terms of the refinancing sufficiently objective?

.15 *Forecast of Refinancing.* The developer has obtained a financing commitment for three years based on local lending practices, and bankers have indicated a willingness to provide permanent financing in a manner that is consistent with these lending practices. Accordingly, it appears that the developer would have a reasonably objective basis for forecasting the project's refinancing for a comparable amount in three years.[8] At that time, the building

[6] See paragraphs .57 and .58 of this SOP for a discussion of the responsibility that an accountant engaged to compile or examine a financial forecast has to evaluate whether a responsible party has a reasonably objective basis for presenting a financial forecast.

[7] This response is based on information presented in the question. Other information, such as that about the size and strength of the local economy, the precise location of the project, local planning regulations, and the availability of third-party guarantees on the proposed refinancing, could change the response.

[8] Support for forecasted interest rates may exist in the form of interest-rate forecasts and current interest-rate trends. If interest-rate fluctuations are a concern, a conclusion that sufficiently objective interest assumptions could be developed may be easier to support if forecasted results are presented as a range (through the use of a range forecast).

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

will still be considered relatively new and, based on maintenance plans, should be in good condition. Further, real estate in the area generally is expected to appreciate in value, and forecasted cash flows before debt service are consistent with a refinancing assumption.

.16 *Amount and Terms of Refinancing.* Although the developer may have a reasonably objective basis for a forecast that includes a refinancing for an amount approximating the original loan, it is not clear that such a basis exists for one that includes a refinancing significantly in excess of that amount. The following factors should be considered:[9]

- Although the local economy is strong and diversified, competing developments are being built and, in fact, there is some risk that supply could exceed demand.
- The developer has factored the effect of an increase in the supply of competing housing units into the forecast and may point to an estimated value of the project at the end of the third year, based on the application of a current capitalization rate to forecasted cash flows. However, capitalization rates may vary over time, and estimated values derived from the application of capitalization rates depend on the achievement of prospective cash flows.
- The developer is an experienced builder; however, both his experience with larger projects and his resources are limited.

.17 In light of the facts presented, it appears that the developer's basis for refinancing the project at an amount significantly greater than the original loan would be highly dependent on future events and circumstances, such as anticipated cash flows, economic conditions, lending practices, and capitalization rates. Although forecasted results may be used as a basis for a refinancing assumption, in the absence of other supporting information, such results ordinarily would not provide a responsible party with a basis for concluding that the refinancing assumption was sufficiently objective. In this case, the developer's limited resources and the length of time until the refinancing is expected to take place are all risk factors that mitigate a reliance on forecasted results to provide support for the developer's assertion that a reasonably objective basis exists for the refinancing. Accordingly, in the absence of additional information, the facts in this case do not appear to support the developer's assertion that a reasonably objective basis exists for presenting a forecast that includes the proposed refinancing assumption.[10]

Example 2

Company Profile

.18 ACTech, Inc. was established to produce a line of flat-panel, AC-plasma computer-display products for use when, because of their bulk and thickness, cathode-ray tubes (CRTs) would not be suitable. The company was incorporated in 19X0 by former members of a management team (the founders) who designed the product and operated the business as a division of BigCo. The

[9] These items were developed by reference to the factors included in the exhibit [paragraph .08].

[10] In this example, the developer could consider including a refinancing for the committed amount ($7,000,000) in the forecast, and supplementing the forecast with a financial projection illustrating prospective results if the permanent financing obtained were for the greater amount ($12,300,000).

founders have purchased equipment and certain technology at a significant discount from BigCo with $1 million in funds raised from private investors. ACTech's goal is to become a leader in the production and sale of AC-plasma-display products by utilizing newly developed but unproven technology to lower the cost of production and thereby compete more effectively with DC-plasma-display products. DC products are currently in common usage because of their lower unit cost, but they are inferior to AC-plasma-display products in brightness and resolution.

.19 *Product Line and Competition.* The mainstay of the ACTech product line will be a "plasma display system," which combines the AC-plasma-display panels with new low-cost drive circuitry. When compared to the most competitive product, the DC-plasma-display, ACTech's product is three times as bright with no flicker, consumes half the power for an equivalent level of light output, has a wider viewing angle, can be produced in much larger sizes, and has a longer life. DC panels are currently cheaper to produce, but with ACTech's circuitry and manufacturing expertise, management hopes to close the cost gap. ACTech is currently working on the implementation of its new technology. Prototypes have been successfully produced, but management estimates that, using the equipment purchased from BigCo, it will need about a year to design and install a high-volume production line.

.20 Competition from other AC-plasma-display manufacturers will come primarily from ACpan, a very large manufacturer that uses most of its output in its own products. ACpan AC-plasma displays have been available for the past five years and are comparable in quality to those of ACTech. Despite continued efforts, ACpan has achieved very little market penetration because, like ACTech and other producers of AC-plasma-displays, ACpan has not been able to successfully design and install a high-volume production line. If successfully developed, ACTech's manufacturing process and the low-cost drive circuits will permit it to compete advantageously with ACpan. Other manufacturers of AC-plasma-displays charge prices that are higher than those of the ACpan products and cater to military and specialty markets. In the market for large-sized screens, management believes that there is no effective flat-panel competition.

.21 Additionally, ACTech has received oral assurances from BigCo that it will purchase plasma displays from ACTech in sufficient quantities to meet its needs, which would account for about 5 percent of ACTech's estimated sales.

.22 *Sales and Marketing.* ACTech will sell primarily to equipment manufacturers via an internal sales force. Additionally, ACTech will utilize manufacturer's representatives or sales organizations to penetrate selected foreign markets. ACTech's products will be demonstrated at various trade shows and will be advertised in the appropriate trade journals.

.23 ACTech has targeted specific markets for its primary growth. These markets include those for (*a*) mainframe interactive applications (ACTech, when it was a division of BigCo, had already established a small market in this area), (*b*) portable personal computers (ACTech is currently involved in discussions with several large companies in this market), (*c*) CAD/CAM/CAE workstations (ACTech is currently involved in discussions with producers serving both financial and design markets), and (*d*) manufacturing control products (ACTech is working with a company that uses a plasma panel with a touch screen to support the manufacturing process).

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.24 ACTech has estimated sales of approximately $600,000 in 19X2, $16 million in 19X3, and $40 million in 19X4. At anticipated levels of industry growth (provided from an outside source), these sales figures represent 0.3 percent, 6 percent, and 11 percent of the plasma-panel market, respectively.

.25 *Product Manufacture.* Management believes that the equipment purchased from BigCo by the founders is state of the art. ACTech is in the process of relocating the equipment to a new facility and setting up a modern, automated production line. This new facility, which requires some renovation, will allow ACTech to begin production on a limited scale in about six months. Ample room exists for future expansion. No significant problems are expected in relocating and setting up the new facility, assuming that design problems related to high-volume production can be overcome.

.26 Production is expected to be at 500 AC-plasma display-system units in 19X2, growing to 36,000 in 19X3 and 115,000 in 19X4.

.27 *Management and Personnel.* The ACTech management team is recognized throughout the computer industry as a leader in plasma-display technology and manufacturing. Together, the four founders have over fifty years of experience in the field of flat-panel displays. Additionally, the founders have demonstrated significant academic and manufacturing achievements in the field of display technology. At present, ACTech has three full-time and eleven part-time employees. Management plans to hire an additional thirty-five employees during 19X2, including three marketing and sales employees.

.28 Management expects employment to grow to about 250 by 19X4. Although production employees must be hired and trained, the labor market is sufficient to supply an adequate labor force with the basic technical skills needed to perform the required tasks, and management has experience in training. Further, management has had discussions with several candidates for the sales positions and does not anticipate difficulties in hiring qualified staff.

Question

.29 Does management have a reasonably objective basis for presenting a financial forecast?[11]

Answer[12]

.30 ACTech, Inc.'s financial forecast is based on two primary assumptions: (*a*) the successful design and installation of a high-volume production line, which would enable the company to significantly reduce unit costs; and (*b*) the timing and quantity of sales.

.31 *High-Volume Production.* ACTech is planning to manufacture and sell AC-plasma-display products for use in computer terminals. Its success will be highly dependent on its ability to produce those products in large quantities for sale at a price competitive with DC-plasma products. Although prototypes of the company's products have been produced, circuitry compatible with high-

[11] See footnote 6 of this SOP.

[12] This response is based on information presented in the question. Other information about the status of engineering plans, the preproduction models, and marketing results could change the response. The response was developed by referring to the factors included in the exhibit [paragraph .08].

volume production has been developed, and experienced management has been hired, the company has yet to design and install the planned high-volume production line. As indicated previously, management's current estimate is that it will be at least twelve months before that work is completed. Further, the facts presented indicate that other manufacturers of AC-plasma-display units have not been successful in reducing production costs. BigCo's willingness to sell its AC-plasma-display division may also indicate uncertainty about its ability to reduce production costs.

.32 For the reasons discussed in the preceding paragraph, management's assumption that it will be able to achieve high-volume, low-cost production is relatively subjective. That assumption is critical to the company's sales assumptions, which depend on the reduction of production costs to a level that permits a pricing structure competitive with that of DC-plasma units. Without a competitive pricing structure, the company's sales assumptions do not appear to be valid. Accordingly, ACTech does not appear to have a reasonably objective basis for presenting a financial forecast.

.33 *Other Matters.* If the feasibility of establishing a high-volume production line capable of producing AC-plasma units at a cost that permits ACTech to competitively price its product could be reasonably assured, a reasonably objective basis might exist for presenting a financial forecast. Before that conclusion can be reached, consideration should be given to ACTech's assumptions regarding market penetration. ACTech has developed a sales and marketing plan; however, questions exist concerning its assumptions of an aggressive market penetration (for example, capturing 11 percent of the plasma-panel market by the end of 19X4). There are several factors that appear to support its sales assumption: the technological superiority of its products, competitive pricing, management's experience with the products, and the acceptability of the product to current users, such as BigCo. Nevertheless, it would be appropriate to gather additional information concerning marketing results to date before concluding whether a sufficiently objective basis exists for the assumptions regarding market penetration. Further, uncertainty concerning the company's sales assumptions may indicate that such assumptions would be easier to support if a range forecast were presented. (Exhibit 8.09 of the Guide illustrates a range forecast.)

Example 3

Company Profile

[***Note:*** *As indicated in paragraph .46 of this SOP, it may be difficult to support an assertion that a reasonably objective basis exists for presenting a financial forecast for certain start-up companies. The following example illustrates a situation in which a two-year forecast for a start-up company may be appropriate.*]

.34 Newco was established to manufacture wall panels with self-contained insulation for use in commercial and industrial projects. The panels provide a lightweight interior and exterior wall combination. The company was incorporated in 19X0 by a former executive of one of the leaders in the wall-panel market, and by an individual who helped develop the original technology ten years ago (the founders). The founders have invested $1,000,000, which was used to order initial equipment and lease a building. Newco has sufficient capital to operate during the forecast period.

.35 Although more expensive than those using traditional materials, the panels have proven to be easier to install than rolled or blown-in insulation and

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

wall surface combinations. Therefore, the use of the insulated wall panels in construction has been increasing. Competitors in the wall-panel market include two divisions of publicly held corporations that produce the panels, along with a variety of other construction materials, in a number of plants. These competitors generally service the large-project market and are known to have significant backlogs. From interviews with industry sources, it has been determined that these companies have been unable to respond to small or rush orders. Newco believes that, as an entrepreneurial company having low overhead and specializing in one product, it can service the small-order market effectively and profitably.

.36 Sales would be generated through bid contracts advertised by a clearinghouse that provides information to contractors and through the establishment of long-term relationships with engineering and architectural professionals. After lengthy correspondence with these professionals, Newco has obtained commitments for approximately 5 percent of its production capacity for 19X1 and 19X2 (about 25 percent and 15 percent of forecasted sales in 19X1 and 19X2, respectively). In addition, the initial equipment installation has allowed Newco to respond to selected advertised bids and obtain contracts for one-third of the opportunities pursued. These contracts account for 10 to 12 percent of the plant's capacity and extend through 19X2 (representing 50 percent and 35 percent of forecasted sales in 19X1 and 19X2, respectively). Newco plans to expand its sales force to enable it to respond to additional opportunities.

.37 In estimating its sales, Newco considered the growth in the construction market, the increasing conversion to manufactured wall panels, its success rate in bidding opportunities, the planned growth in its sales force, and the number of orders received to date. Newco has estimated sales of approximately 20 and 33 percent of production capacity in 19X1 and 19X2, respectively. These sales figures would represent market shares of 2 to 3 percent of the bid market for insulated wall panels. In addition to clearinghouse data used to assess market growth and size, management has considered industry sources that provide significant information on construction and usage potentials in making its sales estimates.

.38 The application of the technology involved in the production process continues to serve as a deterrent to entering the small-order market. Newco's initial investment has allowed for limited-scale production, and no significant problems are expected in obtaining the additional equipment and achieving forecasted capacity. Further, the company has been able to manufacture a quality product within its range of estimated costs.

.39 The founders are recognized within the industry for their technological and manufacturing expertise. Management has hired financial and production management executives, and is in the process of making its selection of three additional salespeople from a number of candidates experienced in the industry. Although additional production employees must be hired and trained, the labor market is sufficient to supply an adequate labor force with the basic technical skills needed to perform the required tasks.

Question

.40 Does management have a reasonably objective basis for presenting a financial forecast for 19X1 and 19X2?[13]

---

[13] See footnote 6 of this SOP.

Answer[14]

.41 Yes. Given the facts in this case, it appears that Newco has a reasonably objective basis for forecasting its operations for the years 19X1 and 19X2.

.42 Newco's product currently exists in the market and represents a technologically proven alternative that competes with similar technologies and alternatives based upon price. Further, the quality of its production and costs incurred to date have been in line with management's expectations. Accordingly, Newco's ability to forecast operating results depends on the primary assumption of the timing and quantity of sales.

.43 Management's ability to identify competitors, analyze customers' buying motives, and evaluate the market as well as the potential end usage demand are important determinants in forecasting sales. However, it is management's demonstrated success in identifying and establishing a specific customer base and in establishing a bidding track record that provides an important validation of its assessments of competition, pricing, and industry practices; it also provides the basis for management's sales forecast capabilities. Current contracts and commitments would account for a substantial portion of forecasted sales for 19X1 and 19X2, and the company's bidding success rate, coupled with the imminent hiring of experienced sales personnel, appears to provide a basis for estimated increases in sales during those years.

Consideration of the Length of the Forecast Period

Question

.44 In practice, financial forecasts have been presented for various periods of time, some of which exceed ten years. What factors should be considered in determining the time period to be covered by a financial forecast?

Answer

.45 The Guide does not specify any fixed minimum or maximum time period to be covered by a financial forecast. The period that appropriately may be covered depends to a large extent on the particular circumstances of the company involved.[15] In evaluating the period to be covered by a forecast, the responsible party should balance the information needs of users with his or her ability to estimate prospective results; however, a reasonably objective basis should exist for each forecasted period (month, quarter, or year) presented.[16]

.46 In order to be meaningful to users, the presentation of a financial forecast ordinarily should cover at least one full year of normal operations.[17] However, the degree of uncertainty generally increases with the time

---

[14] This response is based on information presented in the question. Other information, such as that about the economy and its effect on Newco's industry and its forecasted results, could change this response. The response was developed by reference to the factors included in the exhibit [paragraph .08].

[15] SEC Regulation S-K, 229.10(b)(2) states that, for certain companies in certain industries, a (forecast) covering a two- or three-year period may be entirely reasonable. Other companies may not have a reasonable basis for (forecasts) beyond the current year. Accordingly, the responsible party should select the period most appropriate in the circumstances.

[16] See question entitled "Periods Covered by an Accountant's Report on Prospective Financial Statements," included in SOP 89-3, *Questions Concerning Accountants' Services on Prospective Financial Statements* [section 14,110.21 through .23].

[17] [Footnote deleted, April 1996, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

span of the forecast, and at some point, the underlying assumptions may become so subjective that no reasonably objective basis may exist for presenting a financial forecast. It ordinarily would be difficult to establish that a reasonably objective basis[18] exists for a financial forecast extending beyond three to five years,[19] and depending on the circumstances, a shorter period may be appropriate (for example, in the case of certain start-up or high-tech companies it may be difficult to support an assertion that a reasonably objective basis exists to present a financial forecast and, if so, for more than one year). If it is not practical to present a financial forecast for enough future periods to demonstrate the long-term results of an investment or other decision, the presentation should include a description of the potential effects of such results.[20]

Disclosure of Long-Term Results

Question

.47 Paragraph 8.34 of the Guide states that short-term forecasts may not be meaningful in situations in which long-term results are necessary to evaluate the investment consequences involved. However, because uncertainty generally increases with the time span, it may not be practical in all situations to present financial forecasts for enough future periods to demonstrate long-term results.[21] In those circumstances, the presentation should include a description of the potential effects of such results. What form of disclosure would be appropriate in such circumstances when a financial forecast for general use will be presented?

Answer

.48 The Guide does not provide a standard format for disclosures[22] intended to demonstrate operating or other results beyond the forecast period (that is, post-forecast-period disclosures),[23] because it is not possible to anticipate all the circumstances that might arise in practice. However, such disclosures should be based on the responsible party's plans and knowledge of specific events or circumstances, at the date of the forecast, that are expected to have a material effect on results beyond the forecast period.

.49 Specific plans, events, or circumstances that might be disclosed include the following:

---

[18] See paragraphs .01 through .43 of this SOP for a discussion of factors to be considered when evaluating whether a reasonably objective basis exists to present a financial forecast.

[19] Financial forecasts for longer periods may be appropriate, for example, when long-term leases or other contracts exist that specify the timing and amount of revenues, and when costs can be controlled within reasonable limits.

[20] See paragraph 8.34 of the Guide and paragraphs .47 through .56 of this SOP.

[21] See paragraphs .44 through .46 of this SOP for a discussion of matters to consider when evaluating the length of a forecast period.

[22] Exhibit 9.10 of the Guide illustrates a disclosure that is appropriate for describing long-term results of certain real estate projects. That illustration includes a projection that discloses the effect on limited partners of a hypothetical sale of the property at the end of the forecast period.

[23] Paragraph 4.05 of the Guide states that "because a financial projection is not appropriate for general use, it should not be distributed to those who will not be negotiating directly with the responsible party . . . unless the projection is used to supplement a financial forecast and is for a period covered by the forecast." A financial projection is defined in paragraph 3.05 of the Guide as prospective financial statements that present, to the best of the responsible party's knowledge and belief, an entity's expected financial position, results of operations, and changes in financial position (cash flows), given one or more hypothetical assumptions.

- Scheduled increases in loan principal
- A planned refinancing
- Existing plans for future expansion of production or operating facilities or for the introduction of new products
- Expiration of a significant patent or contract
- The expected sale of a major portion of an entity's assets[24]
- Scheduled or anticipated taxes that have adverse consequences for investors

.50 Disclosures may be limited to a narrative discussion of the responsible party's plans, or they may include estimates of expected effects of future transactions or events. In all cases, however, the disclosure should be included in, or incorporated by a reference to, the summary of significant assumptions and accounting policies. It should also—

- Include a title indicating that it presents information about periods beyond the financial forecast period.
- Include an introduction indicating that the information presented does not constitute a financial forecast and indicating its purpose.
- Disclose significant assumptions and identify those that are hypothetical, as well as the specific plans, events, or circumstances that are expected to have a material effect on results beyond the forecast period.
- State that (*a*) the information is presented for analysis purposes only, (*b*) there is no assurance that the events and circumstances described will occur, and (*c*) if applicable, the information is less reliable than the information presented in the financial forecast.

.51 The purpose of the disclosures discussed herein is to provide users with additional information useful in analyzing forecasted results. However, the information relates to periods beyond the forecast period, and management generally does not have a reasonably objective basis for presenting it as forecasted information. Accordingly, the disclosures are less reliable than those that are included in a financial forecast. Such disclosures should not be presented comparatively to forecasted results on the face of the financial forecast or in related summaries of results (for example, in a summary of investor benefits), or as a financial projection,[25] since such presentations could be misleading. The following examples illustrate the types of disclosures that may be appropriate.

Example 1

Note A: Supplemental Information Related to the Three Years Ending December 31, 19X8[26]

---

[24] See footnote 22 of this SOP.

[25] Paragraph 3.05 of the Guide provides the definition of a financial projection. Paragraph 4.05 states that a financial projection is not appropriate for general use unless it supplements a financial forecast and is for a period covered by the forecast. SOP 89-3, *Questions Concerning Accountants' Services on Prospective Financial Statements* [section 14,110], provides guidance for reporting on a projection that supplements a financial forecast and is for a period covered by the forecast.

[26] See exhibit 9.10 of the Guide and SOP 89-3 [section 14,110] for an alternate presentation of long-term results when a projection is used to supplement a financial forecast and is for a period covered by the forecast (for example, the projected sale of real estate on the last day of the forecasted period).

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

While management is unable to prepare a financial forecast for the three-year period ending December 31, 19X8, it believes that the following information is necessary for users to make a meaningful analysis of the forecasted results.

Management's forecast anticipates operation of each of the three properties described therein during the five-year period ending December 31, 19X5. Current plans are to continue operation of all three properties through December 31, 19X8, at which time the properties will be offered for sale. The following table illustrates the pre-tax effect to limited partners of a sale of properties at December 31, 19X8, and the subsequent liquidation of the partnership. The table is based on the following hypothetical assumptions:[27]

- Column A is based on the assumption that the property will be sold (or foreclosed) for the balance of the mortgage notes at December 31, 19X8.
- Columns B and C are based on the assumption that the properties will be sold at estimated market values, which are calculated by capitalizing estimated cash flows from operations for the year immediately preceding the sale at rates of 7 percent and 9 percent, respectively.
- The estimated balance of outstanding mortgage notes at December 31, 19X8, is based on the assumption that the partnership will continue to make payments in accordance with existing terms of the mortgage notes. Note 7 to the financial forecast describes the partnership's outstanding mortgage notes and related payment terms.
- Management has estimated net operating cash flow (in total and per unit) for the three years ending December 31, 19X8, using assumptions substantially the same as those used in its financial forecast for the five years ending December 31, 19X5. In preparing the estimate, 19X5 forecasted rental income and forecasted operating expenses and management fees were increased by 5 percent per year.

	A	*B*	*C*
	Sale for Existing Mortgage Balance	*Sale at a 7% Capitalization Rate*	*Sale at a 9% Capitalization Rate*
Cash distributions to limited partners:			
For the forecast period	$XXX	$XXX	$XXX
For the three-year period ending December 31, 19X8	XXX	XXX	XXX
Net from sale and dissolution	XXX	XXX	XXX
Less original capital contribution	(XXX)	(XXX)	(XXX)
Net pre-tax cash flow from partnership	$XXX	$XXX	$XXX
Taxable income—gains and losses:			
For the forecast period	$XXX	$XXX	$XXX
For the three-year period ending December 31, 19X8	$XXX	$XXX	$XXX
From sale and dissolution	$XXX	$XXX	$XXX

[27] To be consistent with the purpose of disclosing the hypothetical sale of the entity's real estate investment, the capitalization rate assumed should be consistent with the assumptions used in the forecast as well as the entity's and the industry's experience.

This information is less reliable than the information presented in the financial forecast and, accordingly, is presented for analysis purposes only. Further, there can be no assurance that events and circumstances described in this analysis will occur.

Example 2

Note B: Supplemental Information Related to Periods Beyond the Forecast Period

While management is unable to prepare a financial forecast for periods beyond 19X5, it believes that the following information is necessary for users to make a meaningful analysis of the forecasted results.

Management's forecast for the three years ending December 31, 19X5, anticipates sales of its Model 714 High Tech Laser Analyzers and related equipment in the amounts of $13,500,000, $14,000,000, and $14,500,000, respectively. Such sales represent approximately 50 percent of the Company's sales for the forecast period and were the major reason for the Company's growth in 19X0 and 19X1. The Company is currently a leader in laser technology, and its Model 714 Analyzer is now widely used by the industry. However, the Company expects sales of this product to peak in 19X5 and decline in periods subsequent to the forecast period. The Company is currently developing the Model 714A High Tech Analyzer, which is an improvement on the Model 714 Analyzer, and an X series visual modulator and laser scanner.

This information is less reliable than the information presented in the financial forecast and, accordingly, is presented for analysis purposes only. Further, there can be no assurance that the events and circumstances described herein will occur.

Question

.52 A responsible party may prepare a financial forecast that requires disclosures like those illustrated in paragraphs .47 through .51 of this SOP, and he or she may request an accountant to compile or examine the forecast. What is the accountant's responsibility for such disclosures when he or she provides a compilation or examination service?

Answer

.53 In applying procedures to provide assurance that the forecast conforms to AICPA presentation guidelines in an examination, or in reading the forecast for conformity with the guidelines in a compilation, the accountant should consider whether such disclosures are required and, if so, whether they are made. The accountant is not required to design specific procedures to identify conditions and events that might occur beyond the forecast period. Rather, the accountant's consideration is based on information about management's existing plans, future events, and circumstances obtained during the course of the engagement.[28]

.54 Disclosures of long-term results are included in the notes to the financial forecast and are, therefore, covered by the accountant's standard report. Accordingly, the extent of procedures performed depends on whether the engagement is a compilation or an examination. Compilation and examination procedures for engagements for prospective financial statements are included in chapters 12 and 15 of the Guide, respectively. When those procedures are performed, consideration should be given to whether (*a*) the disclo-

[28] The accountant is not responsible for anticipating future events, circumstances, or management plans. Further, the accountant's report does not imply assurance that all such matters that might occur beyond the forecast period have been disclosed.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

sures are consistent with management's existing plans and knowledge of future events and circumstances, and (*b*) the disclosures are presented in conformity with the guidelines in paragraph .50 of this SOP.

.55 If, when performing a compilation engagement, the accountant concludes, on the basis of known facts, that the disclosures are obviously inappropriate, incomplete, or misleading, given their purpose, or the disclosures are not presented in conformity with the guidelines given in paragraph .50, the accountant should discuss the matter with the responsible party and propose an appropriate revision of the disclosures. If the responsible party does not agree to revise the disclosures, the accountant should follow the guidance in chapters 12 and 14 of the Guide.

.56 If, when performing an examination engagement, the accountant has reservations about the disclosures or if he or she is unable to apply procedures to such disclosures considered necessary in the circumstances, the accountant should discuss such matters with the responsible party and propose appropriate revision of the disclosures. If the responsible party will not agree to revision of the disclosures, the accountant should follow the guidance in chapter 16 of the Guide.

The Accountant's Consideration of Whether the Responsible Party Has a Reasonably Objective Basis for Presenting a Financial Forecast

Question

.57 Paragraph 10.14 of the Guide indicates that an accountant who has been engaged to compile or examine a financial forecast should consider whether the responsible party has a reasonably objective basis to present a forecast.[29] In considering whether the responsible party has a reasonably objective basis, the accountant would consider whether sufficiently objective assumptions can be developed for each key factor. Do the procedures in chapters 12 and 15 of the Guide, "Compilation Procedures" and "Examination Procedures," respectively, contemplate such a consideration?

Answer

.58 Yes. An accountant may become aware of information that raises questions about whether the responsible party has a reasonably objective basis for presenting a financial forecast as he or she performs the procedures required for a compilation (see paragraph 12.10 of the Guide), particularly when making inquiries about key factors (see paragraph 12.10c of the Guide), reading the forecast, and considering whether significant assumptions appear to be not obviously inappropriate (see paragraph 12.10(ii) of the Guide). In any event, paragraph 10.14 of the Guide states that whether the responsible party has a reasonably objective basis to present a forecast would be a factor in the accountant's consideration about whether the presentation would be misleading (see paragraph 12.10j of the Guide).[30] In an examination engagement, the

[29] See paragraph 7.03 of the Guide.

[30] The accountant's compilation procedures do not contemplate an evaluation of the support for underlying assumptions, which is required in an examination of prospective information. Because of the limited nature of the procedures, a compilation does not provide assurance that the accountant will become aware of significant matters that might be disclosed by more extensive procedures.

accountant considers whether the responsible party has a reasonably objective basis for presenting a financial forecast when he or she evaluates the support underlying the assumptions thereto. In either case, the guidance for preparers given in paragraphs .01 through .43 of this SOP may be useful to the accountant.[31]

Effective Date

.59 The presentation guidelines in this SOP are effective for prospective financial information prepared on or after August 31, 1992. The guidance on accountants' services is effective for engagements in which the date of completion of the accountants' services on prospective financial information is August 31, 1992, or later. Early application of the provisions of this statement is encouraged.

[31] Often, an accountant considers whether a preparer has a reasonable objective basis to present a financial forecast before accepting an engagement to perform compilation or examination services. In that case, the guidance in paragraphs .01 through .43 of this SOP may be particularly useful.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Forecasts and Projections Task Force (1991)

KENNETH J. DIRKES, *Chairman*
BRUCE BALTIN
RICHARD DIETER
HARVEY J. GITEL
JOHN M. HOLLENBECK
DAVID KUTSCHER
DON PALLAIS
RICHARD M. STEINBERG
ERNEST L. TEN EYCK
GERALD N. TUCH

DAN M. GUY
Vice President, Auditing
MIMI BLANCO-BEST
Consulting Technical Manager

The task force gratefully acknowledges the contributions made to the development of this statement of position by former task force members Richard M. Steinberg and Robert W. Berliner.

[The next page is 30,551.]

Section 14,230

Statement of Position 92-4 Auditing Insurance Entities' Loss Reserves

May, 1992

NOTE

This Statement of Position presents the recommendations of the Auditing Insurance Entities' Loss Reserves Task Force of the Insurance Companies Committee regarding the audit of the liability for loss reserves on the financial statements of property and liability insurance entities in an audit conducted in accordance with generally accepted auditing standards. It has been reviewed by the chairman of the Auditing Standards Board for consistency with existing auditing standards. AICPA members may have to justify departures from the recommendations in this Statement of Position if their work is challenged.

Introduction

.01 This statement of position (SOP) is designed to assist auditors in developing an effective audit approach when auditing loss reserves of insurance entities. It is intended to supplement the AICPA Audit and Accounting Guide *Audits of Property and Liability Insurance Companies* (audit guide). The SOP assumes the reader is familiar with the audit guide, particularly those sections in chapter 4 that describe the claims cycle.

Scope

.02 The guidance in this SOP applies to audits of property and liability insurance enterprises (stock and mutuals), reciprocal or interinsurance exchanges, pools, syndicates, captive insurance companies, and other similar organizations such as public entity risk pools. The overall concepts discussed herein are applicable to all lines of insurance; however, this study uses examples and illustrations from the more traditional lines of property and liability insurance.

.03 This SOP does not cover certain auditing issues tangentially related to loss reserves, including the evaluation of—

- Premium deficiencies.
- Transfer of risk.
- Credit risk on reinsurance contracts.
- Effects of discounting loss reserves.
- Other financial statement amounts that may be affected by loss reserves such as contingent commissions.

Effective Date

.04 This statement of position is effective for audits of financial statements for periods ending after December 15, 1992.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Chapter 1

ACCOUNTING FOR LOSS RESERVES

.05 This chapter provides background on accounting for loss reserves and describes the applicable authoritative literature in this area. The audit guide (paragraphs 4.01 through 4.04) presents the following description of generally accepted accounting principles and statutory accounting practices for insurance entities.

Accounting Practices

4.01 The specialized industry accounting principles for insurance enterprises are described in FASB Statement No. 60, FASB Statement No. 97, FASB Statement No. 113, SOP 92-5, *Accounting for Foreign Property and Liability Reinsurance*, SOP 94-5, *Disclosures of Certain Matters in the Financial Statements of Insurance Enterprises*, and SOP 97-3, *Accounting by Insurance and Other Enterprises for Insurance-Related Assessments*.

4.02 Under GAAP, liabilities for the cost of unpaid claims, including estimates of the cost of claims incurred but not reported, are accrued when insured events occur. The liability for unpaid claims should be based on the estimated ultimate cost of settling the claims (that is, the total payments expected to be made) and should include the effects of inflation and other social and economic factors. Estimated recoveries on unpaid claims, such as salvage, subrogation, and reinsurance, are deducted from the liability for unpaid claims. A liability for those adjustment expenses expected to be incurred in the settlement of unpaid claims should be accrued when the related liability for unpaid claims is accrued. Changes in estimates of the liabilities resulting from their periodic review and differences between estimates and ultimate payments are reflected in the income of the period in which the estimates are changed or the claim is settled. If the liabilities for unpaid claims and claim-adjustment expenses are discounted (that is, the liabilities are not recorded at their ultimate cost because the time value of the money is taken into consideration), the amount of the liabilities presented at present value in the financial statements and the range of interest rates used to discount those liabilities are required to be disclosed. For public companies, the SEC staff issued Staff Accounting Bulletin No. 62, *Discounting by Property/Casualty Insurance Companies*, which discusses the appropriate accounting and financial reporting when a company adopts or changes its policy with respect to discounting certain unpaid claims liabilities related to short-duration insurance contracts. The SEC issued Financial Reporting Release No. 20, *Rules and Guide for Disclosures Concerning Reserves for Unpaid Claims and Claim Adjustment Expenses of Property-Casualty Underwriters*, which requires additional disclosures concerning the underwriting and claims reserving experience of property-casualty underwriters. The SEC staff also issued Staff Accounting Bulletin No. 87, *Contingency Disclosures on Property/Casualty Insurance Reserves for Unpaid Claim Costs*, which provides guidance concerning those uncertainties surrounding property and casualty loss reserves that may require FASB Statement No. 5 contingency disclosures and Staff Accounting Bulletin No. 92, *Accounting and Disclosures Relating to Loss Contingencies*, which provides the SEC staff's interpretation of current accounting literature relating to the following:

- Offsetting of probable recoveries against probable contingent liabilities
- Recognition of liabilities for costs apportioned to other potential responsible parties

- Uncertainties in estimation of the extent of environmental or product liability
- The appropriate discount rate for environmental or product liability, if discounting is appropriate
- Accounting for exit costs
- Financial statement disclosures and disclosure of certain information outside the basic financial statements

Statutory Accounting Practices

4.03 Statutory accounting practices (SAP), which vary by state, are similar to GAAP for transactions in the claims cycle—estimated liabilities for unpaid claims, including IBNR [incurred but not reported] and claim-adjustment expenses, are accrued when the insured events occur; however, there are certain differences. Under SAP, reinsurance recoverable on unpaid losses is deducted from the liability for unpaid claims. For certain lines of insurance, such as auto liability, general liability, medical malpractice, and workers' compensation, a minimum statutory reserve may be required. The formula for determining this reserve is described in the footnotes to Schedule P in the NAIC Annual Statement. If it is determined that an additional statutory reserve is needed, this amount is reported as a separate liability and a reduction from surplus.

4.04 Discounting of loss reserves varies by state. SAP generally permits discounting settled lifetime workers' compensation claims and accident and health long-term disability claims at discount rates of 4 percent or less. In some states, medical malpractice liability claims may also be discounted. For statutory reporting purposes, reinsurance recoverable balances are segregated between those recoverable from companies authorized by the state to transact reinsurance and those recoverable from other companies, called unauthorized reinsurers. Insurance companies are required to provide a reserve by a charge to surplus for reinsurance that is recoverable from unauthorized companies. The reserve is provided to the extent that funds held or retained for account of such companies are exceeded or not secured by trust accounts or by letters of credit.

[Revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Chapter 2

THE LOSS RESERVING PROCESS

Types of Business and Their Effect on the Estimation Process

.06 The reporting and payment characteristics of a company's losses will differ depending on the types of policies written. Insurance policies may be categorized in several different ways:

- By policy duration (short duration or long duration)
- By type of coverage provided (occurrence basis or claims-made basis)
- By kind of insurance underwritten (for example, property, liability, workers' compensation, and reinsurance)[1]

Policy Duration

.07 Insurance policies are considered to be either short-duration or long-duration. Policies are considered short-duration when the contract provides for insurance coverage for a fixed period of short duration and enables the insurer to cancel the contract or adjust the provisions of the contract at the end of the contract period. Policies are considered long-duration when the contract provides for insurance coverage for an extended period and is not generally subject to unilateral changes in its provisions. Because most policies written by property and liability insurance companies are short-duration policies, only short-duration contracts are considered in this SOP.

Type of Coverage

.08 Insurance policies may be issued on either an occurrence basis or a claims-made basis. Occurrence-basis policies provide coverage for insured events occurring during the contract period, regardless of the length of time that passes before the insurance company is notified of the claim. Under occurrence-basis policies, claims may be filed months or years after the policy contract has expired, making it difficult to estimate the eventual number of claims that will be reported. Theoretically, a pure claims-made policy only covers claims reported to the insurer during the contract period; however, in practice, claims-made policies generally cover claims reported to either the insurer or the insured during the contract period. As a result, claims may be reported to the insurer after the contract expires. Even if claims have been reported to the insurer during the contract period, it may take several months for the insurer to investigate and establish a case reserve for reported claims. In practice, most claims-made insurance policies contain "extended reporting" clauses or endorsements that provide for coverage, in specified circumstances, of claims occurring during the contract period but reported after the expiration of the policy. In many states, a claims-made insurance policy is required to (*a*) contain an extended-reporting clause, (*b*) provide for the purchase, at the policyholder's option, of "tail coverage," that is, coverage for events occurring

[1] The terms *line of business* and *type of risk* are used interchangeably to mean kind of insurance underwritten.

during the policy term but reported after the initial policy expires, or (c) provide for automatic tail coverage upon the death, disability, or retirement of the insured. Thus, in practice, claims-made policies can resemble occurrence-basis policies. If a claims-made insurance policy provides for coverage of claims incurred during the policy period but reported to the insurer after the end of the policy period, loss reserve requirements for such claims should be considered.

Kind of Insurance Underwritten, Line of Business, or Type of Risk

.09 The kind of insurance underwritten by property and liability insurance companies may be broadly categorized into five classes of coverage: property, liability, workers' compensation, surety, and fidelity. Additionally, policies may be written as primary coverage or reinsurance assumed. Paragraphs 4.09 through 4.13 in chapter 4 of the audit guide describe the loss characteristics of different types of coverage.

.10 Some lines of insurance are commonly referred to as "long-tail" lines because of the extended time required before claims are ultimately settled. Examples of long-tail lines are automobile bodily injury liability, workers' compensation, professional liability, and other lines such as products and umbrella. Lines of insurance in which claims are settled relatively quickly are called "short-tail" lines. It is generally more difficult to estimate loss reserves for long-tail lines because of the long period that elapses between the occurrence of a claim and its final disposition, and the difficulty of estimating the settlement value of the claim.

Components of Loss Reserves

.11 Loss reserves are an insurer's estimate of its liability for the unpaid costs of insured events that have occurred. An insurance company's loss reserves consist of one or more of the components described below. All of these components should be considered in the loss-reserving process but may not have to be separately estimated.

Case-basis reserves—The sum of the values assigned by claims adjusters to specific known claims that were recorded by the insurance company but not yet paid at the financial statement date. Chapter 4 of the audit guide describes the most common methods used by companies to establish case-basis reserves.

Case-development reserves—The difference between the case-basis reserves and the estimated ultimate cost of such recorded claims. This component recognizes that case-basis reserves, which are estimates based on incomplete or preliminary data, will probably differ from ultimate settlement amounts. Accordingly, a summation of case-basis reserve estimates may not produce the most reasonable estimate of their ultimate cost.

Incurred but not reported (IBNR)—The estimated cost to settle claims arising from insured events that occurred but were not reported to the insurance company as of the financial statement date. This component includes reserves for claims "in transit," that is, claims reported to the company but not yet recorded and included in the case-basis reserve.

Reopened-claims reserve—The cost of future payments on claims closed as of the financial statement date that may be reopened due to circumstances unforeseen at the time the claims were closed.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Sometimes, case-development reserves, IBNR, and the reopened-claims reserve are calculated as a single reserve and broadly referred to as IBNR. In addition to the basic components of loss reserves, a company will also need to estimate the effect of the following components:

Reserves for loss adjustment expenses (LAE). These include the following:

- *Allocated loss adjustment expenses (ALAE)*—Expenses incurred in the claim settlement process that can be directly associated with specific claims, such as legal fees or outside adjuster fees. If this reserve is estimated on a case basis, a reserve for ALAE development, IBNR, and reopened claims should be provided.
- *Unallocated loss adjustment expenses (ULAE)*—Expenses incurred in the claim settlement process that cannot be directly associated with specific claims, such as costs incurred by the insurer's claims operations to record, process, and adjust claims.

Reduction for salvage—The estimated amount recoverable by the insurer from the disposition of damaged or recovered property. Potential salvage on paid and unpaid losses should be considered in this estimate.

Reduction for subrogation—The estimated amount recoverable from third parties from whom the insured may have the right to recover damages. The insured, having collected benefits from the insurer, is required to subrogate such rights to the insurer.

Drafts outstanding—Some insurance companies may elect to pay claims by draft rather than by check and may not record the drafts as cash disbursed until the drafts are presented to the insurer by the bank. A liability for drafts outstanding is required only if cash disbursements and claim statistical information are not recorded concurrently, thereby creating a timing difference. Because the claim statistical information is updated to reflect the payment, no loss reserve is recorded for the claim; however, because the draft has not been presented, a drafts outstanding liability is required.

Reserves for assessments based on paid losses—The estimated amount of future assessments relating to payments on losses incurred prior to the financial statement date. An example is assessments by state workers' compensation second-injury funds. Such assessments are recorded as losses and should be considered in the loss reserving process.

Reinsurance receivables—Amounts that will be recovered from reinsurers for losses and LAE accrued, including IBNR losses accrued. Amounts receivable from reinsurers on paid and unpaid losses are generally classified as assets.

[Revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.12 Many insurance companies do not separately value each of the reserve components listed above. Frequently, an insurance company's reserve for case development is combined with its reserve for IBNR claims. Reinsurance and other recoveries may be netted against claim payments in the insurance company's records. In those situations, all reserve estimates are also net of recoveries; separate analysis is then performed to determine the appropriate amount to record as the reinsurance receivable asset. ALAE may be combined with loss payments and included in these components. [Revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Estimating Methods

.13 Various analytical techniques exist to assist management, consulting actuaries, and independent auditors in estimating and evaluating the reasonableness of loss reserves. These techniques generally consist of statistical analyses of historical experience and are commonly referred to as loss reserve projections.

.14 Loss reserve projections are used to develop loss reserve estimates. Understanding and assessing the variability of these estimates and the reliability of historical experience as an indicator of future loss payments require a careful analysis of the historical loss data and the use of projection methods that are sensitive to the particular circumstances.

.15 The data used for projections is generally grouped by line of business and may be further classified by attributes such as geographic location, underwriting class, or type of coverage to improve the homogeneity of the data within each group. The data is then arranged chronologically. The following are dates that are key to classifying the chronology of the data.

Policy date—The date on which the contract becomes effective (also referred to as the underwriting date).

Accident date—The date on which the accident (or loss) occurs.

Report date—The date on which the company first receives notice of the claim.

Record date—The date on which the company records the claim in its statistical system.

Closing date—The date on which the claim is closed.

.16 After the data has been grouped by line of business and by chronology, it may then be arrayed to facilitate the analysis of the data, highlight trends, and permit ready extrapolation of the data. The following are examples of types of data that are commonly arrayed and analyzed:

- Losses paid
- Losses incurred
- Case reserves outstanding
- Claim units reported
- Claim units paid
- Claim units closed
- Claim units outstanding
- ALAE paid
- ALAE outstanding
- Salvage and subrogation recovered
- Reinsurance recovered
- Reinsurance receivable
- Premiums earned
- Premiums in force
- Exposures earned
- Policies in force

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

[Revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.17 The data may be cumulative or incremental, gross or net of reinsurance, gross or net of salvage and subrogation, or combined with allocated loss adjustment data. The data may be stratified by size of loss or other criteria. Because claim data and characteristics such as dates, type of loss, and claim counts significantly affect reserve estimation, controls should be established over the recording, classification, and accumulation of historical data used in the determination of loss reserves. Exhibit B-2 in appendix B of the audit guide presents examples of such control activities. [Revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.18 Loss reserve projections can be performed using a variety of mathematical approaches ranging from simple arithmetic projections using loss development factors to complex statistical models. Projection methods basically fall into three categories:

- Extrapolation of historical loss dollars
- Projection of separate frequency and severity data (the number of claims that will be paid or closed and the average costs of these claims)
- Use of expected loss ratios

.19 Within each of these methods, there are a variety of techniques and loss data that may be used; there are also methods that combine features of these basic methods. No single projection method is inherently better than any other in all circumstances.

.20 Following is a brief summary of some commonly used projection methods.

Method	*Basis*
Loss Extrapolation	
Paid loss	Uses only paid losses. Outstanding case reserves are not considered.
Incurred loss	Uses paid losses plus reserves on outstanding claims.
Average Severities	Uses various claim count and average cost per claim data on either a paid or incurred basis.
Loss Ratio	Uses various forms of expected losses in relation to premiums earned.

.21 The decision to use a particular projection method and the results obtained from that method should be evaluated by considering the inherent assumptions underlying the method and the appropriateness of these assumptions to the circumstances. Stability and consistency of data are extremely important. Changes in variables, such as rates of claim payments, claim department practices, case-basis reserving adequacy, claim reporting rates, mix of business, reinsurance retention levels, and the legal environment, may have a significant effect on the projection and may produce distortions or conflicting results. Reference should be made to the section in this chapter titled "Changes in the Environment" for a discussion of how changes in variables may affect the loss-reserving process. The results of any projection should be reviewed for reasonableness by analyzing the resultant loss ratios and losses per measure of exposure.

Illustrative Projection Data

.22 The following tables are simple illustrations of the use of the loss extrapolation method to estimate ultimate losses, as well as the effects of considering the results of more than one projection. In these illustrations, the result of extrapolating incurred-loss data is compared with the result of extrapolating paid-loss data. These tables are presented solely for the purpose of illustrating the mathematical mechanics of the two projections. They do not illustrate the required analysis of the data, and consideration of internal and external environmental variables that may affect the claim payment and loss reserving process.

.23 Table 1 presents an illustration of historical incurred-loss data. It reflects, as an example, that the sum of paid losses and case reserves outstanding at the end of 19X0 was $2,054; that sum increased to $2,717 in the next year and increased to $3,270 five years later.

.24 This incurred-loss data is first used to calculate historical period-to-period incurred-loss development factors. These factors are used to compare the amount of incurred losses at successive development stages, and are illustrated in table 2, part 1.

.25 The calculation of average historical period-to-period incurred-loss development factors may be based on the use of simple averages of various period-to-period factors or may be based on more complex weighting or trending techniques. These techniques can significantly affect the reserving process and require judgment, understanding, and experience. In this example, a simple average of the latest three period-to-period factors has been calculated and is presented in table 2, part 2.

Table 1

Case-Basis Incurred-Loss Data as of 12/31/X9

Accident Year	*Development Period (in months)*									
	12	*24*	*36*	*48*	*60*	*72*	*84*	*96*	*108*	*120*
19X0	$2,054	$2,717	$2,979	$3,095	$3,199	$3,348	$3,270	$3,286	$3,299	$3,301
19X1	2,213	2,980	3,269	3,461	3,551	3,592	3,631	3,643	3,651	
19X2	2,341	3,125	3,513	3,695	3,798	3,849	3,872	3,876		
19X3	2,492	3,502	3,928	4,177	4,313	4,369	4,392			
19X4	2,964	4,246	4,859	5,179	5,315	5,376				
19X5	3,394	4,929	5,605	5,957	6,131					
19X6	3,715	5,433	6,162	6,571						
19X7	4,157	5,912	6,771							
19X8	4,573	6,382								
19X9	4,785									

.26 Once historical period-to-period incurred-loss development factors are calculated, future period-to-period incurred-loss development factors must be selected. The future period-to-period factors must reflect anticipated differences between historical and future conditions that affect loss development, such as changes in the underlying business, different inflation rates, or case-basis reserving practices. In the example, no differences are anticipated and the average historical factors have been chosen as the selected factors as shown in table 2, part 2. The selected future period-to-period factors are then used to produce ultimate incurred development factors. The ultimate factors are presented in table 2, part 3.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Table 2

Period-to-Period Incurred-Loss Development Factors as of 12/31/X9

Accident Year	Development Period (in months) 12-24	24-36	36-48	48-60	60-72	72-84	84-96	96-108	108-120	Est. Tail*
Part 1: Period-to-Period Historical Loss Development Factors										
19X0	1.323†	1.096	1.039	1.034	1.047	0.977	1.005	1.004	1.001	
19X1	1.347	1.097	1.059	1.026	1.012	1.011	1.003	1.002		
19X2	1.335	1.124	1.052	1.028	1.013	1.006	1.001			
19X3	1.405	1.122	1.063	1.033	1.013	1.005				
19X4	1.433	1.144	1.066	1.026	1.011					
19X5	1.452	1.137	1.063	1.029						
19X6	1.462	1.134	1.066							
19X7	1.422	1.145								
19X8	1.396									
Part 2: Period-to-Period Average Development Factors										
Simple Average of Latest Three	1.427	1.139	1.065	1.029	1.012	1.007	1.003	1.003	1.001	1.000
Selected Factors	1.427	1.139	1.065	1.029	1.012	1.007	1.003	1.003	1.001	1.000
Part 3: Ultimate Development Factors Selected for the Projection	1.828‡	1.281	1.125	1.056	1.026	1.014	1.007	1.004	1.001	1.000

* Applies when the development period is determined to be longer than the period covered by the model (assumed to be 1.000 in this illustration).

† The 24-month developed losses are divided by the 12-month developed losses from table 1 ($2,717/$2,054 = 1.323).

‡ The product of the remaining factors (1.427 × 1.139 × 1.065 × 1.029 × 1.012 × 1.007 × 1.003 × 1.003 × 1.001 × 1.000 = 1.828) or the product of the 12-24 selected factor times the 24-36 ultimate factor (1.427 × 1.281 = 1.828).

.27 The loss reserve analysis has now reached the point where an initial projection of ultimate losses, as well as an indicated provision for unreported losses for each accident year, can be made by using the historical incurred-loss data and the ultimate incurred-loss development factors. This initial projection of ultimate losses is presented in table 3.

.28 Tables 4 and 5 present paid-loss data for the same company whose incurred-loss data was presented in table 1. The array of paid-loss period-to-period development factors presented in table 5 is derived from table 4 using the same calculation methods used for incurred losses in table 2. The importance of the use of a tail factor in this calculation is apparent from the period-to-period historical loss development factors calculated in table 5. The tail factor represents an estimate of the development of losses beyond the period covered by the data array. In this instance, a tail factor of 1.01 was selected to project an additional 1 percent of losses to be paid from the tenth development year to ultimate. Selection of a tail factor requires careful judgment based on consideration of industry experience for the line of business, actuarial studies, case reserves, and any other relevant information.

.29 The initial projection of ultimate losses, using the historical paid losses and the paid-loss ultimate development factors, is presented in table 6.

.30 Table 7 compares the results of extrapolating paid-loss data (table 6) with the results of extrapolating incurred-loss data (table 3).

.31 Although all accident periods should be analyzed and trends evaluated, it is clear that additional analysis of accident year 19X9 losses is required. The difference between the results obtained from the two different projections is significant. Initial inspection will trace the source of the difference to the high level of losses paid in 19X9 for accident year 19X9 relative to case-basis incurred losses for the same period. The loss reserving analysis must focus on whether the increase in payments represents an acceleration of payment activity or an increase in the overall level of losses incurred in 19X9. The benefit of using more than one projection is that it allows for this kind of analysis and comparison in the evaluation of loss reserves.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Table 3

Incurred-Loss Projection as of 12/31/X9

Accident Year	*Case-Basis Incurred Losses as of 19X9*[11]	*Ultimate Incurred-Loss Development Factors*[#]	*Projected Ultimate Losses (2) × (3)*	*Projected Unreported Losses (4) – (2)*
(1)	(2)	(3)	(4)	(5)
19X0	$ 3,301	1.000	$ 3,301	$ 0
19X1	3,651	1.001	3,655	4
19X2	3,876	1.004	3,892	16
19X3	4,392	1.007	4,423	31
19X4	5,376	1.014	5,451	75
19X5	6,131	1.026	6,290	159
19X6	6,571	1.056	6,939	368
19X7	6,771	1.125	7,617	846
19X8	6,382	1.281	8,175	1,793
19X9	4,785	1.828	8,747	3,962
Total	$51,236		$58,490	$7,254

[11] From table 1
[#] From table 2, part 3

Table 4

Paid-Loss Data as of 12/31/X9

Accident Year	*Development Period (in months)*									
	12	*24*	*36*	*48*	*60*	*72*	*84*	*96*	*108*	*120*
19X0	$ 896	$1,716	$2,291	$2,696	$3,041	$3,096	$3,185	$3,235	$3,262	$3,276
19X1	872	1,840	2,503	2,973	3,261	3,429	3,538	3,589	3,624	
19X2	968	1,975	2,683	3,185	3,494	3,670	3,763	3,819		
19X3	968	2,130	2,968	3,571	3,942	4,147	4,274			
19X4	1,201	2,580	3,673	4,421	4,860	5,114				
19X5	1,348	2,996	4,207	5,115	5,632					
19X6	1,340	3,146	4,520	5,496						
19X7	1,384	3,428	4,960							
19X8	1,568	3,696								
19X9	2,243									

Table 5

Period-to-Period Paid-Loss Development Factors as of 12/31/X9

Accident Year	*Development Period (in months)*									
	12-24	*24-36*	*36-48*	*48-60*	*60-72*	*72-84*	*84-96*	*96-108*	*108-120*	*Est. Tail***
***Part 1: Period-to-Period Historical Loss Development Factors*††										
19X0	1.915	1.335	1.177	1.128	1.018	1.029	1.016	1.008	1.004	
19X1	2.110	1.360	1.188	1.097	1.052	1.032	1.014	1.010		
19X2	2.040	1.358	1.187	1.097	1.050	1.025	1.015			
19X3	2.200	1.393	1.203	1.104	1.052	1.031				
19X4	2.148	1.424	1.204	1.099	1.052					
19X5	2.223	1.404	1.216	1.101						
19X6	2.348	1.437	1.216							
19X7	2.477	1.447								
19X8	2.357									
Part 2: Period-to-Period Average Development Factors										
Simple Average of Latest Three	2.394	1.429	1.212	1.101	1.051	1.029	1.015	1.009	1.004	1.010
Selected Factors	2.394	1.429	1.212	1.101	1.051	1.029	1.015	1.009	1.004	1.010
***Part 3: Ultimate Development Factors Selected for the Projection*††	5.127	2.142	1.499	1.237	1.123	1.069	1.039	1.023	1.014	1.010

** Applies when the development period is determined to be longer than the period covered by the model (assumed to be 1.010 in this illustration).

†† Computations are the same as those explained in table 2.

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Table 6

Paid-Loss Projection as of 12/31/X9

Accident Year	*Paid Losses as of 19X9*	*Ultimate Loss Development Factors*	*Projected Ultimate Losses (2) × (3)*	*Projected Unreported Losses*[#]
(1)	(2)	(3)	(4)	(5)
19X0	$ 3,276	1.010	$ 3,309	$ 8
19X1	3,624	1.014	3,675	24
19X2	3,819	1.023	3,907	31
19X3	4,274	1.039	4,439	47
19X4	5,114	1.069	5,465	89
19X5	5,632	1.123	6,325	194
19X6	5,496	1.237	6,796	225
19X7	4,960	1.499	7,434	663
19X8	3,696	2.142	7,916	1,534
19X9	2,243	5.127	11,500	6,715
Total	$42,134		$60,766	$9,530

[#] Represents the projected ultimate losses from table 6, column 4, less the recorded case-basis incurred losses from table 3, column 2.

Table 7

Alternative Projections of Ultimate Losses and Unreported Losses as of 12/31/X9

	Ultimate Losses		*Unreported Losses*	
Accident Year	*Incurred*	*Paid*	*Incurred*	*Paid*
19X0	$ 3,301	$ 3,309	$ 0	$ 8
19X1	3,655	3,675	4	24
19X2	3,892	3,907	16	31
19X3	4,423	4,439	31	47
19X4	5,451	5,465	75	89
19X5	6,290	6,325	159	194
19X6	6,939	6,796	368	225
19X7	7,617	7,434	846	663
19X8	8,175	7,916	1,793	1,534
19X9	8,747	11,500	3,962	6,715
Total	$58,490	$60,766	$7,254	$9,530

Loss Adjustment Expense Reserves

.32 Loss adjustment expense reserves are the costs that will be required to settle claims that have been incurred as of the valuation date. As explained in paragraph .11, loss adjustment expenses (LAE) can be classified into two broad categories: allocated loss adjustment expenses (ALAE) and unallocated loss adjustment expenses (ULAE).

ALAE Reserve Calculation Approaches

.33 ALAE is generally analyzed by line of business; however, it is also important to monitor the composition of the paid ALAE by cost component. A shift in the composition of the costs in relation to the total might affect the statistical data used in the related loss projections. This shift would need to be considered in future loss reserve projections.

.34 Many companies calculate ALAE reserves based on the relationship of ALAE to losses. Underlying this approach is a basic assumption that ALAE will increase or decrease in proportion to losses. The setting of reserves for ALAE based on the relationship of paid ALAE to paid losses is referred to as the "paid-to-paid ratio" approach. Separate ratios are normally developed for each accident year. Inflation in ALAE is not typically evaluated separately; rather, it is estimated to occur at the same rate as the rate of inflation in the losses. The validity of this assumption can be tested by reviewing historical relationships between ALAE and losses over time. The effects of a pattern of increasing or decreasing ratio of ALAE to losses should be considered in establishing ALAE reserves. An understanding of the claim department's operations and philosophy over time is essential to a proper interpretation of the data.

.35 Other approaches to ALAE reserve calculation and analysis include (*a*) analyzing ALAE entirely apart from the related loss costs using methods that compare the development of ALAE payments at various stages and (*b*) using combined loss and ALAE data in situations where it appears likely that this would produce more accurate estimates (e.g., when the company has changed its claim defense posture so that defense costs increase and loss costs decrease). In this latter approach, statistical tests and projections are based on the combined data for losses and ALAE.

.36 Some companies establish case-basis reserves for certain types of ALAE or increase case-basis loss reserves by a stated percentage to provide for ALAE. In either case, additional ALAE reserves should be provided for the development of case-basis reserves and IBNR.

ULAE Reserve Calculation Approaches

.37 ULAE reserves are often provided for by using the calendar year paid-to-paid method rather than the accident year paid-to-paid method used for ALAE reserves. Although the paid-to-paid ratios establish the relationship of the ULAE payments to the loss payments, the timing of the ULAE payments is also critical to estimation of the ULAE reserves. For example, some companies assume that a portion of ULAE costs is incurred when a claim is placed on the books and the remaining portion is incurred when the claim is settled. For reported claims, the cost of placing the claim on the books has been incurred, so it is only necessary to provide a reserve for the remaining portion at settlement. For IBNR claims, it is necessary to provide for all of the ULAE. Some companies perform internal studies to establish the methods and ratios to be used in their calculations.

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

.38 The ULAE reserves should provide for inflation. The assumption that ULAE will inflate at a rate equal to the rate at which losses inflate should be periodically reviewed. The rate should also be adjusted for expected technological or operational changes that might cause economies or inefficiencies in the claim settlement process.

.39 If paid-to-paid ULAE ratios will be calculated for each line of business, a reasonable basis for allocating paid ULAE by line of business should be established.

Changes in the Environment

.40 Loss reserve projections are used to estimate loss reporting patterns, loss payment patterns, and ultimate claim costs. An inherent assumption in such projections is that historical loss patterns can be used to predict future patterns with reasonable accuracy. Because many variables can affect past and future loss patterns, the effect of changes in such variables on the results of loss projections should be carefully considered.

.41 Identification of changes in variables and consideration of their effect on loss reserve projections are critical steps in the loss reserving process. The evaluation of these factors requires the involvement of a loss reserve specialist as well as input from various operating departments within the company such as the marketing, underwriting, claims, actuarial, reinsurance, and legal departments. Management's use of a specialist in determining loss reserves is discussed in paragraphs .44 through .47 of this SOP.

.42 Variables to be considered in evaluating the results of loss reserve projections include those variables affecting inherent and control risk described in the Appendix [paragraph .107] of this SOP. If changes in variables have occurred, mechanical application of loss projection methods may result in unreasonable estimates of ultimate claim costs. Changes in variables can be considered in the loss reserving process in a variety of ways, including—

- *Selection of loss projection method(s).* Loss projection methods vary in their sensitivity to changes in the underlying variables and to the length of the claim emergence pattern. When selecting a loss projection method, consideration should be given to how a change in the underlying data will affect that method. For example, if management has adopted a policy to defer or accelerate the settlement of claims, a paid-loss extrapolation method will probably produce unreliable results. In that case, an incurred-loss extrapolation or other methods may produce better estimates of ultimate losses.
- *Adjustment of underlying historical loss data.* In certain cases, the effect of changed variables can be isolated and appropriately reflected in the historical loss data used in the loss projection. For example, if policy limits are relatively consistent for all policies in a block of business, and if these limits have recently been reduced by a constant amount, historical loss data can be adjusted to exclude amounts in excess of the revised policy limits.
- *Further segregation of historical loss data.* Certain changes in variables can be addressed by further differentiating and segregating historical loss data. For example, if a company begins to issue claims-made policies for a line of business for which it traditionally issued occurrence-basis policies, segregation of data between the two types of

policies should minimize the effect of the different reporting patterns. Such segregation should produce more accurate loss reserve projections for the occurrence-basis policies. (However, loss development data relating to the claims-made policies will be limited in the initial years.)

- *Separate calculation of the effect of variables.* The effect of certain changes in variables can be isolated and separately computed as an adjustment to the results of other loss projection methods. For example, if claim cost severity has increased (an increase in auto repair costs) or is expected to increase beyond historic trends, an additional reserve can be separately computed to reflect the effect of such actual or anticipated increases.

- *Qualitative assessments.* In many instances, the magnitude or effect of a change in a variable will be uncertain. The establishment of loss reserves in such situations requires considerable judgment and knowledge of the company's business. Following is an example of an environmental variable that may have uncertain effects on loss reserve estimates.

Superfund legislation enacted by Congress seeks recovery from anyone who ever owned or operated a particular contaminated site or from anyone who ever generated or transported hazardous materials to a site. These parties are commonly referred to as potentially responsible parties, or PRPs. Potentially, the liability can extend to subsequent owners or to the parent company of a PRP.

Estimates of the cost of cleaning up hazardous waste sites currently on the so-called Superfund list are in the hundreds of billions of dollars. Third-party damages, legal defense costs, and cleanup expenses for non-Superfund sites will add significantly to this figure. It is conceivable, but by no means certain, that some portion of these costs will ultimately be borne by the insurance industry under pre-1986 liability coverages because insurance companies that wrote general liability or commercial multiperil policies prior to 1986 used policy forms that did not contain the "absolute" pollution exclusion currently in standard use within the industry. Some insureds are arguing that coverage should be afforded under these contracts for their potential liability for the cleanup of inactive hazardous waste sites or other similar environmental liabilities. Most insurers are vigorously resisting such arguments with mixed success in the courts. Although some major U.S. corporations and specialized industries have begun to litigate pollution liability coverage issues, these cases may represent only the tip of the iceberg. Potential for additional litigation exists in the form of non-Superfund claims that will be reported to insurers in the future.

Although the largest environmental liabilities are likely to arise from chemical producers, petroleum processors, and other "heavy" industries, any company writing liability coverage has some environmental liability exposure for service stations, dry cleaners, hardware stores, paint stores, gardening supply stores, small metal plating operations, and the like. Even homeowners' policies are potentially exposed to the cleanup costs for leaks from underground heating oil storage tanks.

The development of environmental and similar claims may not follow the usual development pattern of general liability claims, with which they are usually grouped. When the activity of these claims is sufficient to distort the recorded

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

development of the company, the distorting activity should be isolated from the development history so that an accurate projection of the remaining claims can be made. Management's process of assessing its environmental and similar exposure should include procedures to—

- Insure that all data elements are recorded on each incoming claim or precautionary notice.
- Assess the company's exposure to these types of liability claims by considering such factors as the types of risks historically written, layers of coverage provided, the policy language employed, and recent decisions rendered by courts.
- Determine whether any portion of potential liability costs is probable and reasonably estimable.

.43 Financial Accounting Standards Board (FASB) Statement of Financial Accounting Standards No. 5, *Accounting for Contingencies*, and Interpretation No. 14, *Reasonable Estimation of the Amount of a Loss*, provide guidance for the accounting and disclosure of loss contingencies.

Use of Specialists by Management in Determining Loss Reserves

.44 Management is responsible for making the accounting estimates included in the financial statements. As explained in the previous sections of this chapter, the process of estimating loss reserves is complex and involves many subjective judgments. Accordingly, the determination of loss reserves should involve an individual with a sufficient level of competence and experience in loss reserving, including knowledge about the kind(s) of insurance for which a reserve is being established and an understanding of appropriate methods available for calculating loss reserve estimates. These individuals are referred to as "loss reserve specialists" in this SOP. The specialist's level of competence and experience should be commensurate with the complexity of the company's business, which is affected by such factors as the kind(s) of insurance underwritten and the environmental and risk considerations listed in the Appendix [paragraph .107] of this SOP. Criteria that may be considered in determining whether an individual qualifies as a loss reserve specialist include the aforementioned as well as the following:

- Knowledge of various projection techniques, including their strengths and weaknesses and applicability to various lines of insurance
- Knowledge of changes in the environment in which the company operates, including regulatory developments, social and legal trends, court decisions, and other factors described in more detail in the Appendix and the effect that these factors will have on the emergence and ultimate cost of these claims

.45 The Casualty Actuarial Society (CAS) offers a course of study and examinations that are designed to train individuals to be, among other things, loss reserve specialists. In addition, the American Academy of Actuaries establishes qualification standards for its members who practice in this area. Although many casualty actuaries may therefore be qualified to be loss reserve specialists, other individuals, through their experience and training, may also be qualified. Training and experience should provide individuals with knowledge

about different policy forms and coverages, current developments in insurance, and environmental factors that might affect the loss reserving process. Training and experience should also provide individuals with knowledge that will enable them to apply appropriate methods of estimating loss reserves. The extent of this knowledge and ability should be commensurate with the complexity and kinds of business written.

.46 Many insurance companies use loss reserve specialists who are employees or officers of the company. In addition, many companies engage consulting casualty actuaries to either assist in the determination of the loss reserve estimate or to perform a separate review of the company's loss reserve estimate. The scope of work to be performed by the consulting actuary is a matter of judgment by company management. Usually, the consulting actuary will issue a report summarizing the nature of the work performed and the results. Since 1990, the Annual Statement has required a Statement of Actuarial Opinion relating to loss and loss adjustment expense reserves.

.47 Because the process of estimating loss reserves is complex and involves many subjective judgments, the absence of involvement by a loss reserve specialist in the determination of management's estimate may constitute a reportable condition and possibly a material weakness in the entity's internal control structure. Statement on Auditing Standards (SAS) No. 60, *Communication of Internal Control Related Matters Noted in an Audit*, describes the auditor's responsibility to communicate reportable conditions to the audit committee. A discussion of the auditor's use of loss reserve specialists is included in chapter 4.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Chapter 3

AUDIT PLANNING

Audit Objectives

.48 SAS No. 57, *Auditing Accounting Estimates*, states that the auditor's objective when evaluating accounting estimates is to obtain sufficient competent evidential matter to provide reasonable assurance that—

a. All accounting estimates that could be material to the financial statements have been developed.

b. Those accounting estimates are reasonable in the circumstances.

c. The accounting estimates are presented in conformity with applicable accounting principles and are properly disclosed.

.49 When auditing loss reserves, the auditor is primarily concerned with obtaining sufficient competent evidential matter to support the assertions inherent in a company's financial statements. SAS No. 31, *Evidential Matter*, as amended by SAS No. 80, describes the relationship between assertions embodied in the financial statements, audit objectives, and substantive audit procedures. The financial statement assertions related to loss reserves are set forth below. This listing supplements the illustrations of financial statement assertions for the claims cycle presented in exhibit B-2 in appendix B of the audit guide. [Revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Financial Statement Assertions	*Audit Objectives*
Existence, Rights, Obligations	• Claims represent valid obligations of the insurance company. The policy is in force when the loss is incurred and covers the related risk event. Claimants and others receiving payment are bona fide and entitled to payments within applicable policy provisions. • Guidelines for adjusting claims and authorizing payment are established and being followed.
Completeness and Valuation	• Loss reserves are established for all losses resulting from insured events (reported and unreported) that occurred prior to the balance sheet date. • Appropriate reserving methods are accurately applied and result in loss reserve estimates that represent the ultimate cost of settling all probable losses. Appropriate reductions in reserves have been taken for reinsurance ceded and salvage and subrogation recoverable.

Financial Statement Assertions	*Audit Objectives*
	• All relevant claims data, including payment and recovery data, are appropriately recorded in the underlying financial and statistical records. • All loss reserves are appropriately recorded on the balance sheet and the income statement reflects the changes therein. • Loss reserves are properly accumulated in the underlying financial records. • Claims transactions are properly accumulated in the underlying financial and statistical records. • Payments and recoveries are recorded in the proper period; a proper cutoff is established.
Presentation and Disclosure	• Loss reserves and related components have been properly summarized, classified, and described and all matters necessary to a proper understanding of these items have been disclosed.

Audit Planning

.50 In planning the audit, the auditor should obtain a thorough understanding of the company's overall operations and its claim reserving and payment practices. In addition, the auditor should obtain or update his or her knowledge of the entity's business and the various economic, financial, and organizational conditions that create risks for companies in the insurance industry.

.51 The auditor performing or supervising the audit of loss reserves should have knowledge about loss reserving including knowledge about the kind(s) of insurance for which a reserve is being established and an understanding of the appropriate methods available for calculating loss reserves. Knowledge about loss reserving is ordinarily obtained through experience, training courses, and by consulting sources such as industry publications, textbooks, periodicals, and individuals knowledgeable about loss reserving. As stated in paragraph .98 of this SOP, if the auditor is not a loss reserve specialist, he or she should use the work of an outside loss reserve specialist in the audit. The auditor should obtain a level of knowledge about loss reserving that would enable him or her to understand the methods or assumptions used by the specialist.

.52 Ordinarily, audit procedures performed to obtain sufficient evidence to support assertions about loss reserves are time consuming and may be performed most efficiently when initiated early in the fieldwork.

.53 The auditor should determine that all loss reserve components, all lines of business, and all accident years that could be material to the financial

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

statements have been considered in developing the overall reserve estimate. The components of loss reserves are described in chapter 2 of this SOP.

.54 The estimate of loss reserves will frequently affect other accounting estimates contained in the financial statements. While these other accounting estimates are not the subject of this SOP, the auditor should also evaluate accounting estimates for such items as contingent commissions, retrospective premium adjustments, policyholder dividends, recoverability of deferred acquisition costs, premium deficiencies, state assessments based on losses paid, minimum statutory reserves, and the liability or allowance for unauthorized or uncollectible reinsurance.

Audit Risk and Materiality

.55 Audit risk and materiality are the key criteria in determining the nature, timing, and extent of audit procedures to be performed and in evaluating whether the financial statements taken as a whole are presented fairly. Considerations of audit risk and materiality should be addressed in the planning stage of an audit and should be used to develop and support an audit approach. For most insurance companies, the largest liability on the balance sheet is loss reserves, and the largest expense on the income statement is incurred losses; therefore, both are material to the financial statements. In addition, loss reserve estimates are based on subjective judgments and, therefore, involve a high level of inherent risk. For these reasons, loss reserves typically are the area with the highest audit risk in a property and liability insurance entity. Reference should be made to the Appendix [paragraph .107] of this SOP for examples of factors that may affect the auditor's assessment of inherent and control risk.

Audit Risk

.56 SAS No. 47, *Audit Risk and Materiality in Conducting an Audit*, provides guidance on audit risk and materiality as they relate to planning and performing an audit. Materiality judgments are made in light of surrounding circumstances and necessarily involve both quantitative and qualitative considerations. The auditor's consideration of materiality is a matter of professional judgment and is influenced by the auditor's perception of the needs of a reasonable person relying on the financial statements. Some factors to be considered in establishing materiality levels for estimates such as loss reserves are the company's operating results and the company's financial position. The auditor should also consider the measurement bases that external financial statement users will focus on when making decisions. [Paragraph added, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.57 SAS No. 47 states that the auditor has a responsibility to plan and perform the audit to obtain reasonable assurance that misstatements, whether caused by error or fraud, that are material to the financial statements are detected. SAS No. 82, *Consideration of Fraud in a Financial Statement Audit*, provides specific guidance to auditors in fulfilling their responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement caused by fraud. [Paragraph added, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.58 SAS No. 82 requires the auditor to assess the risk of material misstatement due to fraud and consider that assessment in designing the audit procedures to be performed. In making this assessment, the auditor should consider fraud risk factors that relate to both (*a*) misstatements arising from fraudulent financial reporting and (*b*) misstatements arising from misappropriation of assets in the following categories:

Fraudulent Financial Reporting

- Management's characteristics and influence over the control environment.
- Industry conditions.
- Operating characteristics and financial stability.

Misappropriation of Assets

- Susceptibility of assets to misappropriation.
- Controls.

[Paragraph added, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.59 In addition to requiring the auditor to assess the risk of material misstatement due to fraud, SAS No. 82 provides guidance on how the auditor responds to the results of that assessment, provides guidance on the evaluation of audit test results as they relate to the risk of material misstatement due to fraud, describes related documentation requirements, and provides guidance regarding the auditor's communication about fraud to management, the audit committee, and others. [Paragraph added, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.60 SAS No. 47 defines audit risk as "the risk that the auditor may unknowingly fail to appropriately modify his opinion on financial statements that are materially misstated." In other words, audit risk is the risk that the auditor will give an unqualified opinion on financial statements that are materially incorrect. SAS No. 47 states that audit risk consists of three components (see paragraphs .61 through .63 below). [Paragraph renumbered and revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.61 *Inherent Risk.* Inherent risk is the susceptibility of an assertion to a material misstatement, assuming that there are no related controls. The risk of such misstatement is greater for some assertions and related balances or classes than for others. In addition to those factors that are peculiar to a specific assertion for an account balance or class of transactions, factors that relate to several or all of the balances or classes may influence the inherent risk related to an assertion for a specific balance or class. Loss reserves generally are based on subjective judgments about the occurrence of certain events that have not yet been fully reported, developing trends, and the outcome of future events. Due to the subjectivity and inherent imprecision involved in making such judgments, estimating loss reserves requires considerable analytical ability and an extensive understanding of the business. [Paragraph renumbered and revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.62 *Control Risk.* Control risk is the risk that a material misstatement that could occur in an assertion will not be prevented or detected on a timely

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

basis by the entity's controls. That risk is a function of the effectiveness of the design and operation of controls in achieving the entity's broad control objectives relevant to an audit of the entity's financial statements. Some control risk will always exist because of the inherent limitations of internal control. The degree of control risk associated with significant accounting estimates is usually greater than the risk for other accounting processes because accounting estimates involve a greater degree of subjectivity, are less susceptible to control, and are more subject to management influence. It is difficult to establish controls over errors in assumptions or estimates of the future outcome of events in the same way that controls can be established over the routine accounting for completed transactions. In addition, there is a potential for management to be biased about their assumptions; accordingly, a high level of professional skepticism should be exercised by the auditor. The likelihood that loss reserve estimates will contain misstatements of audit importance can be reduced by using competent people in the estimation process and by implementing practices to enhance the reasonableness of estimates, such as requiring that persons making the estimates retain documented explanations and other support for assumptions and methodologies used, and perform retrospective tests of past performance. [Paragraph renumbered and revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.63 *Detection Risk.* Detection risk is the risk that the auditor will not detect a material misstatement that exists in an assertion. Detection risk is a function of the effectiveness of an auditing procedure and of its application by the auditor. It arises partly from uncertainties that exist when the auditor does not examine 100 percent of an account balance or class of transactions and partly because of other uncertainties that exist even if he or she were to examine 100 percent of the balance or class. Such other uncertainties arise because an auditor might select an inappropriate auditing procedure, misapply an appropriate procedure, or misinterpret the audit results. These other uncertainties can be reduced to a negligible level through adequate planning and supervision and conduct of a firm's audit practice in accordance with appropriate quality control standards. Due to the relatively high inherent and control risk associated with loss reserves, detection risk is significant in the audit of loss reserves but may be mitigated by adequate planning, supervision, and conduct of the audit. Adequate planning should identify the existing inherent and control risk factors so that they may be adequately addressed in the audit. [Paragraph renumbered and revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Materiality

.64 SAS No. 47 provides guidance on audit risk and materiality as they relate to planning and performing an audit. Materiality judgments are made in light of surrounding circumstances and necessarily involve both quantitative and qualitative considerations. The auditor's consideration of materiality is a matter of professional judgment and is influenced by the auditor's perception of the needs of a reasonable person relying on the financial statements. Some factors to be considered in establishing materiality levels for loss reserve estimates are the company's operating results and the company's financial position. The auditor should also consider the measurement bases that external financial statement users will focus on when making decisions. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Chapter 4

AUDITING LOSS RESERVES

Auditing the Claims Data Base

.65 The historical experience of an insurance entity is generally the primary source of information on which loss reserve estimates are based; therefore, the creation of reliable data bases, within an insurance company, is extremely critical to the determination of loss reserve estimates. When evaluating loss reserves, the auditor should consider the reliability of the historical information generated by the insurance company. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.66 The auditor should determine what historical data and methods have been used by management in developing the loss reserve estimate and whether he or she will rely on the same data or other statistical data in evaluating the reasonableness of the loss reserve estimate. After identifying the relevant data, the auditor should obtain an understanding of the controls related to the completeness, accuracy, and classification of the loss data; assess control risk for assertions about loss reserves; and determine the nature, timing, and extent of substantive tests that will be performed for these assertions. Because claim data and characteristics such as dates and type of loss can significantly influence reserve estimation, the auditor should test the completeness, accuracy, and classification of the claim loss data. Chapter 4 and exhibit B-2 in appendix B of the audit guide provide more extensive guidance on auditing the claims cycle. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Evaluating the Reasonableness of the Estimate

Selecting an Audit Approach

.67 SAS No. 57 states that the auditor should obtain an understanding of how management developed the accounting estimates included in the financial statements. The loss reserve estimate is a significant estimate on the financial statements of an insurance entity. Accordingly, regardless of the approach used to audit the loss reserve estimate, the auditor should gain an understanding of how management developed the estimate. The auditor should use one or a combination of the following approaches in evaluating the reasonableness of the accounting estimates:

a. Review and test the process used by management to develop the estimate.

b. Develop an independent expectation of the estimate to corroborate the reasonableness of management's estimate.

c. Review subsequent events or transactions occurring prior to completion of fieldwork.

[Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.68 When auditing loss reserve estimates, usually approach *a*, *b*, or a combination of the two is used. Normally, approach *c* alone is insufficient to provide reasonable assurance because claims are usually reported to insurance companies and settled over a period of time extending well beyond a normal opinion date. However, approach *c* may provide additional information concerning the reasonableness of loss reserve estimates, particularly for short-tail lines of business, when used in combination either with approach *a* or *b* or with both. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.69 When planning the audit, the auditor chooses to use either approach *a* or *b*, or a combination of both approaches, depending on his or her expectation of what approach will result in sufficient competent evidential matter in the most cost-effective manner. Either approach can be used and, depending on client circumstances, either approach may be effective. However, when management has not used the services of a loss reserve specialist in developing its loss reserve estimate, approach *a*, reviewing and testing management's process, is not appropriate. In this circumstance, approach *b*, developing an independent expectation, should be used. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Reviewing and Testing the Process Used by Management to Develop the Estimate

.70 The auditor may assess the reasonableness of an accounting estimate by performing procedures to test the process used by management to make the estimate. This approach may be appropriate when loss reserve estimates are recommended by an outside loss reserve specialist and management accepts those recommendations, when loss reserve specialists employed by the company are responsible for recommending the estimates, or when both outside and internal specialists are used. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.71 A company that uses an outside loss reserve specialist to develop loss reserve recommendations may engage the specialist to evaluate only the company's major lines of business or only certain components of the loss reserves. In either circumstance, the auditor should determine whether a different approach is needed for auditing the items not reported on by the loss reserve specialist. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.72 If the auditor reviews and tests the process used by management to develop its estimate, and management's estimate differs significantly from the recommendations developed by its specialists, appropriate procedures should be applied to the factors and assumptions that resulted in the difference between management's estimate and the specialists' recommendations. Such procedures should include discussion with management and its specialists. It is management's responsibility to record its best estimate of loss reserves in the financial statements. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.73 SAS No. 57 identifies the following as procedures the auditor may consider performing when using this approach. Some of the procedures listed

below apply to the process management uses to supply data to the loss reserve specialist, some apply to the process used by the specialist to develop recommendations, some apply to the process used by management to review and evaluate those recommendations, and some apply to the process management uses to translate the specialist's recommendations into the loss reserve estimates recorded in the financial statements.

a. *Identify whether there are controls over the preparation of accounting estimates and supporting data that may be useful in the evaluation.* Controls over the preparation of accounting estimates may include—

- Procedures for selecting independent loss reserve specialists or hiring internal specialists, including procedures for determining that the specialist has the requisite competence in loss reserving, knowledge of the company's types of business, and understanding of the different methods available for calculating loss reserve estimates.
- Procedures for reviewing and evaluating the recommendations of the loss reserve specialist.
- Procedures to ensure that the methods used to calculate the loss reserve estimate are appropriate and sufficient in the circumstances.

Controls over the preparation of supporting data, in addition to those discussed in chapter 4 and exhibit B-2 in appendix B of the audit guide, may include—

- Procedures for verifying that data used by the loss reserve specialist is appropriately summarized and classified from the company's claims data base.
- Procedures for ensuring that data actually used by the loss reserve specialist is complete and accurate.
- Procedures to substantiate and determine the appropriateness of industry or other external data sources used in developing assumptions (for example, data received from involuntary risk pools).

b. *Identify the sources of data and factors that management used in forming the assumptions, and consider whether such data and factors are relevant, reliable, and sufficient for the purpose, based on information gathered in other audit tests.* Sources of data and factors used may include—

- Company historical claims data from its own data bases, including changes and trends in the data.
- Company information on reinsurance levels and changes from prior years' reinsurance programs.
- Data received from involuntary risk pools such as the National Council on Compensation Insurance.
- Industry loss data from published sources.
- Internal company experience or information from published sources concerning recent trends in socioeconomic factors affecting claim payments, such as—

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

— General inflation rates and specific inflation rates for medical costs, wages, automobile repair costs, and the like.

— Judicial decisions assessing liability.

— Judicial decisions regarding noneconomic damages.

— Changes in legislation affecting payment levels and settlement practices.

Consider whether the company's data is sufficient to have adequate statistical credibility (e.g., to allow the "law of large numbers" to work for the company's estimates). Consider whether the types of industry data used in developing assumptions are relevant to the company's book of business, considering policy limits, reinsurance retention, geographic and industry concentrations, and other appropriate factors.

c. *Consider whether there are additional key factors or alternative assumptions about the factors.* Key factors and potential alternative assumptions that might be considered include—

- Changes in the company's experience or trends in loss reporting and settlements. Increases in the speed of the settlement of claims may lead to assumptions that paid development levels will be lower in the future, or may indicate changes in the company's procedures for processing claims that could lead to increased development in the future.
- Divergence in company experience relative to industry experience. Such divergence might later result in company development experience that reduces the divergence or might be indicative of a change in a company's experience with a book of business.
- Changes in a company's practices and procedures relating to recording and settling claims.
- A company's reinsurance programs and changes therein.
- Changes in a company's underwriting practices such as new or increased use of managing general agents.
- New or changed policy forms or coverages.
- Recent catastrophic occurrences.

d. *Evaluate whether the assumptions are consistent with each other, the supporting data, relevant historical data, and industry data.* Assumptions that should be evaluated include not only explicit assumptions but also the assumptions inherent in various loss projection methods.

- Paid loss projection methods assume that a company's historical experience relating to the timeliness of settlement will be predictive of future results.
- Reported (incurred) loss development projection methods assume that a company's experience in estimating case-basis reserves will be repeated in the future.

e. *Analyze historical data used in developing the assumptions to assess whether it is comparable and consistent with data of the period under audit, and consider whether the data is sufficiently reliable for the purpose.* Consider whether the company's past methods of estimating loss reserves have resulted in appropriate estimates and whether current data (for example, current-year development factors) indicate changes from prior experience. Consider how known changes in the company's loss reporting procedures and settlement practices have been factored into the estimate. Consider how changes in reinsurance programs, in the current period and during historical periods, have been factored into management's estimates.

f. *Consider whether changes in the business or industry may cause other factors to become significant to the assumptions.* Consider such changes as—

- New lines of business and classes of business within lines.
- Changes in reinsurance programs.
- Changes in the regulatory environment, such as premium rate rollbacks and regulation.
- Changes in the method of establishing rates and changes in methods of underwriting business.

g. *Review available documentation of the assumptions used in developing the accounting estimates, inquire about any other plans, goals, and objectives of the entity, and consider their relationship to the assumptions.* A company's practices concerning loss settlement, such as a practice of vigorously defending suits or of quickly settling suits, can have a significant effect on a company's loss experience.

h. *Consider using the work of a specialist regarding certain assumptions.* Using the work of a specialist is discussed in SAS No. 73, *Using the Work of a Specialist*, and in paragraphs .98 through .100 of this SOP.

i. *Test the calculations used by management to translate the assumptions and key factors into the accounting estimate.* Consider whether all lines of business and accident years are included in the loss reserve estimate. Consider how reinsurance recoverable, salvage, and subrogation have been included.

[Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Developing an Independent Expectation of the Estimate

.74 Based on his or her understanding of the facts and circumstances, the auditor may independently develop an expectation of the estimate by using other key factors or alternative assumptions about those factors. This approach is required whenever management has not used the services of a loss reserve specialist in developing its loss reserve estimate and may be appropriate to assist the auditor in assessing the variability of the loss reserve estimates, even when management does use a loss reserve specialist. The auditor frequently develops independent projections because this method may result in a more cost-effective method of obtaining sufficient competent evidential matter. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.75 When this approach is used, the auditor should use an outside loss reserve specialist (the auditor may also be a loss reserve specialist) to develop the independent expectation of the loss reserve estimate. The use of a specialist is discussed in paragraphs .98 through .100 of this SOP. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Analytical Procedures

.76 Various analytical procedures may be used in the evaluation of loss reserve trends and data, such as the analysis of—

- Loss ratios.
- Loss frequency and severity statistics.
- Claim cost by exposure units.
- Adequacy/redundancy of prior year reserves.
- Average case reserves.
- Claim closure rates.
- Paid to incurred ratios.

[Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.77 Such analyses include comparison of trends and data with industry averages or other expectations. Evaluation would normally be performed by line of business and accident or report year. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Loss Reserve Ranges

.78 As stated in SAS No. 57:

> Estimates are based on subjective as well as objective factors and, as a result, judgment is required to estimate an amount at the date of the financial statements. Management's judgment is normally based on its knowledge and experience about past and current events and its assumptions about conditions it expects to exist and courses of action it expects to take.

Accordingly, loss reserves may develop in a number of ways and a reserve for a particular line of business or accident year may prove to be redundant or deficient when analyzed in a following period. Loss reserves considered to be adequate in prior periods may need to be adjusted at a later date as a result of events outside the control of the insurance company that create the need for a change in estimate. Such events include future court decisions and periods of inflation, in which rates may change significantly from period to period and affect the payout of claims. As a result of the circumstances described above, the need to adjust loss reserve estimates in future periods because of future events that are not predictable at the balance sheet date should not be interpreted as evidence of an error or poor loss reserving practices in the past. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.79 Because the ultimate settlement of claims is subject to future events, no single loss reserve estimate can be considered accurate with certainty. An audit approach should address the inherent variability of loss reserve estimates and the effect of that variability on audit risk. The development of a single loss reserve projection, by itself, does not address the concept of variability and may not provide sufficient evidence to evaluate the reasonableness of the loss reserve provision in the financial statements. An analysis of the reasonableness of loss reserve estimates ordinarily should include an analysis of the amount of variability in the estimate. One way to perform this analysis is to consider a range of loss reserve estimates bounded by a high and a low estimate. The high and low ends of the range should not correspond to an absolute best-and-worst-case scenario of ultimate loss settlements, because such estimates may be the result of unlikely assumptions. The range should be realistic and therefore should not include the set of all possible outcomes but instead only those outcomes that are considered reasonable. Extreme projections should be critically analyzed and, if appropriate, be adjusted, given less credence, or discarded (this would apply to projections outside a cluster of other logical projections that fall within a narrower range). [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.80 Another way to address the variability of the loss reserve estimate is to develop a best estimate and to supplement it with qualitative analysis that addresses the variability of the estimate. Qualitative analysis involves consideration of the factors affecting the variability of loss reserves and integrating such factors into a determination of the range of reasonable estimates around a best estimate. Such factors, among others, include the mix of products underwritten, losses incurred by the insurance industry for similar coverages and underwriting years, and the correlation between past and current business written. In any analysis, a thorough working knowledge of the risk factors is a prerequisite to setting a realistic range. Whether the auditor prepares a formal reserve range or a selected estimate, factors affecting the variability of the recorded loss reserve should be considered. The audit procedures performed for this purpose will vary based on the characteristics of the business, the controls the company uses to monitor such variability, and other audit procedures used. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.81 The size of the loss reserve range will vary by line of business. For example, automobile physical damage claims may be estimated with greater precision than product liability claims. In extreme cases, the top-to-bottom range could extend to 50 percent and upward of the amount provided. An example of an extreme case might be a newly formed company that writes primarily volatile types of business. The results of operations in such a situation are sensitive to future fluctuations since the loss reserve estimate is based primarily on assumptions that will undoubtedly change over time. More important, however, is the strain that any extremely adverse loss development would place on such a company's surplus. In an opposite extreme case, the top-to-bottom range might only be 5 percent of the amount provided for a company that only writes automobile physical damage coverages. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.82 When evaluating the variability of loss reserves for an entity, the auditor should be aware that variability within an individual risk group or line of business may be mitigated by the variability within other risk groups or lines

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

of business. In other words, it is unlikely that ultimate claim settlements for each line of business will fall at the same end of the range. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Risk Factors and Developing a Range

.83 Because loss reserves represent both reported and unreported claims that have occurred as of the valuation date, the auditor needs to gain an understanding of the company's exposure to risk through the business it writes as well as an understanding of environmental factors that may affect the company's loss development at the valuation date. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.84 Some risk factors existing within the company that may affect the variability of the company's loss reserves are—

- *The frequency and severity of claims associated with a line of business.* Medical malpractice, directors' and officers' liability, and other lines of business that typically produce few claims with large settlement amounts tend to have a high degree of variability.
- *Policy characteristics.* Individual lines of business can be written on different policy forms. For example, loss reserving and its related variability for medical malpractice written on an occurrence basis will differ markedly when the policy is written on a claims-made basis, especially during the early years of conversion from an occurrence to a claims-made basis.
- *Retention levels.* The greater a company's retention level, the more variable the results are likely to be. This increased variability is due to the effect that one or several large losses can have on the overall book of business. For reinsurance assumed, the concepts analogous to retention levels are referred to as attachment points and limits.
- *The mix of a company's business with respect to long-tail liability lines and short-tail property lines.* Typically, loss reserves on business with longer tails exhibit greater variability than on business with shorter tails because events affecting ultimate claim settlements may occur at a later date.

[Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.85 Some external factors that may affect the variability of loss reserves are—

- Catastrophes or major civil disorders.
- Jury awards and social inflation arising from the legal environment in principal states in which a company's risks are underwritten.
- The effect of inflation.

[Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.86 Other risk factors that may affect the variability of loss reserve estimates are described in the Appendix [paragraph .107] of this SOP. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.87 The auditor should obtain an understanding of both internal and external risk factors. This may be accomplished by a review of contracts, inquiries of underwriters, a review of pertinent trade publications, and any other procedures deemed necessary under the circumstances. The auditor should consider these factors in evaluating a reasonable loss reserve range. The best estimate may not necessarily be midway between the highest and lowest estimates in the range, because certain factors (for example, risk retention limits and retrospectively rated contracts) may reduce the variability at one end of the range but not at the other. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.88 When analyzing the variability of loss reserves, the auditor should be aware of potential offsets that may serve to reduce the financial statement effects of misstatements in the recorded loss reserves. Two common examples are ceded reinsurance and retrospectively rated contracts (primary or reinsurance). Such offsets, if material, should be included in an analysis of reserve ranges to quantify the true income statement or balance sheet effect that results from an increase or decrease in loss reserves. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.89 As noted previously in the discussion of internal risk factors and per-risk retention levels, a lower net retention level typically would translate into a lower variability of reserves. In addition, the auditor should consider the workings of all significant reinsurance ceded contracts and the effect that these contracts have on best estimates and high and low points in a range. In considering the effect of reinsurance ceded agreements on loss reserves, the auditor should also consider the effect on ceded reinsurance premiums. See paragraphs .104 through .106 of this SOP for a discussion of the effects of ceded reinsurance on loss reserve estimates. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.90 A retrospectively rated feature in an insurance contract means that increases or decreases in incurred losses may be wholly or partially offset by changes to earned but unbilled premiums. As a result of such a clause, an increase in loss reserves may lead to a receivable for additional premiums while a decrease in loss reserves may be offset by a reduction in premiums. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Evaluating the Financial Effect of a Reserve Range

.91 To determine the amount of variability that is significant to the financial statements, the financial leverage of a company should be analyzed. Financial leverage refers to items such as reserve-to-surplus ratios. The financial position of a company with a 2-to-1 reserve-to-surplus ratio is less affected by variability in its loss reserves than is a company operating at a 4-to-1 ratio. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.92 Additionally, an analysis comparing the difference between recorded loss reserves and the high and low ends of a range with key financial statement balances, such as surplus or recorded loss reserves, might be performed. Combining financial leverage with other materiality factors pertinent to the

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

company (for example, loan covenant agreements) may provide insights into the amount of variability that is acceptable to the auditor. Because of the imprecise nature of estimating loss reserves, the acceptable range of loss reserve estimates will generally be higher than that of a more tangible balance such as accounts receivable or payable. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.93 According to SAS No. 47, "If the auditor believes the estimated amount included in the financial statements is unreasonable, he should treat the difference between the estimate and the closest reasonable estimate as a likely misstatement and aggregate it with other likely misstatements." Therefore, if the recorded loss reserve is outside the realistic range, the difference between the recorded reserve and the nearer end of the realistic reserve range should be treated as an audit difference. This audit difference should be considered with any other audit differences to evaluate the materiality of the effects on the financial statements. If the difference is deemed material, the auditor should first ask management for additional information that may have been overlooked in the original evaluation. Then, if still necessary, the auditor should attempt to persuade management to make an appropriate adjustment. If management does not make an appropriate adjustment, the auditor should consider modifying his or her report on the financial statements. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.94 SAS No. 47 also states, "Since no one accounting estimate can be considered accurate with certainty, the auditor recognizes that a difference between an estimated amount best supported by the audit evidence and the estimated amount included in the financial statements may be reasonable, and such difference would not be considered to be a likely misstatement." Accordingly, if the recorded loss reserve is within the reasonable range developed by the auditor, an audit adjustment may not be appropriate. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.95 The significance of the variability within a realistic reserve range should also be evaluated against the financial statements. If the difference between the company's recorded reserve and the farther end of the reserve range is deemed significant, the auditor should consider extending audit procedures to obtain additional evidential matter relating to the reserve estimate. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.96 Management must select a single loss reserve estimate that represents its judgment about the most likely circumstances and events. If management develops a reasonable range, the amount recorded should be the best estimate within that range. The auditor should obtain an understanding of the process used by management in arriving at this estimate. In determining the reasonableness of loss reserves, the auditor also should consider the consistency of reserve estimates and any changes in the degree of conservatism of recorded reserves. A change in the degree of conservatism of management's estimate may be indicative of a change in management's reserve process. SAS No. 32, *Adequacy of Disclosure in Financial Statements*, discusses the auditor's responsibility to consider whether the financial statements include adequate disclosure of material matters in light of the circumstances and facts of which the auditor is aware. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Auditor Uncertainty About the Reasonableness of Management's Estimate and Reporting Implications

.97 Ordinarily, the auditor would look to historical data to obtain evidential matter that will provide reasonable assurance that management's estimate of loss reserves is reasonable in the circumstances. Such historical data may not currently exist for certain new companies, for companies writing significant amounts of new lines of business, or for companies with a low volume of claims. When the historical data is not sufficient to resolve uncertainty about the reasonableness of management's estimate of loss reserves and the auditor is unable to resolve that uncertainty through other means, the auditor should consider whether management has adequately disclosed the uncertainty in the notes to the financial statements as required by FASB Statement No. 5, *Accounting for Contingencies*, and paragraphs 4 and 6 of FASB Interpretation No. 14, *Reasonable Estimation of the Amount of a Loss*, and SOP 94-6. A matter involving an uncertainty is one that is expected to be resolved at a future date at which time conclusive evidential matter concerning its outcome would be expected to become available. Conclusive evidential matter concerning the ultimate outcome of uncertainties cannot be expected to exist at the time of the audit because the outcome and related evidential matter are prospective. In these circumstances, management is responsible for estimating the effect of future events on the financial statements, or determining that a reasonable estimate cannot be made and making the required disclosures, all in accordance with GAAP, based on management's analysis of existing conditions. Absence of the existence of information related to the outcome of an uncertainty does not necessarily lead to a conclusion that the evidential matter supporting management's assertion is not sufficient. Rather, the auditor's judgment regarding the sufficiency of the evidential matter is based on the evidential matter that is, or should be, available. If, after considering the existing conditions and available evidence, the auditor concludes that sufficient evidential matter supports management's assertion about the nature of a matter involving an uncertainty and its presentation or disclosure in the financial statements, an unqualified opinion ordinarily is appropriate. If the auditor is unable to obtain sufficient evidential matter to support management's assertions about the nature of a matter involving an uncertainty and its presentation or disclosure in the financial statements, the auditor should consider the need to express a qualified opinion or to disclaim an opinion because of a scope limitation. A qualification or disclaimer of opinion because of a scope limitation is appropriate if sufficient evidential matter related to an uncertainty does or did exist but was not available to the auditor for reasons such as management's record retention policies or a restriction imposed by management. [Paragraph renumbered and revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Use of Specialists by Auditors in Evaluating Loss Reserves

.98 It is the auditor's responsibility to evaluate the reasonableness of the loss reserve established by management. The procedures that the auditor should consider in evaluating the reasonableness of the loss reserve are described in SAS No. 57. One of the procedures the auditor may consider in evaluating the reasonableness of the loss reserve is using the work of a special-

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

ist. SAS No. 73 provides guidance to the auditor who uses the work of a specialist in performing an audit of financial statements. It states that the auditor is not expected to have the expertise of a person trained for or qualified to engage in the practice of another profession or occupation. The Statement also states that the auditor should evaluate the relationship of the specialist to the client, including circumstances that might impair the specialist's objectivity. When a specialist does not have a relationship with the client, the specialist's work usually will provide the auditor with greater assurance of reliability. Although SAS No. 73 does not preclude the auditor from using the work of a specialist who is related to the client, because of the significance of loss reserves to the financial statements of insurance companies and the complexity and subjectivity involved in making loss reserve estimates, the audit of loss reserves requires the use of an outside loss reserve specialist, that is, a specialist who is not an employee or officer of the company. The term *loss reserve specialist* is defined in paragraphs .44 and .45 of this SOP. When the auditor has the requisite knowledge and experience in loss reserving, the auditor may serve as the loss reserve specialist. If the auditor does not possess the level of competence in loss reserving to qualify as a loss reserve specialist, the auditor should use the work of an outside specialist. [Paragraph renumbered and revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.99 In accordance with SAS No. 73, whenever the auditor uses the work of a specialist, the auditor should fulfill certain fundamental requirements. The auditor should satisfy himself or herself concerning the professional qualifications and reputation of the specialist by inquiry or other procedures. The auditor also should consider the relationship, if any, of the specialist to the client. An understanding should be established between the auditor, the client, and the specialist as to the scope and nature of the work to be performed by the specialist and the form and content of the specialist's report. The auditor has the responsibility to obtain an understanding of the methods or assumptions used by the specialist to determine whether the findings of the specialist are suitable for corroborating representations in the financial statements. These responsibilities apply to all the situations described in paragraph .100. [Paragraph renumbered and revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.100 The following are descriptions of situations involving the presence or absence of a loss reserve specialist in management's determination of loss reserves and the recommended response by the auditor in each situation.

Situation 1—The company has no loss reserve specialist involved in the determination of loss reserves.

Auditor response to situation 1—As stated in paragraph .47, this situation may constitute a reportable condition and possibly a material weakness in the internal control. The auditor should use an outside loss reserve specialist to develop an independent expectation of the loss reserve estimate recorded by the company.

Situation 2—The company has an in-house loss reserve specialist who is involved in the determination of loss reserves and the company does not use an outside loss reserve specialist.

Auditor response to situation 2—The auditor would be required to use an outside loss reserve specialist to evaluate the reasonableness of the company's loss reserve estimate.

Situation 3—The company has no in-house specialist but involves an outside loss reserve specialist in the determination of loss reserves.

Auditor response to situation 3—The auditor should evaluate the relationship, if any, of the specialist to the company. If the specialist is related to the client, the auditor should perform additional procedures with respect to some or all of the specialist's assumptions, methods, or findings to determine that the findings are not unreasonable or should use an outside specialist for that purpose.

Situation 4—The company involves an in-house loss reserve specialist in the determination of loss reserves and involves an outside loss reserve specialist to separately review the loss reserves.

Auditor response to situation 4—The auditor could use the separate review performed by the outside loss reserve specialist.

[Paragraph renumbered and revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Evaluating the Reasonableness of Loss Adjustment Expense Reserves

.101 Evaluation of the reasonableness of LAE reserves involves many of the same skills that are needed to evaluate the reasonableness of loss reserves; therefore, such an evaluation ordinarily requires the use of an outside loss reserve specialist. Frequently, both ALAE reserves and ULAE reserves are calculated based on formulas related to paid losses; therefore, in conjunction with the audit of loss adjustment expenses, the auditor should perform sufficient procedures to obtain assurance about the reliability of the paid-loss data. Although ALAE and ULAE frequently are calculated using formulas based on paid losses, they are calculated differently; accordingly, different procedures are used in the evaluation of these two types of reserves. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.102 In most circumstances, a development test cannot be used as a test of the reasonableness of the ULAE reserve. The reasonableness of the ULAE reserve is primarily dependent on the application of sound techniques of cost accounting and expense allocation. The basis of this allocation should be reviewed by the auditor because the way that the company allocates its expenses will have an effect on the ULAE reserve calculation. This review should focus on the allocation of costs to the loss adjustment classification as well as the allocation within that classification to the individual lines of business. [Paragraph renumbered, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Ceded Reinsurance Receivable

.103 This section discusses certain concepts and procedures that the auditor should be aware of to make a proper evaluation of the reasonableness of reinsurance receivable. This section does not address the following items, which are discussed in detail in the audit guide. Reference should be made to the audit guide for information about—

- The purpose and nature of reinsurance.
- Forms and types of reinsurance.
- Generally accepted accounting practices for reinsurance transactions.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- Internal control structure considerations relating to ceded and assumed reinsurance and a description of audit procedures to verify the integrity of recorded transaction data pursuant to such agreements.

[Paragraph renumbered and revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Understanding an Insurance Company's Reinsurance Program

.104 The audit guide recommends that the auditor obtain an understanding of an insurance company's reinsurance program to properly perform audit procedures to verify the accuracy and completeness of recorded cessions and assess the ability of reinsurers to meet their financial obligations under such agreements. This understanding is also essential to properly evaluate the reasonableness of reinsurance receivable balances. The scope of this understanding should not be limited to the reinsurance program currently in effect but should also include reinsurance program(s) in effect during historical periods from which loss experience will be used to project current year net ultimate losses and reinsurance recoveries. [Paragraph renumbered and revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.105 Net loss development patterns will vary to the extent that current reinsurance arrangements (coverages, levels of retention, and type and form of reinsurance) differ from arrangements in effect during the claim experience period used to project losses. Accordingly, the effect of such differences on reinsurance receivables will need to be carefully assessed by the auditor. The level of complexity involved in making this assessment is largely dependent on the types of reinsurance used and the amount of experience available under the program. [Paragraph renumbered and revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.106 Special difficulties arise in estimating reinsurance receivable on excess of loss reinsurance arrangements in which claim frequency is sporadic, retention levels have changed, and aggregate excess of loss arrangements is used. Estimates of reinsurance receivables are generally easiest for primary coverages (first dollar coverage of either property or casualty business). Additionally, relying on expected loss ratios as a guide for estimating recoveries on excess reinsurance arrangements will not be very helpful if the pricing of such arrangements has varied from year to year with little correlation to the underlying economics of these agreements. Some companies separately project reinsurance receivable on IBNR by stratifying the data base by size of loss. [Paragraph renumbered and revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Appendix

Inherent and Control Risk Factors Affecting Loss Reserves

This Appendix describes various factors that may affect the auditor's assessment of inherent and control risk when auditing insurance entities' loss reserves.

Factors Affecting Inherent Risk

- A company's product mix may have a significant effect on the variability of loss reserves. It is more difficult to estimate loss reserves for long-tail lines of business than it is to estimate reserves for short-tail lines of business because events affecting ultimate claim settlement amounts will occur at a later date.
- New products or new types of risks generally will add to the subjectivity of the loss reserving process because of the company's lack of experience with the new product and relative lack of relevant historical data.
- Deductibles, policy limits, and the retention level of specific lines of business may have a significant effect on the volatility of losses to be settled.
- Policy lines with a low frequency and high severity of claim settlements may exhibit more variability than policy lines associated with a high frequency and low severity of claim settlements.
- Future inflation may result in ultimate loss settlements different from the amounts originally anticipated.
- Social inflation, which arises from the legal environment, as well as recent jury awards have the potential to increase ultimate loss settlements.
- The level and consistency of backlogs in processing claims affect the stability of loss reserve analyses.
- The degree of management's optimism or skepticism when establishing loss reserve assumptions may lead to fluctuations in reserves.
- The introduction of new policy forms may result in an unanticipated expansion of coverage. In addition, the company may lack historical data for losses under the new policy forms.
- Changes in regulations may cause insurance companies to change their claims adjusting practices; for example, a change in regulations may require an increase in the waiting period before workers' compensation benefits begin, or "bad faith" claim settlement laws may alter settlement practices.
- Catastrophic or unusual losses may distort historical experience. Reserves for catastrophic losses, particularly losses that occur near the end of the period, are difficult to estimate.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- Insurance company cash flow considerations may result in a change in loss payment practices.

Factors Affecting Control Risk

- The quality and experience of personnel reviewing a company's loss reserves affect the overall control environment. For example, a company that employs a qualified actuary or an experienced loss reserve specialist to review reserves is usually better equipped to estimate loss reserves than is a company that uses a less qualified individual to perform that task.
- The proper functioning of controls over claim processing will reduce the possibility of error in the data underlying loss reserve estimates. The risk of error in the claims data base will be minimized if controls are functioning as designed.
- The completeness and accuracy of a company's data base will affect the risk of misstatement in assertions about loss reserves.
- The accuracy and reliability of claims data received from outside sources (cedants, reinsurers, voluntary and involuntary risk pools, etc.) will also affect the risk of misstatement in assertions about loss reserves.
- The adequacy of information and data produced by a company is critical in projecting loss reserves. For example, a company capable of accumulating only basic data on premium and loss experience generally poses a greater risk, all other things being equal, than does a company that is capable of accumulating and analyzing more sophisticated data.
- Significant decentralization of operations and reliance on intermediaries may increase control risk.
- A high level of delegation of claims processing or adjusting functions to intermediaries or outside adjusters, without adequate supervision, may result in inefficient claim handling and inappropriate case reserve estimates.
- Changes in delegated responsibilities may result in changes in claims settlement patterns and thereby invalidate historical claim experience.
- The quality of a company's underwriting and claims staff and its knowledge of the industry and control over the company's exposure to loss will have a significant effect on the loss reserving process.
- Existing manual or computerized systems may not be able to cope with a change in the volume of claims.
- Changes in the insurance company's claims processing system may invalidate the historical data used to develop and evaluate loss reserves. Types of changes that may have this result include—
  - — Changes in claim classification, such as counting claimants instead of counting claims, considering reopened claims as IBNR claims rather than as development on reported claims, and changing the definition of claims closed without payment.

- Changes in settlement patterns, such as slowing down the payment of claims to increase the holding period of investable assets or speeding up the payment of claims to decrease the effects of inflation.
- Changes in case reserving methodologies, either explicit or implicit, such as a change from estimating case basis reserves on an ultimate cost basis to estimating case-basis reserves on a current cost basis.
- Changes in computerized information systems that result in faster or slower recognition and payment of claims.

[Paragraph renumbered and revised, April 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Auditing Insurance Entities' Loss Reserves Task Force

RUBEN D. NAVA, *Chairman*
RICHARD W. BEUTER
ROD P. FARRELL
THOMAS W. GENRICH
R. LARRY JOHNSON
STEPHEN P. LOWE
PETER R. PORRINO
BOB W. TICE

DAN M. GUY
Vice President, Auditing
JUDITH M. SHERINSKY
Technical Manager
Auditing Standards

Insurance Companies Committee (1990-1991)

JOHN T. BAILY, *Chairman*
SHIRLEY L. ABEL
EDWARD F. BADER
WILLIAM J. BAWDEN
ANTHONY R. BIELE
HOWARD E. DALTON
FREDERICK W. DEICHMANN
JOSEPH HEATH FITZSIMMONS
WILLIAM C. FREDA
ROBERT W. GRANOW
R. LARRY JOHNSON
WAYNE KAUTH
DAVID DEWAYNE REAL
GARY W. ROUBINEK
FREDRICKA TAUBITZ

Also, the contributions of Arnold Brousell and Carolyn Monchelli are greatly appreciated.

[The next page is 30,761.]

Section 14,250

Statement of Position 92-8 Auditing Property/Casualty Insurance Entities' Statutory Financial Statements—Applying Certain Requirements of the NAIC Annual Statement Instructions

October, 1992

NOTE

This Statement of Position presents the recommendations of the Insurance Companies Committee regarding the audit of property/casualty insurance entities' statutory financial statements in applying certain requirements of the National Association of Insurance Commissioners' (NAIC's) Annual Statement Instructions. It has been reviewed by the chairman of the Auditing Standards Board for consistency with auditing standards. AICPA members may have to justify departures from the recommendations in this Statement of Position if their work is challenged.

Applicability

.01 This statement of position (SOP) provides guidance on the impact of certain requirements of the National Association of Insurance Commissioners' (NAIC's) Annual Statement Instructions—Property and Casualty on the auditor's procedures in the audit of statutory financial statements of property/casualty insurance entities.

Introduction

.02 The NAIC's Annual Statement Instructions direct property/casualty insurers to require their independent certified public accountants to subject the current Schedule P-Part 1 (excluding those amounts related to bulk and incurred-but-not-reported [IBNR] reserves and claim counts) to the auditing procedures applied in the audit of the current statutory financial statements to determine whether Schedule P-Part 1 is fairly stated in all material respects in relation to the basic statutory financial statements taken as a whole. Schedule P-Part 1 includes Part 1-Summary and Part 1A-1R.

.03 Although no separate report on Schedule P-Part 1 is required by the NAIC, the auditor should consider the provisions of SAS No. 29, *Reporting on Information Accompanying the Basic Financial Statements in Auditor-Submitted Documents*, and the provisions of this SOP. However, the requirements of this SOP do not preclude an auditor from issuing a report similar to that illustrated in paragraph 12 of SAS No. 29.

Auditing Procedures

.04 Certain of the information in Schedule P-Part 1 is typically subjected to auditing procedures applied in the audit of the basic statutory financial state-

ments (for example, premiums earned and losses paid). Other information not directly related to the basic statutory financial statements is also presented (for example, lines of business classifications for immaterial lines). Although such information may not have been subjected to auditing procedures applied in the audit of the basic statutory financial statements in all instances, such information may have been derived from accounting records that have been tested by the auditor.

.05 Paragraph 7 of SAS No. 29 states that although an auditor is not required by generally accepted auditing standards to apply auditing procedures to information presented outside of the basic financial statements, he or she may choose to modify or redirect certain of the procedures to be applied in the audit of the basic financial statements.

.06 In applying auditing procedures to the information presented in Schedule P-Part 1, the guidance about auditing the claims data base in paragraphs 4.1 and 4.2 of AICPA's SOP 92-4, *Auditing Insurance Entities' Loss Reserves* [section 14,230.61 and .62], applies. The auditor should also refer to chapter 4 and exhibit B-2 in appendix B of the AICPA Audit and Accounting Guide *Audits of Property and Liability Insurance Companies*.

.07 As stated in paragraph 4.2 of SOP 92-4 [section 14,230.62], because claim data and characteristics such as dates and types of loss can significantly influence reserve estimation, the auditor should test the completeness, reliability, and classification of the claim loss and loss expense data during the audit of the statutory financial statements. In extending those procedures to Schedule P-Part 1, the auditor should determine that—

a. The data presented on Schedule P-Part 1 is properly reconciled to the statistical records of the company.

b. Changes between the prior-year and current-year Schedule P-Part 1 are properly reconciled to the current-year audited statutory financial statements.

c. The source of the data for the auditing procedures applied to the claim loss and loss adjustment expense data during the current calendar year (for example, tests of payments on claims for all accident years that were paid during the current calendar year) is the same as (or reconciles to) the statistical records that support the data presented on Schedule P-Part 1.

.08 If, as a result of the procedures performed during the audit of the statutory financial statements, the auditor becomes aware that Schedule P-Part 1 is not fairly stated in relation to the financial statements taken as a whole, the auditor should communicate to the company's management and the opining actuary that Schedule P-Part 1 is not fairly stated and should describe the misstatement. If the company will not agree to revise Schedule P-Part 1, the auditor should issue a report on Schedule P-Part 1 and should include a description of the misstatement in that report. (The auditor should refer to SAS No. 29 when a report will be issued.) The auditor should consider the impact of a misstatement in Schedule P-Part 1 on the auditor's report on the statutory financial statements.

Effective Date

.09 This SOP is effective for audits of statutory-basis financial statements of property/casualty insurance entities for periods ending after December 15, 1992.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Insurance Companies Committee (1991-1992)

JOHN T. BAILY, *Chairman*
SHIRLEY L. ABEL
EDWARD F. BADER
RICHARD H. BERTHOLDT
ANTHONY R. BIELE
HOWARD E. DALTON
FREDERICK W. DEICHMANN
J. HEATH FITZSIMMONS
WILLIAM C. FREDA
ROBERT W. GRANOW
WAYNE R. HUNEKE
R. LARRY JOHNSON
PETER E. JOKIEL
JOHN W. MCCULLOUGH
GARY W. ROUBINEK
BRUCE E. SCHOWENGERDT
FREDRICKA TAUBITZ

AICPA Staff

DAN M. GUY
Vice President
Auditing Standards

ELLISE G. KONIGSBERG
Technical Manager
Accounting Standards

[The next page is 30,941.]

Section 14,270

Statement of Position 93-5 Reporting on Required Supplementary Information Accompanying Compiled or Reviewed Financial Statements of Common Interest Realty Associations

April 23, 1993

NOTE

This Statement of Position presents the recommendations of the AICPA Accounting and Review Services Committee on the application of Statements on Standards for Accounting and Review Services to compilations and reviews of financial statements of common interest realty associations. It has been reviewed by the chairman of the Accounting and Review Services Committee for consistency with existing compilation and review standards. AICPA members should be prepared to justify departures from the recommendations in this Statement of Position.

.01 The American Institute of Certified Public Accountants (AICPA) has issued the Audit and Accounting Guide *Common Interest Realty Associations* (the CIRA guide), which requires common interest realty associations (CIRAs) to disclose certain supplementary information outside the basic financial statements. This requirement also applies to nonpublic CIRAs whose financial statements are compiled or reviewed in accordance with Statements on Standards for Accounting and Review Services (SSARSs). Paragraph 43 of SSARS 1, *Compilation and Review of Financial Statements*, describes the accountant's responsibility when the financial statements are accompanied by information voluntarily presented for supplementary analysis purposes; however, SSARSs do not address the accountant's responsibility when the financial statements are accompanied by required supplementary information. This statement of position (SOP) amends chapter 8, "Review and Compilation Engagements," of the CIRA guide by providing accountants with performance and reporting guidance when required supplementary information accompanies the basic financial statements in a compilation or review engagement.

.02 Paragraph 4.31 of the CIRA guide describes the required supplementary information that should accompany the basic financial statements. That information consists of—

- Estimates of current or future costs of future major repairs and replacements of all existing components, such as roofs, including estimated amounts required, methods used to determine the costs, the basis for calculations (including assumptions, if any, about interest and inflation rates), sources used, and the dates of studies made for this purpose, if any.[1]

[1] There is no requirement for CIRAs to obtain studies prepared by professional engineers. Estimates made by the board of directors or estimates obtained from licensed contractors are satisfactory, as discussed in paragraphs 3.06 and 3.07 of the CIRA guide, *Common Interest Realty Associations*.

- A presentation of components to be repaired and replaced, estimates of the remaining useful lives of those components, estimates of current or future replacement costs, and amounts of funds accumulated for each to the extent designated by the board.

.03 When the basic financial statements have been compiled or reviewed, the required supplementary information accompanying the basic financial statements should, at a minimum, be compiled. If the entity chooses to omit the required supplementary information, the guidance in paragraph .06 should be followed. To compile the required supplementary information, the accountant should—

a. Establish an understanding with the entity regarding the services the accountant will perform with respect to the required supplementary information and how that information will affect the report the accountant expects to render.

b. Consider what supplementary information is required by the CIRA guide and how that information is to be presented.

c. Obtain an understanding of how the required supplementary information was developed. This understanding ordinarily includes the following:

— The source of the information, for example, engineering reports, estimates obtained from licensed contractors, tables in technical manuals on useful lives

— Whether the required supplementary information is based on current or future replacement costs

— The interest and inflation rates used to determine funding requirements if the information is based on future replacement costs

d. Consider whether it will be necessary to perform other accounting services in order to compile the required supplementary information.

e. Read the required supplementary information and consider whether it appears to be appropriate in form and free from obvious material error.

f. Obtain additional or revised information, if the accountant becomes aware that the required supplementary information is incorrect, incomplete, or otherwise unsatisfactory.

g. If the entity is unable or refuses to provide additional or revised information, consider whether a modification of the standard report is adequate to disclose the deficiency in the measurement or presentation of the required supplementary information. If modification of the standard report is adequate to disclose the deficiency, the accountant should follow the guidance in paragraph .05. If modification of the standard report is not adequate to disclose the deficiency, the accountant should withdraw from the engagement.

.04 When the basic financial statements have been compiled or reviewed and the accompanying required supplementary information has been compiled, the accountant should indicate in the report, or in a separate report, the

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

degree of responsibility he or she is taking for the supplementary information. The report should—

a. Identify the required supplementary information accompanying the financial statements. (Identification may be by descriptive title or page number of the document.)

b. State that the supplementary information is not a required part of the basic financial statements but is supplementary information required by the AICPA.

c. State that the accountant has compiled the accompanying supplementary information from information that is the representation of management, without audit or review.

d. State that the accountant does not express an opinion or any other form of assurance on the supplementary information.

An example of an additional paragraph that may be added to a compilation report follows:

> The [*identify the supplementary information*] on page XX is not a required part of the basic financial statements but is supplementary information required by the American Institute of Certified Public Accountants. We (I) have compiled [*identify the supplementary information*] from information that is the representation of management of XYZ Company, without audit or review. Accordingly, we (I) do not express an opinion or any other form of assurance on the supplementary information.

.05 If, on the basis of facts known to him or her, the accountant becomes aware that the supplementary information has not been measured or presented in accordance with prescribed guidelines, the accountant should indicate in his or her report that the information does not conform to the guidelines and should describe the nature of any material departure(s). An example of a sentence that might be added to the illustrative paragraph presented in paragraph .04 follows:

> However, we (I) did become aware that the supplementary information about future major repairs and replacements of common property is not presented in conformity with the guidelines established by the American Institute of Certified Public Accountants because [*describe the material departure from the AICPA guidelines*].

.06 When the compiled or reviewed financial statements are not accompanied by the required supplementary information, a paragraph should be added to the compilation or review report indicating that the required supplementary information has been omitted. The accountant need not present the supplementary information in the accountant's report. The following is an example of a paragraph that the accountant might use in these circumstances:

> The American Institute of Certified Public Accountants has determined that supplementary information about future major repairs and replacements of common property is required to supplement, but not required to be a part of, the basic financial statements. The Association has not presented this supplementary information.

.07 In an engagement to review the basic financial statements, the required supplementary information is not subjected to the inquiry and analytical procedures applied in the review of the basic financial statements; therefore,

SSARSs are not applicable to the review of this information. If the accountant has been engaged to review the required supplementary information, he or she may do so in accordance with Statement on Standards for Attestation Engagements No. 1, *Attestation Standards*.

Effective Date

.08 This SOP is effective for compilations and reviews of financial statements for periods ending on or after December 15, 1993. Earlier application is encouraged.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Accounting and Review Services Committee (1992-1993)

JOHN C. COMPTON, *Chairman*
HEIDI M. BARRINGER
CASSANDRA A. CAMP
D. RONALD DAVIS
J. LARRY GRIFFITH
DON PALLAIS
O. RAY WHITTINGTON

AICPA Staff

DAN M. GUY
Vice President
Auditing Standards
ALAN J. WINTERS
Director
Audit Research
JUDITH M. SHERINSKY
Technical Manager
Auditing Standards

[The next page is 30,951.]

Section 14,280

Statement of Position 93-8 The Auditor's Consideration of Regulatory Risk-Based Capital for Life Insurance Enterprises

December 29, 1993

NOTE

This Statement of Position presents the recommendations of the AICPA Insurance Companies Committee regarding the application of generally accepted auditing standards to audits of financial statements of insurance enterprises. Members of the AICPA Auditing Standards Board have found the recommendations in this Statement of Position to be consistent with existing standards covered by Rule 202 of the AICPA Code of Professional Conduct. AICPA members should be prepared to justify departures from the recommendations in this Statement of Position.

Introduction and Scope

.01 Life insurance enterprises operate in a highly regulated environment. The regulation of life insurance enterprises is directed primarily toward safeguarding policyholders' interests and maintaining public confidence in the safety and soundness of the life insurance system. One of the primary tools used by state insurance departments for ensuring that those objectives are being achieved is risk-based capital (RBC).

.02 This Statement of Position (SOP) addresses the auditors' responsibility that arises from the RBC requirements imposed on life insurance enterprises. These RBC requirements affect audits of life insurance enterprises in the following three primary areas:

a. Audit planning

b. Going-concern considerations

c. Other reporting considerations

Overview of Risk-Based Capital

.03 Regulation of life insurance enterprises has historically focused on their capital. The National Association of Insurance Commissioners (NAIC) requires life insurance enterprises to disclose RBC in their statutory filings. The RBC calculation serves as a benchmark for the regulation of life insurance enterprises' solvency by state insurance regulators. RBC requirements set forth dynamic surplus formulas similar to target surplus formulas used by commercial rating agencies. The formulas specify various weighting factors that are applied to financial balances or various levels of activity based on the perceived degree of risk. Such formulas focus on four general types of risk:

a. The risk related to the insurer's assets (asset or default risk)

b. The risk of adverse insurance experience with respect to the insurer's liabilities and obligations (insurance or underwriting risk)

c. The interest rate risk from the insurer's business (asset/liability matching)

d. All other business risks (management, regulatory action, and contingencies)

The amount determined under such formulas is called the authorized control level RBC (ACLC).

.04 RBC requirements establish a framework for linking various levels of regulatory corrective action to the relationship of a life insurance entity's total adjusted capital (TAC) (equal to the sum of statutory capital and surplus and such other items, if any, as the NAIC's RBC instructions[1] may provide) to the calculated ACLC. The levels of regulatory action, the trigger point, and the corrective actions are summarized as follows:

Risk-Based Capital Levels and Corrective Actions

Level	*Trigger*	*Corrective Action*
Company Action Level RBC (CALC)	TAC is less than or equal to 2 × ACLC, or TAC is less than or equal to 2.5 × ACLC with negative trend	The life insurance enterprise must submit a comprehensive plan to the insurance commissioner.
Regulatory Action Level RBC (RALC)	TAC is less than or equal to 1.5 × ACLC, or unsatisfactory RBC Plan	In addition to the action above, the insurance commissioner is required to perform an examination or analysis deemed necessary and issue a *corrective order* specifying corrective actions required.
Authorized Control Level RBC (ACLC)	TAC is less than or equal to 1 × ACLC	In addition to the actions described above, the insurance commissioner is permitted but not required to place the life insurance enterprise under regulatory control.
Mandatory Control Level RBC (MCLC)	TAC is less than or equal to .7 × ACLC	The insurance commissioner is required to place the life insurance enterprise under regulatory control.

[1] The NAIC's RBC instructions may be amended by the NAIC from time to time in accordance with procedures adopted by the NAIC.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.05 Under the RBC requirements, the comprehensive financial plan should—

a. Identify the conditions in the insurer that contribute to the failure to meet the capital requirements.

b. Contain proposals of corrective actions that the insurer intends to take and that would be expected to result in compliance with capital requirements.

c. Provide projections of the insurer's financial results in the current year and at least the four succeeding years, both in the absence of proposed corrective actions and giving effect to the proposed corrective actions.

d. Identify the key assumptions impacting the insurer's projections and the sensitivity of the projections to the assumptions.

e. Identify the quality of, and problems associated with, the insurer's business, including but not limited to its assets, anticipated business growth and associated surplus strain, extraordinary exposure to risk, mix of business, and use of reinsurance in each case, if any.

Audit Planning

.06 The objective of an audit of a life insurance enterprise's financial statements is to express an opinion on whether they present fairly, in all material respects, the enterprise's financial position, results of operations, and cash flows in conformity with generally accepted accounting principles (GAAP). To accomplish that objective, the auditor assesses the risk that the financial statements contain material misstatements and plans and performs audit procedures to provide reasonable assurance that the financial statements are free of material misstatements. Because of the importance of RBC to life insurance enterprises, RBC should be considered in assessing risk and planning the audit. The auditor should ordinarily obtain and review the client's RBC reports and should understand the RBC requirements for preparing such reports and the actual regulations associated with RBC.

Going-Concern Considerations

.07 Statement on Auditing Standards (SAS) No. 59, *The Auditor's Consideration of an Entity's Ability to Continue as a Going Concern*, requires auditors to evaluate, as part of every audit, whether there is substantial doubt about the ability of the entity to continue as a going concern for a reasonable period of time, not to exceed one year beyond the financial statement date. A significant consideration in the auditor's evaluation of a life insurance enterprise's ability to continue as a going concern is whether the enterprise complies with regulatory RBC requirements.[2]

---

[2] Auditors should evaluate a life insurance enterprise's ability to continue as a going concern even if the enterprise meets the minimum RBC standards. There are other conditions and events that may indicate that there could be substantial doubt about a life insurance enterprise's ability to continue as a going concern, such as recurring operating losses, indications of strained liquidity, concerns expressed by regulators, and indications of strained relationships with regulators. However, this SOP discusses only failure to meet RBC standards.

.08 In view of the serious ramifications of noncompliance with regulatory RBC requirements for life insurance enterprises (see paragraph .04), such failure is a condition that indicates that there could be substantial doubt about the entity's ability to continue as a going concern for a reasonable period of time. Accordingly, the auditor should obtain information about management's plans that are intended to mitigate the adverse effects of the noncompliance with regulatory RBC capital requirements or events that gave rise to the condition and assess the likelihood that such plans can be implemented. In evaluating management's plans, the auditor should consider—

a. The life insurance enterprise's existing regulatory capital position.

b. Whether a comprehensive financial plan has been filed and, if so, whether it has been accepted by the regulators.

.09 The auditor should consider the amount of any RBC capital deficiency. In general, the lower the ratio of total adjusted capital to authorized control level RBC, the greater the doubt about the enterprise's ability to continue as a going concern for a reasonable period. The auditor should, however, also assess the likelihood that the life insurance enterprise's regulatory capital position will improve or deteriorate in the next twelve months.

.10 The auditor should also consider the nature or source (asset quality, underwriting, asset/liability matching, or other) of the deficiency. Curing deficiencies from certain sources may be more within the control of the management of the life insurance enterprise than curing deficiencies from other sources.

.11 Furthermore, the auditor should ascertain whether a comprehensive financial plan has been filed and accepted by the commissioner. If the commissioner has accepted the comprehensive financial plan, the auditor should identify those elements of the comprehensive financial plan that are particularly significant to overcoming the adverse effects of the failure to comply with regulatory RBC requirements and should identify and perform auditing procedures to obtain evidential matter about the significant elements. For example, the auditor should consider the adequacy of support regarding an enterprise's ability to obtain additional capital or a planned disposal of assets. When prospective financial information is particularly significant to management's plans, the auditor should request that management provide the information and should consider the adequacy of support for significant assumptions that underlie it. Further, the auditor should identify those elements of the comprehensive financial plan and conditions placed on the life insurance enterprise by the commissioner that are most difficult to achieve and consider the likelihood that the life insurance enterprise will not be able to implement the elements successfully.

.12 If the commissioner has rejected the comprehensive financial plan, the auditor should consider the commissioner's reasons for rejecting it, any revisions proposed by the commissioner to render the comprehensive financial plan satisfactory, management's intentions for revising the comprehensive financial plan, and possible regulatory sanctions. If the commissioner has not yet notified the insurer whether the comprehensive financial plan has been accepted,[3] the auditor should review related communication between the commissioner and the life insurance enterprise and make inquiries of both management and regulatory officials to determine the current status of the

[3] The RBC Requirements require the commissioner to notify the insurer whether the comprehensive financial plan is accepted or is unsatisfactory within sixty days of submission of the plan.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

comprehensive financial plan. If the life insurance enterprise has not filed a financial plan with the commissioner,[4] the auditor should make inquiries of management officials about their comprehensive financial plan and their plans for filing.

.13 After the auditor has evaluated management's plans, the auditor should conclude whether substantial doubt about the life insurance enterprise's ability to continue as a going concern for a reasonable period of time remains or is alleviated. This is often a complex judgment requiring considerable professional experience.

Substantial Doubt Remains

.14 If the auditor concludes that substantial doubt about the life insurance enterprise's ability to continue as a going concern for a reasonable period of time remains, the auditor should (*a*) consider the possible effects on the financial statements and the adequacy of the related disclosures[5] and (*b*) modify his or her report.

Independent Auditor's Reports

.15 The auditor's report should either (*a*) include an explanatory paragraph (following the opinion paragraph) to reflect the auditor's conclusion about the existence of substantial doubt that the entity can continue as a going concern for a reasonable period of time (see paragraph .17) or (*b*) disclaim an opinion (see paragraph .18).

.16 The illustrative auditors' reports in this SOP are presented to assist auditors in drafting their reports under various RBC circumstances. Each illustration intentionally describes the same general fact situation to avoid suggesting that particular facts always lead to a particular form of opinion. The appropriate form of opinion depends on the auditor's judgment as to the severity and most probable outcome of the matter described.

.17 The following is an illustration of an auditor's report (unqualified opinion) on the financial statements of a life insurance enterprise with an explanatory paragraph added because of the existence of substantial doubt about the enterprise's ability to continue as a going concern.

Independent Auditor's Report[6]

To the Board of Directors and Shareholders
ABC Life Company

We have audited the accompanying balance sheets of ABC Life Company as of December 31, 19X2 and 19X1, and the related statements of income, changes in stockholders' equity, and cash flows for the years then ended. These financial

[4] The RBC Requirements require that a comprehensive financial plan be filed with the commissioner within forty-five days of the failure to meet RBC standards.

[5] Auditors of publicly held life insurance enterprises should consider SEC Financial Reporting Release No. 16, *Rescission of Interpretation Relating to Certification of Financial Statements*, which states, ". . . filings containing accountants' reports that are qualified as a result of questions about the entity's continued existence must contain appropriate and prominent disclosure of the registrant's financial difficulties and viable plans to overcome these difficulties."

[6] The circumstances described in the fourth paragraph of this illustrative report represent assumptions made for purposes of illustration only. They are not intended to provide criteria or other guidelines to be used by independent auditors in deciding whether an explanatory paragraph should be added to their reports.

statements are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with generally accepted auditing standards. Those standards require that we plan and perform the audits to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of ABC Life Company as of December 31, 19X2 and 19X1, and the results of its operations and its cash flows for the years then ended in conformity with generally accepted accounting principles.

The accompanying financial statements have been prepared assuming that ABC Life Company will continue as a going concern. As discussed in Note XX to the financial statements, [*State of Domicile's Insurance Regulatory Body*] imposes risk-based capital requirements on life insurance enterprises, including the Company. At December 31, 19X2, the Company's total adjusted capital is at the company action level based on the risk-based capital calculation required by [*State of Domicile's Insurance Regulatory Body*]. The Company has filed a comprehensive financial plan with the commissioner outlining the Company's plans for attaining the required levels of regulatory capital by December 31, 19XX. To date, the Company has not received notification from the commissioner regarding acceptance or rejection of its comprehensive financial plan. Failure to meet the capital requirements and interim capital targets included in the Company's plan would expose the Company to regulatory sanctions that may include restrictions on operations and growth, mandatory asset dispositions, and placing the Company under regulatory control. These matters raise substantial doubt about the ability of ABC Life Company to continue as a going concern. The ability of the Company to continue as a going concern is dependent on many factors, one of which is regulatory action, including ultimate acceptance of the Company's comprehensive financial plan. Management's plans in regard to these matters are described in Note XX. The financial statements do not include any adjustments that might result from the outcome of this uncertainty.

[*Signature*]

[*Date*]

.18 SAS No. 59 states that inclusion of an explanatory paragraph (following the opinion paragraph) in the auditor's report as described above serves adequately to inform users of the financial statements of the auditor's substantial doubt. Nonetheless, SAS No. 59 does not preclude the auditor from declining to express an opinion in cases involving uncertainties. If the auditor disclaims an opinion, the uncertainties and their possible effects should be disclosed in an appropriate manner and the auditor's report should state all of the substantive reasons for the disclaimer of opinion. The following is an illustration of an auditor's report containing a disclaimer of opinion as the result of uncertainties relating to an auditor's substantial doubt about a life insurance enterprise's ability to continue as a going concern for a reasonable period of time.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Independent Auditor's Report[7]

To the Board of Directors and Shareholders
XYZ Life Company

We have audited the accompanying balance sheets of XYZ Life Company as of December 31, 19X2 and 19X1, and the related statements of income, changes in stockholders' equity, and cash flows for the years then ended. These financial statements are the responsibility of the Company's management. Our responsibility is to report on these financial statements based on our audits.

We conducted our audits in accordance with generally accepted auditing standards. Those standards require that we plan and perform the audits to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our report.

The accompanying financial statements have been prepared assuming that XYZ Life Company will continue as a going concern. As discussed in Note XX to the financial statements, [*State of Domicile's Insurance Regulatory Body*] imposes risk-based capital requirements on life insurance enterprises, including the Company. At December 31, 19X2, the Company's total adjusted capital is at the company action level based on the risk-based capital calculation required by [*State of Domicile's Insurance Regulatory Body*]. The Company has filed a comprehensive financial plan with the commissioner outlining its plans for attaining the required levels of regulatory capital by December 31, 19XX. To date, the Company has not received notification from the commissioner regarding acceptance or rejection of its comprehensive financial plan. Failure to meet the capital requirements and interim capital targets included in the Company's plan would expose the Company to regulatory sanctions that may include restrictions on operations and growth, mandatory asset dispositions, and placing the Company under regulatory control. These matters raise substantial doubt about the ability of XYZ Life Company to continue as a going concern. The ability of the Company to continue as a going concern is dependent on many factors, one of which is regulatory action, including ultimate acceptance of the Company's comprehensive financial plan. Management's plans in regard to these matters are described in Note XX. The financial statements do not include any adjustments that might result from the outcome of this uncertainty.

Because of the significance of the uncertainty discussed above, we are unable to express, and we do not express, an opinion on the financial statements for the year ended December 31, 19X2.

In our opinion, the 19X1 financial statements referred to above present fairly, in all material respects, the financial position of XYZ Life Company as of December 31, 19X1, and the results of its operations and its cash flows for the year then ended in conformity with generally accepted accounting principles.

[*Signature*]

[*Date*]

[7] The circumstances described in the third paragraph of this illustrative report represent assumptions made for purposes of illustration only. They are not intended to provide criteria or other guidelines to be used by independent auditors in deciding whether to disclaim an opinion on financial statements.

Substantial Doubt Alleviated

.19 If the auditor concludes that substantial doubt about the life insurance enterprise's ability to continue as a going concern for a reasonable period of time is alleviated, the auditor should consider the adequacy of disclosure in the financial statements of the principal conditions or events that initially raised the substantial doubt. The auditor should follow the guidance in SAS No. 59, paragraphs .10 and .11. Furthermore, the auditor may wish to add an emphasis of matter paragraph to the auditor's report (see paragraphs .27 and .28, below).

Other Reporting Considerations

Uncertainties

.20 A matter involving an uncertainty is one that is expected to be resolved at a future date, at which time conclusive evidential matter concerning its outcome would be expected to become available. Uncertainties include, but are not limited to, contingencies covered by FASB Statement No. 5, *Accounting for Contingencies*, and matters related to estimates covered by SOP 94-6, *Disclosure of Certain Significant Risks and Uncertainties* [section 10,640]. [Paragraph revised, June 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.21 Conclusive evidential matter concerning the ultimate outcome of uncertainties cannot be expected to exist at the time of the audit because the outcome and related evidential matter are prospective. In these circumstances, management is responsible for estimating the effect of future events on the financial statements, or determining that a reasonable estimate cannot be made and making the required disclosures, all in accordance with GAAP, based on management's analysis of existing conditions. An audit includes an assessment of whether the evidential matter is sufficient to support management's analysis. Absence of the existence of information related to the outcome of an uncertainty does not necessarily lead to a conclusion that the evidential matter supporting management's assertion is not sufficient. Rather, the auditor's judgment regarding the sufficiency of the evidential matter is based on the evidential matter that is, or should be, available. If, after considering the existing conditions and available evidence, the auditor concludes that sufficient evidential matter supports management's assertions about the nature of a matter involving an uncertainty and its presentation or disclosure in the financial statements, an unqualified opinion ordinarily is appropriate. [Paragraph added, June 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.22 If the auditor is unable to obtain sufficient evidential matter to support management's assertion about the nature of a matter involving an uncertainty and its presentation or disclosure in the financial statements, the auditor should consider the need to express a qualified opinion or to disclaim an opinion because of a scope limitation. A qualified opinion or disclaimer of opinion because of a scope limitation is appropriate if sufficient evidential matter related to an uncertainty does or did exist but was not available to the auditor for reasons such as management's record retention policies or a restriction imposed by management. [Paragraph added, June 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.23 Scope limitations related to uncertainties should be differentiated from situations in which the auditor concludes that the financial statements are materially misstated due to departures from GAAP related to uncertainties. Such departures may be caused by inadequate disclosure concerning the uncertainty, the use of inappropriate accounting principles, or the use of unreasonable accounting estimates. [Paragraph added, June 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.24 The auditor's decision to add an explanatory paragraph to the auditor's report because of the existence of such an uncertainty that affects the financial statements is one that requires a high degree of professional judgment. Prior to considering whether an explanatory paragraph should be added to the auditor's report because of the existence of a material uncertainty, the auditor should have concluded that substantial doubt about the life insurance enterprise's ability to continue as a going concern does not exist (see paragraphs .07 to .19, above). An explanatory paragraph for a material uncertainty should not be used for situations in which the auditor's uncertainty involves substantial doubt about the ability of the life insurance enterprise to continue as a going concern. [Paragraph renumbered, June 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.25 Because its resolution is prospective, management generally cannot estimate the effect of the uncertainty on the entity's financial statements. Uncertainties should not be confused with future events that generally are susceptible to reasonable estimation by management in preparing financial statements. If the auditor believes that financial statements are materially misstated as a result of the use of inappropriate accounting principles, the auditor should express a qualified or adverse opinion. A scope limitation should result in a qualified opinion or a disclaimer of opinion. [Paragraph renumbered, June 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.26 If the auditor decides to include an explanatory paragraph(s) in the report because of the existence of a material uncertainty that affects the financial statements, the explanatory language should follow the opinion paragraph and should describe the matter giving rise to the uncertainty and indicate that its outcome cannot presently be determined. The explanatory language may be shortened by referring to disclosures made in a note to the financial statements. No reference to the uncertainty should be made in the introductory, scope, or opinion paragraphs of the auditor's report. The following is an illustration of an auditor's report (unqualified opinion) on the financial statements of a life insurance enterprise with an explanatory paragraph because of the existence of a material uncertainty as a result of possible regulatory sanctions.

Independent Auditor's Report[8]

To the Board of Directors and Shareholders
GHI Life Insurance Company

We have audited the accompanying balance sheets of GHI Life Insurance Company as of December 31, 19X2 and 19X1, and the related statements of

[8] The circumstances described in the fourth paragraph of this illustrative report represent assumptions made for purposes of illustration only. They are not intended to provide criteria or other guidelines to be used by independent auditors in deciding whether an explanatory paragraph should be added to their reports.

income, changes in stockholders' equity, and cash flows for the years then ended. These financial statements are the responsibility of the Company's management. Our responsibility is to report on these financial statements based on our audits.

We conducted our audits in accordance with generally accepted auditing standards. Those standards require that we plan and perform the audits to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of GHI Life Insurance Company as of December 31, 19X2 and 19X1, and the results of its operations and its cash flows for the years then ended in conformity with generally accepted accounting principles.

As discussed in Note XX to the financial statements, [*State of Domicile's Insurance Regulatory Body*] imposes risk-based capital requirements on life insurance enterprises, including the Company. At December 31, 19X2, the Company's total adjusted capital is at the company action level based on the risk-based capital calculation required by [*State of Domicile's Insurance Regulatory Body*]. The ultimate outcome of this situation cannot presently be determined. Accordingly, no adjustments that may result from the ultimate resolution of this uncertainty have been made in the accompanying financial statements.

[*Signature*]

[*Date*]

[Paragraph renumbered, June 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Emphasis of a Matter

.27 In some circumstances, the auditor may wish to emphasize a matter regarding the financial statements, but nevertheless intends to express an unqualified opinion. An example of such a circumstance is the failure to comply with regulatory RBC requirements. Prior to considering whether an emphasis of a matter paragraph should be added to the auditor's report for a failure to comply with regulatory RBC requirements, however, the auditor should have concluded that the matter being emphasized does not create substantial doubt about the life insurance enterprise's ability to continue as a going concern (see paragraphs .07 to .19, above) and does not reflect a material uncertainty (see paragraphs .20 to .26, above). [Paragraph renumbered, June 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

.28 Emphasis of a matter should be presented in a separate paragraph of the auditor's report. Phrases such as "with the foregoing explanation" should not be used in the opinion paragraph in situations of this type. The following is an illustration of an unqualified opinion with an emphasis of a matter paragraph regarding the possible effects of a life insurance enterprise's failure to comply with regulatory RBC requirements on its financial statements.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Independent Auditor's Report[9]

To the Board of Directors and Shareholders
DEF Life Company

We have audited the accompanying balance sheets of DEF Life Company as of December 31, 19X2 and 19X1, and the related statements of income, changes in stockholders' equity, and cash flows for the years then ended. These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with generally accepted auditing standards. Those standards require that we plan and perform the audits to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

As discussed in Note XX to the financial statements, [*State of Domicile's Insurance Regulatory Body*] imposes risk-based capital requirements on life insurance enterprises, including the Company. At December 31, 19X2, the Company's total adjusted capital is at the company action level based on the risk-based capital calculation required by [*State of Domicile's Insurance Regulatory Body*].

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of DEF Life Company as of December 31, 19X2 and 19X1, and the results of its operations and its cash flows for the years then ended in conformity with generally accepted accounting principles.

[*Signature*]

[*Date*]

[Paragraph renumbered, June 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Effective Date

.29 This statement of position is effective for audits of life insurance enterprises' financial statements for periods ending after December 15, 1993. [Paragraph renumbered, June 1998, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

[9] The circumstances described in the third paragraph of this illustrative report represent assumptions made for purposes of illustration only. They are not intended to provide criteria or other guidelines to be used by independent auditors in deciding whether an emphasis paragraph should be added to their reports.

Insurance Companies Committee (1992-1993)

GARY W. ROUBINEK, *Chairman*
SHIRLEY L. ABEL
EDWARD F. BADER
RICHARD H. BERTHOLDT
ANTHONY R. BIELE
JOSEPH P. BRANDON
DARREN F. COOK
WILLIAM C. FREDA
ROBERT W. GRANOW
WAYNE R. HUNEKE
R. LARRY JOHNSON
PETER E. JOKIEL
JOHN W. MCCULLOUGH
JAMES L. MORGAN III
JAMES E. TAIT
FREDRICKA TAUBITZ

AICPA Staff

DAN M. GUY
Vice President
Auditing Standards
DIONNE D. MCNAMEE
Senior Technical Manager
Accounting Standards
ARLEEN K. RODDA
Director
Accounting Standards
ROSEMARY REILLY
Technical Manager
Audit and Accounting Guides

[The next page is 30,971.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 14,290

Statement of Position 94-1
Inquiries of State Insurance Regulators

April 20, 1994

NOTE

This Statement of Position (SOP) presents the recommendations of the AICPA Insurance Companies Committee regarding the application of generally accepted auditing standards to audits of financial statements of insurance enterprises. Members of the AICPA Auditing Standards Board have found the recommendations in this SOP to be consistent with existing standards covered by Rule 202 of the AICPA Code of Professional Conduct. AICPA members should be prepared to justify departures from the recommendations in this SOP.

SOP 94-1 is amended by SOP 01-5, *Amendments to Specific AICPA Pronouncements for Changes Related to the NAIC Codification*. SOP 01-5 is effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001.

Introduction

.01 This Statement of Position (SOP) addresses the auditor's consideration of regulatory examinations as a source of evidential matter in conducting an audit of an insurance enterprise's financial statements and the auditor's evaluation of material permitted statutory accounting practices.

Applicability

.02 This SOP applies to audits of financial statements of life insurance enterprises,[1] property and casualty insurance enterprises, title insurance enterprises, mortgage guaranty insurance enterprises, assessment enterprises, fraternal benefit societies, reciprocal or interinsurance exchanges, pools other than public-entity risk pools, syndicates, and captive insurance companies. It amends chapter 2 ("Audit Considerations") of the AICPA Audit and Accounting Guides *Audits of Property and Liability Insurance Companies* and *Life and Health Insurance Entities*.[2] As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.03 The insurance laws and regulations of most states require insurance companies domiciled in those states to comply with the guidance provided in the NAIC *Accounting Practices and Procedures Manual* except as prescribed

---

[1] FASB Interpretation No. 40, *Applicability of Generally Accepted Accounting Principles to Mutual Life Insurance and Other Enterprises*, clarifies that FASB Statements and Interpretations and Accounting Principles Board (APB) Opinions apply to mutual life insurance enterprises, except when specifically exempted, that prepare financial statements in conformity with generally accepted accounting principles. This SOP applies to audits of mutual life insurance enterprises.

[2] [Footnote deleted by the issuance of Statement of Position 01-5, December 2001.]

by state law. In 1999, the NAIC completed a process to codify statutory accounting practices for certain insurance enterprises, resulting in a revised *Accounting Practices and Procedures Manual* (the revised Manual), effective January 1, 2001. It is expected that all states will require insurers to comply with most, if not all, provisions of the revised Manual. Auditors of an insurance enterprise should monitor the status of the adoption of the revised Manual by the various state regulatory authorities. [Paragraph added, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

Auditor's Consideration of State Regulatory Examinations

.04 The auditor should consider evaluating "information contained in regulatory or examination reports, supervisory correspondence, and similar materials from applicable regulatory agencies" (Statement on Auditing Standards [SAS] No. 57, *Auditing Accounting Estimates* [AICPA, *Professional Standards*, vol. 1, AU sec. 342]). The auditor may encounter specific information that may raise a question concerning possible illegal acts, such as . . . violations of laws or regulations cited in reports of examinations by regulatory agencies that have been available to the auditor" (SAS No. 54, *Illegal Acts by Clients* [AICPA, *Professional Standards*, vol. 1, AU sec. 317]). Accordingly, it is appropriate that the auditor review examination reports and related communications between regulators and the insurance enterprise to obtain competent evidential matter. [Paragraph renumbered and amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.05 The auditor should review reports of examinations and communications between regulators and the insurance enterprise and make inquiries of the regulators. The auditor should—

- Request that management provide access to all reports of examinations and related correspondence including correspondence relating to financial conditions.
- Read reports of examinations and related correspondence between regulators and the insurance enterprise during the period under audit through the date of the auditor's report.
- Inquire of management and communicate with the regulators, with the prior approval of the insurance enterprise, when the regulators' examination of the enterprise is in process or a report on an examination has not been received by the insurance enterprise regarding conclusions reached during the examination.

[Paragraph renumbered by the issuance of Statement of Position 01-5, December 2001.]

.06 A refusal by management to allow the auditor to review communications from, or to communicate with, the regulator would ordinarily be a limitation on the scope of the audit sufficient to preclude an unqualified opinion (SAS No. 58, *Reports on Audited Financial Statements* [AICPA *Professional Standards*, vol. 1, AU sec. 508]). A refusal by the regulator to communicate with the auditor may be a limitation on the scope of the audit sufficient to preclude an unqualified opinion, depending on the auditor's assessment of other relevant facts and circumstances. [Paragraph renumbered by the issuance of Statement of Position 01-5, December 2001.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Auditor's Consideration of Permitted Statutory Accounting Practices

.07 Prescribed statutory accounting practices are those practices incorporated directly or by reference in state laws, regulations, and general administrative rules applicable to all insurance enterprises domiciled in a particular state. States may adopt the revised Manual in whole, or in part, as an element of prescribed statutory accounting practices in those states. If, however, the requirements of state laws, regulations, and administrative rules differ from the guidance provided in the revised Manual or subsequent revisions, those state laws, regulations, and administrative rules will take precedence. Auditors of insurance enterprises should review state laws, regulations, and administrative rules to determine the specific prescribed statutory accounting practices applicable in each state. [Paragraph renumbered and amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.08 Permitted statutory accounting practices include practices not prescribed by the domiciliary state, as described in paragraph .07 above, but allowed by the domiciliary state regulatory authority. An insurance enterprise may request permission from the domiciliary state regulatory authority to use a specific accounting practice in the preparation of the enterprise's statutory financial statements (*a*) if it wishes to depart from the prescribed statutory accounting practices, or (*b*) if prescribed statutory accounting practices do not address the accounting for the transaction. Accordingly, permitted accounting practices differ from state to state, may differ from company to company within a state, and may change in the future. [Paragraph renumbered and amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.09 Auditors should exercise care in concluding that an accounting treatment is *permitted*, and should consider the adequacy of disclosures in the financial statements regarding such matters.[3] For each examination, auditors should obtain sufficient competent evidential matter to corroborate management's assertion that permitted statutory accounting practices that are significant to an insurance enterprise's financial statements are permitted by the domiciliary state regulatory authority. [Paragraph renumbered and amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.10 Sufficient competent evidential matter consists of any one or combination of—

- Written acknowledgment sent directly from the regulator to the auditor. (This type of corroboration includes letters similar to attorneys' letters and responses to confirmations.)
- Written acknowledgment prepared by the regulator, but not sent directly to the auditor, such as a letter to the client.
- Direct oral communications between the regulator and the auditor, supported by written memorandum. (If the auditor, rather than the regulator, prepares the memorandum, the auditor should send such memorandum to the regulator to make sure it accurately reflects the communication.)

---

[3] [Footnote deleted by the issuance of Statement of Position 01-5, December 2001.]

Auditors should use judgment to determine the type of corroboration that is necessary in the circumstances. [Paragraph renumbered by the issuance of Statement of Position 01-5, December 2001.]

.11 If the auditor is unable to obtain sufficient competent evidential matter to corroborate management's assertion regarding a permitted statutory accounting practice that is material to the financial statements, the auditor should qualify or disclaim an opinion on the statutory financial statements because of the limitation on the scope of the audit (SAS No. 58 [AU sec. 508]). [Paragraph renumbered by the issuance of Statement of Position 01-5, December 2001.]

Effective Dates

.12 The provisions of this SOP as originally issued in 1994 should be applied to audits of financial statements performed for periods ending on or after December 15, 1994. The amendments to this SOP are effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001. Retroactive application is not permitted. [Paragraph renumbered and amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Insurance Companies Committee (1993–1994)

GARY W. ROUBINEK, *Chairman*
JOSEPH P. BRANDON
ROBERT E. BROATCH
PETER S. BURGESS
DARREN F. COOK
RICHARD DADDARIO
HOWARD E. DALTON
WAYNE R. HUNEKE
PETER E. JOKIEL
JOHN F. MAJORS
JAMES L. MORGAN III
ALBERT J. REZNICEK
PATRICK J. SHOUVLIN
MARY TODD STOCKARD
JAMES E. TAIT

AICPA Staff

DAN M. GUY
Vice President
Auditing Standards
DIONNE D. MCNAMEE
Senior Technical Manager
Accounting Standards
ARLEEN K. RODDA
Director
Accounting Standards

[The next page is 30,991.]

Section 14,300

Statement of Position 95-4 Letters for State Insurance Regulators to Comply With the NAIC Model Audit Rule

November 3, 1995

NOTE

This Statement of Position presents the recommendations of the AICPA Insurance Companies Committee regarding the application of generally accepted auditing standards to audits of financial statements of insurance enterprises. Members of the AICPA Auditing Standards Board have found the recommendations in this Statement of Position to be consistent with existing standards covered by Rule 202 of the AICPA Code of Professional Conduct. AICPA members should be prepared to justify departures from the recommendations in this Statement of Position.

Introduction

.01 This Statement of Position (SOP) provides guidance to auditors on the form and content of communications with state insurance regulators. Such communications are required by the National Association of Insurance Commissioners (NAIC) *Annual Statement Instructions Requiring Annual Audited Financial Statements,* which incorporates the January 1991 *Model Rule (Regulation) Requiring Annual Audited Financial Reports* (reissued in July 1995) (hereinafter called the Model Audit Rule). The Model Audit Rule was designed by the NAIC to promote uniformity in state laws and regulations dealing with audits of insurance enterprises' statutory financial statements. Though some states have laws or regulations that differ from the Model Audit Rule, this SOP addresses only the requirements of the Model Audit Rule.

.02 To the extent that the Model Audit Rule is changed in the future, the illustrations in this SOP may need to be changed to reflect the revised provisions of the Model Audit Rule. For example, at the time of this SOP, the NAIC is in the process of codifying statutory accounting practices for certain insurance enterprises. The *Annual Statement Instructions Requiring Annual Audited Financial Statements* currently requires that statutory financial statements be prepared using accounting practices prescribed or otherwise permitted by the insurance department of the state of domicile. It is expected that when the NAIC completes the codification of statutory accounting practices, the Model Audit Rule will be amended to require auditors to express opinions on statutory financial statements as to their conformity with the newly codified statutory accounting principles rather than as to their conformity with statutory accounting practices prescribed or permitted by the insurance department of the state of domicile.

Scope

.03 This SOP applies to audits of financial statements of all insurance companies that file audited financial statements with state insurance departments in accordance with the NAIC's Model Audit Rule. It amends the American Institute of Certified Public Accountants (AICPA) Audit and Accounting Guide *Audits of Property and Liability Insurance Companies* and the AICPA Industry Audit Guide *Audits of Stock Life Insurance Companies.*[1]

Conclusions—Form and Content

Awareness

.04 Section 6 of the Model Audit Rule requires that the insurer notify the insurance commissioner of the state of domicile of the name and address of the insurer's independent certified public accountant (hereinafter referred to as *auditor*). In connection with that notification, the insurer is required to obtain an awareness letter from its auditor stating that the auditor—

a. Is aware of the provisions of the insurance code and the rules and regulations of the insurance department of the state of domicile that relate to accounting and financial matters.

b. Will issue a report on the financial statements in terms of their conformity to the statutory accounting practices prescribed or otherwise permitted by the insurance department of the state of domicile, specifying exceptions as appropriate.

.05 The following is an illustration of the awareness letter:

To the Board of Directors of ABC Insurance Company:

We have been engaged by ABC Insurance Company (the Company) to perform annual audits in accordance with generally accepted auditing standards of the Company's statutory financial statements. In connection therewith, we acknowledge the following:

We are aware of the provisions relating to the accounting and financial reporting matters in the Insurance Code of [*name of state of domicile*] and the related rules and regulations of the Insurance Department of [*name of state of domicile*] that are applicable to audits of statutory financial statements of insurance enterprises. Also, after completion of our audits, we expect that we will issue our report on the statutory financial statements of ABC Insurance Company as to their conformity with accounting practices prescribed or permitted by the Insurance Department of [*name of state of domicile*].

This letter is intended solely for the information and use of the Insurance Department of [*name of state of domicile*] and other state insurance departments and is not intended to be and should not be used by anyone other than these specified parties.

[Revised, June 1999, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

---

[1] The AICPA has a project under way to prepare an Audit and Accounting Guide *Audits of Life and Health Insurance Entities* which covers audits of mutual life insurance companies as well as stock life insurance companies. The new Audit and Accounting Guide would replace the Industry Audit Guide *Audits of Stock Life Insurance Companies* and would incorporate the guidance in this Statement of Position.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Change in Auditor

.06 Section 6 of the Model Audit Rule requires that insurers notify the insurance department of the state of domicile within five business days of the dismissal or resignation of the auditor for the immediately preceding filed audited statutory financial statements. Within ten business days of that notification, the insurer also is required to provide a separate letter stating whether, in the twenty-four months preceding that event, there were any disagreements, subsequently resolved or not, with the former auditor on any matter of accounting principles or practices, financial statement disclosure, or auditing scope or procedure, which disagreements, if not resolved to the satisfaction of the former auditor, would have caused the auditor to make reference to the subject matter of the disagreement in connection with the auditor's opinion. The Model Audit Rule requires that the insurer provide the insurance department of the state of domicile a letter from the former auditor to the insurer indicating whether the auditor agrees with the statements in the insurer's letter and, if not, stating the reasons for the disagreement.

.07 The following is an illustration of the change in auditor letter:

To the Board of Directors of DEF Insurance Company:

We previously were auditors for DEF Insurance Company and, under the date of [*report date*], we reported on the statutory financial statements of DEF Insurance Company as of and for the years ended December 31, 19X1 and 19X0.[2] Effective [*date of termination*], we are no longer auditors of DEF Insurance Company. We have read DEF Insurance Company's statements in its letter dated [*date of insurer's letter*], which is attached hereto, and we agree with the statements therein. [*However, if the auditor is* (a) *not in a position to agree or disagree or* (b) *does not agree with the insurer's statement, the auditor's letter should state that the auditor is not in a position to agree or disagree or that the auditor does not agree with such statements and give the reasons.*][3]

Qualifications

.08 Section 12 of the Model Audit Rule requires the auditor to provide a letter to the insurer to be included in the annual financial report stating—

a. The auditor is independent with respect to the insurer and conforms with the standards of his or her profession as contained in the Code of Professional Conduct and pronouncements of the AICPA and the Rules of Professional Conduct of the appropriate state board of public accountancy.

b. The background and experience in general and of the individuals used for an engagement and whether each is a certified public accountant.

---

[2] If the auditor had not reported on any financial statements, the first sentence should be modified as follows:

We previously were engaged to audit the statutory financial statements of DEF Insurance Company as of and for the year ending December 31, 19X1.

[3] The insurer's letter may contain a statement, such as—

In connection with the audits of the statutory financial statements of the Company for the years ended December 31, 19X2 and 19X1, and the subsequent interim period through [*date of termination*], there were no disagreements with [*CPA Firm*] on any matter of accounting principles, statutory accounting practices prescribed or permitted by the Insurance Department of [*name of state of domicile*], financial statement disclosure, or auditing scope or procedures, which disagreements if not resolved to their satisfaction would have caused them to make reference to the subject matter of the disagreement in their reports.

c. The auditor understands that the annual audited statutory financial statements and his or her opinion thereon will be filed in compliance with the requirement of the Model Audit Rule and that the domiciliary commissioner will be relying on the information in the monitoring and regulating of the financial position of insurers.

d. The auditor consents to the workpaper requirements contained in the Model Audit Rule and agrees to make the workpapers available for review by the domiciliary commissioner or the commissioner's designee under the auditor's control.[4]

e. The engagement partner is licensed by an appropriate state licensing authority and is a member in good standing of the AICPA.

f. The auditor meets the qualifications and is in compliance with the "Qualifications of Independent Certified Public Accountant" section of the Model Audit Rule.

.09 The following is an illustration of the qualification letter:

To the Board of Directors of GHI Insurance Company:

We have audited, in accordance with generally accepted auditing standards, the statutory financial statements of GHI Insurance Company (the Company) for the years ended December 31, 19X1 and 19X0, and have issued our report thereon dated [*date of report*]. In connection therewith, we advise you as follows:

a. We are independent certified public accountants with respect to the Company and conform to the standards of the accounting profession as contained in the Code of Professional Conduct and pronouncements of the American Institute of Certified Public Accountants, and the Rules of Professional Conduct of the [*state*] Board of Public Accountancy.

b. The engagement partner and engagement manager, who are certified public accountants, have [ ] years and [ ] years, respectively, of experience in public accounting and are experienced in auditing insurance enterprises. Members of the engagement team, most (some) of whom have had experience in auditing insurance enterprises and [*X*] percent of whom are certified public accountants, were assigned to perform tasks commensurate with their training and experience.

c. We understand that the Company intends to file its audited statutory financial statements and our report thereon with the Insurance Department of [*name of state of domicile*] and other state insurance departments in states in which the Company is licensed and that the insurance commissioners of those states will be relying on that information in monitoring and regulating the statutory financial condition of the Company.

While we understand that an objective of issuing a report on the statutory financial statements is to satisfy regulatory requirements, our audit was not planned to satisfy all objectives or responsibilities of insurance regulators. In this context, the Company and insurance commissioners should understand that the objective of an audit of statutory financial statements in accordance with generally accepted auditing

[4] Refer to AICPA, *Professional Standards*, vol. 1, AU 9339, *Working Papers: Auditing Interpretations of Section 339*.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

standards is to form an opinion and issue a report on whether the statutory financial statements present fairly, in all material respects, the admitted assets, liabilities, and capital and surplus, results of operations and cash flow in conformity with accounting practices prescribed or permitted by the Insurance Department of [*name of state of domicile*]. Consequently, under generally accepted auditing standards, we have the responsibility, within the inherent limitations of the auditing process, to plan and perform our audit to obtain reasonable assurance about whether the statutory financial statements are free of material misstatement, whether caused by error or fraud, and to exercise due professional care in the conduct of the audit. The concept of selective testing of the data being audited, which involves judgment both as to the number of transactions to be audited and the areas to be tested, has been generally accepted as a valid and sufficient basis for an auditor to express an opinion on financial statements. Audit procedures that are effective for detecting errors, if they exist, may be ineffective for detecting misstatements resulting from fraud. Because of the characteristics of fraud, particularly those involving concealment and falsified documentation (including forgery), a properly planned and performed audit may not detect a material misstatement resulting from fraud. In addition, an audit does not address the possibility that material misstatements resulting from fraud may occur in the future. Also, our use of professional judgment and the assessment of materiality for the purpose of our audit means that matters may exist that would have been assessed differently by insurance commissioners.

It is the responsibility of the management of the Company to adopt sound accounting policies, to maintain an adequate and effective system of accounts, and to establish and maintain an internal control structure that will, among other things, provide reasonable, but not absolute, assurance that assets are safeguarded against loss from unauthorized use or disposition and that transactions are executed in accordance with management's authorization and recorded properly to permit the preparation of financial statements in conformity with accounting practices prescribed or permitted by the Insurance Department of [*name of state of domicile*].

The Insurance Commissioner should exercise due diligence to obtain whatever other information that may be necessary for the purpose of monitoring and regulating the statutory financial position of insurers and should not rely solely upon the independent auditor's report.

d. We will retain the workpapers[5] prepared in the conduct of our audit until the Insurance Department of [*name of state of domicile*] has filed a Report of Examination covering 19X1, but not longer than seven years. After notification to the Company, we will make the workpapers available for review by the Insurance Department of [*name of state of domicile*]

---

[5] Section 13 of the Model Audit Rule defines workpapers as follows:

Workpapers are the records kept by the independent certified public accountant of the procedures followed, the tests performed, the information obtained, and the conclusions reached pertinent to the accountant's examination of the financial statements of an insurer. Workpapers, accordingly, may include audit planning documentation, work programs, analyses, memoranda, letters of confirmation and representation, abstracts of company documents and schedules or commentaries prepared or obtained by the independent certified public accountant in the course of his or her examination of the financial statements of an insurer and which support the accountant's opinion.

[Footnote added, September 1997, to reflect conforming changes necessary due to the issuance of the Notice to Practitioners on communications with state insurance regulators.]

at the offices of the insurer, at our offices, at the Insurance Department or at any other reasonable place designated by the Insurance Commissioner. Furthermore, in the conduct of the aforementioned periodic review by the Insurance Department of [*name of state of domicile*], photocopies of pertinent audit workpapers may be made (under the control of the accountant) and such copies may be retained by the Insurance Department of [*name of state of domicile*].[6]

e. The engagement partner has served in that capacity with respect to the Company since [*year that current "term" started*], is licensed by the [*state name*] Board of Public Accountancy, and is a member in good standing of the American Institute of Certified Public Accountants.

f. To the best of our knowledge and belief, we are in compliance with the requirements of section 7 of the NAIC's *Model Rule (Regulation) Requiring Annual Audited Financial Reports* regarding qualifications of independent certified public accountants.

This letter is intended solely for the information and use of the Insurance Department of [*name of state of domicile*] and other state insurance departments and is not intended to be and should not be used by anyone other than these specified parties.

[Revised, September 1997 and September 1998, to reflect conforming changes necessary due to the issuance of the Notice to Practitioners on communications with state insurance regulators. Revised, June 1999, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Notification of Adverse Financial Condition

.10 Section 10 of the Model Audit Rule requires that the auditor notify the insurer's board of directors or audit committee in writing within five business days of a determination that (*a*) the insurer has materially misstated its financial condition as reported to the domiciliary commissioner as of the balance-sheet date currently under examination or (*b*) the insurer does not meet the minimum capital and surplus requirements of the state insurance statute as of the balance-sheet date. The Model Audit Rule also requires the insurer to provide (*a*) to the insurance commissioner of the state of domicile a copy of the notification of adverse financial condition within five days of its receipt and (*b*) to the auditor evidence that the notification has been provided to the insurance commissioner. If the auditor receives no such evidence, the Model Audit Rule requires the auditor to send the notification to the insurance commissioner directly within the next five business days.

.11 The following is an illustration of the auditor's notification of adverse financial condition letter when the audit is complete:[7]

To the Board of Directors of MNO Insurance Company:

We have audited, in accordance with generally accepted auditing standards, the statutory financial statements of MNO Insurance Company (the Company) as of December 31, 19X1 and 19X0, and have issued our report thereon dated [*date of report*].

---

[6] See footnote 4. [Footnote renumbered, September 1997, to reflect conforming changes necessary due to the issuance of the Notice to Practitioners on communications with state insurance regulators.]

[7] A determination that financial statements filed with a state insurance department contain a material misstatement does not necessarily always occur when an audit is complete. The Model Audit Rule requires notification to be provided within five business days of such determination. The language in this illustrative letter should be modified depending on the relevant facts and circumstances. [Footnote renumbered, September 1997, to reflect conforming changes necessary due to the issuance of the Notice to Practitioners on communications with state insurance regulators.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

In connection with our audit, we determined that capital and surplus reflected in the statement of admitted assets, liabilities, and capital and surplus of the Company as of December 31, 19X1, as reported on the 19X1 Annual Statement filed with the Insurance Department of [*name of state*] is materially misstated because [*provide explanation*]. Statutory capital and surplus of $ reported on the 19X1 Annual Statement should be reduced by $ as a result of the matter in the preceding sentence.[8]

If we do not receive evidence that the Company has forwarded a copy of this letter to the insurance commissioner of [*name of state*] within five business days of receipt, we are required to give the insurance commissioner a copy of this letter within the next five business days.

This letter is intended solely for the information and use of the Insurance Department of [*name of state of domicile*] and other state insurance departments and is not intended to be and should not be used by anyone other than these specified parties.

[Revised, June 1999, to reflect conforming changes necessary due to the issuance of recent authoritative literature.]

Report on Internal Controls

.12 Section 11 of the Model Audit Rule requires that insurers provide the insurance commissioner of the state of domicile a written report describing significant deficiencies in the insurer's internal control structure noted during the audit. Auditors should follow the guidance in Statement on Auditing Standards No. 60, *Communication of Internal Control Structure Related Matters Noted in an Audit*. Additionally, the Model Audit Rule requires insurers to provide a description of remedial actions taken or proposed to correct significant deficiencies, if not covered in the auditor's report. The reports on internal controls should be filed by the insurer within sixty days after filing the annual audited financial statements. No report is required to be issued if the auditor does not identify significant deficiencies.

Effective Date

.13 This SOP should be applied to audits of statutory financial statements performed for periods ending on or after December 15, 1995. Early application is encouraged.

[8] The wording of this paragraph is intended for those situations in which audit adjustments would not cause minimum capital and surplus of an insurer to fall below statutory requirements. The paragraph should be reworded if the company did not meet minimum capital and surplus requirements as presented on its Annual Statement as filed with the domiciliary commissioner. [Footnote renumbered, September 1997, to reflect conforming changes necessary due to the issuance of the Notice to Practitioners on communications with state insurance regulators.]

Insurance Companies Committee (1994-1995)

WILLIAM C. FREDA, *Chair*
JOSEPH P. BRANDON
PETER S. BURGESS
DARREN F. COOK
RICHARD DADDARIO
HOWARD E. DALTON
DAVID A. DIAMOND
JOHN F. MAJORS
MARTHA F. MARCON
JAMES L. MORGAN III
ROBERT J. PRICE
PATRICK J. SHOUVLIN
MARY TODD STOCKER
GARY A. SWORDS
JAMES E. TAIT

Audit Issues Task Force

EDMUND R. NOONAN, *Chair*
LUTHER E. BIRDZELL
JAMES E. BROWN
JAMES S. GERSON
DEBORAH D. LAMBERT
GEORGE F. PATTERSON, JR.

AICPA Staff

DAN M. GUY
Vice President
Auditing Standards

ELAINE M. LEHNERT
Technical Manager
Accounting Standards

ARLEEN RODDA THOMAS
Director
Accounting Standards

[The next page is 31,011.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 14,310

Statement of Position 95-5 Auditor's Reporting on Statutory Financial Statements of Insurance Enterprises

December 21, 1995

NOTE

This Statement of Position (SOP) presents the recommendations of the AICPA Insurance Companies Committee regarding the application of generally accepted auditing standards to audits of financial statements of insurance enterprises. Members of the AICPA Auditing Standards Board have found the recommendations in this SOP to be consistent with existing standards covered by Rule 202 of the AICPA Code of Professional Conduct. AICPA members should be prepared to justify departures from the recommendations in this SOP.

SOP 95-5 is amended by SOP 01-5, *Amendments to Specific AICPA Pronouncements for Changes Related to the NAIC Codification*. SOP 01-5 is effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001.

Introduction and Background

.01 All states require domiciled insurance enterprises to submit to the state insurance commissioner an annual statement on forms developed by the National Association of Insurance Commissioners (NAIC). The states also require that audited statutory financial statements be provided as a supplement to the annual statements. Statutory financial statements are prepared using accounting principles and practices "prescribed or permitted by the regulatory authority of the state of domicile," referred to in this Statement of Position (SOP) as *statutory accounting practices*. Statutory accounting practices are considered an other comprehensive basis of accounting (OCBOA) as described in Statement on Auditing Standards (SAS) No. 62, *Special Reports* (AICPA, *Professional Standards*, vol. 1, AU sec. 623). [As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.02 The insurance laws and regulations of most states require insurance companies domiciled in those states to comply with the guidance provided in the NAIC *Accounting Practices and Procedures Manual* except as otherwise prescribed by state law. In 1999, the NAIC completed a process to codify statutory accounting practices for certain insurance enterprises, resulting in a revised *Accounting Practices and Procedures Manual* (the revised Manual), effective January 1, 2001. It is expected that all states will require insurers to comply with most, if not all, provisions of the revised Manual. Auditors of an insurance enterprise should monitor the status of the adoption of the revised

Manual by the various state regulatory authorities. [As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

[.03] [Paragraph deleted by the issuance of Statement of Position 01-5, December 2001.]

Prescribed-or-Permitted Statutory Accounting Practices

.04 Prescribed statutory accounting practices are those practices that are incorporated directly or by reference in state laws, regulations, and general administrative rules applicable to all insurance enterprises domiciled in a particular state. States may adopt the revised Manual in whole or in part as an element of prescribed statutory accounting practices in those states. If, however, the requirements of state laws, regulations, and administrative rules differ from the guidance provided in the revised Manual or subsequent revisions, those state laws, regulations, and administrative rules will take precedence. Auditors of insurance enterprises should review state laws, regulations, and administrative rules to determine the specific prescribed statutory accounting practices applicable in each state. [As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.05 Permitted statutory accounting practices include practices not prescribed by the domiciliary state as described in paragraph .04, above, but allowed by the domiciliary state regulatory authority. An insurance enterprise may request permission from the domiciliary state regulatory authority to use a specific accounting practice in the preparation of the enterprise's statutory financial statements (*a*) if it wishes to depart from the state prescribed statutory accounting practices, or (*b*) if prescribed statutory accounting practices do not address the accounting for the transaction. Accordingly, permitted accounting practices differ from state to state, may differ from company to company within a state, and may change in the future. [As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

NAIC-Codified Statutory Accounting[1]

[.06] [Paragraph deleted by the issuance of Statement of Position 01-5, December 2001.]

Other Relevant AICPA Pronouncements

.07 During 1994, the AICPA issued the following two pronouncements that address statutory accounting practices and statutory financial statements. These documents were amended by SOP 01-5, *Amendments to Specific AICPA Pronouncements for Changes Related to the NAIC Codification* [section 10,840].

a. SOP 94-1, *Inquiries of State Insurance Regulators* [section 14,290], requires, for each audit, auditors to obtain sufficient competent evidential matter to corroborate management's assertion that permitted statutory accounting practices that are material to an insurance enterprise's financial statements are permitted by the regulatory authority of the state of domicile.

---

[1] [Footnote deleted by the issuance of Statement of Position 01-5, December 2001.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

b. SOP 94-5, *Disclosures of Certain Matters in the Financial Statements of Insurance Enterprises* [section 10,630], requires insurance enterprises to disclose information about prescribed and permitted statutory accounting practices in their financial statements.

[As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

Applicability

.08 This SOP applies to all audits of statutory financial statements of insurance enterprises that file financial statements with state regulatory authorities, including stock and mutual insurance enterprises. Insurance enterprises that prepare statutory financial statements include life and health insurance enterprises, property and casualty insurance enterprises, title insurance enterprises, mortgage guaranty insurance enterprises, assessment enterprises, fraternal benefit societies, reciprocal or interinsurance exchanges, pools, syndicates, captive insurance companies, financial guaranty insurance enterprises, health maintenance organizations, and hospital, medical, and dental service or indemnity corporations. [As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.09 This SOP supersedes SOP 90-10, *Reports on Audited Financial Statements of Property and Liability Insurance Companies*. It also amends the AICPA Audit and Accounting Guides *Audits of Property and Liability Insurance Companies* and *Life and Health Insurance Entities*. [As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.][2]

Conclusions

Superseding Statement of Position 90-10, *Reports on Audited Financial Statements of Property and Liability Insurance Companies*

.10 Auditors should not issue reports on statutory financial statements as to fair presentation in conformity with statutory accounting practices that include a disclaimer of opinion as to fair presentation in conformity with generally accepted accounting principles (GAAP). [As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

General-Use Reports

.11 If an insurance enterprise's statutory financial statements are intended for distribution other than for filing with the regulatory authorities to whose jurisdiction the insurance enterprise is subject, the auditor of those statements should use the general-use form of report for financial statements that lack conformity with GAAP (SAS No. 62, *Special Reports* [AICPA, *Professional Standards*, vol. 1, AU sec. 623]). SAS No. 1, section 544, *Lack of Conformity With Generally Accepted Accounting Principles,* paragraph .04 (AICPA, *Professional Standards*, vol. 1, AU sec. 544.04), requires the auditor to use the standard form of report described in SAS No. 58, *Reports on Audited*

[2] [Footnote deleted by the issuance of Statement of Position 01-5, December 2001.]

Financial Statements (AICPA, *Professional Standards*, vol. 1, AU sec. 508), modified as appropriate because of departures from GAAP. [As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.12 Although it may not be practicable to determine the amount of difference between GAAP and statutory accounting practices, the nature of the differences is known. The differences generally exist in significant financial statement items, and are believed to be material and pervasive to most insurance enterprises' financial statements. Therefore, there is a rebuttable presumption that the differences between GAAP and statutory accounting practices are material and pervasive. Auditors should express an adverse opinion with respect to conformity with GAAP (AU sec. 508.58), unless the auditor determines the differences between GAAP and statutory accounting practices are not material and pervasive. [As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.13 The auditor, when expressing an adverse opinion, is required to disclose in a separate explanatory paragraph(s) preceding the opinion paragraph in his or her report (*a*) all of the substantive reasons for the adverse opinion, and (*b*) the principal effects of the subject matter of the adverse opinion on financial position, results of operations, and cash flows, if practicable[3] (AU sec. 508.59 and .60). If the effects are not reasonably determinable, the report should so state, and also should state that the differences are presumed to be material. Furthermore, the notes to the statutory financial statements should discuss statutory accounting practices and describe how those practices differ from GAAP. [As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.14 After expressing an opinion on the statutory financial statements as to conformity with GAAP, auditors may express an opinion on whether the statutory financial statements are presented in conformity with statutory accounting practices. If departures from statutory accounting practices are found to exist and are considered to be material, the auditors should express a qualified or adverse opinion on the statutory financial statements just as they would under SAS No. 58 (AICPA, *Professional Standards*, vol. 1, AU sec. 508) regarding conformity with GAAP.[4] [As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.15 Following is an illustration of an independent auditor's report on the general-use financial statements of an insurance enterprise prepared in conformity with statutory accounting practices, which contains an adverse opinion as to conformity with GAAP, and an unqualified opinion as to conformity with statutory accounting practices . In this illustrative report, it is assumed that the effects on the statutory financial statements of the differences between GAAP and statutory accounting practices are not reasonably determinable.

---

[3] SAS No. 32, *Adequacy of Disclosure in the Financial Statements* (AICPA, *Professional Standards*, vol. 1, AU sec. 431), defines practicable as "the information is reasonably obtainable from management's accounts and records and that providing the information in his report does not require the auditor to assume the position of a preparer of financial information." For example, if the information can be obtained from the accounts and records without the auditor substantially increasing the effort that would normally be required to complete the audit, the information should be presented in the auditor's report.

[4] [Footnote deleted by the issuance of Statement of Position 01-5, December 2001.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Independent Auditor's Report

To the Board of Directors
ABC Insurance Company

We have audited the accompanying statutory statements of admitted assets, liabilities, and surplus of ABC Insurance Company as of December 31, 20X2 and 20X1, and the related statutory statements of income and changes in surplus, and cash flows for the years then ended. These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

As described more fully in Note X to the financial statements, the Company prepared these financial statements using accounting practices prescribed or permitted by the Insurance Department of the State of [*state of domicile*],[5] which practices differ from generally accepted accounting principles. The effects on the financial statements of the variances between statutory accounting practices and accounting principles generally accepted in the United States of America, although not reasonably determinable, are presumed to be material.

In our opinion, because of the effects of the matter discussed in the preceding paragraph, the financial statements referred to above do not present fairly, in conformity with accounting principles generally accepted in the United States of America, the financial position of ABC Insurance Company as of December 31, 20X2 and 20X1, or the results of its operations or its cash flows for the years then ended.

In our opinion, the financial statements referred to above present fairly, in all material respects, the admitted assets, liabilities, and surplus of ABC Insurance Company as of December 31, 20X2 and 20X1, and the results of its operations and its cash flows for the years then ended, on the basis of accounting described in Note X.

[As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

Limited-Use Reports

.16 Prescribed-or-permitted statutory accounting practices for insurance enterprises are considered an OCBOA as described in SAS No. 62 (AICPA, *Professional Standards*, vol. 1, AU sec. 623). If an insurance enterprise's statutory financial statements are intended solely for filing with state regulatory authorities to whose jurisdiction the insurance enterprise is subject, the auditor may use the form of report for financial statements prepared in accordance with a comprehensive basis of accounting other than GAAP. Such reporting is appropriate even though the auditor's report may be made a matter of public record (AU sec. 623.05*f*). However, that paragraph further states that limited-use reports may be used only if the financial statements and

[5] [Footnote deleted by the issuance of Statement of Position 01-5, December 2001].

report are intended solely for filing with the regulatory agencies to whose jurisdiction the insurance enterprise is subject. The auditor's report should contain a statement that there is a restriction on the use of the statutory financial statements to those within the insurance enterprise and for filing with the state regulatory authorities to whose jurisdiction the insurance enterprise is subject. [As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.17 Although auditing standards do not prohibit an auditor from issuing limited-use and general-use reports on the same statutory financial statements of an insurance enterprise, it is preferable to issue only one of those types of reports. Few, if any, insurance enterprises that do not prepare financial statements in conformity with GAAP will be able to fulfill all of their reporting obligations with limited-use statutory financial statements. [As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.18 Following is an illustration, adapted from paragraph 8 of SAS No. 62 (AICPA, *Professional Standards*, vol. 1, AU sec. 623.08), of an unqualified auditor's report on limited-use financial statements prepared in conformity with statutory accounting practices.

Independent Auditor's Report

To the Board of Directors
XYZ Insurance Company

We have audited the accompanying statutory statements of admitted assets, liabilities, and surplus of XYZ Insurance Company as of December 31, 20X2 and 20X1, and the related statutory statements of income and changes in surplus, and cash flow, for the years then ended. These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

As described more fully in Note X to the financial statements, these financial statements were prepared in conformity with accounting practices prescribed or permitted by the Insurance Department of the State of [*state of domicile*],[6] which is a comprehensive basis of accounting other than generally accepted accounting principles.

In our opinion, the financial statements referred to above present fairly, in all material respects, the admitted assets, liabilities, and surplus of XYZ Insurance Company as of December 31, 20X2 and 20X1, and the results of its operations and its cash flows for the years then ended, on the basis of accounting described in Note X.

[6] [Footnote deleted by the issuance of Statement of Position 01-5, December 2001.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

This report is intended solely for the information and use of the board of directors and the management of XYZ Insurance Company and state insurance departments to whose jurisdiction the company is subject and is not intended to be and should not be used by anyone other than these specified parties.

[Revised, June 1999, to reflect conforming changes necessary due to the issuance of recent authoritative literature. As amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

[.19] [Paragraph deleted by the issuance of Statement of Position 01-5, December 2001.]

General-Use and Limited-Use Reports

.20 The notes accompanying an insurance enterprise's statutory financial statements should contain a summary of significant accounting policies that discuss statutory accounting practices and describe how this basis differs from GAAP (AU sec. 623.10). In general-use statutory financial statements, the effects of the differences should be disclosed, if quantified. However, in limited-use statutory financial statements, the effects of the differences need not be quantified or disclosed. [Paragraph added, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.21 The auditor should consider the need for an explanatory paragraph (or other explanatory language) under the circumstances described in SAS No. 58 (AU sec. 508.11) and SAS No. 62 (AU sec. 623.31) regardless of any of the following:

a. The type of report—general-use or limited-use

b. The opinion expressed—unqualified, qualified, or adverse

c. Whether the auditor is reporting as to conformity with GAAP or conformity with the statutory accounting practices

For example, in a general-use report, an auditor may express an adverse opinion as to conformity with GAAP and an unqualified opinion as to conformity with the statutory accounting practices, and also conclude there is a need to add an explanatory paragraph regarding substantial doubt about the insurance enterprise's ability to continue as a going concern; such paragraph should follow both opinion paragraphs. [Paragraph renumbered and amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.22 The auditor may wish to emphasize a matter in a separate paragraph of the auditor's report (AU secs. 508.37 and 623.31). When an insurance enterprise prepares its financial statements using accounting practices prescribed or permitted by the regulatory authority of the state of domicile and has significant transactions that it reports using permitted accounting practices that materially affect the insurance enterprise's statutory capital,[7] the auditor is strongly encouraged to include an emphasis-of-a-matter paragraph in the report describing the permitted practices and their effects on statutory

[7] [Footnote deleted by the issuance of Statement of Position 01-5, December 2001.]

capital. [Paragraph renumbered and amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.23 An example of an emphasis-of-a-matter paragraph follows:

> As discussed in Note X to the financial statements, the Company received permission from the Insurance Department of the [*state of domicile*] in 20XX to write up its home office property to appraised value; under prescribed statutory accounting practices home office property is carried at depreciated cost. As of December 31, 20X5, that permitted accounting practice increased statutory surplus by $XX million over what it would have been had the prescribed accounting practices been followed.

[Paragraph renumbered and amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.24 If subsequent to the initial adoption of the revised Manual there has been a change in accounting principles or in the method of their application that has a material effect on the comparability of the company's financial statements, the auditor should refer to the change in an explanatory paragraph of the report (AU sec. 508.16). The explanatory paragraph (following the opinion paragraph) should identify the nature of the change and refer to the note in the financial statements that discusses the change. The auditor's concurrence with a change is implicit, unless the auditor takes exception to the change in expressing the opinion as to the fair presentation of the financial statements in conformity with GAAP or the statutory accounting practices. [Paragraph added, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

.25 An example of an explanatory paragraph follows:

> As discussed in Note X to the financial statements, the Company changed its method of accounting for guaranty funds and other assessments.

[Paragraph added, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

Mutual Life Insurance Enterprises

.26 In April 1993, the Financial Accounting Standards Board (FASB) issued Interpretation No. 40, *Applicability of Generally Accepted Accounting Principles to Mutual Life Insurance and Other Enterprises*, which concludes that mutual life insurance enterprises can no longer issue statutory financial statements that are described as "in conformity with generally accepted accounting principles." Interpretation No. 40, as amended by FASB Statement of Financial Accounting Standards No. 120, *Accounting and Reporting by Mutual Life Insurance Enterprises and by Insurance Enterprises for Certain Long-Duration Participating Contracts*, is effective for financial statements issued for fiscal years beginning after December 15, 1995. (FASB Statement No. 120 does not change the disclosure and other transition provisions of Interpretation No. 40.) For statutory financial statements of mutual life insurance enterprises issued before that effective date, auditors may report on the statutory financial statements as being in conformity with generally accepted accounting principles. [Paragraph renumbered by the issuance of Statement of Position 01-5, December 2001.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Effective Dates

.27 The provisions of this SOP as originally issued in 1995 should be applied to audits of statutory financial statements for years ended on or after December 31, 1996. The amendments to this SOP are effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001. Retroactive application is not permitted. [Paragraph renumbered and amended, effective for audits of statutory financial statements for fiscal years ending on or after December 15, 2001, by Statement of Position 01-5.]

Insurance Companies Committee (1994–1995)

WILLIAM C. FREDA, *Chair*
JOSEPH P. BRANDON
PETER S. BURGESS
DARREN F. COOK
RICHARD DADDARIO
HOWARD E. DALTON
DAVID A. DIAMOND
JOHN F. MAJORS
MARTHA E. MARCON
JAMES L. MORGAN III
ROBERT J. PRICE
PATRICK J. SHOUVLIN
MARY TODD STOCKER
GARY A. SWORDS
JAMES E. TAIT

Auditing Standards Board (1994–1995)

EDMUND R. NOONAN, *Chair*
LUTHER E. BIRDZELL
JAMES E. BROWN
ROBERT E. FLEMING
JOHN A. FOGARTY, JR.
JAMES S. GERSON
NORWOOD J. JACKSON, JR.
JOHN J. KILKEARY
DEBORAH D. LAMBERT
CHARLES J. MCELROY
KURT PANY
GEORGE F. PATTERSON, JR.
EDWARD F. ROCKMAN
GLENN J. VICE
W. RONALD WALTON

AICPA Staff

DAN M. GUY
Vice President
Professional Standards and Technical Services

ELAINE M. LEHNERT
Technical Manager
Accounting Standards

The AICPA gratefully acknowledges the contributions to this SOP by Gary W. Roubinek, the former chair of the Insurance Companies Committee, and Dionne D. McNamee, former staff aide to the Insurance Companies Committee.

[The next page is 31,285.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 14,330

Statement of Position 98-6 Reporting on Management's Assessment Pursuant to the Life Insurance Ethical Market Conduct Program of the Insurance Marketplace Standards Association

April 9, 1998

NOTE

This Statement of Position presents the recommendations of the AICPA Insurance Companies Committee regarding the application of Statements on Standards for Attestation Engagements to engagements to report on management's assessment pursuant to the Life Insurance Ethical Market Conduct Program of the Insurance Marketplace Standards Association. Members of the AICPA Auditing Standards Board have found the recommendations in this Statement of Position to be consistent with existing standards covered by Rule 202 of the AICPA Code of Professional Conduct. AICPA members should be prepared to justify departures from the recommendations in this Statement of Position.

Summary

This Statement of Position (SOP) provides guidance to practitioners in conducting and reporting on an independent examination performed pursuant to the AICPA Statement on Standards for Attestation Engagements to assist an entity in meeting the requirements of the Insurance Marketplace Standards Association (IMSA) program (the IMSA program). IMSA requires that such engagements use the criteria it sets forth; consequently, users of this SOP should be familiar with the IMSA program and its *Assessment Handbook* and requirements.

The SOP amends chapter 9, "Auditor's Reports," of the AICPA Audit and Accounting Guide *Audits of Property and Liability Insurance Companies* and chapter 11, "Auditors' Reports," of the AICPA Industry Audit Guide *Audits of Stock Life Insurance Companies*. It is effective for independent assessments with IMSA report dates after January 31, 1998.

Introduction and Background

.01 Within the past several years, the life insurance industry has experienced allegations of improper market conduct practices such as questionable sales practices and potentially misleading policyholder illustrations. These allegations have triggered regulatory scrutiny, class action litigation, significant monetary settlements, and negative publicity related to market conduct issues. As a result, the industry is taking steps to promote a higher standard of ethical behavior that it hopes will reverse the negative perceptions held by many customers. In that regard, the American Council of Life Insurers (ACLI),

the largest life insurance trade organization, has established the Insurance Marketplace Standards Association (IMSA) as a nonaffiliated membership organization with its own board of directors composed of chief executives of life insurance companies. IMSA seeks to encourage and assist participating life insurance entities (hereinafter referred to as entities) in the design and implementation of sales and marketing policies and procedures that are intended to benefit and protect the consumer. Entities that desire to join IMSA will be required to adopt the IMSA Principles of Ethical Market Conduct (the Principles) and the Code of Ethical Market Conduct (the Code) and Accompanying Comments and respond affirmatively to an assessment questionnaire (the Questionnaire). Each prospective member also will be required to conduct a self-assessment to determine that it has policies and procedures in place that will enable it to respond affirmatively to the Questionnaire. An entity's self-assessment responses to the Questionnaire will need to be validated by an independent examination of the self-assessment. On obtaining an unqualified third-party assessment report, entities will be eligible for IMSA membership. Membership in IMSA is valid for a three-year period. Members are permitted to use IMSA's logo subject to rules set forth by IMSA for advertising and other promotional activities. The assessment process is intended to encourage entities and help them continually review and modify their policies and procedures in order to improve their market conduct practices and those of the industry and to strengthen consumer confidence in the life insurance business.

.02 Certified public accountants in the practice of public accounting (herein referred to as practitioners as defined by Statement on Standards for Attestation Engagements [SSAE] No. 1, *Attestation Standards* [AICPA, *Professional Standards*, vol. 1, AT sec. 100, "Attestation Engagements"]), may be engaged to examine and/or provide various consulting services related to the entity's self-assessment. This Statement of Position (SOP) provides guidance to practitioners in conducting and reporting on an independent examination performed pursuant to the American Institute of Certified Public Accountants (AICPA) SSAEs to assist an entity in meeting the requirements of the IMSA Life Insurance Ethical Market program (the IMSA program). As described herein, IMSA requires that such engagements use the criteria it sets forth; consequently, users of this SOP should be familiar with the IMSA program and its *Assessment Handbook* and requirements.

Scope

.03 This SOP applies to engagements to report on an entity's assertion that the affirmative responses to the Questionnaire relating to the IMSA Principles and Code and Accompanying Comments are based on policies and procedures in place at the IMSA report date. Reporting on assertions made in connection with the IMSA program are examination engagements that should be performed under SSAE No. 1 (AT sec. 100).

Overview of the IMSA Life Insurance Ethical Market Conduct Program

Principles of Ethical Market Conduct

.04 The Principles consist of six statements that set certain standards with respect to the sale and service of individually sold life and annuity products. The Principles that the entity is required to adopt are as follows:

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Principle 1

To conduct business according to high standards of honesty and fairness and to render that service to its customers which, in the same circumstances, it would apply to or demand for itself.

Principle 2

To provide competent and customer-focused sales and service.

Principle 3

To engage in active and fair competition.

Principle 4

To provide advertising and sales materials that are clear as to purpose and honest and fair as to content.

Principle 5

To provide for fair and expeditious handling of customer complaints and disputes.

Principle 6

To maintain a system of supervision and review that is reasonably designed to achieve compliance with these Principles of Ethical Market Conduct.

.05 IMSA developed the Code of Ethical Market Conduct to expand the Principles of Ethical Market Conduct to the operating level and to identify the attributes of the sales, marketing, and compliance systems that IMSA believes should support each of the Principles.

.06 To further expand on the Principles and Code, IMSA developed Accompanying Comments, which further define the intention of the Principles and Code and, in some instances, provide examples of implementation.

IMSA Assessment Questionnaire

.07 As noted above, IMSA developed the Questionnaire to provide prospective members with uniform criteria to demonstrate for self-assessment purposes that they have policies and procedures in place that meet the objective of the questions in the Questionnaire.

Insurance Marketplace Standards Association Membership and Certification Process

.08 Participation in the IMSA program requires an entity to adopt the Principles and Code and to undertake a two-step assessment process. First, an entity conducts a self-assessment, using the Questionnaire and *Assessment Handbook*, with the objective of concluding that it can respond affirmatively to every question in the Questionnaire in conformity with the criteria set forth in IMSA's Principles, Code, and Accompanying Comments. Second, an independent assessor from a list of IMSA-approved assessors examines the self-assessment materials to determine whether the entity has a reasonable basis for its affirmative responses to the Questionnaire.

.09 Once the assessment process is complete, the entity submits its IMSA Membership Application (the application) and Self-Assessment Report. The Self-Assessment Report states that the entity has adopted the Principles and

Code, has conducted a self-assessment of its policies and procedures, and has determined that the answer to each of the questions in the Questionnaire is "yes" in conformity with the *Assessment Handbook*. The entity also submits an unqualified examination report from an IMSA-approved independent assessor.

IMSA Independent Assessor Application Process and Required Training

.10 IMSA will accept independent assessor reports only from those assessors that have been preapproved by IMSA. To become an independent assessor, a candidate is required to submit an IMSA Independent Assessor Application that requires that the candidate meet specific educational and professional requirements established by the IMSA board of directors. IMSA also requires that all independent assessors attend IMSA training as outlined by the board of IMSA. Independent assessors may be of various occupations or professional disciplines, including certified public accountants.

IMSA Assessment Handbook

.11 IMSA developed an *Assessment Handbook* (the Handbook or the IMSA Handbook) to assist companies in the implementation of the IMSA program and provide guidance to independent assessors. Entity personnel and independent assessors should use the Handbook to gain an understanding of the assessment process and as a source of information for performing an assessment. The Handbook is intended for companies of all sizes regardless of the means by which they distribute individually sold life and annuity products. IMSA acknowledges that this is a new program that will evolve over time. Therefore, the Handbook may be revised as companies and independent assessors provide IMSA with suggestions for improvement. Practitioners should ensure that they are utilizing the most current version of the Handbook in planning and performing their work.

Conclusions

Planning the Engagement

.12 To satisfy IMSA program requirements, practitioners need to perform an examination engagement pursuant to SSAE No. 1 (AT sec. 100), which states that planning an attest engagement involves developing an overall strategy for the expected conduct and scope of the engagement. To develop such a strategy, practitioners should have adequate technical training and proficiency in the attest function and have adequate knowledge in life insurance market conduct and the IMSA program to enable them to sufficiently understand the events, transactions, and practices that, in their judgment, have a significant effect on the presentation of the assertions.

.13 The examination should be made in accordance with standards established by the AICPA, including obtaining an understanding of the policies and procedures in place upon which the affirmative responses to the Questionnaire are based. To be acceptable to IMSA, the engagement also should be performed in accordance with the criteria set forth in the IMSA Handbook. This SOP is intended to provide neither all the required criteria set forth in the IMSA Handbook nor all the applicable standards established by the AICPA.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.14 In accordance with SSAE No. 1 (AT sec. 100.33–.35) and the Handbook, a practitioner performing the examination should supervise the engagement team, which involves directing the efforts of the engagement team in accomplishing the objectives of the engagement and determining whether the engagement objectives were met. If the practitioner is not an IMSA-approved independent assessor, such an assessor should be a member of the engagement team with responsibility for, among other things, assisting the practitioner in performing these functions.

.15 The engagement team should be informed of its responsibilities, including the objectives of the procedures that they are to perform and matters that may affect the nature, extent, and timing of such procedures. The work performed by each member of the engagement team should be reviewed to determine if it was adequately performed.

.16 IMSA, through its Handbook, has adopted a methodology to foster a uniform determination by entities and their independent assessor on whether policies and procedures are in place. The Handbook requires the following three aspects be present: approach, deployment, and monitoring. (See appendix B, paragraph B-2 [paragraph .38], for further discussion.)

Establishing an Understanding With the Client

.17 The practitioner should consider the risks associated with accepting an engagement to examine and report on an entity's assertion about its responses to the IMSA Questionnaire. The practitioner should establish an understanding with the client regarding the services to be performed. The understanding should include the objectives of the engagement, management's responsibilities, the practitioner's responsibilities, limitations of the engagement, provision for changes in the scope of the engagement, and the expected form of the report. The practitioner should document the understanding in the working papers, preferably through a written communication with the client, such as an engagement letter. Appendix C [paragraph .39] contains a sample engagement letter that may be used for this type of engagement.

Assessments of Attestation Risk

.18 The practitioner should evaluate the attestation risk that policies and procedures may not be in place to support affirmative responses to the Questionnaire and should consider this risk in designing the attest procedures to be performed. In examining whether policies and procedures are in place, the practitioner determines whether the policies and procedures have been adopted and are in operation and whether such policies and procedures satisfy the six components required by IMSA for the entity to respond affirmatively to each question, as discussed in appendix B [paragraph .38]. Whether an entity has policies and procedures in place does not encompass whether those policies and procedures operated effectively as of a particular date, or over any period of time, to ensure compliance with the Principles, Code, and Accompanying Comments or about whether the entity or its employees have complied with applicable laws and regulations.

.19 Examples of risk considerations that may affect the nature, timing, and extent of testing procedures are listed in appendix A [paragraph .37]. Not all the examples are relevant in all circumstances, and some may be of greater or lesser significance in entities of different size, distribution channels, product lines, or sales volume. In determining the examination procedures to be performed, practitioners should assess the impact that those risk considerations, individually and in combination, may have on attestation risk.

.20 Before performing attestation procedures, the practitioner should be adequately trained and should obtain an understanding of the entity's overall operations and market conduct practices, as well as its policies and procedures that have been identified in the self-assessment as supporting its affirmative responses to the Questionnaire. In addition, the practitioner should obtain an understanding of the operation and history of the entity's distribution systems and products sold and of sales volume by product and distribution system. The practitioner should also obtain an understanding of the entity's past market conduct issues and related corrective measures.

Evidential Matter

.21 In an examination engagement performed under the attestation standards, the practitioner's objective is to accumulate sufficient evidence to limit attestation risk to a level that is, in the practitioner's professional judgment, appropriately low for the high level of assurance that may be imparted by his or her report. In such an engagement, the practitioner should select from all available procedures any combination that can limit attestation risk to such an appropriately low level. Accordingly, in an examination engagement it is necessary for a practitioner's procedures to go beyond reading relevant policies and procedures and making inquiries of appropriate members of management to determine whether the policies and procedures supporting affirmative responses to the Questionnaire were in place. Examination procedures should also include verification procedures, such as inspecting documents and records, confirming assertions with employees or agents, and observing activities. See appendix B [paragraph .38] for examples of illustrative procedures.

.22 As outlined in the Handbook, the entity should provide the practitioner with adequate information for the practitioner to obtain reasonable assurance that there is a basis for an affirmative response to each of the questions in the Questionnaire. The AICPA's concept of reasonable assurance in the context of an attestation engagement is set forth in SSAE No. 2, *Reporting on an Entity's Internal Control Over Financial Reporting* (AICPA, *Professional Standards*, vol. 1, AT sec. 400.13), and SSAE No. 3, *Compliance Attestation* (AICPA, *Professional Standards*, vol. 1, AT sec. 500.30). These concepts are consistent with IMSA's concept of reasonable assurance as defined in the Handbook.[1]

.23 In an examination of management's assertion about an entity's affirmative responses to the Questionnaire, the practitioner's evaluation of sufficiency and competency of evidential matter should include consideration of (*a*) the nature of management's assertion and the related indicators used to support such assertions, (*b*) the nature and frequency of deviations from expected results of applying examination procedures, and (*c*) qualitative considerations, including the needs and expectations of the report's users.

Reporting Considerations

.24 SSAE No. 1 (AT sec. 100) defines an attest engagement as one in which a practitioner is engaged to issue a written communication that expres-

[1] *Reasonable (assurance)* is defined in the Handbook as follows: "In the context of the IMSA program documents, the term *reasonable* is used to modify assurance, as an acknowledgment that it is virtually impossible to provide absolute and certain assurance that an event will happen (e.g., that a policy will address every possible circumstance, or that procedures will be applied without exception). *Reasonable*, as a qualifier, suggests that there exists a standard in both design and performance, and that such a standard, while conforming to the judgment or discernment of a knowledgeable person, is neither excessive nor extreme."

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

ses a conclusion about the reliability of a written assertion that is the responsibility of another party. The accompanying affirmative responses to the questions in the Questionnaire are written assertions of the entity. When a practitioner is engaged by an entity to express a written conclusion about management's assertions about its policies and procedures, such an engagement involves a written conclusion about the reliability of an assertion that is the responsibility of the entity. The entity is responsible for the design, implementation, and monitoring of the policies and procedures upon which the responses to the Questionnaire are based.

.25 Self-assessment is based in part on criteria set forth in the IMSA Handbook, which is prepared by an industry organization for the specific use of its members. Such criteria are not suitable for general distribution reporting. Accordingly, the independent accountant's report should contain a statement that it is intended solely for the information and use of the entity's board of directors and management as well as IMSA.

.26 IMSA has adopted a uniform assessment report that all independent assessors (regardless of professional discipline) are required to use when reporting on the results of an independent assessment. IMSA has indicated that deviations from its standard report format, except as discussed below, will not be accepted. The following is an illustration of an independent accountant's report on a company's assertion relating to its affirmative responses to the IMSA Questionnaire. The third paragraph in the following report deviates from the IMSA format, where the practitioner specifies that the examination was made in accordance with standards established by the AICPA, and refers to those standards before referring to the criteria set forth in the IMSA Handbook. The other deviation is that the report is titled "Independent Accountant's Report" rather than "Independent Assessor Report." Representatives of IMSA have indicated that they will accept only these deviations for reports issued by practitioners.

Independent Accountant's Report

To [*name of insurer*] Board of Directors and the Insurance Marketplace Standards Association:

We have examined management's assertion that the affirmative responses of [*name of insurer*] to the Questionnaire relating to the Principles of Ethical Market Conduct and the Code of Ethical Market Conduct and Accompanying Comments for individually sold life and annuity products, adopted by the Insurance Marketplace Standards Association ("IMSA"), are based on policies and procedures in place as of [*the IMSA report date*]. The Company is responsible for the design, implementation, and monitoring of the policies and procedures in place upon which the responses to the Questionnaire are based.

Our examination was made in accordance with standards established by the American Institute of Certified Public Accountants and in accordance with the criteria set forth in the IMSA *Assessment Handbook*, and included obtaining an understanding of the policies and procedures in place upon which the affirmative responses to the Questionnaire are based and such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion. Our examination was not designed to evaluate whether the policies and procedures, upon which the Company's responses to the Questionnaire are based, have or will operate effectively, nor have we evaluated whether or not the Company has or will comply with applicable laws or regulations. Accordingly, we do not express an opinion or any other form of assurance thereon.

In our opinion, management's assertion that the affirmative responses to the Questionnaire are based on policies and procedures in place as of [*the IMSA report date*] is fairly stated, in all material respects, based upon the criteria set forth in the Principles of Ethical Market Conduct, the Code of Ethical Market Conduct and Accompanying Comments, and the *Assessment Handbook*.

This report is intended solely for the information and use of the board of directors and management of the Company and the Insurance Marketplace Standards Association and should not be used for any other purpose.

_____

[*IMSA Report Date; see paragraph .28*]

_____

[*Company (Insurer)*]

_____

[*Name of Independent Assessor; see paragraph .27*]

_____

[*Signature of Independent Accountant or Firm*]

_____

[*Date of Signature; see paragraph .29*]

Note: In any instance where an alternative indicator is used to support an affirmative answer to any question in the Questionnaire, such alternative indicator must be fully set forth in an attachment to this Assessor Report (see paragraph .30).

Elements of the Report

.27 *Signatures and Identification of the Independent Assessor.* IMSA prefers that the independent assessor sign his or her name on the report. However, many AICPA member firms require that a manual or printed signature of the firm name be presented on the face of the report and prohibit a member of the firm from signing the report as an individual. Although IMSA will accept this practice, it requires the identification on the face of the independent accountant's report of the IMSA-approved independent assessor who actively participated in and supervised relevant portions of the engagement on behalf of the firm. In addition, in circumstances where the IMSA-approved independent assessor does not sign the report as an individual, IMSA requires an affirmation from the independent assessor to be attached to the independent accountant's report. A sample affirmation follows:

Affirmation of Independent Assessor

I, [*print name*], affirm that I have reviewed the attached Independent Accountant's Report on management's assertions regarding the IMSA program for [*insurer*] as of [*IMSA report date*] and that I was the Independent Assessor responsible for supervising relevant portions of the assessment identified herein.

[*Signature*]
[*Date of Signature*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.28 *IMSA Report Date.* The IMSA report date referred to in the independent accountant's report is the date of the self-assessment and the date to which the entity and the independent assessor have agreed as the point in time which the policies and procedures supporting the affirmative response to the Questionnaire are in place. Due care should be taken to ensure that representations made by management on the basis of a self-assessment are current as of the IMSA report date. If a significant amount of time has elapsed between the date of the performance of the practitioner's procedures on certain questions and the IMSA report date, due care should be taken to ensure that policies and procedures were in place as of the IMSA report date.

.29 *Date of Signature.* The date of signature is the date fieldwork is completed. Changes in the policies and procedures, personnel changes, or other considerations that might significantly affect responses to the Questionnaire may occur subsequent to the IMSA report date but before the date of signature or the date when the report is issued. The practitioner should obtain management's representations relating to such matters and perform such other procedures regarding subsequent events considered necessary in the circumstances. The practitioner has no responsibility to perform examination procedures or update his or her report for events subsequent to the date when the report is issued; however, the practitioner may later become aware of conditions that existed at that date that might have affected the practitioner's opinion had he or she been aware of them. The practitioner's consideration of such subsequent information is similar to an auditor's consideration of information discovered subsequent to the date of a report on an audit of financial statements described in SAS No. 1 (AICPA, *Professional Standards*, vol. 1, AU sec. 561, "Subsequent Discovery of Facts Existing at the Date of the Auditor's Report").

.30 *Alternative Indicators.* A list of indicators in the Handbook corresponds to each of the questions in the Questionnaire and lists possible policies and procedures identified by IMSA that an entity can have in place to be able to respond affirmatively to a question. A company must support each "yes" response to a question by the selection of indicators sufficient to meet the six required components and to meet the objective of each question. IMSA has established limitations on the use of indicators other than those contained in the Handbook. Alternative indicators that are used as support for an affirmative response to a question in the Questionnaire may require preapproval by IMSA in certain situations, as noted in the Handbook. It will be necessary for the practitioner to evaluate whether an alternative indicator used by the entity supports an affirmative response to the question. The alternative indicators should be disclosed by the practitioner to IMSA in the basic independent accountant's report as an attached appendix, and an explanatory paragraph should be added to the standard independent accountant's report in paragraph .26. The following is an example of a paragraph that should be included in the examination report when alternative indicators are used by management. The paragraph should precede the opinion paragraph.

> Management's assertion supporting an affirmative response to certain questions is supported by the use of alternative indicators, as that term is defined in the IMSA Handbook. The attached appendix to this report lists the questions and alternative indicators used by management.

.31 *Negative Responses.* IMSA will not grant membership applications to an entity whose application contains a "no" response to any question. In circumstances where no report will be issued to IMSA, management may request the practitioner to report findings to management or the board of dir-

ectors. In this situation, the practitioner and management should agree on the means and format of such communication and document this understanding in writing.

.32 *Working Papers.* The practitioner should prepare and maintain working papers in connection with an engagement under the attestation standards; such working papers should be appropriate to the circumstances and the practitioner's needs on the engagement to which they apply. Although it is not possible to specify the form or content of the working papers that a practitioner should prepare in connection with an assessment because circumstances vary in individual engagements, the practitioner's working papers ordinarily should indicate that—

a. The work was adequately planned and supervised.

b. Evidential matter (SSAE No. 1 [AT sec. 100.36–.39]) was obtained to provide a reasonable basis for the conclusion that the policies and procedures underlying the affirmative responses contained in the Questionnaire are in place.

In its required training, IMSA has advised IMSA-approved independent assessors to appreciate the sensitivity of insurers to litigation risks and the production of documents that litigation typically requires. IMSA has reminded assessors and insurers alike that the self-assessment process is designed to demonstrate compliance currently with IMSA assessment criteria and that reports will not be accepted by IMSA unless all questions are answered in the affirmative. Accordingly, IMSA has stated its belief that IMSA-approved assessors will have no need, at least for IMSA's purposes, to maintain documentation of noncompliance with the IMSA assessment criteria currently or in the past.

.33 Concern over access to the practitioner's working papers might cause some clients to inquire about working paper requirements. In situations where the practitioner is requested to not maintain copies of certain client documentation, or to not prepare and maintain documentation similar to client documents, the practitioner may refer to the auditing Interpretation "The Effect of an Inability to Obtain Evidential Matter Relating to Income Tax Accruals" (AICPA, *Professional Standards*, vol. 1, AU sec. 9326.06–.17) for guidance. See the attest Interpretation "Providing Access to or Photocopies of Working Papers to a Regulator" (AICPA, *Professional Standards*, vol. 1, AT sec. 9100.58) for guidance related to providing access to or photocopies of working papers to a regulator in connection with work performed on an attestation engagement.

.34 *Management's Representations.* The practitioner should obtain written representation from management—

a. Acknowledging management's responsibility for the design, implementation, and monitoring of the policies and procedures in place upon which the responses to the Questionnaire are based and that the affirmative responses to the Questionnaire are based on such policies and procedures in place as of a specific point in time.

b. Stating that management has adopted the Principles and Code, and has performed and made available to the practitioners all documentation related to a self-assessment of the policies and procedures in place as of the IMSA report date upon which the affirmative responses to the Questionnaire are based.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

c. Stating that management has disclosed to the practitioner all matters regarding the design, implementation, and monitoring of policies and procedures that could adversely affect the entity's ability to answer affirmatively the questions in the Questionnaire.

d. Describing any related material fraud or other fraud or illegal acts that, whether or not material, involve management or other employees who have a significant role in the entity's design, implementation, and monitoring of the policies and procedures in place upon which the responses to the Questionnaire were made.

e. Stating whether there were, subsequent to the date of management's self-assessment (that is, the IMSA report date), any known changes or deficiencies in the design, implementation, and monitoring of the policies and procedures in place, including any personnel changes or other considerations of reference to the IMSA Questionnaire subject matter.

f. Stating that management has disclosed any communication from regulatory agencies, internal auditors, and other parties concerning matters regarding the design, implementation, and monitoring of the policies and procedures in place, including communication received between the IMSA report date (the date of management's assertion) and the date of the practitioner's report (the date of signature).

g. Stating that management has disclosed to the practitioners, orally or in writing, information about past market conduct issues (for example, policyholder complaints or litigation) of relevance to the IMSA Questionnaire subject matter and the related corrective measures taken to support affirmative responses in those areas.

.35 Management's refusal to furnish all appropriate written representations constitutes a limitation on the scope of the examination sufficient to preclude an unqualified report suitable for submission to IMSA. Further, the practitioner should consider the effects of management's refusal on his or her ability to rely on other management representations.

Effective Date

.36 This SOP is effective for independent assessments with IMSA report dates after January 31, 1998. Early application is permissible.

.37

Appendix A

Assessment of Attestation Risk

A.1. The following are examples of considerations that may influence the nature, timing, and extent of a practitioner's testing procedures relating to an entity's assertion of its affirmative responses to the Questionnaire. The considerations may also affect a practitioner's decision to accept such an engagement. The examples are not intended to be a complete list.

Management Characteristics and Influence Over the Control Environment

- Management's attitude regarding internal control over sales and marketing practices, which may affect its ability to foster a more comprehensive and effective compliance program
- Management's financial support of the internal resources allocated to the development and maintenance of compliance with the IMSA program through adequate funding, resources, time, etc.
- Management's history of ensuring that sales personnel are qualified, trained, licensed, and supervised
- Management's history and systems for tracking complaint and replacement trends
- Management's ability to generate timely, complete, and accurate information on issues of regulatory concern regarding sales and marketing practices
- The entity's relationship with its current independent assessor, regulatory authorities, or both (The practitioner should gain an understanding of the circumstances surrounding the disengagement of predecessor independent assessors, any issues identified in prior self-assessments or independent assessments, and consider making inquires of predecessor assessors.)
- Consistent application of policies and procedures across product lines and distribution channels (If the entity did not address each distribution channel, product line, or both because it deemed certain ones to be immaterial in terms of premiums earned or in force, or because of low volume of production, the practitioner will need to use his or her professional judgment to assess whether the omitted product lines or distribution channels should have been considered in the entity's self-assessment and assess the impact on his or her ability to opine on management's assertions by exercising that judgment. The definition of the term *appropriate to its size* in the Handbook may also apply.)
- Whether the entity's approach to its self-assessment includes validation of the information it collected to support that policies and procedures are in place

Industry Conditions

- Changes in regulations or laws, such as those governing various products, sales methods and materials, agent compensation, and customer disclosure

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- Publicity about sales and marketing practices and increased litigation to seek remedy
- Rapid changes in the industry, such as the introduction of new and complex product offerings or information technology
- The degree of competition or market saturation

Distribution, Sales Volume, and Products

- The diversity of distribution systems
- The relative volume of business for different products and distribution systems
- The length of time that products, distribution systems, or both have been available, used, or both
- Limitations of an entity's ability to assert control over producers
- Compliance training provided by management to its producers and employees involved in the sales process
- The complexity of product offerings
- The targeted markets for various products
- Whether the entity is applying for IMSA membership as a fleet of entities or as an individual entity (If the entity is applying for fleet membership, the independent assessor should plan the engagement to address whether the policies and procedures are in place at each company within the fleet, including newly acquired subsidiaries or affiliates in the fleet.)

Other Considerations

- Issues identified in prior self-assessments, independent assessments, and other services provided
- Findings from recent market conduct examinations conducted by regulatory authorities or internal auditors
- Policyholder concerns expressed through complaints or litigation
- Ratings received from rating agencies

Appendix B

Illustrative Procedures

B.1. Examples of illustrative procedures are provided in this appendix. The procedures are organized by the three aspects of each question. Many of these procedures can be used for more than one question. The illustrative procedures are intended to be used as a guide and are not to be considered all-inclusive. Because the objective and the types of policies and procedures for each question will differ according to the methods for establishing, maintaining, communicating, deploying, and monitoring as they differ by entity and for each question, no single methodology for testing can be suggested. Practitioners should use judgment to determine the procedures necessary to be performed to render an opinion. It will be more difficult to obtain objective evidence about some indicators than others. Accordingly, the practitioner should adjust the procedures selected for testing. A challenging aspect of the IMSA program is its application to various distribution channels, including independent producers, and how entities will satisfy questions relating to these various channels. This is because an entity's ability to enforce or encourage producers to use its policies and procedures varies by channel. The practitioner needs to clearly understand how an entity manages each significant distribution channel.

B.2. IMSA has identified three aspects of each question: approach, deployment, and monitoring. The aspects are defined in the glossary of the Handbook as follows:

> *Approach*—A systematic method or means used by the entity to address the requirements of the Principles and Code, as queried by the specific question.
>
> *Deployment*—Refers to the extent to which the entity's approach is actually being applied to the provisions of the Principles and Code.
>
> *Monitoring* —To check routinely and systematically with a view to collecting certain specified categories of information, to investigate and resolve questions concerning anomalous or unexpected information, and to identify the need for or to make recommendations designed to reduce the probability of future anomalies. The Principles, Code, Accompanying Comments, and Questionnaire require that monitoring be performed to provide reasonable assurance that policies accurately reflect management's (or other applicable governing bodies') point of view, that procedures are designed to support those policies, and that procedures are appropriately executed.

Approach

B.3. The two components underlying the first aspect, *approach*, as defined by the Handbook are as follow:

a. Does the insurer have in place policies and procedures that address the objective of the question?

b. Is someone (an individual or a team) responsible for establishing, maintaining, communicating, deploying, and monitoring these policies and procedures?

B.4. The following are examples of procedures the practitioner and engagement team may employ to test the affirmative responses for the *approach* aspect:

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Examine Documentation

- Obtain and read written policies and procedures to obtain an understanding of—
  - *a.* The policies and procedures that are supposed to be in place and to which distribution systems, products, and markets those policies and procedures apply.
  - *b.* How the policies and procedures respond to the objective of the question.
  - *c.* Who (a person or department) is responsible for establishing, maintaining, communicating, deploying, and monitoring those policies and procedures.
- Examine job descriptions, titles, organization charts, and other communications for those identified as being responsible for the policies and procedures to support the assignment of those responsibilities.

Inquiry

- Through inquiry, obtain an understanding of—
  - *a.* How the policies and procedures are being used in practice.
  - *b.* Who is responsible for the policies and procedures being addressed.
  - *c.* The responsibilities of management and employees who oversee the policies and procedures.
  - *d.* Evidence that supports that the policies and procedures exist.
  - *e.* Evidence that policies and procedures have been in place for a sufficient period.
  - *f.* The distribution systems, products, and markets to which the policies and procedures apply.
  - *g.* How the policies and procedures respond to the selected indicator.

Deployment

B.5. The two components underlying the second aspect, *deployment*, as defined by the Handbook are as follow:

a. Are the policies and procedures communicated?

b. Does the insurer consistently use these policies and procedures?

B.6. The following are examples of procedures the practitioner and engagement team may employ to test the affirmative responses for the *deployment* aspect:

Examine/Inspect Documentation

- Obtain and read internal documents—including memos, e-mail, handbooks, policy manuals, and contracts—to verify that communications have been made.
- Obtain and read written confirmation or other evidence that the intended audience of the policies and procedures has received and read the communication.

- Obtain independent confirmation that policies and procedures are being used.

Observation

- Observe that reference materials (internal or external) that may be required for personnel to adequately perform the policies and procedures are reasonably accessible.
- For a sample of items, perform a walkthrough of the policies and procedures deemed to be in place in the *approach* aspect to support that those policies and procedures are being consistently applied for distribution channels and product lines that use those policies and procedures. Determine that the policies and procedures have also been consistently applied for a sufficient time by including transactions for various dates in the sample of transactions for the walkthrough.

Inquiry

- Interview personnel who perform the activities described in the policies and procedures documents to support that policies and procedures have been communicated to them.

Monitoring

B.7. The two components underlying the third aspect, *monitoring*, as defined by the Handbook are as follow:

a. Does the insurer routinely monitor the operation of these policies and procedures with a view toward achieving the intended result?

b. Does the insurer act upon the information received?

B.8. The following are examples of procedures the practitioner and engagement team may employ to test the affirmative responses for the *monitoring* aspect:

Examine Documentation

- Obtain and examine documents prepared by entity personnel that provide the responsible party with appropriate monitoring tools (for example, management reports, trend analyses, and tracking logs).
- Examine monitoring tools to identify deviations from the expected results, provide analysis of these deviations, and demonstrate investigation has occurred.
- Examine documentation of the corrective actions taken in response to information received by the responsible parties.
- Examine monitoring documents subsequent to corrective action taking place to ascertain whether the incidence of an identified problem or complaint has decreased in frequency because of the corrective action.

Inquiry

- Interview the personnel responsible for preparing reports used as monitoring tools to determine that the appropriate information is being gathered in a reasonable manner.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- Interview the personnel responsible for acting on the information provided and identify the procedures in place to perform corrective actions.

Observation

- Examine monitoring reports to ascertain whether they are prepared and distributed on a regular basis to the responsible personnel.
- Perform a walkthrough for a selection of transactions in which the action described by the identified responsible party should have occurred and ascertain whether the procedure was put in place.
- Observe changes in policies and procedures or communications to entity personnel that have occurred because of the recurrence of an identified problem or complaint.

Appendix C

Sample Engagement Letter

The following is an illustration of a sample engagement letter that may be used for this type of engagement.

[*CPA Firm Letterhead*]

[*Client's Name and Address*]

Dear _____:

This will confirm our understanding of the arrangements for our examination of management's assertion that the affirmative responses of [*name of client entity*] to the Insurance Marketplace Standards Association ("IMSA") questionnaire (the "Questionnaire") relating to the Principles of Ethical Market Conduct and the Code of Ethical Market Conduct and Accompanying Comments for individually sold life and annuity products, are based on policies and procedures in place as of [*the IMSA report date*].

We will examine management's assertion that the affirmative responses to the Questionnaire are based on policies and procedures in place as of the IMSA report date for the purpose of expressing an opinion as to whether management's assertion is fairly stated, in all material respects, based upon the criteria set forth in the Principles of Ethical Market Conduct, Code of Ethical Market Conduct and Accompanying Comments, and Assessment Handbook. The Company is responsible for the design, implementation, and monitoring of the policies and procedures in place upon which the responses are based. Our responsibility is to express an opinion on management's assertion based on our examination.

We will conduct our examination in accordance with standards established by the American Institute of Certified Public Accountants and in accordance with the criteria set forth in the IMSA Assessment Handbook. Our examination will include obtaining an understanding of the policies and procedures in place upon which the affirmative responses to the Questionnaire are based and such other procedures as we consider necessary in the circumstances. Our examination will not be designed to evaluate whether the policies and procedures, upon which [*the entity's*] responses to the Questionnaire are based, operate effectively, nor will we evaluate whether [*the entity*] has complied with applicable laws or regulations. Accordingly, we will not express an opinion or any other form of assurance thereon.[2]

Working papers that are prepared in connection with this engagement are the property of the independent accountant. The working papers are prepared for the purpose of providing the principal support for the independent accountant's report.

At the completion of our work we expect to issue an examination report in a form acceptable to IMSA (example attached). If, however, we are not able to conclude that management's assertion that the affirmative responses to the

[2] The independent accountant may wish to include an understanding with the client about any limitation or other arrangements regarding liability of the practitioner or the client in the engagement letter.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Questionnaire are based on policies and procedures in place as of the IMSA report date, we will so advise you. At that time we will discuss with you the form of communication, if any, that you desire for our findings. We will ask you to confirm your request in writing at that time. If no report is requested, we understand that our engagement will be terminated, our working papers will be destroyed (at your request), our professional fees will be payable in full, and our professional responsibilities to you will be complete. We will have no responsibility to report in writing at a later date. If you request written or oral communication of our findings, we will do so and our working papers will be retained in accordance with our firm's working paper retention policy. Our professional fees will be subject to adjustment. If you request that we delay issuance of our report until corrective action is taken that will result in affirmative answers to all questions, we will do so only at your written request. Our working papers will be retained in accordance with our firm's working paper retention policy. Again, our fees will be subject to adjustment. If we conclude that we are unable to issue an unqualified report, we reserve the right to bring the matter to the attention of an appropriate level of management or the board of directors.

The distribution of the independent accountant's report will be restricted to the board of directors and management of [*the entity*] and IMSA. [*The entity*] agrees that it will not use the CPA firm's name in advertising materials referring to [*the entity's*] membership in IMSA.

Our fees will be billed as work progresses and are based on the amount of time required at various levels of responsibility plus actual out-of-pocket expenses. Invoices are payable upon presentation. We will notify you immediately of any circumstances we encounter that could significantly affect our initial estimate of total fees.

If this letter correctly expresses your understanding of this engagement, please sign the enclosed copy where indicated and return it to us.

We appreciate the opportunity to serve you.

Sincerely,

_____

[*Partner's Signature*]
[*Firm Name or Firm Representative*]

Accepted and agreed to:

_____

[*Client Representative's Signature*]

_____

[*Title*]

_____

[*Date*]

Auditing Standards Board (1997)

EDWARD R. NOONAN, *Chair*
JOHN ARCHAMBAULT
LUTHER E. BIRDZELL
JOHN FOGARTY, JR.
JAMES S. GERSON
STEPHEN HOLTON
J. MICHAEL INZINA
NORWOOD JACKSON, JR.
JOHN J. KILKEARY
CHARLES LANDES
STEPHEN MCEACHERN
KURT PANY
EDWARD F. ROCKMAN
ALAN ROSENTHAL
RONALD WALTON

Insurance Companies Committee (1996–1997)

WILLIAM C. FREDA, *Chair*
THOMAS L. BROWN
DAVID A. DIAMOND
DAVID L. HOLMAN
WILLIAM O. KEIM, JR.
JOHN L. LAGUE, JR.
DEBORAH D. LAMBERT
MARTHA E. MARCON
PETER R. PORRINO
PETER W. PRESPERIN
ROBERT J. PRICE
JOSEPH B. SIEVERLING
ROBERT M. SOLITRO
GARY A. SWORDS
THOMAS W. WALSH

Market Conduct Task Force

PATRICK J. SHOUVLIN, *Chair*
THOMAS FINNELL
SUSAN MCGRATH
LAWRENCE J. MOLONEY
MARGARET C. SPENCER

AICPA Staff

THOMAS J. RAY
Director
Audit and Attest Standards

ELAINE M. LEHNERT
Technical Manager
Accounting Standards

[The next page is 31,381.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 14,350

Statement of Position 99-1 Guidance to Practitioners in Conducting and Reporting on an Agreed-Upon Procedures Engagement to Assist Management in Evaluating the Effectiveness of Its Corporate Compliance Program

May 21, 1999

NOTE

This Statement of Position presents the recommendations of the AICPA Health Care Pilot Task Force regarding the application of Statements on Standards for Attestation Engagements to agreed-upon procedures attestation engagements performed to assist a health care provider in evaluating the effectiveness of its corporate compliance program consistent with the requirements of a Corporate Integrity Agreement entered into with the Office of Inspector General of the U.S. Department of Health and Human Services. The Auditing Standards Board has found the recommendations in this Statement of Position to be consistent with existing standards covered by Rule 202 of the AICPA Code of Professional Conduct. AICPA members should be prepared to justify departures from the recommendations in this Statement of Position.

Summary

This Statement of Position (SOP) provides guidance to practitioners in conducting and reporting on an agreed-upon procedures engagement performed pursuant to the AICPA Statements on Standards for Attestation Engagements to assist a health care provider in evaluating the effectiveness of its corporate compliance program consistent with the requirements of a Corporate Integrity Agreement (CIA) entered into with the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services. CIAs are specific to the entity involved; consequently, users of this SOP should be familiar with the specific requirements of the entity's CIA.

Introduction and Background

.01 Within the past several years, the health care industry has experienced a significant increase in the number and magnitude of allegations of fraud and abuse involving federal health care programs (for example, Medicare

and Medicaid) and private health care insurance. These allegations have triggered regulatory scrutiny, litigation, significant monetary settlements, and negative publicity related to—among other things—coding and billing practices, patient referrals, cost reporting, quality of care, and clinical practices. Typically, as part of the global resolution of these allegations, the entity enters into a Corporate Integrity Agreement (CIA) with the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services. Such agreements require that management annually report on its compliance with the terms of the CIA and that there be an assessment of the entity's compliance with the CIA. This assessment includes a billing analysis, which may be performed by an independent review organization (such as a practitioner or consultant) or the provider (if permitted by the OIG), and an agreed-upon procedures engagement.

.02 This SOP provides guidance to practitioners in conducting and reporting on an agreed-upon procedures engagement performed pursuant to the American Institute of Certified Public Accountants (AICPA) Statements on Standards for Attestation Engagements (SSAEs) to assist an entity in evaluating the effectiveness of its corporate compliance program consistent with the requirements of a CIA.[1] The terms of a CIA are unique to the entity; consequently, users of this SOP need to be familiar with the actual CIA and its requirements.

.03 This SOP applies to agreed-upon procedures engagements to assist in evaluating an entity's compliance for a specified period. Such engagements should follow the AICPA attestation standards, including SSAE No. 1, *Attestation Standards*; SSAE No. 3, *Compliance Attestation*; and SSAE No. 4, *Agreed-Upon Procedures Engagements*. The engagement should be conducted in accordance with standards established by the AICPA, including the criteria set forth in this SOP. However, this SOP is not intended to provide all the required criteria set forth in individual CIAs, nor all the applicable standards established by the AICPA. Additionally, the SOP contains some guidance that may be applied in evaluating an organization's corporate compliance program, even though the program was not imposed by a CIA.

Overview of a Typical Corporate Integrity Agreement

.04 A CIA is an agreement between a health care provider and the OIG in conjunction with a global settlement of a fraud investigation. Such an agreement typically seeks to establish a compliance program within the health care provider (for example, hospital, clinical lab, physician group) that will promote compliance with the requirements of Medicare, Medicaid, and all other federal health care programs.

.05 CIAs are case-specific. Their terms are tailored to address the organizational and operating deficiencies related to providing and billing for health care services that have been identified by the OIG, the entity, or others. Detailed

[1] The practitioner also might be engaged to assist in other areas beyond an agreed-upon procedures engagement such as providing consulting services in connection with evaluating the company's billing practices, policies, and procedures as required by the CIA or in implementing, assessing, and reporting on voluntarily adopted compliance programs. In addition, the practitioner may assist in preparing an entity's self-disclosure reports to federal health agencies related to billing errors and other compliance matters. Similarly, practitioners may be involved in an entity's preparation of government-required (but not CIA-imposed) compliance reporting (for example, contract requirements for Medicare part C) beyond an agreed-upon procedures engagement.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

compliance requirements are imposed as a condition for continued participation in federal health care programs. A sample CIA, provided by the OIG and intended to identify potential requirements, is included in appendix A [paragraph .32], "Sample Corporate Integrity Agreement." Typical agreements cover five years and require the entity to address the following areas:

- Appointment of a compliance officer and establishment of a compliance committee
- Establishment of a code of conduct
- Establishment of policies and procedures regarding the compliance program
- Development of an information and education program as to CIA requirements, compliance program and code of conduct
- Annual assessment of billing policies, procedures, and practices
- Establishment of a confidential disclosure program
- Prohibition of employment of excluded or convicted persons
- Notification to OIG of investigation or legal proceedings
- Reporting of credible evidence of misconduct
- Notifications to OIG of new provider locations
- Provision of implementation and annual reports
- Proper notification and submission of required reports
- Granting of OIG access to documents and individuals to conduct assessments
- Documentation of record retention requirements
- Awareness of disclosure criteria
- Agreement to comply with certain default provisions, penalties, and remedies
- Review of rights as to dispute resolution
- Review of effective and binding agreement clauses

Conditions for Engagement Performance

.06 A practitioner may perform an agreed-upon procedures engagement related to management's compliance with a CIA if all of the conditions specified in SSAE No. 4 and SSAE No. 3 are met.

.07 As discussed more fully in the SSAEs noted in paragraph .06, management's assertions as to its compliance must be capable of evaluation against reasonable criteria that either have been established by a recognized body or are stated in or attached to the practitioner's report in a sufficiently clear and comprehensive manner. Generally, to avoid confusion, management's assertions, which are based on the specific terms of its CIA, should be attached to the practitioner's report. If the entity is not subject to a CIA, management may develop its assertions using the model CIA. A sample based on the model CIA, which is not meant to be all-inclusive, is included as appendix B [paragraph .33], "Sample Statement of Management's Assertions."

Establishing an Understanding With the Client

.08 The practitioner should document the understanding in the working papers, preferably through a written communication with the client, such as an engagement letter. Appendix C [paragraph .34], "Sample Engagement Letter," contains a sample engagement letter that may be used for this kind of engagement.

Users' Responsibilities

.09 Users typically would be the management of the health care provider and the OIG. Management is responsible for ensuring that the entity complies with the requirements of the CIA. That responsibility encompasses (*a*) identifying applicable compliance requirements, (*b*) establishing and maintaining internal control policies and procedures to provide reasonable assurance that the entity complies with those requirements, (*c*) evaluating and monitoring the entity's compliance, and (*d*) preparing reports that satisfy legal, regulatory, or contractual requirements. Management's evaluation may include documentation such as accounting or statistical data, policy manuals, accounting manuals, narrative memoranda, procedural write-ups, flowcharts, completed questionnaires, internal auditors' reports, and other special studies or analyses. The form and extent of documentation will vary depending on the nature of the compliance requirements and the size and complexity of the entity. Management may engage the practitioner to gather information to assist it in evaluating the entity's compliance. Regardless of the procedures performed by the practitioner, management must accept responsibility for its assertions and must not base such assertions solely on the practitioner's procedures.

.10 Specified users are responsible for the sufficiency (nature, timing, and extent) of the agreed-upon procedures because they best understand their own needs. The specified users assume the risk that such procedures might be insufficient for their purposes. In addition, the specified users assume the risk that they might misunderstand or otherwise inappropriately use findings properly reported by the practitioner.

Practitioner's Responsibilities

.11 The objective of the practitioner's agreed-upon procedures is to present specific findings to assist users in evaluating an entity's compliance with the requirements specified in the CIA. (See appendix D [paragraph .35], "Sample Procedures.")

.12 The practitioner's procedures generally may be as limited or extensive as the specified users desire, as long as the specified users agree upon the procedures performed or to be performed and take responsibility for the sufficiency of the agreed-upon procedures for their purposes.

.13 To satisfy the requirements that the practitioner and the specified users agree upon the procedures performed or to be performed and that the specified users take responsibility for the sufficiency of the agreed-upon procedures for their purposes, ordinarily the practitioner should communicate directly with and obtain affirmative acknowledgment from each of the specified users. For the purposes of these engagements, an effective way to obtain this agreement ordinarily is to distribute a draft of the report, detailing the procedures, that is expected to be issued to the OIG with a request for any comments it may have.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.14 To avoid possible misunderstandings, the practitioner should circulate the draft with a legend stating that these are the procedures expected to be performed, and unless informed otherwise, the practitioner assumes that there are no additional procedures that he or she is expected to perform. A legend such as the following might be used.

> This draft is furnished solely for the purpose of indicating the form of report that we would expect to be able to furnish pursuant to the request by Management of [*Provider*] for our performance of limited procedures relating to [*Provider's*] compliance with the Corporate Integrity Agreement with the Office of Inspector General (OIG) of the U.S. Department of Heath and Human Services. Based on our discussions with [*Provider*], it is our understanding that the procedures outlined in this draft report are those we are expected to follow. Unless informed otherwise within ninety (90) days of this transmittal, we shall assume that there are no additional procedures that we are expected to follow. The text of the definitive report will depend, of course, on the results of the procedures.

Involvement of a Specialist[2]

.15 The practitioner's education and experience enable him or her to be knowledgeable about business matters in general, but he or she is not expected to have the expertise of a person trained for or qualified to engage in the practice of another profession or occupation. In certain circumstances, it may be appropriate to involve a specialist to assist the practitioner in the performance of one or more procedures. The following are examples:

- An attorney might provide assistance concerning the application of laws, regulations, or rules to a client's situation.
- A medical specialist might provide assistance in understanding the characteristics of diagnosis codes documented in patient medical records.

.16 The practitioner and the specified users should agree to the involvement of a specialist in assisting a practitioner in the performance of an agreed-upon procedures engagement. This agreement may be reached when obtaining agreement on the procedures performed or to be performed and acknowledgment of responsibility for the sufficiency of the procedures, as discussed previously. The practitioner's report should describe the nature of the assistance provided by the specialist.

.17 A practitioner may agree to apply procedures to the report or work product of a specialist that does not constitute assistance by the specialist to the practitioner in an agreed-upon procedures engagement. For example, the practitioner may make reference to information contained in a report of a specialist in describing an agreed-upon procedure. However, it is inappropriate for the practitioner to agree to merely read the specialist's report solely to describe or repeat the findings, or to take responsibility for all or a portion of any procedures performed by a specialist or the specialist's work product.

Internal Auditors and Other Personnel[3]

.18 The agreed-upon procedures to be enumerated or referred to in the practitioner's report are to be performed entirely by the practitioner except as

---

[2] A *specialist* is a person (or firm) possessing special skill or knowledge in a particular field other than the attest function. As used herein, a specialist does not include a person employed by the practitioner's firm who participates in the attestation engagement.

[3] SAS No. 65, *The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements* (AICPA, *Professional Standards*, vol. 1, AU sec. 322), does not apply to agreed-upon procedures engagements.

discussed in paragraphs .15–.17 of this SOP. However, internal auditors or other personnel may prepare schedules, accumulate data, perform an internal assessment of management's compliance, or provide other information for the practitioner's use in performing the agreed-upon procedures.

.19 A practitioner may agree to perform procedures on information documented in the working papers of internal auditors. For example, the practitioner may agree to—

- Repeat all or some of the procedures.
- Determine whether the internal auditors' working papers contain documentation of procedures performed and whether the findings documented in the working papers are presented in a report by the internal auditors.

.20 However, it is inappropriate for the practitioner to—

- Agree to merely read the internal auditor's report solely to describe or repeat its findings.
- Take responsibility for all or a portion of any procedures performed by internal auditors by reporting those findings as the practitioner's own.
- Report in any manner that implies shared responsibility for the procedures with the internal auditors.

Planning the Engagement

.21 Planning an agreed-upon procedures engagement involves working with the users to develop an overall strategy for the expected conduct and scope of the engagement. To develop such a strategy, practitioners should have adequate technical training and proficiency in the attestation standards and have adequate knowledge in health care regulatory matters to enable them to sufficiently understand the events, transactions, and practices that, in their judgment, have a significant effect on the presentation of the assertions.

Working Papers

.22 The practitioner should prepare and maintain working papers in connection with an engagement under the attestation standards; such working papers should be appropriate to the circumstances and the practitioner's needs on the engagement to which they apply.

.23 Concern over access to the practitioner's working papers might cause some clients to inquire about working paper requirements. In situations where the practitioner is requested to not maintain copies of certain client documentation, or to not prepare and maintain documentation similar to client documents, the practitioner may refer to the Auditing Interpretation, "The Auditor's Consideration of the Completeness Assertion" (AICPA, *Professional Standards*, vol. 1, AU sec. 9326.06–.17), for guidance. See the Attest Interpretation, "Providing Access to or Photocopies of Working Papers to a Regulator," for guidance related to providing access to or photocopies of working papers to a regulator in connection with work performed on an attestation engagement.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Management's Representations

.24 The practitioner should obtain written representation from management on various matters including the following:

a. Acknowledging management's responsibility for complying with the CIA

b. Acknowledging management's responsibility for establishing and maintaining effective internal control over compliance

c. Stating that management has performed an evaluation of the entity's compliance with CIA-specified requirements

d. Stating management's assertions about the entity's compliance with all aspects of the CIA, including the specific issues that gave rise to the CIA[4]

e. Stating that management has disclosed to the practitioner all known noncompliance with the CIA

f. Stating that management has made available all documentation relating to compliance with the CIA

g. Stating management's interpretation of any compliance requirements that have varying interpretations

h. Stating that management has disclosed any communication from regulatory agencies, internal auditors, legal counsel, and other parties concerning matters regarding the design, implementation, and monitoring of the policies and procedures in place, including communication received between the end of the reporting period and the date of the practitioner's report (the date of signature)

i. Stating that management has disclosed any known noncompliance occurring subsequent to the end of the reporting period

j. Describing any related material fraud or abuse, other fraud, abuse or illegal acts that, whether or not material, involve management or other employees who have a significant role in the entity's design, implementation, and monitoring of the policies and procedures in place upon which compliance is based

k. Stating that management has disclosed to the practitioners, orally or in writing, information about past noncompliance issues covered in the settlement agreement that gave rise to the CIA and the related corrective measures taken to support compliance in those areas

Management's refusal to furnish all appropriate written representations constitutes a limitation on the scope of the engagement sufficient to require withdrawal from the engagement.

---

[4] Depending on the circumstances, representations in the following areas might be appropriate.
- Violations or possible violations of laws or regulations, such as those related to the Medicare and Medicaid antifraud and abuse statutes
- Compliance of third-party billings with applicable coding guidelines (for example, ICD-9-CM, CPT) and laws and regulations (including medical necessity, proper approvals, and proper rendering of care)
- Proper filing of all required Medicare, Medicaid, and similar reports under the applicable reimbursement rules and regulations (including nature of costs—allowable, patient-related, properly allocated, in accordance with applicable rules and regulations, properly adjusted to reflect prior audit adjustments) and adequacy of disclosures (including disputed costs)

Reporting Considerations

.25 A practitioner should present the results of applying agreed-upon procedures to the specific subject matter in the form of findings. The practitioner should not provide negative assurance about whether the assertion is fairly stated in accordance with established or stated criteria. For example, the practitioner should not include a statement that "nothing came to my attention that caused me to believe that the assertion is not fairly stated in accordance with (established or stated) criteria."

.26 The practitioner should report all findings from the application of the agreed-upon procedures. The concept of materiality does not apply to findings to be reported in an agreed-upon procedures engagement unless the definition of materiality is agreed to by the specified users. Any agreed-upon materiality limits should be described in the practitioner's report.

.27 The practitioner has no obligation to perform procedures beyond the agreed-upon procedures. However, if noncompliance related to management's assertion comes to the practitioner's attention by other means, such information ordinarily should be included in his or her report.

.28 The practitioner may become aware of noncompliance related to management's assertion that occurs subsequent to the reporting period but before the date of the practitioner's report. The practitioner should consider including information regarding such noncompliance in his or her report. However, the practitioner has no responsibility to perform procedures to detect such noncompliance other than obtaining management's representation about noncompliance in the subsequent period.

.29 The practitioner should follow the reporting guidance in SSAE No. 4. A sample report is included in appendix E [paragraph .36], "Sample Report."

.30 Evaluating compliance with certain requirements may require interpretation of the laws, regulations, rules, contracts, or other agreements that establish those requirements. In such situations, the practitioner should consider whether he or she is provided with the reasonable criteria required to evaluate an assertion under the third general attestation standard. If these interpretations are significant, the practitioner may include a paragraph stating the description and the source of interpretations made by the entity's management. An example of such a paragraph, which should precede the procedures and findings paragraph(s), follows:

> We have been informed that, under [*name of entity's*] interpretation of [*identify the compliance requirement*], [*explain the nature and source of the relevant interpretation*].

.31 The date of completion of the agreed-upon procedures should be used as the date of the practitioner's report.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.32

Appendix A

Sample Corporate Integrity Agreement Between the Office of Inspector General of the Department of Health and Human Services and [*Provider*]

I. Preamble

[*Provider*] ("[*Provider*]") hereby enters into this Corporate Integrity Agreement ("CIA") with the Office of Inspector General ("OIG") of the United States Department of Health and Human Services ("HHS") to ensure compliance by its employees with the requirements of Medicare, Medicaid and all other Federal health care programs (as defined in 42 U.S.C. 1320a-7b(f)) (hereinafter collectively referred to as the "Federal health care programs"). [*Provider's*] compliance with the terms and conditions in this CIA shall constitute an element of [*Provider's*] present responsibility with regard to participation in the Federal health care programs. Contemporaneously with this CIA, [*Provider*] is entering into a Settlement Agreement with the United States, and this CIA is incorporated by reference into the Settlement Agreement.

II. Term of the CIA

The period of the compliance obligations assumed by [*Provider*] under this CIA shall be 5 years from the effective date of this CIA (unless otherwise specified). The effective date of this CIA will be the date on which the final signatory of this CIA executes this CIA (the "effective date").*

III. Corporate Integrity Obligations

[*Provider*] shall establish a compliance program that includes the following elements:

A. Compliance Officer

Within ninety (90) days after the effective date of this CIA, [*Provider*] shall appoint an individual to serve as Compliance Officer, who shall be responsible for developing and implementing policies, procedures, and practices designed to ensure compliance with the requirements set forth in this CIA and with the requirements of the Federal health care programs. The Compliance Officer shall be a member of senior management of [*Provider*], shall make regular (at least quarterly) reports regarding compliance matters directly to the CEO and/or to the Board of Directors of [*Provider*] and shall be authorized to report to the Board of Directors at any time. The Compliance Officer shall be responsible for monitoring the day-to-day activities engaged in by [*Provider*] to further its compliance objectives as well as any reporting obligations created under this CIA. In the event a new Compliance Officer is appointed during the term of this CIA, [*Provider*] shall notify the OIG, in writing, within fifteen (15) days of such a change.

---

* *Source:* Office of the Inspector General of the United States Department of Health and Human Services.

[*Provider*] shall also appoint a Compliance Committee within ninety (90) days after the effective date of this CIA. The Compliance Committee shall, at a minimum, include the Compliance Officer and any other appropriate officers as necessary to meet the requirements of this CIA within the provider's corporate structure (e.g., senior executives of each major department, such as billing, clinical, human resources, audit, and operations). The Compliance Officer shall chair the Compliance Committee and the Committee shall support the Compliance Officer in fulfilling his/her responsibilities.

B. Written Standards

1. *Code of Conduct.* Within ninety (90) days of the effective date of this CIA, [*Provider*] shall establish a Code of Conduct. The Code of Conduct shall be distributed to all employees within ninety (90) days of the effective date of this CIA. [*Provider*] shall make the promotion of, and adherence to, the Code of Conduct an element in evaluating the performance of managers, supervisors, and all other employees. The Code of Conduct shall, at a minimum, set forth:

   a. [*Provider's*] commitment to full compliance with all statutes, regulations, and guidelines applicable to Federal health care programs, including its commitment to prepare and submit accurate billings consistent with Federal health care program regulations and procedures or instructions otherwise communicated by the Health Care Financing Administration ("HCFA") (or other appropriate regulatory agencies) and/or its agents;

   b. [*Provider's*] requirement that all of its employees shall be expected to comply with all statutes, regulations, and guidelines applicable to Federal health care programs and with [*Provider's*] own policies and procedures (including the requirements of this CIA);

   c. the requirement that all of [*Provider's*] employees shall be expected to report suspected violations of any statute, regulation, or guideline applicable to Federal health care programs or with [*Provider's*] own policies and procedures;

   d. the possible consequences to both [*Provider*] and to any employee of failure to comply with all statutes, regulations, and guidelines applicable to Federal health care programs and with [*Provider's*] own policies and procedures or of failure to report such non-compliance; and

   e. the right of all employees to use the confidential disclosure program, as well as [*Provider's*] commitment to confidentiality and non-retaliation with respect to disclosures.

   Within ninety (90) days of the effective date of the CIA, each employee shall certify, in writing, that he or she has received, read, understands, and will abide by [*Provider's*] Code of Conduct. New employees shall receive the Code of Conduct and shall complete the required certification within two (2) weeks after the commencement of their employment or within ninety (90) days of the effective date of the CIA, whichever is later.

   [*Provider*] will annually review the Code of Conduct and will make any necessary revisions. These revisions shall be distributed within

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

thirty (30) days of initiating such a change. Employees shall certify on an annual basis that they have received, read, understand and will abide by the Code of Conduct.

2. *Policies and Procedures.* Within ninety (90) days of the effective date of this CIA, [*Provider*] shall develop and initiate implementation of written Policies and Procedures regarding the operation of [*Provider's*] compliance program and its compliance with all federal and state health care statutes, regulations, and guidelines, including the requirements of the Federal health care programs. At a minimum, the Policies and Procedures shall specifically address *[insert language relevant to allegations in the case].* In addition, the Policies and Procedures shall include disciplinary guidelines and methods for employees to make disclosures or otherwise report on compliance issues to [*Provider*] management through the Confidential Disclosure Program required by section III.E. [*Provider*] shall assess and update as necessary the Policies and Procedures at least annually and more frequently, as appropriate. A summary of the Policies and Procedures will be provided to OIG in the Implementation Report. The Policies and Procedures will be available to OIG upon request.

   Within ninety (90) days of the effective date of the CIA, the relevant portions of the Policies and Procedures shall be distributed to all appropriate employees. Compliance staff or supervisors should be available to explain any and all policies and procedures.

C. Training and Education

1. *General Training.* Within ninety (90) days of the effective date of this CIA, [*Provider*] shall provide at least two (2) hours of training to each employee. This general training shall explain [*Provider's*]:

   a. Corporate Integrity Agreement requirements;

   b. Compliance Program (including the Policies and Procedures as they pertain to general compliance issues); and

   c. Code of Conduct.

   These training materials shall be made available to the OIG, upon request.

   New employees shall receive the general training described above within thirty (30) days of the beginning of their employment or within ninety (90) days after the effective date of this CIA, whichever is later. Each year, every employee shall receive such general training on an annual basis.

2. *Specific Training.* Within ninety (90) days of the effective date of this CIA, each employee who is involved directly or indirectly in the delivery of patient care and/or in the preparation or submission of claims for reimbursement for such care (including, but not limited to, coding and billing) for any Federal health care programs shall receive at least [*insert number of training hours*] hours of training in addition to the general training required above. This training shall include a discussion of:

   a. the submission of accurate bills for services rendered to Medicare and/or Medicaid patients;

b. policies, procedures and other requirements applicable to the documentation of medical records;

c. the personal obligation of each individual involved in the billing process to ensure that such billings are accurate;

d. applicable reimbursement rules and statutes;

e. the legal sanctions for improper billings; and

f. examples of proper and improper billing practices.

These training materials shall be made available to OIG, upon request. Persons providing the training must be knowledgeable about the subject area.

Affected new employees shall receive this training within thirty (30) days of the beginning of their employment or within ninety (90) days of the effective date of this CIA, whichever is later. If a new employee has any responsibility for the delivery of patient care, the preparation or submission of claims and/or the assignment of procedure codes prior to completing this specific training, a [*Provider*] employee who has completed the substantive training shall review all of the untrained person's work regarding the assignment of billing codes.

Each year, every employee shall receive such specific training on an annual basis.

3. *Certification.* Each employee shall certify, in writing, that he or she has attended the required training. The certification shall specify the type of training received and the date received. The Compliance Officer shall retain the certifications, along with specific course materials. These shall be made available to OIG upon request.

D. Review Procedures

[*Provider*] shall retain an entity, such as an accounting, auditing or consulting firm (hereinafter "Independent Review Organization"), to perform review procedures to assist [*Provider*] in assessing the adequacy of its billing and compliance practices pursuant to this CIA. This shall be an annual requirement and shall cover a twelve (12) month period. The Independent Review Organization must have expertise in the billing, coding, reporting and other requirements of the Federal health care programs from which [*Provider*] seeks reimbursement. The Independent Review Organization must be retained to conduct the assessment of the first year within ninety (90) days of the effective date of this CIA. For purposes of complying with this review procedures requirement, the OIG at its discretion, may permit the [*Provider*] to utilize internal auditors to perform the review(s). In such case, the [*Provider*] will engage the Independent Review Organization to verify the propriety of the internal auditors' methods and accuracy of their results. The [*Provider*] will request the Independent Review Organization to produce a report on its findings which report shall be included in the Annual Report to the OIG.

The Independent Review Organization (or the [*Provider*], if permitted by the OIG, as set forth above) will conduct two separate engagements. One will be an analysis of [*Provider's*] billing to the Federal health care programs to assist the [*Provider*] and OIG in determining compliance

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

with all applicable statutes, regulations, and directives/guidance ("billing engagement"). The second engagement will assist the [*Provider*] and OIG in determining whether [*Provider*] is in compliance with this CIA ("compliance engagement").

1. *Billing Engagement.* The billing engagement shall consist of a review of a statistically valid sample of claims for the relevant period. The sample size shall be determined through the use of a probe sample.[1] At a minimum, the full sample must be within a ninety (90) percent confidence level and a precision of twenty-five (25) percent. The probe sample must contain at least thirty (30) sample units and cannot be used as part of the full sample. Both the probe sample and the sample must be selected through random numbers. [*Provider*] shall use OIG's Office of Audit Services Statistical Sampling Software, also known as "RAT-STATS", which is available through the Internet at www.hhs.gov/progorg/ratstat.html.

   Each annual billing engagement analysis shall include the following components in its methodology:

   a. Billing Engagement Objective: Provide a statement stating clearly the objective intended to be achieved by the billing engagement and the procedure or combination of procedures that will be applied to achieve the objective.

   b. Billing Engagement Population: Identify the population, which is the group about which information is needed. Explain the methodology used to develop the population and provide the basis for this determination.

   c. Sources of Data: Provide a full description of the source of the information upon which the billing engagement conclusions will be based, including the legal or other standards applied, documents relied upon, payment data, and/or any contractual obligations.

   d. Sampling Unit: Define the sampling unit, which is any of the designated elements that comprise the population of interest.

   e. Sampling Frame: Identify the sampling frame, which is the totality of the sampling units from which the sample will be selected.

   As part of the billing engagement:

   a. Inquire of management as to the procedures and controls affecting the billing process subject to the annual assessment as specified in the CIA. Document that aspect of the billing process (e.g., flow of documents, processing activities), and those controls that will be tested in the sample. The documentation may consist of flow charts, excerpts from policies and procedures manuals, control questionnaires, etc.

   b. Report the sample results, including the overall error rate and the nature of the errors found (e.g., no documentation, inadequate documentation, assignment of incorrect code).

---

[1] Probe sample is defined as a small, random preliminary sample.

c. Document findings related to [*Provider's*] procedures to correct inaccurate billings and codings to the Federal health care programs and findings regarding the steps [*Provider*] is taking to bring its operations into compliance or to correct problems identified by the audit.

2. *Agreed-upon Procedures or Compliance Engagement.* An Independent Review Organization (or the [*Provider*], if permitted by the OIG) shall also conduct an agreed-upon procedures or compliance engagement, which shall assist the users in determining whether [*Provider's*] program, policies, procedures, and operations comply with the terms of this CIA. This engagement shall include a section by section analysis of the requirements of this CIA.

   A complete copy of the Independent Review Organization's billing and agreed-upon procedures or compliance engagement shall be included in each of [*Provider's*] Annual Reports to OIG.

3. *Disclosure of Overpayments and Material Deficiencies.* If, as a result of these engagements, [*Provider*] or the Independent Review Organization identifies any billing, coding or other policies, procedures and/or practices that result in an overpayment, [*Provider*] shall notify the payor (e.g., Medicare fiscal intermediary or carrier) within 30 days of discovering the deficiency or overpayment and take remedial steps within 60 days of discovery (or such additional time as may be agreed to by the payor) to correct the problem, including preventing the deficiency from recurring. The notice to the payor shall include:

   a. a statement that the refund is being made pursuant to this CIA;

   b. a description of the complete circumstances surrounding the overpayment;

   c. the methodology by which the overpayment was determined;

   d. the amount of the overpayment;

   e. any claim-specific information used to determine the overpayment (e.g., beneficiary health insurance number, claim number, service date, and payment date);

   f. the cost reporting period; and

   g. the provider identification number under which the repayment is being made.

   If [*Provider*] determines an overpayment represents a material deficiency, contemporaneous with [*Provider's*] notification to the payor as provided above, [*Provider*] shall also notify OIG of:

   a. a complete description of the material deficiency;

   b. amount of overpayment due to the material deficiency;

   c. [*Provider's*] action(s) to correct and prevent such material deficiency from recurring;

   d. the payor's name, address, and contact person where the overpayment was sent;

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

e. the date of the check and identification number (or electronic transaction number) on which the overpayment was repaid.

For purposes of this CIA, an "overpayment" shall mean the amount of money the provider has received in excess of the amount due and payable under the Federal health care programs' statutes, regulations or program directives, including carrier and intermediary instructions.

For purposes of this CIA, a "material deficiency" shall mean anything that involves: (i) a substantial overpayment or improper payment relating to the Medicare and/or Medicaid programs; (ii) conduct or policies that clearly violate the Medicare and/or Medicaid statute, regulations or directives issued by HCFA and/or its agents; or (iii) serious quality of care implications for federal health care beneficiaries or recipients. A material deficiency may be the result of an isolated event or a series of occurrences.

4. *Verification / Validation.* In the event that the OIG determines that it is necessary to conduct an independent review to determine whether or the extent to which [*Provider*] is complying with its obligations under this CIA, [*Provider*] agrees to pay for the reasonable cost of any such review or engagement by the OIG or any of its designated agents.

E. Confidential Disclosure Program

Within ninety (90) days after the effective date of this CIA, [*Provider*] shall establish a Confidential Disclosure Program, which must include measures (e.g., a toll-free compliance telephone line) to enable employees, contractors, agents or other individuals to disclose, to the Compliance Officer or some other person who is not in the reporting individual's chain of command, any identified issues or questions associated with [*Provider's*] policies, practices or procedures with respect to the Federal health care program, believed by the individual to be inappropriate. [*Provider*] shall publicize the existence of the hotline (e.g., e-mail to employees or post hotline number in prominent common areas).

The Confidential Disclosure Program shall emphasize a non-retribution, non-retaliation policy, and shall include a reporting mechanism for anonymous, confidential communication. Upon receipt of a complaint, the Compliance Officer (or designee) shall gather the information in such a way as to elicit all relevant information from the individual reporting the alleged misconduct. The Compliance Officer (or designee) shall make a preliminary good faith inquiry into the allegations set forth in every disclosure to ensure that he or she has obtained all of the information necessary to determine whether a further review should be conducted. For any disclosure that is sufficiently specific so that it reasonably: (1) permits a determination of the appropriateness of the alleged improper practice, and (2) provides an opportunity for taking corrective action, [*Provider*] shall conduct an internal review of the allegations set forth in such a disclosure and ensure that proper follow-up is conducted.

The Compliance Officer shall maintain a confidential disclosure log, which shall include a record and summary of each allegation received, the status of the respective investigations, and any corrective action taken in response to the investigation.

F. Ineligible Persons

[*Provider*] shall not hire or engage as contractors any "Ineligible Person." For purposes of this CIA, an "Ineligible Person" shall be any individual or entity who: (i) is currently excluded, suspended, debarred or otherwise ineligible to participate in the Federal health care programs; or (ii) has been convicted of a criminal offense related to the provision of health care items or services and has not been reinstated in the Federal health care programs after a period of exclusion, suspension, debarment, or ineligibility.

Within ninety (90) days of the effective date of this CIA, [*Provider*] will review its list of current employees and contractors against the General Services Administration's List of Parties Excluded from Federal Programs (available through the Internet at http://www.arnet.gov/ epls) and the HHS/OIG Cumulative Sanction Report (available through the Internet at http://www.dhhs.gov/progorg/oig) to ensure that it is not currently employing or contracting with any Ineligible Person. Thereafter, [*Provider*] will review the list once semi-annually to ensure that no current employees or contractors are or have become Ineligible Persons.

To prevent hiring or contracting with any Ineligible Person, [*Provider*] shall screen all prospective employees and prospective contractors prior to engaging their services by (i) requiring applicants to disclose whether they are Ineligible Persons, and (ii) reviewing the General Services Administration's List of Parties Excluded from Federal Programs (available through the Internet at http://www.arnet.gov/epls) and the HHS/OIG Cumulative Sanction Report (available through the Internet at http://www.dhhs.gov/progorg/oig).

If [*Provider*] has notice that an employee or agent is charged with a criminal offense related to any Federal health care program, or is suspended or proposed for exclusion during his or her employment or contract with [*Provider*], within 10 days of receiving such notice [*Provider*] will remove such employee from responsibility for, or involvement with, [*Provider's*] business operations related to the Federal health care programs until the resolution of such criminal action, suspension, or proposed exclusion. If [*Provider*] has notice that an employee or agent has become an Ineligible Person, [*Provider*] will remove such person from responsibility for, or involvement with, [*Provider's*] business operations related to the Federal health care programs and shall remove such person from any position for which the person's salary or the items or services rendered, ordered, or prescribed by the person are paid in whole or in part, directly or indirectly, by Federal health care programs or otherwise with Federal funds at least until such time as the person is reinstated into participation in the Federal health care programs.

G. Notification of Proceedings

Within thirty (30) days of discovery, [*Provider*] shall notify OIG, in writing, of any ongoing investigation or legal proceeding conducted or brought by a governmental entity or its agents involving an allegation that [*Provider*] has committed a crime or has engaged in fraudulent activities or any other knowing misconduct. This notification shall include a description of the allegation, the identity of the investigating or prosecuting agency, and the status of such investigation or legal proceeding. [*Provider*] shall also provide written notice to OIG within

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

thirty (30) days of the resolution of the matter, and shall provide OIG with a description of the findings and/or results of the proceedings, if any.

H. Reporting

1. *Credible evidence of misconduct.* If [*Provider*] discovers credible evidence of misconduct from any source and, after reasonable inquiry, has reason to believe that the misconduct may violate criminal, civil, or administrative law concerning [*Provider's*] practices relating to the Federal health care programs, then [*Provider*] shall promptly report the probable violation of law to OIG. Defendants shall make this disclosure as soon as practicable, but, not later than thirty (30) days after becoming aware of the existence of the probable violation. The [*Provider's*] report to OIG shall include:

   a. the findings concerning the probable violation, including the nature and extent of the probable violation;

   b. [*Provider's*] actions to correct such probable violation; and

   c. any further steps it plans to take to address such probable violation and prevent it from recurring.

   To the extent the misconduct involves an overpayment, the report shall include the information listed in section III.D.3 regarding material deficiencies.

2. *Inappropriate Billing.* If [*Provider*] discovers inappropriate or incorrect billing through means other than the Independent Review Organization's engagement, the provider shall follow procedures in section III.D.3 regarding overpayments and material deficiencies.

IV. New Locations

In the event that [*Provider*] purchases or establishes new business units after the effective date of this CIA, [*Provider*] shall notify OIG of this fact within thirty (30) days of the date of purchase or establishment. This notification shall include the location of the new operation(s), phone number, fax number, Federal health care program provider number(s) (if any), and the corresponding payor(s) (contractor specific) that has issued each provider number. All employees at such locations shall be subject to the requirements in this CIA that apply to new employees (e.g., completing certifications and undergoing training).

V. Implementation and Annual Reports

A. Implementation Report

Within one hundred and twenty (120) days after the effective date of this CIA, [*Provider*] shall submit a written report to OIG summarizing the status of its implementation of the requirements of this CIA. This Implementation Report shall include:

1. the name, address, phone number and position description of the Compliance Officer required by section III.A;
2. the names and positions of the members of the Compliance Committee required by section III.A;
3. a copy of [*Provider's*] Code of Conduct required by section III.B.1;

4. the summary of the Policies and Procedures required by section III.B.2;
5. a description of the training programs required by section III.C including a description of the targeted audiences and a schedule of when the training sessions were held;
6. a certification by the Compliance Officer that:
   a. the Policies and Procedures required by section III.B have been developed, are being implemented, and have been distributed to all pertinent employees;
   b. all employees have completed the Code of Conduct certification required by section III.B.1; and;
   c. all employees have completed the training and executed the certification required by section III.C;
7. a description of the confidential disclosure program required by section III.E;
8. the identity of the Independent Review Organization(s) and the proposed start and completion date of the first audit; and
9. a summary of personnel actions taken pursuant to section III.F.

B. Annual Reports

[*Provider*] shall submit to OIG an Annual Report with respect to the status and findings of [*Provider's*] compliance activities. The Annual Reports shall include:

1. any change in the identity or position description of the Compliance Officer and/or members of the Compliance Committee described in section III.A;
2. a certification by the Compliance Officer that:
   a. all employees have completed the annual Code of Conduct certification required by section III.B.1; and
   b. all employees have completed the training and executed the certification required by section III.C;
3. notification of any changes or amendments to the Policies and Procedures required by section III.B and the reasons for such changes (e.g., change in contractor policy);
4. a complete copy of the report prepared pursuant to the Independent Review Organization's billing and compliance engagement, including a copy of the methodology used;
5. [*Provider's*] response/corrective action plan to any issues raised by the Independent Review Organization;
6. a summary of material deficiencies reported throughout the course of the previous twelve (12) months pursuant to III.D.3 and III.H;
7. a report of the aggregate overpayments that have been returned to the Federal health care programs that were discovered as a direct or indirect result of implementing this CIA. Overpayment amounts should be broken down into the following categories: Medicare, Medicaid (report each applicable state separately) and other Federal health care programs;

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

8. a copy of the confidential disclosure log required by section III.E;
9. a description of any personnel action (other than hiring) taken by [*Provider*] as a result of the obligations in section III.F;
10. a summary describing any ongoing investigation or legal proceeding conducted or brought by a government entity involving an allegation that [*Provider*] has committed a crime or has engaged in fraudulent activities, which have been reported pursuant to section III.G. The statement shall include a description of the allegation, the identity of the investigating or prosecuting agency, and the status of such investigation, legal proceeding or requests for information;
11. a corrective action plan to address the probable violations of law identified in section III.H; and
12. a listing of all of the [*Provider's*] locations (including locations and mailing addresses), the corresponding name under which each location is doing business, the corresponding phone numbers and fax numbers, each location's Federal health care program provider identification number(s) and the payor (specific contractor) that issued each provider identification number.

The first Annual Report shall be received by the OIG no later than one year and thirty (30) days after the effective date of this CIA. Subsequent Annual Reports shall be submitted no later than the anniversary date of the due date of the first Annual Report.

C. Certifications

The Implementation Report and Annual Reports shall include a certification by the Compliance Officer under penalty of perjury, that: (1) [*Provider*] is in compliance with all of the requirements of this CIA, to the best of his or her knowledge; and (2) the Compliance Officer has reviewed the Report and has made reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate and truthful.

VI. Notifications and Submission of Reports

Unless otherwise stated in writing subsequent to the effective date of this CIA, all notifications and reports required under this CIA shall be submitted to the entities listed below:

OIG:

Civil Recoveries Branch—Compliance Unit
Office of Counsel to the Inspector General
Office of Inspector General
U.S. Department of Health and Human Services
Cohen Building, Room 5527
330 Independence Avenue, SW
Washington, DC 20201
Phone 202-619-2078; Fax 202-205-0604

[*Provider*]:

[*Address and Telephone number of Provider's Compliance Contact*]

VII. OIG Inspection, Audit and Review Rights

In addition to any other rights OIG may have by statute, regulation, or contract, OIG or its duly authorized representative(s), may examine [*Provider's*] books, records, and other documents and supporting materials for

the purpose of verifying and evaluating: (*a*) [*Provider's*] compliance with the terms of this CIA; and (*b*) [*Provider's*] compliance with the requirements of the Federal health care programs in which it participates. The documentation described above shall be made available by [*Provider*] to OIG or its duly authorized representative(s) at all reasonable times for inspection, audit or reproduction. Furthermore, for purposes of this provision, OIG or its duly authorized representative(s) may interview any of [*Provider's*] employees who consent to be interviewed at the employee's place of business during normal business hours or at such other place and time as may be mutually agreed upon between the employee and OIG. [*Provider*] agrees to assist OIG in contacting and arranging interviews with such employees upon OIG's request. [*Provider's*] employees may elect to be interviewed with or without a representative of [*Provider*] present.

VIII. Document and Record Retention

[*Provider*] shall maintain for inspection all documents and records relating to reimbursement from the Federal health care programs or to compliance with this CIA one year longer than the term of this CIA (or longer if otherwise required by law).

IX. Disclosures

Subject to HHS's Freedom of Information Act ("FOIA") procedures, set forth in 45 C.F.R. Part 5, the OIG shall make a reasonable effort to notify [*Provider*] prior to any release by OIG of information submitted by [*Provider*] pursuant to its obligations under this CIA and identified upon submission by [*Provider*] as trade secrets, commercial or financial information and privileged and confidential under the FOIA rules. [*Provider*] shall refrain from identifying any information as trade secrets, commercial or financial information and privileged and confidential that does not meet the criteria for exemption from disclosure under FOIA.

X. Breach and Default Provisions

[*Provider*] is expected to fully and timely comply with all of the obligations herein throughout the term of this CIA or other time frames herein agreed to.

A. Stipulated Penalties for Failure to Comply with Certain Obligations

As a contractual remedy, [*Provider*] and OIG hereby agree that failure to comply with certain obligations set forth in this CIA may lead to the imposition of the following monetary penalties (hereinafter referred to as "Stipulated Penalties") in accordance with the following provisions.

1. A Stipulated Penalty of $2,500 (which shall begin to accrue on the day after the date the obligation became due) for each day, beginning 120 days after the effective date of this CIA and concluding at the end of the term of this CIA, [*Provider*] fails to have in place any of the following:
   - *a.* a Compliance Officer;
   - *b.* a Compliance Committee;
   - *c.* a written Code of Conduct;
   - *d.* written Policies and Procedures;
   - *e.* a training program; and
   - *f.* a Confidential Disclosure Program;

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

2. A Stipulated Penalty of $2,500 (which shall begin to accrue on the day after the date the obligation became due) for each day [*Provider*] fails to meet any of the deadlines to submit the Implementation Report or the Annual Reports to the OIG.
3. A Stipulated Penalty of $2,000 (which shall begin to accrue on the date the failure to comply began) for each day [*Provider*]:
   a. hires or contracts with an Ineligible Person after that person has been listed by a federal agency as excluded, debarred, suspended or otherwise ineligible for participation in the Medicare, Medicaid or any other Federal health care program (as defined in 42 U.S.C. 1320a7b(f)). This Stipulated Penalty shall not be demanded for any time period if [*Provider*] can demonstrate that it did not discover the person's exclusion or other ineligibility after making a reasonable inquiry (as described in section III.F) as to the status of the person;
   b. employs or contracts with an Ineligible Person and that person: (i) has responsibility for, or involvement with, [*Provider's*] business operations related to the Federal health care programs or (ii) is in a position for which the person's salary or the items or services rendered, ordered, or prescribed by the person are paid in whole or in part, directly or indirectly, by the Federal health care programs or otherwise with Federal funds (this Stipulated Penalty shall not be demanded for any time period during which [*Provider*] can demonstrate that it did not discover the person's exclusion or other ineligibility after making a reasonable inquiry (as described in III.F) as to the status of the person);
   c. employs or contracts with a person who: (i) has been charged with a criminal offense related to any Federal health care program, or (ii) is suspended or proposed for exclusion, and that person has responsibility for, or involvement with, [*Provider's*] business operations related to the Federal health care programs (this Stipulated Penalty shall not be demanded for any time period before 10 days after [*Provider*] received notice of the relevant matter or after the resolution of the matter).
4. A Stipulated Penalty of $1,500 (which shall begin to accrue on the date the [*Provider*] fails to grant access) for each day [*Provider*] fails to grant access to the information or documentation as required in section V of this CIA.
5. A Stipulated Penalty of $1,000 (which shall begin to accrue ten (10) days after the date that OIG provides notice to [*Provider*] of the failure to comply) for each day [*Provider*] fails to comply fully and adequately with any obligation of this CIA. In its notice to [*Provider*], the OIG shall state the specific grounds for its determination that the [Provider] has failed to comply fully and adequately with the CIA obligation(s) at issue.

B. Payment of Stipulated Penalties

1. *Demand Letter.* Upon a finding that [*Provider*] has failed to comply with any of the obligations described in section X.A and

determining that Stipulated Penalties are appropriate, OIG shall notify [*Provider*] by personal service or certified mail of (*a*) [*Provider's*] failure to comply; and (*b*) the OIG's exercise of its contractual right to demand payment of the Stipulated Penalties (this notification is hereinafter referred to as the "Demand Letter").

Within fifteen (15) days of the date of the Demand Letter, [*Provider*] shall either (*a*) cure the breach to the OIG's satisfaction and pay the applicable stipulated penalties, or (*b*) request a hearing before an HHS administrative law judge ("ALJ") to dispute the OIG's determination of noncompliance, pursuant to the agreed-upon provisions set forth below in section X.D. In the event [*Provider*] elects to request an ALJ hearing, the Stipulated Penalties shall continue to accrue until [*Provider*] cures, to the OIG's satisfaction, the alleged breach in dispute. Failure to respond to the Demand Letter in one of these two manners within the allowed time period shall be considered a material breach of this CIA and shall be grounds for exclusion under section X.C.

2. *Timely Written Requests for Extensions.* [*Provider*] may submit a timely written request for an extension of time to perform any act or file any notification or report required by this CIA. Notwithstanding any other provision in this section, if OIG grants the timely written request with respect to an act, notification, or report, Stipulated Penalties for failure to perform the act or file the notification or report shall not begin to accrue until one day after [*Provider*] fails to meet the revised deadline as agreed to by the OIG-approved extension. Notwithstanding any other provision in this section, if OIG denies such a timely written request, Stipulated Penalties for failure to perform the act or *file* the notification or report shall not begin to accrue until two (2) business days after [*Provider*] receives OIG's written denial of such request. A "timely written request" is defined as a request in writing received by OIG at least five (5) business days prior to the date by which any act is due to be performed or any notification or report is due to be filed.
3. *Form of Payment.* Payment of the Stipulated Penalties shall be made by certified or cashier's check, payable to "Secretary of the Department of Health and Human Services," and submitted to OIG at the address set forth in section VI.
4. *Independence from Material Breach Determination.* Except as otherwise noted, these provisions for payment of Stipulated Penalties shall not affect or otherwise set a standard for the OIG's determination that [*Provider*] has materially breached this CIA, which decision shall be made at the OIG's discretion and governed by the provisions in section X.C, below.

C. Exclusion for Material Breach of this CIA

1. *Notice of Material Breach and Intent to Exclude.* The parties agree that a material breach of this CIA by [*Provider*] constitutes an independent basis for [*Provider's*] exclusion from participation in the Federal health care programs (as defined in 42 U.S.C. 1320a7b(f)). Upon a determination by OIG that [*Provider*] has materially breached this CIA and that exclusion should be imposed, the OIG shall notify [Provider] by certified mail of (*a*) [*Provider's*] material breach; and (*b*) OIG's intent to exercise its

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

contractual right to impose exclusion (this notification is hereinafter referred to as the "Notice of Material Breach and Intent to Exclude").

2. *Opportunity to Cure.* [*Provider*] shall have thirty-five (35) days from the date of the Notice of Material Breach and Intent to Exclude Letter to demonstrate to the OIG's satisfaction that:

   a. [*Provider*] is in *full* compliance with this CIA;

   b. the alleged material breach has been cured; or

   c. the alleged material breach cannot be cured within the 35-day period, but that: (i) [*Provider*] has begun to take action to cure the material breach, (ii) [*Provider*] is pursuing such action with due diligence, and (iii) [*Provider*] has provided to OIG a reasonable timetable for curing the material breach.

3. *Exclusion Letter.* If at the conclusion of the thirty-five (35) day period, [*Provider*] fails to satisfy the requirements of section X.C.2, OIG may exclude [*Provider*] from participation in the Federal health care programs. OIG will notify [*Provider*] in writing of its determination to exclude [*Provider*] (this letter shall be referred to hereinafter as the "Exclusion Letter"). Subject to the Dispute Resolution provisions in section X.D, below, the exclusion shall go into effect thirty (30) days after the date of the Exclusion Letter. The exclusion shall have national effect and will also apply to all other federal procurement and non-procurement programs. If [*Provider*] is excluded under the provisions of this CIA, [*Provider*] may seek reinstatement pursuant to the provisions at 42 C.F.R. §§1001.3001–.3004.

4. *Material Breach.* A material breach of this CIA means:

   a. a failure by [*Provider*] to report a material deficiency, take corrective action and pay the appropriate refunds, as provided in section III.D;

   b. repeated or flagrant violations of the obligations under this CIA, including, but not limited to, the obligations addressed in section X.A of this CIA;

   c. a failure to respond to a Demand Letter concerning the payment of Stipulated Penalties in accordance with section X.B above; or

   d. a failure to retain and use an Independent Review Organization for review purposes in accordance with section III.D.

D. Dispute Resolution

1. *Review Rights.* Upon the OIG's delivery to [*Provider*] of its Demand Letter or of its Exclusion Letter, and as an agreed-upon contractual remedy for the resolution of disputes arising under the obligation of this CIA, [*Provider*] shall be afforded certain review rights comparable to the ones that are provided in 42 U.S.C. §§1320a7(f) and 42 C.F.R. §1005 as if they applied to the Stipulated Penalties or exclusion sought pursuant to this CIA. Specifically, the OIG's determination to demand payment of Stipulated Penalties or to seek exclusion shall be subject to review

by an ALJ and, in the event of an appeal, the Departmental Appeals Board ("DAB"), in a manner consistent with the provisions in 42 C.F.R. §§1005.2–.21. Notwithstanding the language in 42 C.F.R. §1005.2(c), the request for a hearing involving stipulated penalties shall be made within fifteen (15) days of the date of the Demand Letter and the request for a hearing involving exclusion shall be made within thirty (30) days of the date of the Exclusion Letter.

2. *Stipulated Penalties Review.* Notwithstanding any provision of Title 42 of the United States Code or Chapter 42 of the Code of Federal Regulations, the only issues in a proceeding for stipulated penalties under this CIA shall be (*a*) whether [*Provider*] was in full and timely compliance with the obligations of this CIA for which the OIG demands payment; and (*b*) the period of noncompliance. [*Provider*] shall have the burden of proving its full and timely compliance and the steps taken to cure the noncompliance, if any. If the ALJ finds for the OIG with regard to a finding of a breach of this CIA and orders [*Provider*] to pay Stipulated Penalties, such Stipulated Penalties shall become due and payable twenty (20) days after the ALJ issues such a decision notwithstanding that [*Provider*] may request review of the ALJ decision by the DAB.

3. *Exclusion Review.* Notwithstanding any provision of Title 42 of the United States Code or Chapter 42 of the Code of Federal Regulations, the only issues in a proceeding for exclusion based on a material breach of this CIA shall be (*a*) whether [*Provider*] was in material breach of this CIA; (*b*) whether such breach was continuing on the date of the Exclusion Letter; and (*c*) the alleged material breach cannot be cured within the 35-day period, but that (i) [*Provider*] has begun to take action to cure the material breach, (ii) [*Provider*] is pursuing such action with due diligence, and (iii) [*Provider*] has provided to OIG a reasonable timetable for curing the material breach.

   For purposes of the exclusion herein, exclusion shall take effect only after an ALJ decision that is favorable to the OIG. [*Provider's*] election of its contractual right to appeal to the DAB shall not abrogate the OIG's authority to exclude [*Provider*] upon the issuance of the ALJ's decision. If the ALJ sustains the determination of the OIG and determines that exclusion is authorized, such exclusion shall take effect twenty (20) days after the ALJ issues such a decision, notwithstanding that [*Provider*] may request review of the ALJ decision by the DAB.

4. *Finality of Decision.* The review by an ALJ or DAB provided for above shall not be considered to be an appeal right arising under any statutes or regulations. Consequently, the parties to this CIA agree that the DAB's decision (or the ALJ's decision if not appealed) shall be considered final for all purposes under this CIA and [*Provider*] agrees to waive any right it may have to appeal the decision administratively, judicially or otherwise seek review by any court or other adjudicative forum.

XI. Effective and Binding Agreement

Consistent with the provisions in the Settlement Agreement pursuant to which this CIA is entered, and into which this CIA is incorporated, [*Provider*] and OIG agree as follows:

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

a. This CIA shall be binding on the successors, assigns and transferees of [*Provider*];

b. This CIA shall become final and binding on the date the final signature is obtained on the CIA;

c. Any modifications to this CIA shall be made with the prior written consent of the parties to this CIA; and

d. The undersigned [*Provider*] signatories represent and warrant that they are authorized to execute this CIA. The undersigned OIG signatory represents that he is signing this CIA in his official capacity and that he is authorized to execute this CIA.

On Behalf of [*Provider*]

_____ _____
[*Date*]

_____ _____
[*Date*]

_____ _____
[*Date*]

[*Please identify all signatories*]

ON BEHALF OF THE OFFICE OF INSPECTOR GENERAL OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES

_____ _____
Lewis Moris [*Date*]

Assistant Inspector General for Legal Affairs
Office of Inspector General
U.S. Department of Health and Human Services

Appendix B

Sample Statement of Management's Assertions

[*Date*]

In connection with the Corporate Integrity Agreement (CIA) entered into with the Office of the Inspector General of the United States Department of Health and Human Services dated [*date*], we make the following assertions, which are true to the best of our knowledge and belief.

Governance

Within 90 days of the date of the CIA, we—

1. Established a Compliance Committee, which meets at least monthly and requires a quorum to meet.
2. Appointed to our Compliance Committee members who include at a minimum those individuals specified in the CIA.
3. Delegated to the Compliance Committee the authority to implement and monitor the CIA, as evidenced by the organization chart or the Compliance Committee's charter.
4. Appointed a compliance officer, who reports directly to the individual specified in the CIA.

We appointed a compliance officer who—

1. Has sufficient staff and resources to carry out his or her responsibilities.
2. Actively participates in compliance training.
3. Has authority to conduct full and complete internal investigations without restriction.
4. Periodically revises the compliance program to meet changing circumstances and risks.

Billing Practices, Policies, and Procedures

Although no system of internal controls can provide absolute assurance that all bills comply in all respects with Medicare, Medicaid, and other federal health care program guidelines, we are not aware of any material weaknesses in our billing practices, policies, and procedures. Billings to third-party payors comply in all material respects with applicable coding principles and laws and regulations (including those dealing with Medicare and Medicaid antifraud and abuse) and only reflect charges for goods and services that were medically necessary, properly approved by regulatory bodies (e.g., the Food and Drug Administration), if required and properly rendered. [*Insert other assertions as necessary to address matters covered in the CIA.*] Any Medicare, Medicaid, and other federal health program billing deficiencies that we identified have been properly reported to the applicable payor within 60 days of discovery of the deficiency.

Corporate Integrity Policy

1. Our policy was developed and implemented within [*number*] days of execution of the CIA.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

2. The policy addresses the Company's commitment to preparation and submission of accurate billings consistent with the standards set forth in federal health care program statutes, regulations, procedures and guidelines or as otherwise communicated by Health Care Financing Administration (HCFA), its agents or any other agency engaged in the administration of the applicable federal health care program.

3. The policy addressed the specific issues that gave rise to the settlement, as well as other risk areas identified by the OIG in published Fraud Alerts issued through [*date*].

4. Further details on the development and implementation of our policy were provided to the OIG in our letter dated [*date*].

5. Our policy was distributed to all employees, physicians and independent contractors involved in submitting or preparing requests for reimbursement.

6. We have prominently displayed a copy of our policy on the Company's premises.

Information and Education Program

As discussed more fully in our letter to the OIG dated [*date*], we conducted an Information and Education Program within [*number*] days of the CIA. The Information and Education Program requires that each officer, employee, agent and contractor charged with administering federal health care programs (including, but not limited to billers, coders, nurses, physicians, medical records, hospital administration and other individuals directly involved in billing federal health care programs) receive at least [*number*] hours of training.

The training provided to employees involved in billing, coding, and/or charge capture consisted of instructions on submitting accurate bills, the personal obligations of each individual to ensure billings are accurate, the nature of company-imposed disciplinary actions on individuals who violate company policies and/or laws and regulations, applicable federal health care program rules, legal sanctions against the company for submission of false or fraudulent information, and how to report potential abuses or fraud. The training material addresses those issues underlying our settlement with the OIG.

The experience of the trainers is consistent with the topics presented.

Confidential Disclosure Program

Our Confidential Disclosure Program—

1. Was established within [*number*] days of the CIA.

2. Enables any employee to disclose any practices or billing procedures relating to federal health care programs.

3. Provides a toll-free telephone line maintained by the Company, which Company representatives have indicated is maintained twenty-four hours a day, seven days a week, for the purpose of making any disclosures regarding compliance with the Company's Compliance Program, the obligations in the CIA, and Company's overall compliance with federal and state standards.

4. Includes policies requiring the review of any disclosures to permit a determination of the appropriateness of the billing practice alleged to be involved and any corrective action to be taken to ensure that proper follow-up is conducted.
5. A detailed summary of the communications (including the number of disclosures by employees and the dates of such disclosures) concerning billing practices reported as, and found to be, inappropriate under the Confidential Disclosure Program, and the results of any internal review and the follow-up on such disclosures are summarized in Attachment [*title*] to our Annual Report.

Excluded Individuals or Entities

Company policy—

1. Prohibits the employment of or contracting with an individual or entity that is listed by a federal agency as convicted of abuse or excluded, suspended or otherwise ineligible for participation in federal health care programs.
2. Includes a process to make an inquiry into the status of any potential employee or independent contractor.
3. Provides for an annual review of the status of all existing employees and contractors to verify whether any individual had been suspended or excluded or charged with a criminal offense relating to the provision of federal health care services.

We are not aware of any individuals employed in contravention of the prohibitions in the CIA.

Record Retention

Our record retention policy is consistent with the requirements of the CIA.

Signed by:

_____
[*Chief Executive Officer*]

_____
[*Chief Financial Officer*]

_____
[*Corporate Compliance Officer*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.34

Appendix C

Sample Engagement Letter

The following is an illustration of a sample engagement letter that may be used for this kind of engagement.

[*CPA Firm Letterhead*]

[*Client's Name and Address*]

Dear _____:

This will confirm our understanding of the arrangements for our performance of certain agreed-upon procedures in connection with management's compliance with the terms of the Corporate Integrity Agreement (CIA) with the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services (HHS) dated [*date of CIA*] for the period ending [*date*].

We will perform those procedures enumerated in the attachment to this letter. Our responsibility is to carry out these procedures and report our findings. We will conduct our engagement in accordance with standards established by the American Institute of Certified Public Accountants. Our planned procedures were agreed to by management and will be communicated to the OIG for its review and are based on the terms specified in the CIA. The sufficiency of these procedures is solely the responsibility of the specified users of the report. Consequently, it is understood that we make no representation regarding the sufficiency of the procedures described in the attachment for the purpose for which this report has been requested or for any other purpose.

Management is responsible for the Company's compliance with all applicable laws, regulations, and contracts and agreements, including the CIA. Management also is responsible for the design, implementation, and monitoring of the policies and procedures upon which compliance is based.

Our engagement to perform agreed-upon procedures is substantially less in scope than an examination, the objective of which is the expression of an opinion on management's compliance with the CIA. Accordingly, we will not express such an opinion or any other form of assurance thereon.[1]

---

[1] The independent accountant may wish to include an understanding with the client about any limitation or other arrangements regarding liability of the practitioner or the client in the engagement letter. For example, the following might be included in the letter:

Our maximum liability relating to services rendered under this letter (regardless of form of action, whether in contract, negligence or otherwise) shall be limited to the charges paid to us for the portion of the services or work products giving rise to liability. We will not be liable for consequential or punitive damages (including lost profits or savings) even if aware of their possible existence.

You will indemnify us against any damage or expense that may result from any third-party claim relating to our services or any use by you of any work product, and you will reimburse us for all expenses (including counsel fees) as incurred by us in connection with any such claim, except to the extent such claim (i) is finally determined to have resulted from our gross negligence or willful misconduct or (ii) is covered by any of the preceding indemnities.

Working papers that are prepared in connection with this engagement are the property of the independent accountant. The working papers are prepared for the purpose of providing the principal support for the independent accountant's report. At the completion of our work, we expect to issue an agreed-upon procedures report in the attached form.

If, however, we are not able to complete all of the specified procedures, we will so advise you. At that time, we will discuss with you the form of communication, if any, that you desire for our findings. We will ask you to confirm your request in writing at that time. If you request that we delay issuance of our report until corrective action is taken that will result in compliance with all aspects of the CIA, we will do so only at your written request. Our working papers will be retained in accordance with our firm's working paper retention policy.

The distribution of the independent accountant's report will be restricted to the governing board and management of the Company and the OIG.

Our fees will be billed as work progresses and are based on the amount of time required at various levels of responsibility plus actual out-of-pocket expenses. Invoices are payable upon presentation. We will notify you immediately of any circumstances we encounter that could significantly affect our initial estimate of total fees.

We agree that to the extent required by law, we will allow the Comptroller General of the United States, HHS, and their duly authorized representatives to have access to this engagement letter and our documents and records to the extent necessary to verify the nature and amount of costs of the services provided to the Company, until the expiration of four years after we have concluded providing services to the Company that are performed pursuant to this Engagement Letter. In the event the Comptroller General, HHS, or their duly authorized representatives request such records, we agree to notify the Company of such request as soon as practicable.

In the event we are requested or authorized by the Company or are required by government regulation, subpoena, or other legal process to produce our documents or our personnel as witnesses with respect to our engagements for the Company, the Company will, so long as we are not a party to the proceeding in which the information is sought, reimburse us for our professional time and expenses, as well as the fees and expenses of our counsel, incurred in responding to such requests.

If this letter correctly expresses your understanding of this engagement, please sign the enclosed copy where indicated and return it to us. We appreciate the opportunity to serve you.

Sincerely, _____
[*Partner's Signature*]
[*Firm Name or Firm Representative*]

Accepted and agreed to: _____
[*Client Representative's Signature*]

[*Title*] _____

[*Date*] _____

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.35

Appendix D

Sample Procedures

Procedure	*Findings*

Governance

1. We read the Company's corporate minutes and organization chart and ascertained that, within [*number*] days of the date of the Corporate Integrity Agreement (CIA), the Company—
   a. Established a Compliance Committee, which is to meet meets at least monthly and requires a quorum to meet.
   b. Appointed to its Compliance Committee members who include, at a minimum, those individuals specified in the CIA.
   c. Delegated to the Compliance Committee the authority to implement and monitor the CIA, as evidenced by the organization chart or the Compliance Committee's charter.
   d. Appointed a compliance officer who reports directly to the individual specified in the CIA.
2. We interviewed the compliance officer and were informed that, in his or her opinion, the Compliance Officer—
   a. Has sufficient staff and resources to carry out his or her responsibilities.
   b. Actively participates in compliance training.
   c. Has the authority to conduct full and complete internal investigations without restriction.
   d. Periodically revises the compliance program to meet changing circumstances and risks.
3. We read the OIG notification letter as specified in the CIA and noted that the appropriate official signed the letter, that it was addressed to the OIG, that it covered items (*a*) through (*d*) in Step 1, and that it was dated within [*number of*] days of the execution of the CIA.

Billing Practices, Policies, and Procedures

The practitioner might be engaged to provide consulting services in connection with the evaluation of the Company's billing practices, policies, and procedures. If so, generally no agreed-upon procedures would be performed relating to this area.

Alternatively, if the procedures relating to the Company's billing practices, policies, and procedures are performed by others such as the Company's internal audit staff, the practitioner performs Steps 4 through 9.

Procedure	*Findings*

4. We read the compliance work plan and noted the following:
   a. The work plan's stated objectives include the determination that billings are accurate and complete, for services rendered that have been deemed by medical specialists as being necessary, and are submitted in accordance with federal program guidelines.
   b. The work plan sampling methodology sets confidence levels consistent with those defined in the CIA.
   c. The work plan identifies risk areas, as defined in the CIA (if applicable), and specifies testing procedures by risk area.
   d. The work plan specifies that samples are taken in risk areas (if applicable) identified by the CIA.
   e. The work plan includes testing procedures, which the practitioner should modify as required by the CIA, for the following risks areas (if applicable) identified in the CIA:
      (1) Clinical documentation, as follows:
         (i) No documentation of service
         (ii) Insufficient documentation of service
         (iii) Improper diagnosis or treatment plan giving rise to the provision of a medically unnecessary service or treatment
         (iv) Service or treatment does not conform medically with the documented diagnosis or treatment plan
         (v) Services incorrectly coded
      (2) Billing and coding, as follows:
         (i) Noncovered or unallowable service
         (ii) Duplicate payment
         (iii) DRG window error
         (iv) Unbundling
         (v) Utilization
         (vi) Medicare credit balances

   [*Note to Practitioner:* Modify the preceding list as required by the CIA.]

5. We selected [*quantity*] probe samples performed by the independent review organization for the following risk areas [*list risk areas tested*]. For the probe samples selected, we noted that the—
   a. Sample patient billing files were randomly selected.
   b. Sample size reflected confidence levels specified in the CIA.
   c. Sample plan describes how missing items (if any) would be treated.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedure	*Findings*

d. Patient billing files tested were pulled per the listing of random numbers and all patient billing files were accounted for in the working papers.

e. Work plans for the specific sample described the risk areas (if applicable) being tested and the testing approach/procedures.

f. Working papers noted the completion of each work plan step.

g. Working papers contained a summary of findings for the sample.

6. We reperformed the work plan steps [*list of specific steps performed*] for the sample patient billing files. The reperformance of work plan steps related to the medical review of the sample patient billing files was performed by the following individuals [*note the professional qualifications of individuals without listing names*]. Any exceptions between our findings and the Company's are summarized in the Attachment to this report.

7. We read the summary findings of all internal compliance reviews that the Company's Internal Audit department indicated it had performed for the Company and noted that all material billing deficiencies [*specify material threshold as defined by the Company*] noted therein were discussed in written communications addressed to the appropriate payor (for example, Medicare Part B carrier) and were dated within 60 days from the time the deficiency occurred.[1]

8. We inquired of [*individual*] as to whether the Company took remedial steps within [*number of*] days (or such additional time as agreed to by the payor) to correct all material billing deficiencies noted in Step 7. We were informed that such remedial steps had been taken.

9. By reading applicable correspondence, we noted that any material billing deficiencies noted in Step 7 were communicated to the OIG, including specific findings relative to the deficiency, the Company's actions taken to correct the deficiency, and any further steps the Company plans to take to prevent any similar deficiencies from recurring.

[1] The CIA provides its own legal definition of a "material deficiency." Determination of whether a billing or other act meets this definition is normally beyond the auditor's professional competence and may have to await final determination by a court of law. Accordingly, to avoid confusion, a working definition different from that provided in the CIA (e.g., a specified dollar threshold) may be necessary.

Procedure	*Findings*

Corporate Integrity Policy

10. We read the Company's Corporate Integrity Policy and noted the following.
    a. The policy was developed and implemented within [*number of*] days of execution of the CIA.
    b. The policy addressed the Company's commitment to preparation and submission of accurate billings consistent with the standards set forth in federal health care program statutes, regulations, procedures, and guidelines or as otherwise communicated by HCFA, its agents, or any other agency engaged in the administration of the applicable federal health care program.
    c. The policy addressed the specific issues that gave rise to the settlement, as well as other risk areas identified by the OIG in published Fraud Alerts issued through [*agency*].
    d. Correspondence addressed to the OIG covered the development and implementation of the policy.
    e. Documentation indicating that the policy was distributed to all employees, physicians, and independent contractors involved in submitting or preparing requests for reimbursement.
    f. The prominent display of a copy of the policy on the Company's premises.
11. We selected a sample of ten employees (involved in submitting and preparing requests for reimbursement) and examined written confirmation in the employee's personnel file indicating receipt of a copy of the Corporate Integrity Policy.

Information and Education Program

12. We read the Company's Information and Education Program and noted the following.
    a. The Information and Education Program agenda was dated within [number of] days of execution of the CIA.
    b. Correspondence covering the development and implementation of the Information and Education Program was addressed to the OIG.
    c. The Information and Education Program requires that each officer, employee, agent, and contractor charged with administering federal health care programs (including, but not limited to billers, coders, nurses, physicians, medical records, hospital administration and other individuals directly involved in billing federal health care programs) receive at least [*number of*] hours of training.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedure	*Findings*

13. We selected a sample of ten employees involved in billing, coding and/or charge capture and examined sign-in logs of the training classes and noted that each had signed indicating that they had received at least *[number of]* hours of training as specified in the Information and Education Program. We also reviewed tests and surveys completed by each of the ten trained employees noting evidence that they were completed.

14. We inquired as to the training of individuals not present during the regularly scheduled training programs and were informed that each such individual is trained either individually or in a separate make-up session. We inquired as to the names of individuals not initially present and selected one such individual and examined that individual's post-training test and survey for completion.

15. We read the course agenda and noted that the training provided to employees involved in billing, coding, and/or charge capture consisted of instructions on submitting accurate bills, the personal obligations of each individual to ensure billings are accurate, the nature of company-imposed disciplinary actions on individuals who violate company policies and/or laws and regulations applicable to federal health care program rules, legal sanctions against the company for submission of false or fraudulent information, and how to report potential abuses or fraud. We also noted that the training material addressed the following issues which gave rise to the settlement [*practitioner list*].

16. We inquired of the Corporate Compliance Officer as to the qualifications and experience of the trainers and were informed that, in the Corporate Compliance Officer's opinion, they were consistent with the topics presented.

17. We noted that the Company's draft Annual Report to the OIG dated [*date*] addresses certification of training.

Confidential Disclosure Program

18. We read documentation of the Company's Confidential Disclosure Program and noted that it—
    a. Includes the printed effective date that was within [*number of*] days of execution of the CIA.
    b. Consists of a confidential disclosure program enabling any employee to disclose any practices or billing procedures relating to federal health care programs.

Procedure	*Findings*

c. Provides a toll-free telephone line maintained by the Company, which Company representatives have indicated is maintained twenty-four hours a day, seven days a week, for the purpose of making any disclosures regarding compliance with the Company's Compliance Program, the obligations in the CIA, and Company's overall compliance with federal and state standards.

d. Includes policies requiring the review of any disclosures to permit a determination of the appropriateness of the billing practice alleged to be involved and any corrective action to be taken to ensure that proper follow-up is conducted.

19. We made five test calls to the toll-free telephone line (hotline) and noted the following.
    a. Each call was captured in the hotline logs and reported with all other incoming calls.
    b. Anonymity is not discouraged.

20. We noted that the Company included in its draft Annual Report addressed to OIG dated [*date*] a detailed summary of the communications (including the number of disclosures by employees and the dates of such disclosures) concerning billing practices reported as, and found to be, inappropriate under the Confidential Disclosure Program, and the results of any internal review and the follow-up on such disclosures.

21. We observed the display of the Company's Confidential Disclosure Program, including notice of the availability of its hotline, on the Company's premises.

Excluded Individuals or Entities

22. We read the Company's written policy relating to dealing with excluded or convicted persons or entities and noted that the policy—
    a. Prohibits the hiring of or contracting with an individual or entity that is listed by a federal agency as convicted of abuse or excluded, suspended, or otherwise ineligible for participation in federal health care programs.
    b. Includes a process to make an inquiry into the status of any potential employee or independent contractor.
    c. Provides for a semi-annual review of the status of all existing employees and contractors to verify whether any individual had been suspended or excluded or charged with a criminal offense relating to the provision of federal health care services.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedure	*Findings*

23. We selected a sample of ten employees hired over the course of the test period as defined in the CIA and examined support in the employee's personnel file documenting inquiries made into the status of the employee, including documentation of comparison to the [*source specified in the CIA*].

24. We performed the following procedures related to the Company's semi-annual review of employee status.
    a. Read documentation of the semi-annual review as evidence that a review was performed.
    b. Selected and reviewed the lesser of ten or all exceptions and determined that such employees were removed from responsibility for or involvement with Provider business operations related to the Federal health care programs.
    c. Examined a notification letter addressed to the OIG and dated within 30 days of the employee's removal from employment.
    d. Inquired of [*officer*] as to whether he or she was aware of any individuals employed in contravention of the prohibitions in the CIA. If so, we further noted that [*indicate specific procedures*] to confirm that such situation was cured within 30 days by [*indicate how situation was cured*].

Annual Report

25. We read the Company's draft Annual Report dated [*date*] and determined that it included the following items, to be modified as appropriate, by the practitioner:
    a. Compliance Program Charter and organization chart
    b. Amendments to policies
    c. Detailed descriptions of reviews and audits
    d. Summary of hotline communications
    e. Summary of annual review of employees
    f. Cross-referencing to items noted in the CIA

Record Retention

26. We read the Company's record retention policy and noted that it was consistent with the requirements as outlined in the CIA.

Appendix E

Sample Report

Independent Accountant's Report

[*Date*]

[*Sample Health Care Provider*]
Office of Inspector General of the U.S. Department of Health and Human Services

We have performed the procedures enumerated in the Attachment, which were agreed to by Sample Health Care Provider (Company) and the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services, solely to assist the users in evaluating management's assertion about [*name of entity's*] compliance with the Corporate Integrity Agreement (CIA) with the OIG dated [*date of CIA*] for the [*period*] ending [*date*], which is included as Attachment A to this report. This agreed-upon procedures engagement was performed in accordance with standards established by the American Institute of Certified Public Accountants. The sufficiency of these procedures is solely the responsibility of the specified users of the report. Consequently, we make no representation regarding the sufficiency of the procedures described in Attachment B either for the purpose for which this report has been requested or for any other purpose.

We were not engaged to and did not perform an examination, the objective of which would be the expression of an opinion on management's compliance with the CIA. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

This report is intended solely for the information and use of the Compliance Committee and management of the Company and the OIG, and is not intended to be and should not be used by anyone other than those specified parties.

[*Include as Attachments the CIA and the summary that enumerates procedures and findings.*]

[*Signature*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Auditing Standards Board
1998

DEBORAH D. LAMBERT, *Chair*
JAMES S. GERSON, *Vice Chair*
JOHN T. BARNUM
ANDREW J. CAPELLI
ROBERT F. DACEY
RICHARD DIETER
SALLY L. HOFFMAN
STEPHEN D. HOLTON
J. MICHAEL INZINA
CHARLES E. LANDES
KEITH O. NEWTON
ALAN ROSENTHAL
R.C. STEINER
GEORGE H. TUCKER III
OLIVER R. WHITTINGTON

Health Care Pilot Task Force
1998

WILLIAM R. TITERA, *Chair*
DIANE CORNWELL
WILLIAM T. CUPPETT
DENNIS J. DUQUETTE
ERIC HOLZBERG
MARY R. MACBAIN
JOSEPH N. STEAKLEY

SOP Task Force

WILLIAM R. TITERA, *Chair*
ROBERT D. BEARD
GARY BREUER
DENNIS J. DUQUETTE
MARK EDDY
WILLIAM HORNBY
LEWIS MORRIS
JOSEPH N. STEAKLEY

AICPA Staff

BARBARA VIGILANTE
Technical Manager
PCPS / MAP

JANE MANCINO
Technical Manager
Audit and Attest Standards

KARYN WALLER
Technical Manager
Industry and Management Accounting

[The next page is 31,431.]

Section 14,360

Statement of Position 00-1 Auditing Health Care Third-Party Revenues and Related Receivables

March 10, 2000

NOTE

This Statement of Position presents the recommendations of the AICPA Health Care Third-Party Revenue Recognition Task Force with regard to auditing financial statement assertions about third-party revenues and related receivables of health care entities. The Auditing Standards Board has found the recommendations in this Statement of Position to be consistent with existing standards covered by rule 202 of the AICPA Code of Professional Conduct. AICPA members should be prepared to justify departures from the recommendations in this Statement of Position.

Summary

This Statement of Position (SOP) provides guidance to auditors regarding uncertainties inherent in health care third-party revenue recognition. It discusses auditing matters to consider in testing third-party revenues and related receivables, and provides guidance regarding the sufficiency of evidential matter and reporting on financial statements of health care entities exposed to material uncertainties.

Introduction and Background

.01 Most health care providers participate in payment programs that pay less than full charges for services rendered. For example, some cost-based programs retrospectively determine the final amounts reimbursable for services rendered to their beneficiaries based on allowable costs. With increasing frequency, even non-cost-based programs (such as the Medicare Prospective Payment System) have become subject to retrospective adjustments (for example, billing denials and coding changes). Often, such adjustments are not known for a considerable period of time after the related services were rendered.

.02 The lengthy period of time between rendering services and reaching final settlement, compounded further by the complexities and ambiguities of reimbursement regulations, makes it difficult to estimate the net patient service revenue associated with these programs. This situation has been compounded due to the frequency of changes in federal program guidelines.

.03 The AICPA Audit and Accounting Guide *Health Care Organizations* (the Guide) requires that patient revenues be reported net of provisions for

contractual and other adjustments (paragraph 10.20). As a result, patient receivables, including amounts due from third-party payors, are also reported net of expected contractual and other adjustments. However, amounts ultimately realizable will not be known until some future date, which may be several years after the period in which the services were rendered.

.04 This SOP provides guidance to auditors regarding uncertainties inherent in health care third-party revenue recognition. It discusses auditing matters to consider in testing third-party revenue and related receivables, including the effects of settlements (both cost-based and non-cost-based third-party payment programs), and provides guidance regarding the sufficiency of evidential matter and reporting on financial statements of health care entities exposed to material uncertainties.

Scope and Applicability

.05 This SOP applies to audits of health care organizations falling within the scope of the Guide. Its provisions are effective for audits of periods ending on or after June 30, 2000. Early application of the provisions of this SOP is permitted.

Third-Party Revenues and Related Receivables—Inherent Uncertainties

.06 Health care entities need to estimate amounts that ultimately will be realizable in order for revenues to be fairly stated in accordance with generally accepted accounting principles (GAAP). The basis for such estimates may range from relatively straightforward calculations using information that is readily available to highly complex judgments based on assumptions about future decisions.

.07 Entities doing business with governmental payors (for example, Medicare and Medicaid) are subject to risks unique to the government-contracting environment that are hard to anticipate and quantify and that may vary from entity to entity. For example—

- A health care entity's revenues may be subject to adjustment as a result of examination by government agencies or contractors. The audit process and the resolution of significant related matters (including disputes based on differing interpretations of the regulations) often are not finalized until several years after the services were rendered.
- Different fiscal intermediaries (entities that contract with the federal government to assist in the administration of the Medicare program) may interpret governmental regulations differently.
- Differing opinions on a patient's principal medical diagnosis, including the appropriate sequencing of codes used to submit claims for payment, can have a significant effect on the payment amount.[1]

[1] Historically, the Health Care Financing Administration (HCFA) contracted with Peer Review Organizations (PROs) to validate the appropriateness of admissions and the clinical coding from which reimbursement was determined. Such reviews were typically performed within ninety days of the claim submission date. However, the government has modified its policies with respect to such reviews and now analyzes coding errors through other means, including in conjunction with investigations conducted by the Office of the Inspector General (OIG) of the U. S. Department of Health and Human Services.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- Otherwise valid claims may be determined to be nonallowable after the fact due to differing opinions on medical necessity.
- Claims for services rendered may be nonallowable if they are later determined to have been based on inappropriate referrals.[2]
- Governmental agencies may make changes in program interpretations, requirements, or "conditions of participation," some of which may have implications for amounts previously estimated.

.08 Such factors often result in retrospective adjustments to interim payments. Reasonable estimates of such adjustments are central to the third-party revenue recognition process in health care, in order to avoid recognizing revenue that the provider will not ultimately realize. The delay between rendering services and reaching final settlement, as well as the complexities and ambiguities of billing and reimbursement regulations, makes it difficult to estimate net realizable third-party revenues.

Management's Responsibilities

.09 Management is responsible for the fair presentation of its financial statements in conformity with GAAP. Management also is responsible for adopting sound accounting policies and for establishing and maintaining internal control that will, among other things, record, process, summarize, and report transactions (as well as events and conditions) consistent with management's assertions embodied in the financial statements. Despite the inherent uncertainties, management is responsible for estimating the amounts recorded in the financial statements and making the required disclosures in accordance with GAAP, based on management's analysis of existing conditions.

.10 Management's assertions regarding proper valuation of its revenues and receivables are embodied in the financial statements. Management is responsible for assuring that revenues are not recognized until their realization is reasonably assured. As a result, management makes a reasonable estimate of amounts that ultimately will be realized, considering—among other things—adjustments associated with regulatory reviews, audits, billing reviews, investigations, or other proceedings. Estimates that are significant to management's assertions about revenue include the provision for third-party payor contractual adjustments and allowances.

.11 Management also is responsible for preparing and certifying cost reports submitted to federal and state government agencies in support of claims for payment for services rendered to government program beneficiaries.

The Auditor's Responsibilities

.12 The auditor's responsibility is to express an opinion on the financial statements taken as a whole. In reaching this opinion, the auditor considers the evidence in support of recorded amounts. If amounts are not known with certainty, the auditor considers the reasonableness of management's estimates in the present circumstances. The auditor also considers the fairness of the presentation and adequacy of the disclosures made by management.

---

[2] Effective January 1, 1995, the Limitation on Certain Physician Referrals law prohibited physicians from referring Medicare and Medicaid patients to health care organizations with which they had a financial relationship for the furnishing of designated health services. Implementing regulations have not yet been adopted as of the date of this publication.

.13 In planning the audit, the auditor considers current industry conditions, as well as specific matters affecting the entity.[3] Among a number of things, the auditor's procedures typically include an analysis of historical results (for example, prior fiscal intermediary audit adjustments and comparisons with industry benchmarks and norms) that enable the auditor to better assess the risk of material misstatements in the current period. When there are heightened risks, the auditor performs more extensive tests covering the current period. Exhibit 5.1 of the Guide includes a number of examples of procedures that auditors may consider.

.14 With respect to auditing third-party revenues, in addition to the usual revenue recognition considerations, the auditor considers whether amounts ultimately realizable are or should be presently known or are uncertain because they are dependent on some other future, prospective actions or confirming events. For example, under a typical fee-for-service contract with a commercial payor, if the provider has performed a service for a covered individual, the revenue to which the provider is entitled should be determinable at the time the service is rendered. On the other hand, if the service was provided under a cost-based government contract, the revenue ultimately collectible may not be known until certain future events occur (for example, a cost report has been submitted and finalized after desk review or audit). In this case, management estimates the effect of such potential future adjustments.

.15 As stated previously, management is responsible for preparing the estimates contained in the financial statements. The auditor evaluates the adequacy of the evidence supporting those estimates, reviews the facts supporting management's judgments, and evaluates the judgments made based on conditions existing at the time of the audit. The fact that net revenues recorded at the time services are rendered differ materially from amounts that ultimately are realized does not necessarily mean the audit was not properly planned or carried out. Similarly, the fact that future events may differ materially from management's assumptions or estimates does not necessarily mean that management's estimates were not valid or the auditor did not follow generally accepted auditing standards (GAAS) as described in this SOP with respect to auditing estimates.

Evidential Matter

.16 The measurement of estimates is inherently uncertain and depends on the outcome of future events. Statement on Auditing Standards (SAS) No. 57, *Auditing Accounting Estimates* (AICPA, *Professional Standards*, vol. 1, AU sec. 342), and SAS No. 79, *Amendment to SAS No. 58*, Reports on Audited Financial Statements (AICPA, *Professional Standards*, vol. 1, AU sec. 508) provide guidance to the auditor when the valuation of revenues is uncertain, pending the outcome of future events. In the current health care environment, conclusive evidence concerning amounts ultimately realizable cannot be expected to exist at the time of the financial statement audit because the uncertainty associated with future program audits, administrative reviews, billing reviews, regulatory investigations, or other actions will not be resolved until sometime in the future.

.17 The fact that information related to the effects of future program audits, administrative reviews, regulatory investigations, or other actions does

[3] Risk factors, including ones related to legislative and regulatory matters, are discussed annually in the AICPA Audit Risk Alert *Health Care Industry Developments*.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

not exist does not lead to a conclusion that the evidential matter supporting management's assertions is not sufficient to support management's estimates. Rather, the auditor's judgment regarding the sufficiency of the evidential matter is based on the evidential matter that is available or can reasonably be expected to be available in the circumstances. If, after considering the existing conditions and available evidence, the auditor concludes that sufficient evidential matter supports management's assertions about the valuation of revenues and receivables, and their presentation and disclosure in the financial statements, an unqualified opinion ordinarily is appropriate.

.18 If relevant evidential matter exists that the auditor needs and is unable to obtain, the auditor should consider the need to express a qualified opinion or to disclaim an opinion because of a scope limitation. For example, if an entity has conducted an internal evaluation (for example, of coding or other billing matters) under attorney—client privilege and management and its legal counsel refuse to respond to the auditor's inquiries and the auditor determines the information is necessary, ordinarily the auditor qualifies his or her opinion for a scope limitation.

.19 The auditor considers the reasonableness of management's assumptions in light of the entity's historical experience and the auditor's knowledge of general industry conditions, because the accuracy of management's assumptions will not be known until future events occur. For certain matters, the best evidential matter available to the auditor (particularly as it relates to clinical and legal interpretations) may be the representations of management and its legal counsel, as well as information obtained through reviewing correspondence from regulatory agencies.

.20 Pursuant to SAS No. 85, *Management Representations* (AICPA, *Professional Standards*, vol. 1, AU sec. 333), the auditor should obtain written representations from management concerning the absence of violations or possible violations of laws or regulations whose effects should be considered for disclosure in the financial statements or as a basis for recording a loss contingency. Examples of specific representations include the following:

- Receivables
  - — Adequate consideration has been given to, and appropriate provision made for, estimated adjustments to revenue, such as for denied claims and changes to diagnosis-related group (DRG) assignments.
  - — Recorded valuation allowances are necessary, appropriate, and properly supported.
  - — All peer review organizations, fiscal intermediary, and third-party payor reports and information have been made available.
- Cost reports filed with third parties
  - — All required Medicare, Medicaid, and similar reports have been properly filed.
  - — Management is responsible for the accuracy and propriety of all cost reports filed.
  - — All costs reflected on such reports are appropriate and allowable under applicable reimbursement rules and regulations and are patient-related and properly allocated to applicable payors.
  - — The reimbursement methodologies and principles employed are in accordance with applicable rules and regulations.

- Adequate consideration has been given to, and appropriate provision made for, audit adjustments by intermediaries, third-party payors, or other regulatory agencies.
- All items required to be disclosed, including disputed costs that are being claimed to establish a basis for a subsequent appeal, have been fully disclosed in the cost report.
- Recorded third-party settlements include differences between filed (and to be filed) cost reports and calculated settlements, which are necessary based on historical experience or new or ambiguous regulations that may be subject to differing interpretations. While management believes the entity is entitled to all amounts claimed on the cost reports, management also believes the amounts of these differences are appropriate.

- Contingencies
  - There are no violations or possible violations of laws or regulations, such as those related to the Medicare and Medicaid antifraud and abuse statutes, including but not limited to the Medicare and Medicaid Anti-Kickback Statute, Limitations on Certain Physician Referrals (the Stark law), and the False Claims Act, in any jurisdiction, whose effects should be considered for disclosure in the financial statements or as a basis for recording a loss contingency other than those disclosed or accrued in the financial statements.
  - Billings to third-party payors comply in all material respects with applicable coding guidelines (for example, ICD-9-CM and CPT-4) and laws and regulations (including those dealing with Medicare and Medicaid antifraud and abuse), and billings reflect only charges for goods and services that were medically necessary; properly approved by regulatory bodies (for example, the Food and Drug Administration), if required; and properly rendered.
  - There have been no communications (oral or written) from regulatory agencies, governmental representatives, employees, or others concerning investigations or allegations of noncompliance with laws and regulations in any jurisdiction (including those related to the Medicare and Medicaid antifraud and abuse statutes), deficiencies in financial reporting practices, or other matters that could have a material adverse effect on the financial statements.

.21 Management's refusal to furnish written representations constitutes a limitation on the scope of the audit sufficient to preclude an unqualified opinion and is ordinarily sufficient to cause an auditor to disclaim an opinion or withdraw from the engagement. However, based on the nature of the representations not obtained or the circumstances of the refusal, the auditor may conclude that a qualified opinion is appropriate.

Potential Departures From GAAP Related to Estimates and Uncertainties

.22 In addition to examining the evidence in support of management's estimates, the auditor determines that there has not been a departure from GAAP with respect to the reporting of those estimates in the financial statements. Such departures generally fall into one of the following categories:

 Copyright © 2003. American Institute of Certified Public Accountants, Inc.

- Unreasonable accounting estimates
- Inappropriate accounting principles
- Inadequate disclosure

Therefore, in order to render an opinion, the auditor's responsibility is to evaluate the reasonableness of management's estimates based on present circumstances and to determine that estimates are reported in accordance with GAAP and adequately disclosed.

.23 As discussed in SAS No. 31, *Evidential Matter* (AICPA, *Professional Standards*, vol. 1, AU sec. 326), the auditor's objective is to obtain sufficient competent evidential matter to provide him or her with a reasonable basis for forming an opinion. As discussed previously, exhibit 5.1 of the Guide provides a number of sample procedures that the auditor might consider in auditing an entity's patient revenues and accounts receivable, including those derived from third-party payors. For example, the Guide notes that the auditor might "test the reasonableness of settlement amounts, including specific and unallocated reserves, in light of the payors involved, the nature of the payment mechanism, the risks associated with future audits, and other relevant factors."[4]

Unreasonable Accounting Estimates

.24 In evaluating the reasonableness of management's estimates, the auditor considers the basis for management's assumptions regarding the nature of future adjustments and management's calculations as to the effects of such adjustments.[5] The auditor cannot determine with certainty whether such estimates are right or wrong, because the accuracy of management's assumptions cannot be confirmed until future events occur.

.25 Though difficult to predict, it is reasonable for the auditor to expect that management has made certain assumptions (either in detail or in the aggregate) in developing its estimates regarding conditions likely to result in adjustments. The auditor gathers evidence regarding the reasonableness of the estimates (for example, consistency with historical experience and basis of management's underlying assumptions). In evaluating reasonableness, the auditor should obtain an understanding of how management developed the estimate. Based on that understanding, the auditor should use one or a combination of the following approaches:

a. Review and test the process used by management to develop the estimate.

b. Develop an independent expectation of the estimate to corroborate the reasonableness of management's estimates.

c. Review subsequent events or transactions occurring prior to completion of fieldwork (AU sec. 342.10).

.26 Since no one accounting estimate can be considered accurate with certainty, the auditor recognizes that a difference between an estimated amount best supported by the audit evidence and the estimated amount included in the financial statements may be reasonable, and such difference would not be considered to be a likely misstatement. However, if the auditor

---

[4] See paragraphs .25–.28.

[5] The lack of such analyses may call into question the reasonableness of recorded amounts.

believes the estimated amount included in the financial statements is unreasonable, he or she should treat the difference between that estimate and the closest reasonable estimate in the range as a likely misstatement and aggregate it with other likely misstatements. The auditor also should consider whether the difference between estimates best supported by the audit evidence and the estimates included in the financial statements, which are individually reasonable, indicate a possible bias on the part of the entity's management. For example, if each accounting estimate included in the financial statements was individually reasonable, but the effect of the difference between each estimate and the estimate best supported by the audit evidence was to increase income, the auditor should reconsider the reasonableness of the estimates taken as a whole (SAS No. 47, *Audit Risk and Materiality in Conducting an Audit* [AICPA, *Professional Standards*, vol. 1, AU sec. 312.36]).

.27 The auditor recognizes that approaches and estimates will vary from entity to entity. Some entities with significant prior experience may attempt to quantify the effects of individual potential intermediary or other governmental (for example, the Office of Inspector General and the Department of Justice) or private payor adjustments, basing their estimates on very detailed calculations and assumptions regarding potential future adjustments. Some may prepare cost report[6] analyses to estimate the effect of potential adjustments. Others may base their estimates on an analysis of potential adjustments in the aggregate, in light of the payors involved; the nature of the payment mechanism; the risks associated with future audits; and other relevant factors.

.28 Normally, the auditor considers the historical experience of the entity (for example, the aggregate amount of prior cost-report adjustments and previous regulatory settlements) as well as the risk of potential future adjustments. The fact that an entity currently is not subject to a governmental investigation does not mean that a recorded valuation allowance for potential billing adjustments is not warranted. Nor do these emerging industry trends necessarily indicate that an accrual for a specific entity is warranted.

.29 In evaluating valuation allowances, the auditor may consider the entity's historical experience and potential future adjustments in the aggregate. For example, assume that over the past few years after final cost report audits were completed, a hospital's adjustments averaged 3 percent to 5 percent of total filed reimbursable costs. Additionally, the hospital is subject to potential billing adjustments, including errors (for example, violations of the three-day window, discharge and transfer issues, and coding errors). Even though specific incidents are not known, it may be reasonable for the hospital to estimate and accrue a valuation allowance for such potential future retrospective adjustments, both cost-based and non-cost-based. Based on this and other information obtained, the auditor may conclude that a valuation allowance for the year under audit of 3 percent to 5 percent of reimbursable costs plus additional amounts for potential non-cost-based program billing errors is reasonable.

---

[6] Medicare cost reimbursement is based on the application of highly complex technical rules, some of which are ambiguous and subject to different interpretations even among Medicare's fiscal intermediaries. It is not uncommon for fiscal intermediaries to reduce claims for reimbursement that were based on management's good faith interpretations of pertinent laws and regulations. Additionally, the Provider Reimbursement Review Board (PRRB) or the courts may be required to resolve controversies regarding the application of certain rules. To avoid recognizing revenues before their realization is reasonably assured, providers estimate the effects of such potential adjustments. This is occasionally done by preparing a cost report based on alternative assumptions to help estimate contractual allowances required by generally accepted accounting principles. The existence of reserves or a reserve cost report does not by itself mean that a cost report was incorrectly or fraudulently filed.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.30 Amounts that ultimately will be realized by an entity are dependent on a number of factors, many of which may be unknown at the time the estimate is first made. Further, even if two entities had exactly the same clinical and coding experience, amounts that each might realize could vary materially due to factors outside of their control (for example, differing application of payment rules by fiscal intermediaries, legal interpretations of courts, local enforcement initiatives, timeliness of reviews, and quality of documentation). As a result, because estimates are a matter of judgment and their ultimate accuracy depends on the outcome of future events, different entities in seemingly similar circumstances may develop materially different estimates. The auditor may conclude that both estimates are reasonable in light of the differing assumptions.

Inappropriate Accounting Principles

.31 The auditor also determines that estimates are presented in the financial statements in accordance with GAAP. If the auditor believes that the accounting principles have not been applied correctly, causing the financial statements to be materially misstated, the auditor expresses a qualified or adverse opinion.

.32 Valuation allowances are recorded so that revenues are not recognized until the revenues are realizable. Valuation allowances are not established based on the provisions of Financial Accounting Standards Board (FASB) Statement of Financial Accounting Standards No. 5, *Accounting for Contingencies*.

.33 The auditor should be alert for valuation allowances not associated with any particular program, issue, or time period (for example, cost-report year or year the service was rendered). Such a reserve may indicate measurement bias. The auditor also considers the possibility of bias resulting in distorted earnings trends over time (for example, building up specific or unallocated valuation allowances in profitable years and drawing them down in unprofitable years).

Inadequate Disclosure

.34 If the auditor concludes that a matter involving a risk or an uncertainty is not adequately disclosed in the financial statements in conformity with GAAP, the auditor should express a qualified or adverse opinion. SOP 94-6, *Disclosure of Certain Significant Risks and Uncertainties* [section 10,640], provides guidance on the information that reporting entities should disclose regarding risks and uncertainties existing as of the date of the financial statements.

.35 In the health care environment, it is almost always at least reasonably possible that estimates regarding third-party payments could change in the near term as a result of one or more future confirming events (for example, regulatory actions reflecting local or national audit or enforcement initiatives). For most entities with significant third-party revenues, the effect of the change could be material to the financial statements. Where material exposure exists, the uncertainty regarding revenue realization is disclosed in the notes to the financial statements. Because representations from legal counsel are often key audit evidence in evaluating the reasonableness of management's estimates of potential future adjustments, the inability of an attorney to form an opinion on matters about which he or she has been consulted may be indicative of an uncertainty that should be specifically disclosed in the financial statements.

.36 Differences between original estimates and subsequent revisions might arise due to final settlements, ongoing audits and investigations, or passage of time in relation to the statute of limitations. The Guide (paragraph 5.07) requires that these differences be included in the statement of operations in the period in which the revisions are made and disclosed, if material. Such differences are not treated as prior period adjustments unless they meet the criteria for prior period adjustments as set forth in FASB Statement No. 16, *Prior Period Adjustments*.

.37 Disclosures such as the following may be appropriate:

General Hospital (the Hospital) is a (not-for-profit, for-profit, or governmental hospital or health care system) located in (City, State). The Hospital provides health care services primarily to residents of the region.

Net patient service revenue is reported at estimated net realizable amounts from patients, third-party payors, and others for services rendered and includes estimated retroactive revenue adjustments due to future audits, reviews, and investigations. Retroactive adjustments are considered in the recognition of revenue on an estimated basis in the period the related services are rendered, and such amounts are adjusted in future periods as adjustments become known or as years are no longer subject to such audits, reviews, and investigations.

Revenue from the Medicare and Medicaid programs accounted for approximately 40 percent and 10 percent, respectively, of the Hospital's net patient revenue for the year ended 1999. Laws and regulations governing the Medicare and Medicaid programs are extremely complex and subject to interpretation. As a result, there is at least a reasonable possibility that recorded estimates will change by a material amount in the near term. The 1999 net patient service revenue increased approximately $10,000,000 due to removal of allowances previously estimated that are no longer necessary as a result of final settlements and years that are no longer subject to audits, reviews, and investigations. The 1998 net patient service revenue decreased approximately $8,000,000 due to prior-year retroactive adjustments in excess of amounts previously estimated.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.38

Appendix

Other Considerations Related to Government Investigations

In recent years, the federal government and many states have aggressively increased enforcement efforts under Medicare and Medicaid anti-fraud and abuse legislation. Broadening regulatory and legal interpretations have significantly increased the risk of penalties for providers; for example, broad interpretations of "false claims" laws are exposing ordinary billing mistakes to scrutiny and penalty consideration. In such circumstances, evaluating the adequacy of accruals for or disclosure of the potential effects of illegal acts in the financial statements of health care organizations is a matter that is likely to require a high level of professional judgment.

As previously discussed in this SOP, the far-reaching nature of alleged fraud and abuse violations creates an uncertainty with respect to the valuation of revenues, because future allegations of illegal acts could, if proven, result in a subsequent reduction of revenues. In addition, management makes provisions in the financial statements and disclosures for any contingent liabilities associated with fines and penalties due to violations of such laws. FASB Statement No. 5, *Accounting for Contingencies*, provides guidance in evaluating contingent liabilities, such as fines and penalties under applicable laws and regulations. Estimates of potential fines and penalties are not accrued unless their payment is probable and reasonably estimable.

The auditor's expertise is in accounting and auditing matters rather than operational, clinical, or legal matters. Accordingly, the auditor's procedures focus on areas that normally are subject to internal controls relevant to financial reporting. However, the further that potential illegal acts are removed from the events and transactions ordinarily reflected in the financial statements, the less likely the auditor is to become aware of the act, to recognize its possible illegality, and to evaluate the effect on the financial statements. For example, determining whether a service was medically necessary, obtained through a legally appropriate referral, properly performed (including using only approved devices, rendered in a quality manner), adequately supervised, accurately documented and classified, or rendered and billed by nonsanctioned individuals typically is not within the auditor's professional expertise. As a result, an audit in accordance with generally accepted auditing standards (GAAS) is not designed to detect such matters.

Further, an audit conducted in accordance with GAAS does not include rendering an opinion or any form of assurance on an entity's compliance with laws and regulations.[1] Nor does an audit under GAAS include providing any assurance on an entity's billings or cost report. In fact, cost reports typically are not prepared and submitted until after the financial statement audit has been completed.

---

[1] Even when auditors undertake a special engagement designed to attest to compliance with certain provisions of laws, regulations, contracts, and grants (for example, an audit in accordance with OMB Circular A-133), the auditor's procedures do not extend to testing compliance with laws and regulations related to Medicare and Medicaid fraud and abuse.

Certain audit procedures, although not specifically designed to detect illegal acts, may bring possible illegal acts to an auditor's attention. When a potentially illegal act is detected, the auditor's responsibilities are addressed in SAS No. 54, *Illegal Acts by Clients* (AICPA, *Professional Standards*, vol. 1, AU sec. 317). Disclosure of an illegal act to parties other than the client's senior management and its audit committee or board of directors is not ordinarily part of the auditor's responsibility, and such disclosure would be precluded by the auditor's ethical or legal obligation of confidentiality, unless the matter affects the auditor's opinion on the financial statements.[2]

[2] Statement on Auditing Standards No. 54, *Illegal Acts by Clients* (AICPA, *Professional Standards*, vol. 1, AU sec. 317.23) discusses circumstances in which a duty to notify parties outside the client of detected illegal acts may exist.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Auditing Standards Board

DEBORAH D. LAMBERT, *Chair*
JAMES S. GERSON, *Vice Chair*
JOHN BARNUM
ANDREW J. CAPELLI
LINDA K. CHEATHAM
ROBERT F. DACEY
RICHARD DIETER
SALLY L. HOFFMAN
J. MICHAEL INZINA
CHARLES E. LANDES
W. SCOTT MCDONALD
KEITH O. NEWTON
ROBERT C. STEINER
GEORGE H. TUCKER
O. RAY WHITTINGTON

AICPA Health Care Third-Party Revenue Recognition Task Force

WILLIAM R. TITERA, *Chair*
MARTHA GARNER
ROBERT A. WRIGHT

AICPA Health Care Committee

ROBERT A. WRIGHT, *Chair*
THOMAS J. AARON
PHILLIP J. BRUMMEL
A. JAMES BUDZINSKI
RICK R. CORCORAN
MICHAEL T. DEFREECE
ROBERT E. MAZER
CHARLES V. ROBB
PEGGY B. SCOTT
ALAN A. SCHACHTER
GORDON J. VETSCH
JONATHAN G. WEAVER
AUDREY L. WENT

AICPA Staff

THOMAS RAY
Director
Audit and Attest Standards

ANNETTE SCHUMACHER BARR
Technical Manager
Professional Standards & Services

[The next page is 31,461.]

Section 14,370

Statement of Position 01-3 Performing Agreed-Upon Procedures Engagements That Address Internal Control Over Derivative Transactions as Required by the New York State Insurance Law

June 15, 2001

NOTE

This Statement of Position represents the recommendations of the AICPA's Reporting on Internal Control Over Derivative Transactions at Insurance Entities Task Force regarding the application of Statements on Standards for Attestation Engagements to agreed-upon procedures engagements performed to comply with the requirements of Section 1410(b)(5) of the New York State Insurance Law, as amended (the Law), which addresses the assessment of internal control over derivative transactions as defined in Section 1401(a) of the Law, and Section 178.6(b) of Regulation No. 163. The Auditing Standards Board has found the recommendations in this Statement of Position to be consistent with existing standards covered by Rule 202 of the AICPA Code of Professional Conduct. AICPA members should be aware that they may have to justify departures from the recommendations in this Statement of Position if the quality of their work is questioned.

Introduction and Background

.01 The New York State Insurance Department (the Department) has issued regulations to implement the New York Derivative Law (the Law) which amends Article 14 of the State of New York Insurance Law, effective July 1, 1999. The Law establishes certain requirements for domestic life insurers, domestic property and casualty insurers, domestic reciprocal insurers, domestic mortgage guaranty insurers, domestic cooperative property and casualty insurance corporations, and domestic financial guaranty insurers. Foreign insurers engaging in derivative transactions and derivative instruments are subject to and required to comply with all of the provisions of the Law. However, a foreign insurer may enter into other derivative transactions provided the insurer meets certain conditions of its domestic state law. In this document, an insurer covered by the Law is referred to as an *insurance company*.

.02 The requirements of the Law include the following:

- Approval by the board of directors, or a similar body, of derivative transactions
- Submission of a derivative use plan (the DUP) to the Department

- Assessment by an independent certified public accountant (CPA) of the insurance company's internal control over derivative transactions.

.03 In addition to the Law, the Department also has established Regulation No. 163, "Derivative Transactions" (11 NYCRR 178) (the Regulation), which provides guidance in implementing the Law. Section 178.6(b) of Regulation No. 163 states the following.

> As set forth in section 1410(b)(5) of the Insurance Law, an insurer engaging in derivative transactions shall be required to include, as part of the evaluation of accounting procedures and internal controls required to be filed pursuant to section 307 of the Insurance Law, a statement describing the assessment by the independent certified public accountant of the internal controls relative to derivative transactions. The purpose of this part of the evaluation is to assess the adequacy of the internal controls relative to the derivative transactions. Such an assessment shall be made whether or not the derivative transactions are material in relation to the insurer's financial statements and shall report all material deficiencies in internal control relative to derivative transactions, whether or not such deficiencies would lead to an otherwise "reportable condition," as that term is used in auditing standards adhered to by certified public accountants. The statement describing the assessment need not be set forth in a separate report.

.04 The Department has proposed that the Regulation be amended to provide that an assessment in the form of an agreed-upon procedures engagement or other attestation engagement, as those terms are used in standards adhered to by CPAs, may be used to meet the requirement for an assessment of internal control over derivative transactions. This proposed amendment to the Regulation has not been promulgated at the date of this Statement of Position (SOP). However, in a letter dated April 27, 2001, the Department stated the following:

> This letter confirms that in determining compliance with Section 1410(b)(5) of the Insurance Law, the Department acknowledges that an agreed-upon procedures engagement, including an engagement performed using the procedures in the proposed SOP ("Performing Agreed-Upon Procedures Engagements that Address Internal Control Over Derivative Transactions as Required by the New York State Insurance Law"), can be used to satisfy the statutory requirement.

.05 The DUP was due to be filed by applicable insurance companies by January 1, 2000. The first independent CPA's report is due on June 1, 2001. The Law expires on June 30, 2003; however, the State of New York may extend the expiration date.

.06 As previously stated, the letter from the Department indicates that an agreed-upon procedures engagement or other attestation engagement may be used to satisfy the requirements of the Law. However, this SOP only describes an agreed-upon procedures engagement. It does not address any other attestation engagements that might be performed, such as an examination-level attestation engagement. For guidance on performing such other attestation engagements, see "Attest Engagements," in Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Standards: Revision and Codification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101).

Applicability

.07 This SOP was developed to provide practitioners with guidance on performing agreed-upon procedures engagements that address an insurance

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

company's internal control over derivative transactions to meet the requirements of the Law. Practitioners should note that the engagement described in this SOP is designed only to satisfy the requirements of the Law. The procedures, as set forth in this SOP, are not necessarily appropriate for use in any other engagement.

.08 Although the Department has indicated that an agreed-upon procedures engagement pursuant to this SOP can be used to satisfy the requirements for an assessment of internal control over derivative transactions, the Department has not agreed to the sufficiency of the procedures included in this SOP for their purposes.

The Law

Definition of a Derivative

.09 Article 14 of the Law defines a derivative instrument as including caps, collars, floors, forwards, futures, options, swaps, swaptions, and warrants.

.10 The following definitions are included in the Law and are applicable when performing the agreed-upon procedures engagement described in this SOP.

Cap—An agreement obligating the seller to make payments to the buyer with each payment based on the amount by which a reference price or level or the performance or value of one or more underlying interests exceeds a predetermined number, sometimes called the strike rate or strike price.

Collar—An agreement to receive payments as the buyer of an option, cap, or floor and to make payments as the seller of a different option, cap, or floor.

Floor—An agreement obligating the seller to make payments to the buyer in which each payment is based on the amount by which a predetermined number, sometimes called the floor rate or price, exceeds a reference price, level, performance, or value of one or more underlying interests.

Forward—An agreement (other than a future) to make or take delivery in the future of one or more underlying interests, or effect a cash settlement, based on the actual or expected price, level, performance, or value of such underlying interests, but shall not mean or include spot transactions effected within customary settlement periods, when-issued purchases, or other similar cash market transactions.

Future—An agreement traded on a futures exchange, to make or take delivery of, or effect a cash settlement based on the actual or expected price, level, performance, or value of one or more underlying interests.

Option—An agreement giving the buyer the right to buy or receive (a *call option*), sell or deliver (a *put option*), enter into, extend or terminate, or effect a cash settlement based on the actual or expected price, spread, level, performance, or value of one or more underlying interests.

Swap—An agreement to exchange or to net payments at one or more times based on the actual or expected price, yield, level, performance, or value of one or more underlying interests.

Swaption—An option to purchase or sell a swap at a given price and time or at a series of prices and times. A swaption does not mean a swap with an embedded option.

Warrant—An instrument that gives the holder the right to purchase or sell the underlying interest at a given price and time or at a series of prices and times outlined in the warrant agreement.

.11 Article 14 of the Law permits an insurance company to enter into *replication transactions* provided that certain conditions set forth in the Law are met. A replication transaction is defined in the Law as follows.

> A derivative transaction or combination of derivative transactions effected either separately or in conjunction with cash market investments included in the insurer's investment portfolio in order to replicate the investment characteristic of another authorized transaction, investment or instrument and/or operate as a substitute for cash market transactions. A derivative transaction entered into by the insurer as a hedging transaction or income generation transaction authorized pursuant to this section [of the Law] shall not be considered a replication transaction.

Derivative Use Plan

.12 An insurance company entering into derivative transactions must file a DUP with the Department. The DUP generally should include the following items:[1]

- A certified copy of the authorization by the insurer's board of directors, or other similar body, to file the DUP, which should include authorization of derivative transactions and an assurance that individuals responsible for derivative transactions, processes, and controls have the necessary experience and knowledge
- A section on management oversight standards including a discussion of the following:
  - — Limits on identified risks
  - — Controls over the nature and amount of identified risks
  - — Processes for identifying such risks
  - — Processes for documenting, monitoring, and reporting risk exposure
  - — Internal audit and review processes that ensure integrity of the overall risk management process
  - — Quarterly reporting to the board of directors
  - — The establishment of risk tolerance levels
  - — Management's measurement and monitoring against those levels
- A section on internal control and reporting including a discussion of the following:
  - — The existence of controls over the valuation and effectiveness of derivative instruments
  - — Credit risk management
  - — The adequacy of professional personnel
  - — Technical expertise and systems
  - — Management reporting
  - — The review and legal enforceability of derivative contracts between parties

[1] Reference should be made to the Law and the Regulation for specific details and exact requirements.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- A section on documentation and reporting requirements which shall for each derivative transaction document the following:
  - The purpose of the transaction
  - The assets or liabilities to which the transaction relates
  - The specific derivative instrument used
  - For over-the-counter (OTC) transactions, the name of the counterparty and counterparty exposure amount
  - For exchange traded transactions, the name of the exchange and the name of the firm handling the trade
- Written guidelines to be followed in engaging in derivative transactions. The guidelines should include or address the following:
  - The type, maturity, and diversification of derivative instruments
  - The limitation on counterparty exposures, including limitations based on credit ratings
  - The limitations on the use of derivatives
  - Asset and liability management practices with respect to derivative transactions
  - The liquidity needs and the insurance company's capital and surplus as it relates to the DUP
  - The policy objectives of management specific enough to outline permissible derivative strategies
  - The relationship of the strategies to the insurer's operations
  - How the strategies relate to the insurer's risk
  - A requirement that management establish and execute management oversight standards as required by the Law
  - A requirement that management establish and execute internal control and reporting standards as required by the Law
  - A requirement that management establish and execute documentation and reporting standards as required by the Law
- Guidelines for the insurer's determination of acceptable levels of basis risk, credit risk, foreign currency risk, interest rate risk, market risk, operational risk, and option risk
- A requirement that the board of directors and senior management comply with risk oversight functions and adhere to laws, rules, regulations, prescribed practices, or ethical standards

Related Professional Standards

AT Section 201, "Agreed-Upon Procedures Engagements," Statement on Standards for Attestation Engagements No. 10

.13 Agreed-upon procedures engagements performed to meet the requirements of the Law are to be performed in accordance with AT section 201, *Agreed-Upon Procedures Engagements*, in SSAE No. 10. As described in AT section 201.03, an agreed-upon procedures engagement is one in which a practitioner is engaged by a client to issue a report of findings based on specific procedures performed on the subject matter. Not all of the provisions of AT section 201 are discussed herein. Rather, this SOP includes guidance to assist practitioners in the application of selected aspects of AT section 201.

.14 AT section 201.06 states, in part, that the practitioner may perform an agreed-upon procedures engagement provided that, ". . . (*c*) the practitioner and the specified parties agree upon the procedures performed or to be performed by the practitioner; and (*d*) the specified parties take responsibility for the sufficiency of the agreed-upon procedures for their purposes."

.15 As previously stated, the letter from the Department states that an agreed-upon procedures engagement may be used to meet the requirement for an independent CPA's assessment of internal control over derivative transactions, and acknowledges the use of this SOP in such engagements. Accordingly, practitioners should not eliminate any of the procedures presented in appendix B, "Agreed-Upon Procedures for Testing Internal Control Over Derivative Transactions" [paragraph .37], of this SOP or reduce the extent of the tests. The Department or the insurance company may request that additional procedures be performed and the practitioner may agree to perform such procedures. In those circumstances, it would be expected that the additional procedures would be performed in the context of a separate agreed-upon procedures engagement.

.16 As previously noted, the Department has not agreed to the sufficiency of the procedures included in this SOP for their purposes. *Therefore, the Department should not be named as a specified party to the agreed-upon procedures report, and the use of a practitioner's agreed-upon procedures report, issued in accordance with this SOP, should be restricted to the board of directors and management of the insurance company.* Although the Department is not a specified party, footnote 15 of AT section 101, *Attest Engagements*, states the following, in part:

> . . . a regulatory agency as part of its oversight responsibility for an entity may require access to restricted-use reports in which they are not named as a specified party.

Statement on Auditing Standards No. 92, *Auditing Derivative Instruments, Hedging Activities, and Investments in Securities*

.17 Statement on Auditing Standards (SAS) No. 92, *Auditing Derivative Instruments, Hedging Activities, and Investments in Securities* (AICPA, *Professional Standards*, vol. 1, AU sec. 332), provides guidance to auditors in planning and performing auditing procedures for financial statement assertions about derivative instruments, hedging activities, and investments in securities in a financial statement audit performed in accordance with generally accepted auditing standards. A practitioner performing the agreed-upon procedures engagement described in this SOP may find it helpful to consider the guidance in SAS No. 92 and the related audit guide of the same name supporting SAS No. 92. Specifically, the practitioner should consider AU sections 332.05 and 332.06 of SAS No. 92 which describe the need for special skill or knowledge to plan and perform the auditing procedures presented in SAS No. 92. That same skill and knowledge is needed to perform the procedures described in this SOP.

.18 The procedures in this SOP are not designed to meet the requirements of generally accepted auditing standards for an audit of the financial statements of an entity that engages in derivative transactions. In addition, performing the audit procedures described in SAS No. 92 would not meet the requirements of this SOP.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.19 In an audit of financial statements, the auditor may determine that he or she will not perform procedures related to derivative transactions because they are not material to the financial statements. There is no requirement to perform the procedures described in this SOP when performing an audit of financial statements. In contrast, the Law requires that an assessment of internal control be performed whether or not the derivative transactions are material to the insurer's financial statements. Accordingly, a decision not to perform procedures related to derivative transactions in an audit of financial statements, because of immateriality, would not alleviate the requirement to perform the agreed-upon procedures engagement described herein.

Procedures to Be Performed

.20 The agreed-upon procedures to be performed are directed toward tests of controls over derivative transactions that occurred during the period covered by the practitioner's report. Any projection of the practitioner's findings to the future is subject to the risk that because of change, the controls may no longer be in existence, suitably designed, or operating effectively. Also, the potential effectiveness of controls over derivative transactions is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected.

.21 The procedures to be performed in the agreed-upon procedures engagement described in this SOP are presented in appendix B [paragraph .37]. The procedures have been designed so that the findings resulting from the application of the procedures can be recorded in a tabular format. The findings for each procedure should be reported as *No Exception*, *Exception*, or *N/A* (not applicable). If a procedure is not applicable to a particular insurance company, the procedure should be marked N/A rather than deleted from the report.

.22 Section 1 of appendix B [paragraph .37] of this SOP is applicable to all insurance companies that enter into derivative transactions. Therefore, the procedures in section 1 are to be performed in all engagements performed in accordance with this SOP. Sections 2 through 10 of appendix B [paragraph .37] of this SOP each address a specific type of derivative. The procedures in those sections are to be performed only if the insurance company entered into derivative transactions of the type covered by the section. Sections that address types of derivatives not used by the insurance company should not be attached to the agreed-upon procedures report.

.23 If any portion of a procedure results in an exception, the findings for that entire procedure should be recorded as an exception and described in the section "Description of Exceptions If Any," at the end of each section. The practitioner should provide a brief factual explanation for each exception that will enable the specified parties to understand the nature of the findings resulting in the exception. If management informs the practitioner that the condition giving rise to the exception was corrected by the date of the practitioner's report, the practitioner's explanation of the exception may include that information; for example, "Management has advised us that the condition resulting in the exception was corrected on Month X, 20XX. We have performed no procedures with respect to management's assertion."

.24 A practitioner may perform significant portions of the agreed-upon procedures engagement before the end of the period covered by the report. If, during that time, the practitioner identifies conditions that result in an exception in one or more agreed-upon procedures, he or she should report the exception in the findings section of the agreed-upon procedures report, even if management corrects the condition prior to the end of the period.

.25 The Law requires the insurance company to provide the Department with a statement describing the independent CPA's assessment of the insurance company's internal control over derivative transactions. It also requires the insurance company to include a description of any remedial actions taken or proposed to be taken to correct any deficiencies identified by the independent CPA.

.26 AT section 201.40 states the following.

> The practitioner need not perform procedures beyond the agreed-upon procedures. However, in connection with the application of agreed-upon procedures, if matters come to the practitioner's attention by other means that significantly contradict the subject matter (or written assertion related thereto) referred to in the practitioner's report, the practitioner should include this matter in his or her report. For example, if during the course of applying agreed-upon procedures regarding an entity's internal control, the practitioner becomes aware of a material weakness by means other than performance of the agreed-upon procedures, the practitioner should include this matter in his or her report.

.27 A practitioner has no obligation to perform procedures beyond the agreed-upon procedures included in appendix B [paragraph .37] of this SOP. However, if information indicating a weakness in internal control over derivative transactions comes to the practitioner's attention by other means, such information should be included in the practitioner's report. This would apply to conditions or events occurring during the subsequent-events period (subsequent to the period covered by the practitioner's report but prior to the date of the practitioner's report) that either contradict the findings in the report or that would have resulted in the reporting of an exception by the practitioner if that condition or event had existed during the period covered by the report. However, the practitioner has no responsibility to perform any procedure to detect such conditions or events.

Establishing an Understanding With the Client

.28 In accordance with AT section 201.10, the practitioner should establish an understanding with the client regarding the services to be performed. Such an understanding reduces the risk that the client may misinterpret the objectives and limitations of an agreed-upon procedures engagement performed to meet the regulatory requirements of the Law. Such an understanding also reduces the risk that the client will misunderstand its responsibilities and the responsibilities of the practitioner. The practitioner should document the understanding in the working papers, preferably through a written communication with the client (an *engagement letter*). The communication should be addressed to the client. Matters that might be included in such an understanding are the following:

- A statement confirming that an agreed-upon procedures engagement is to be performed to meet the requirements of Section 1410(b)(5) of the Law
- A statement identifying the procedures to be performed as those set forth in this SOP
- A statement identifying the client as the specified party to the agreed-upon procedures report

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- A statement acknowledging the client's responsibility for the sufficiency of the procedures in the SOP
- A statement acknowledging that the practitioner makes no representation regarding the sufficiency of the procedures in the SOP
- A statement describing the responsibilities of the practitioner, including but not limited to the responsibility to perform the agreed-upon procedures and to provide the client with a report, and the circumstances under which the practitioner may decline to issue a report
- A statement indicating that the engagement will be conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA)
- A statement indicating that an agreed-upon procedures engagement does not constitute an examination, the objective of which would be the expression of an opinion on the internal control over derivative transactions, and that if an examination were performed, other matters might come to the practitioner's attention
- A statement indicating that the practitioner will not express an opinion or any other form of assurance
- A statement describing the client's responsibility to comply with the Law and the client's responsibility for the design and operation of effective internal control over derivative transactions
- A statement describing the client's responsibility for providing accurate and complete information to the practitioner
- A statement indicating that the practitioner has no responsibility for the completeness or accuracy of the information provided to the practitioner
- A statement restricting the use of the report to the client
- A statement describing any arrangements to involve a specialist

Management Representations

.29 Although AT section 201 does not require a practitioner to obtain a representation letter from management in an agreed-upon procedures engagement, it is recommended that the practitioner obtain such a letter when performing the engagement described in this SOP. The representation letter generally should be signed by the appropriate members of management including the highest ranking officer responsible for internal control over derivative transactions. Management's refusal to furnish written representations that the practitioner has determined to be appropriate for the engagement constitutes a limitation on the performance of the engagement that requires either modification of the report or withdrawal from the engagement.

.30 The representations that a practitioner deems appropriate will depend on the specific nature of the engagement; however, the practitioner ordinarily would obtain the following representations from management:

- A statement acknowledging responsibility for establishing and maintaining effective internal control over derivative transactions
- A statement that there have been no errors or fraud that might indicate a weakness in the internal control over derivative transactions

- A statement that management has disclosed to the practitioner all significant deficiencies in the design or operation of the internal control over derivative transactions
- A statement that management has disclosed to the practitioner any communications from regulatory agencies, internal auditors, and other practitioners or consultants relating to the internal control over derivative transactions
- A statement that management has made available to the practitioner all information they believe is relevant to the internal control over derivative transactions
- A statement that management has responded fully to all inquiries made by the practitioner during the engagement
- A statement that no events have occurred subsequent to the date as of which the procedures were applied that would require adjustment to or modification to responses to the agreed-upon procedures

.31 An illustrative representation letter is presented in appendix C, "Illustrative Management Representation Letter" [paragraph .38] of this SOP. For additional information regarding management's representations in an agreed-upon procedures engagement, see AT sections 201.37–.39.

Restriction on the Performance of Procedures

.32 As previously stated, a practitioner should not agree to do either of the following.

a. Eliminate any of the procedures presented in appendix B [paragraph .37] of this SOP, unless a section is not applicable because the insurance company did not enter into derivative transactions addressed by the section.

b. Reduce the extent of the tests in an applicable section.

.33 If circumstances impose restrictions on the performance of the agreed-upon procedures presented in appendix B [paragraph .37] of this SOP, the practitioner should describe the restriction(s) in his or her report or withdraw from the engagement.

Dating the Report

.34 The date of completion of the agreed-upon procedures should be used as the date of the practitioner's report.

Effective Date

.35 This SOP is effective upon issuance and is applicable only to agreed-upon procedures engagements that address internal control over derivative transactions required by the Law.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.36

Appendix A

Illustrative Agreed-Upon Procedures Report

The following is an illustrative agreed-upon procedures report based on the guidance in AT section 201, *Agreed-Upon Procedures Engagements*, in Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 201).

Independent Accountant's Report
on Applying Agreed-Upon Procedures

To the Management of ABC Insurance Company:

We have performed the applicable procedures enumerated in the American Institute of Certified Public Accountants' Statement of Position (SOP), 01-3, *Performing Agreed-Upon Procedures Engagements That Address Internal Control Over Derivative Transactions as Required by the New York State Insurance Law*, which were agreed to by ABC Insurance Company, solely to assist you in complying with the requirements of Section 1410(b)(5) of the New York State Insurance Law, as amended (the Law), which addresses the assessment of internal control over derivative transactions as defined in Section 1401(a) of the Law, and Section 178.6(b) of Regulation No. 163 during the year ended December 31, 20XX. Management of ABC Insurance Company is responsible for maintaining effective internal control over derivative transactions. This agreed-upon procedures engagement was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. The sufficiency of these procedures is solely the responsibility of ABC Insurance Company. Consequently, we make no representation regarding the sufficiency of the procedures described in the attached appendix either for the purpose for which this report has been requested or for any other purpose.

The procedures performed and the findings are included in the attached appendix.

We were not engaged to and did not conduct an examination, the objective of which would be the expression of an opinion on the internal control over derivative transactions of ABC Insurance Company for the year ended December 31, 20XX. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

This report is intended solely for the information and use of the management and Board of Directors of ABC Insurance Company and is not intended to be and should not be used by anyone other than these specified parties.

[*Signature*]

[*Date*]

Appendix B

Agreed-Upon Procedures for Testing Internal Control Over Derivative Transactions

The following table lists the types of derivative transactions permitted by the New York Derivative Law (the Law). We inquired of management of the insurance company as to whether the insurance company used the type of derivative addressed by each section, and marked the column entitled "Is the Section Applicable?" either *Yes* or *No* based on management's response to the inquiry. For each type of derivative with a *Yes* response, we performed the procedures in the applicable section and attached the section to the report. For each type of derivative with a *No* response, we did not perform procedures nor did we attach the applicable section to the report. We compared the types of derivative reported by the insurance company in its "Schedule of Derivative Transactions" included in the Annual Statement with the types of derivatives listed in the following table and found that the types of derivatives included in the schedule were marked *Yes* in the table.

Attachments to the Report

No.	**Section of the Agreed-Upon Procedures** *Type of Derivative*	**Is the Section Applicable?** *Yes or No*
1	All Derivative Types	Yes
2	Cap Contracts	
3	Collar Contracts	
4	Floor Contracts	
5	Forward Contracts	
6	Future Contracts	
7	Option Contracts	
8	Swap Contracts	
9	Swaption Contracts	
10	Warrant Contracts	

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 1—All Derivative Types

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
The following procedures were performed to test controls applicable to all derivative transactions. The procedures were applied to the internal control over derivative transactions in existence during the year ended December 31, 20XX.			
Documentation of Controls, Policies, and Procedures			
1. Read the insurance company's derivative use plan (DUP), amendments thereto, and its documentation of controls, policies, and procedures that describe internal control over derivative transactions and found that the DUP and the documentation of controls, policies, and procedures include a description of controls that address the following:			
a. Systems or processes for the periodic valuation of derivative transactions including mechanisms for compensating for any lack of independence in valuing derivative positions (Valuation)	_____	_____	_____
b. Systems or processes for determining whether a derivative instrument used for hedging or replication has been effective (Effectiveness)	_____	_____	_____
c. Credit risk management systems or processes for over-the-counter (OTC) derivative transactions that measure credit risk exposure using the counterparty exposure amount and policies for the establishment of collateral arrangements with counterparties (Credit Risk Management)	_____	_____	_____
d. Management assessment of the adequacy and technical expertise of personnel associated with derivative transactions and systems to implement and control investment practices involving derivatives (Professional Competence)	_____	_____	_____
e. Systems or processes for regular reports to management, segregation of duties, and internal review procedures (Reporting)	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
f. Procedures for conducting initial and ongoing legal reviews of derivative transactions including assessments of contract enforceability (Legal Reviews)	_____	_____	_____
Nontransaction-Specific Procedures			
2. Read the minutes of meetings of the board of directors and found an indication that the board of directors of the insurance company approved the DUP and any amendments thereto.	_____	_____	_____
3. Inquired of management as to whether the DUP and any amendments thereto were approved by the New York State Insurance Department and was advised that the DUP and any amendments thereto were approved.	_____	_____	_____
4. Read the minutes of meetings of the board of directors and found an indication that the board of directors of the insurance company approved the commitment of financial resources determined by management to be sufficient to accomplish the objectives of the insurance company's DUP.	_____	_____	_____
This procedure does not provide an assessment of or assurance about the adequacy of the resources determined by management to be sufficient to accomplish the objectives of the DUP.			
In performing the following procedures, the practitioner should be aware that management frequently will have designated and will have in place limits, controls, or procedures that are more restrictive than those approved for use in the DUP.			
5. For the year ended December 31, 20XX, inquired of management and was advised that—			
a. There was monitoring of derivative transactions by a control staff, such as internal audit or other internal review group, that is independent of derivatives trading activities.	_____	_____	_____

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
b. There were procedures in place for derivative personnel to obtain, prior to exceeding limits prescribed by management, at least oral approval from members of senior management who are independent of derivatives trading activities.	_____	_____	_____
c. There were procedures in place for senior management to address excesses related to management-established limits and divergences from management-approved derivative strategies, and that such management has authority to grant exceptions to derivatives limits.	_____	_____	_____
d. There were procedures in place requiring that management be informed when limits prescribed in the DUP were exceeded and for management to approve corrective action(s) in such circumstances.	_____	_____	_____
e. There were procedures in place for the accurate transmittal of derivatives positions to the risk measurement systems when management had implemented risk management systems.	_____	_____	_____
f. There were procedures in place for the performance of appropriate reconciliations to ensure data integrity across the full range of derivatives, including any new or existing derivatives that may be monitored apart from the main processing networks.	_____	_____	_____
g. There were procedures in place for risk managers and senior management to define constraints on derivative activities to ensure compliance with the DUP and to justify excesses with respect to specified management limits.	_____	_____	_____
h. There were procedures in place for senior management, an independent group, or an individual that management designated to perform at least an annual assessment of the identified controls and financial results of the derivative activities to determine that controls were effectively implemented and that the insurance company's business objectives and strategies were achieved.	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
i. There were procedures in place for a review of limits in the context of changes in strategy, risk tolerance of the insurance company, and market conditions.			

Reporting to the Board of Directors or Committee Thereof

The Law contains provisions regarding management oversight of derivative and replication transactions.

6. Read the minutes of the board of directors meetings or committees thereof and found an indication that the board of directors or committee thereof received, at least quarterly, a report regarding derivative and replication transactions.			
7. Read one quarterly report referred to in procedure 6 and found that the report contained—			
a. A list, or appropriate summaries, of the following:			
(1) Derivative transactions during the period			
(2) Derivative transactions outstanding at the end of the period			
(3) Unrealized gains or losses on open derivative positions			
(4) Derivative transactions closed during the period			
b. A summary of the performance of the derivatives in comparison to the objective of the derivative transactions			
c. An evaluation of the risks and benefits of the derivative transactions			
d. A summary of the amount, type, and performance of replication transactions			
8. If the report referred to in the preceding procedure was received, reviewed, and approved by a committee of the board of directors, read the minutes of the board of directors meeting and found an indication that a report of such committee was reviewed at the next board of directors meeting.			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
9. Read the board of directors minutes and found an indication that the board of directors received a report during the year describing the level of knowledge and experience of individuals conducting, monitoring, controlling, and auditing derivative and replication transactions.	_____	_____	_____

Derivative and Replication Limitations

The Law contains limits on hedging and replication transactions. An insurance company may enter into hedging or replication transactions if, as a result of and after giving effect to the transaction, the derivative investments and replication investments do not exceed certain specified percentages of admitted assets. The following procedures were performed using one analysis per quarter prepared by the insurance company to monitor compliance with the limitations.

10. Obtained and read the insurance company's analysis used to test limitations on investments in derivatives and replication transactions and found that the amounts shown in the analysis indicated that—			
a. The aggregate statement value of options, swaptions, caps, floors, and warrants purchased was not in excess of seven and one-half percent of the insurance company's admitted assets, per the last annual statement.	_____	_____	_____
b. The aggregate statement value of options, swaptions, caps, and floors written was not in excess of three percent of admitted assets.	_____	_____	_____
c. The aggregate potential exposure of collars, swaps, forwards, and futures entered into and options, swaptions, caps, and floors written was not in excess of six and one-half percent of admitted assets.	_____	_____	_____
d. The aggregate statement value of all assets being replicated did not exceed ten percent of the insurance company's admitted assets.	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
e. The extent of derivative transactions did not exceed the insurance company's internal limitations or that any excess had been specifically authorized by management.			
11. Inquired of the preparer of the analysis read in procedure 10 and was advised that the analysis excluded transactions entered into to hedge the currency risk of investments denominated in a currency other than United States dollars.			
12. Obtained and read the insurance company's analysis used to test limitations on counterparty exposure, as defined in section 178.3(e) of the Regulation, and found that the report indicated that—			
a. The counterparty exposure under one or more derivative transactions for any single counterparty, other than a "qualified counterparty," was not in excess of one percent of the insurance company's admitted assets.			
b. The counterparty exposure under one or more derivative transactions for all counterparties, other than qualified counterparties, was not in excess of three percent of the insurance company's admitted assets.			
13. If the insurance company required collateral arrangements with the counterparties, obtained and read the insurance company's analysis used to monitor the adequacy of the collateral held in accordance with the terms of the arrangement and found that the amount of the collateral held as shown on the analysis was equal to or in excess of the amount to be held.			

Description of Exceptions if Any

Procedure Number	*Description of Exception*

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 2—Cap Contracts

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Performed the following procedures on selected cap contracts to test internal control over cap transactions. Selected five percent of each type of cap transaction (that is, purchases [premium disbursements], sales [premium receipts], and closeouts [closings and settlings of the position]), with the selections distributed throughout the year. If five percent of a given type of transaction exceeded 40, the number of items selected for that type of transaction was limited to 40. If five percent of a type of transaction resulted in less than four items, selected four or fewer items that represented all the transactions of that type.			
Reporting			
1. Read the insurance company's derivative use plan (DUP) and any amendments thereto and found that the DUP permits the insurance company to enter into cap contracts.	_____	_____	_____
2. For each cap selected for testing, read management's documentation describing the intended use of the cap and performed the following procedures, as applicable.	_____	_____	_____
For caps used as a hedge—			
3. Determined that the documentation described the following:			
a. The risk hedged	_____	_____	_____
b. How the hedge was consistent with the overall risk management strategy	_____	_____	_____
c. How the cap was expected to be effective in offsetting the exposure	_____	_____	_____
d. The approach in assessing the effectiveness of the hedge	_____	_____	_____
4. Determined that the following items were documented:			
a. The purpose(s) of the cap as a hedge	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
b. The terms of the cap, the name of the counterparty, and the counterparty exposure amount			
c. The assets or liabilities (or portion thereof) that the cap hedged			
d. Evidence that the cap continued to be an effective hedge			
e. Evidence that the cap was consistent with the insurance company's parameters, as specified in the DUP or applicable company policies and procedures, for entering into hedge transactions; for example, the notional amount or underlying			
If the cap was an exact offset to an outstanding cap—			
5. Read documentation indicating that the cap offset an outstanding cap previously purchased or sold by the insurance company and that the cap was an exact offset of the market risk of the cap being offset.			
For caps used in a replication transaction—			
6. Determined that the documentation described the following:			
a. The investment type and characteristics replicated			
b. How the replication was consistent with the overall management investment strategy			
c. How the cap was expected to be effective in replicating the investment characteristics of the replicated investment			
d. The approach for assessing the effectiveness of the replication transaction			
7. Determined that the following items were documented:			
a. The instruments used in the replication and the investment type and characteristics replicated			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	Findings: No Exception	Findings: Exception	Findings: N/A
b. The terms of the cap, the name of the counterparty, and the counterparty exposure amount			
For all selected caps including those that are a part of a replication transaction—			
8. Obtained a list of individuals, approved by the board of directors or a committee thereof, who had the authority to authorize cap transactions. Compared the name of the individual who authorized the cap transaction with the names on the list and found the name of the individual on the list.			
9. Based on the details of the transaction identified in procedure 2 and company policy, compared the terms of the transaction with the insurance company's policy regarding the requirement for the board of directors or a committee thereof to authorize the specific transaction tested; for example, a transaction in which the notional amount or strike price exceeded a limit requiring additional approval. If the board of directors or a committee thereof was required to approve the transaction, read minutes of the board of directors or a committee thereof or other appropriate support and found evidence of approval of the transaction tested.			
10. Obtained a list of *qualified* and *nonqualified* counterparties, approved by the board of directors or a committee thereof. Compared the name of the counterparty involved in the cap transaction with names on the list and found the name of the counterparty on the respective qualified or nonqualified list.			
11. Determined that the counterparty was listed as qualified or nonqualified in the analysis used for monitoring the insurance company's limitations on counterparty exposure consistent with the classification in the listing obtained in procedure 10.			

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
12. Obtained a list of individuals authorized by the board of directors or a committee thereof to trade cap contracts. Compared the name of the individual who executed the purchase, sale, or closeout of the cap with the names on the list and found the name of the individual on the list.			
13. Obtained a list of individuals authorized to approve payments relating to caps. Compared the name of the individual who approved any payment relating to the cap with the names on the list and found the name of the individual on the list.			
14. Compared the name of the individual who approved any payment relating to the cap with the name of the individual who approved entering into the contract and found that the names were different.			
15. Compared the name of the individual who received cash or other consideration in connection with the cap with the name of the individual who entered into the contract and found that the names of the individuals were different.			
16. Obtained the deal ticket and confirmation for the purchase, sale, or closeout of the cap and found that the purchase, sale, or closeout was confirmed by the counterparty.			
17. Compared the name of the individual who received the deal ticket and confirmation with the names on a list of individuals authorized to trade caps and found that the name was not on the list.			
18. Compared the terms of the cap contract, as stated on the deal ticket and confirmation, with the terms of the cap contract recorded in the insurance company's accounting records and found them to be in agreement.			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
19. Obtained documentation for one reporting period (for example, monthly or quarterly), indicating that the insurance company determined that its accounting records for caps tested in procedure 18, agreed with or reconciled to the related control account; for example, the subsidiary ledger to the general ledger.			
20. Obtained the accounting record documenting modifications, if any, to the cap agreement. Compared the name of the individual who approved the modification with a list of individuals authorized to approve modifications and found the name of the individual who approved the modification on the list.			
21. Compared the terms of the cap agreement recorded in the insurance company's accounting records with the terms shown in the executed copy of the cap agreement and found them to be in agreement.			
22. Obtained documentation for one reporting period (for example, monthly or quarterly), indicating that the insurance company physically inventoried the cap agreements.			
23. Using the list of authorized traders obtained in procedure 12, compared the name of the individual who had custody or access to the cap agreement with the names of individuals authorized to execute purchases, sales, or closeouts of cap contracts and found that the name of the individual was not on the list.			
24. Compared information regarding the cap, such as type of derivative, notional amount, and fair value, with the comparable information included in the report to the board of directors or appropriate committee thereof and found them to be in agreement.			

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
25. If the cap should have been included in the monitoring analysis separately tested in procedure 10 within section 1, "All Derivative Types," compared information regarding the cap, such as type of derivative, notional amount, and fair value, with the comparable information in the monitoring analysis and found them to be in agreement.			
26. Read accounting documentation indicating that the insurance company monitored periodic cash settlements related to the cap tested, meaning, the insurance company had controls in place to determine that periodic cash settlements, if any, were received.			
Effectiveness of Caps Used As Hedges and in Replication Transactions			
27. Read the insurance company's documentation of effectiveness and found that the insurance company evaluated the effectiveness of the cap as a hedge or replication in accordance with the policies regarding effectiveness.			
28. If the cap was no longer effective as a hedge or replication, compared the action taken by the insurance company with the action required by the accounting policies and procedures and found that the action taken was consistent with the accounting policy.			
Legal Review			
29. Read documentation indicating that the legal department reviewed the cap agreement to assess contract compliance with the DUP and enforceability.			
30. Read documentation indicating that the legal department updated its assessment of agreement enforceability at least annually.			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Valuation			
31. Obtained the insurance company's policies and procedures for valuing caps and found that the insurance company determined the fair value of the cap in accordance with the policy described in the insurance company's procedures for the valuation of caps.	_____	_____	_____
32. Read documentation supporting the fair value of the cap and found that the fair value was either (*a*) obtained from an independent source, (*b*) checked against an independent source, or (*c*) calculated internally by an authorized person.	_____	_____	_____

Description of Exceptions if Any

Procedure Number	*Description of Exception*

Section 3—Collar Contracts

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Performed the following procedures on selected collar contracts to test internal control over collar transactions. Selected five percent of each type of collar transaction (that is, executions [entering into a collar transaction in which the net position at inception may result in either no cash outlay, cash received, or cash disbursed] and closeouts [closings and settlings of the position]), with the selections distributed throughout the year. If five percent of a given type of transaction exceeded 40, the number of items selected for that type of transaction was limited to 40. If five percent of a type of transaction resulted in less than four items, selected four or fewer items that represented all the transactions of that type.			
Reporting			
1. Read the insurance company's derivative use plan (DUP) and any amendments thereto and found that the DUP permits the insurance company to enter into collar contracts.	_____	_____	_____
2. For each collar selected for testing, read management's documentation describing the intended use of the collar and performed the following procedures, as applicable.	_____	_____	_____
For collars used as a hedge—			
3. Determined that the documentation described the following:			
a. The risk hedged	_____	_____	_____
b. How the hedge was consistent with the overall risk management strategy	_____	_____	_____
c. How the collar was expected to be effective in offsetting the exposure	_____	_____	_____
d. The approach in assessing the effectiveness of the hedge	_____	_____	_____

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
4. Determined that the following items were documented:			
a. The purpose(s) of the collar as a hedge	_____	_____	_____
b. The terms of the collar, the name of the counterparty, and the counterparty exposure amount	_____	_____	_____
c. The assets or liabilities (or portion thereof) that the collar hedged	_____	_____	_____
d. Evidence that the collar continued to be an effective hedge	_____	_____	_____
e. Evidence that the contract was consistent with the insurance company's parameters, as specified in the DUP or applicable company policies and procedures, for entering into hedge transactions; for example, the notional amount or underlying	_____	_____	_____
If the collar was an exact offset of an outstanding collar—			
5. Read documentation indicating that the collar offset an outstanding collar previously purchased or sold by the insurance company and that the collar was an exact offset of the market risk of the collar being offset.	_____	_____	_____
For collars used in a replication transaction—			
6. Determined that the documentation described the following:			
a. The investment type and characteristics replicated	_____	_____	_____
b. How the replication was consistent with the overall management investment strategy	_____	_____	_____
c. How the collar was expected to be effective in replicating the investment characteristics of the replicated investment	_____	_____	_____
d. The approach in assessing the effectiveness of the replication transaction	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
7. Determined that the following items were documented:			
a. The instruments used in the replication and the investment type and characteristics replicated	_____	_____	_____
b. The terms of the collar, the name of the counterparty, and the counterparty exposure amount	_____	_____	_____
For all selected collars including those that are a part of a replication transaction—			
8. Obtained a list of individuals, approved by the board of directors or a committee thereof, who had the authority to authorize collar transactions. Compared the name of the individual who authorized the collar transaction with the names on the list and found the name of the individual on the list.	_____	_____	_____
9. Based on the details of the transaction identified in procedure 2 and company policy, compared the terms of the transaction with the insurance company's policy regarding the requirement for the board of directors or a committee thereof to authorize the specific transaction tested; for example, a transaction in which the notional amount or strike price exceeded a limit requiring additional approval. If the board of directors or a committee thereof was required to approve the transaction, read minutes of the board of directors or a committee thereof or other appropriate support and found evidence of approval of the transaction tested.	_____	_____	_____
10. Obtained a list of *qualified* and *nonqualified* counterparties approved by the board of directors or a committee thereof. Compared the name of the counterparty involved in the collar transaction with names on the list and found the name of the counterparty on the respective qualified or nonqualified list.	_____	_____	_____

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
11. Determined that the counterparty was listed as qualified or nonqualified in the analysis used for monitoring the insurance company's limitations on counterparty exposure consistent with the classification in the listing obtained in procedure 10.	_____	_____	_____
12. Obtained a list of individuals authorized by the board of directors or a committee thereof to trade collar contracts. Compared the name of the individual who executed the execution or closeout of the collar contract with the names on the list and found the name of the individual on the list.	_____	_____	_____
13. Obtained a list of individuals authorized to approve payments relating to collars. Compared the name of the individual who approved any payment relating to the collar with the names on the list and found the name of the individual on the list.	_____	_____	_____
14. Compared the name of the individual who approved any payment relating to the collar with the name of the individual who approved entering into the contract and found that the names were different.	_____	_____	_____
15. Compared the name of the individual who received cash or other consideration in connection with the collar with the name of the individual who entered into the contract and found that the names of the individuals were different.	_____	_____	_____
16. Obtained the deal ticket and confirmation for the execution or closeout of the collar and found that the execution or closeout was confirmed by the counterparty.	_____	_____	_____
17. Compared the name of the individual who received the deal ticket and confirmation with the names on a list of individuals authorized to trade collars and found that the name was not on the list.	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
18. Compared the terms of the collar contract, as stated on the deal ticket and confirmation, with the terms of the collar contract recorded in the insurance company's accounting records and found them to be in agreement.			
19. Obtained documentation for one reporting period (for example, monthly or quarterly) indicating that the insurance company determined that its accounting records for collars, tested in procedure 18, agreed with or reconciled to the related control account; for example, the subsidiary ledger to the general ledger.			
20. Obtained the accounting record documenting modifications, if any, to the collar agreement. Compared the name of the individual who approved the modification with a list of individuals authorized to approve modifications and found the name of the individual who approved the modification on the list.			
21. Compared the terms of the collar agreement recorded in the insurance company's accounting records with the terms shown in the executed copy of the collar agreement and found them to be in agreement.			
22. Obtained documentation for one reporting period (for example, monthly or quarterly), indicating that the insurance company physically inventoried the collar agreement.			
23. Using the list of authorized traders obtained in procedure 12, compared the name of the individual who had custody or access to the collar contracts with the names of individuals authorized to enter into trades, executions, or closeouts of collar contracts and found that the name of the individual was not on the list.			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
24. Compared information regarding the collar, such as type of derivative, notional amount, and fair value, with the comparable information included in the report to the board of directors or appropriate committee thereof and found them to be in agreement.			
25. If the collar should have been included in the monitoring analysis separately tested in procedure 10 within section 1, "All Derivative Types," compared information regarding the collar, such as type of derivative, notional amount, and fair value, with the comparable information in the monitoring analysis and found them to be in agreement.			
26. Read accounting documentation indicating that the insurance company monitored periodic cash settlements related to the collar tested, meaning, the insurance company had controls in place to determine that periodic cash settlements, if any, were received.			
Effectiveness of Collars Used As Hedges and in Replication Transactions			
27. Read the insurance company's documentation of effectiveness and found that the insurance company evaluated the effectiveness of the collar as a hedge or replication in accordance with the policies regarding effectiveness.			
28. If the collar was no longer effective as a hedge or replication, compared the action taken by the insurance company with the action required by the accounting policies and procedures and found that the action taken was consistent with the accounting policy.			

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Legal Review			
29. Read documentation indicating that the legal department reviewed the collar agreement to assess contract compliance with the DUP and enforceability.			
30. Read documentation indicating that the legal department updated its assessment of agreement enforceability at least annually.			
Valuation			
31. Obtained the insurance company's policies and procedures for valuing collars and found that the insurance company determined the fair value of the collar in accordance with the policy described in the insurance company's procedures for the valuation of collars.			
32. Read documentation supporting the fair value of the collar and found that the fair value was either (*a*) obtained from an independent source, (*b*) checked against an independent source, or (*c*) calculated internally by an authorized individual.			

Description of Exceptions if Any

Procedure Number	*Description of Exception*

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 4—Floor Contracts

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Performed the following procedures on selected floor contracts to test internal control over floor transactions. Selected five percent of each type of floor transaction (that is, purchases [premium disbursements], sales [premium receipts], and closeouts [closings and settlings of the position]), with the selections distributed throughout the year. If five percent of a given type of transaction exceeded 40, the number of items selected for that type of transaction was limited to 40. If five percent of a type of transaction resulted in less than four items, selected four or fewer items that represented all the transactions of that type.			
Reporting			
1. Read the insurance company's derivative use plan (DUP) and any amendments thereto and found that the DUP permits the insurance company to enter into floor contracts.	_____	_____	_____
2. For each floor selected for testing, read management's documentation describing the intended use of the floor and performed the following procedures, as applicable.	_____	_____	_____
For floors used as a hedge—			
3. Determined that the documentation described the following:			
a. The risk hedged	_____	_____	_____
b. How the hedge was consistent with the overall risk management strategy	_____	_____	_____
c. How the floor was expected to be effective in offsetting the exposure	_____	_____	_____
d. The approach in assessing the effectiveness of the hedge	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
4. Determined that the following items were documented:			
a. The purpose(s) of the floor as a hedge	_____	_____	_____
b. The terms of the floor, the name of the counterparty, and the counterparty exposure amount	_____	_____	_____
c. The assets or liabilities (or portion therof) that the floor hedged	_____	_____	_____
d. Evidence that the floor continued to be an effective hedge	_____	_____	_____
e. Evidence that the floor was consistent with the insurance company's parameters, as specified in the DUP or applicable company policies and procedures for entering into hedge transactions; for example, the notional amount or underlying	_____	_____	_____
If the floor was an exact offset of an outstanding floor—			
5. Read documentation indicating that the floor offset an outstanding floor previously purchased or sold by the insurance company and that the floor was an exact offset of the market risk of the floor being offset.			
For floors used in a replication transaction—			
6. Determined that the documentation described the following:			
a. The investment type and characteristics replicated	_____	_____	_____
b. How the replication was consistent with the overall management investment strategy	_____	_____	_____
c. How the floor was expected to be effective in replicating the investment characteristics of the replicated investment	_____	_____	_____
d. The approach in assessing the effectiveness of the replication transaction	_____	_____	_____

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
7. Determined that the following items were documented:			
a. The instruments used in the replication and the investment type and characteristics replicated	_____	_____	_____
b. The terms of the floor, the name of the counterparty, and the counterparty exposure amount	_____	_____	_____
For all selected floors including those that are a part of a replication transaction—			
8. Obtained a list of individuals approved by the board of directors or a committee thereof who had the authority to authorize floor transactions. Compared the name of the individual who authorized the floor transaction with the names on the list and found the name of the individual on the list.	_____	_____	_____
9. Based on the details of the transaction identified in procedure 2 and company policy, compared the terms of the transaction with the insurance company's policy regarding the requirement for the board of directors or a committee thereof to authorize the specific transaction tested; for example, a transaction in which the notional amount or strike price exceeded a limit requiring additional approval. If the board of directors or a committee thereof was required to approve the transaction, read minutes of the board of directors or a committee thereof or other appropriate support and found evidence of approval of the transaction tested.	_____	_____	_____
10. Obtained a list of *qualified* and *nonqualified* counterparties, approved by the board of directors or a committee thereof. Compared the name of the counterparty involved in the floor transaction with names on the list and found the name of the counterparty on the respective qualified or nonqualified list.	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
11. Determined that the counterparty was listed as qualified or nonqualified in the analysis used for monitoring the insurance company's limitations on counterparty exposure consistent with the classification in the listing obtained in procedure 10.			
12. Obtained a list of individuals authorized by the board of directors or a committee thereof to trade floor contracts. Compared the name of the individual who executed the purchase, sale, or closeout of the floor with the names on the list and found the name of the individual on the list.			
13. Obtained a list of individuals authorized to approve payments relating to floors. Compared the name of the individual who approved any payment relating to the floor with the names on the list and found the name of the individual on the list.			
14. Compared the name of the individual who approved any payment relating to the floor with the name of the individual who approved entering into the contract and found that the names were different.			
15. Compared the name of the individual who received cash or other consideration in connection with the floor with the name of the individual who entered into the contract and found that the names of the individuals were different.			
16. Obtained the deal ticket and confirmation for the purchase, sale, or closeout of the floor and found that the purchase, sale, or closeout was confirmed by the counterparty.			
17. Compared the name of the individual who received the deal ticket and confirmation with the names on a list of individuals authorized to trade floors and found that the name was not on the list.			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
18. Compared the terms of the floor contract, as stated on the deal ticket and confirmation, with the terms of the floor contract recorded in the insurance company's accounting records and found them to be in agreement.			
19. Obtained documentation for one reporting period (for example, monthly or quarterly), that the insurance company determined that its accounting records for floors, tested in procedure 18, agreed with or reconciled to the related control account; for example, the subsidiary ledger to the general ledger.			
20. Obtained the accounting record documenting modifications, if any, to the floor agreement. Compared the name of the individual who approved the modification with a list of individuals authorized to approve modifications and found the name of the individual who approved the modification on the list.			
21. Compared the terms of the floor agreement recorded in the insurance company's accounting records with the terms shown in the executed copy of the floor agreement and found them to be in agreement.			
22. Obtained documentation for one reporting period (for example, monthly or quarterly), indicating that the insurance company physically inventoried the floor agreements.			
23. Using the list of authorized traders obtained in procedure 12, compared the name of the individual who had custody or access to the floor agreement with the names of individuals authorized to execute purchases, sales, or closeouts of floor contracts and found that the name was not on the list.			

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
24. Compared information regarding the floor, such as type of derivative, notional amount, and fair value, with the comparable information included in the report to the board of directors or appropriate committee thereof and found them to be in agreement.			
25. If the floor should have been included in the monitoring analysis separately tested in procedure 10 within section 1, "All Derivative Types," compared information regarding the floor, such as type of derivative, notional amount, and fair value, with the comparable information in the monitoring analysis and found them to be in agreement.			
26. Read accounting documentation indicating that the insurance company monitored periodic cash settlements related to the floor tested, meaning, the insurance company had controls in place to determine that periodic cash settlements, if any, were received.			
Effectiveness of Floors Used As Hedges and in Replication Transactions			
27. Read the insurance company's documentation of effectiveness and found that the insurance company evaluated the effectiveness of the floor as a hedge or replication in accordance with the policies regarding effectiveness.			
28. If the floor was no longer effective as a hedge or replication, compared the action taken by the insurance company with the action required by the accounting policies and procedures and found that the action taken was consistent with the accounting policy.			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Legal Review			
29. Read documentation indicating that the legal department reviewed the floor agreement to assess contract compliance with the DUP and enforceability.	_____	_____	_____
30. Read documentation indicating that the legal department updated its assessment of agreement enforceability at least annually.	_____	_____	_____
Valuation			
31. Obtained the insurance company's policies and procedures for valuing floors and found that the insurance company determined the fair value of the floor in accordance with the policy described in the insurance company's procedures for the valuation of floors.	_____	_____	_____
32. Read documentation supporting the fair value of the floor and found that the fair value was either (*a*) obtained from an independent source, (*b*) checked against an independent source, or (*c*) calculated internally by an authorized individual.	_____	_____	_____

Description of Exceptions if Any

Procedure Number	*Description of Exception*

Section 5—Forward Contracts

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Performed the following procedures on selected forward contracts to test internal control over forward transactions. Selected five percent of each type of forward transaction, with the selections distributed throughout the year. These are, (1) forward contracts entered into to make delivery, (2) forward contracts entered into to take delivery, (3) forward contracts settled by making delivery, (4) forward contracts settled by taking delivery, (5) forward contracts settled by cash. If five percent of a given type of transaction exceeded 40, the number of items selected for that type of transaction was limited to 40. If five percent of a type of transaction resulted in less than four items, selected four or fewer items that represented all of the transactions of that type.			
Reporting			
1. Read the insurance company's derivative use plan (DUP) and any amendments thereto and found that the DUP permits the insurance company to enter into forward contracts.	_____	_____	_____
2. For each forward selected for testing, read management's documentation describing the intended use of the forward and performed the following procedures, as applicable.	_____	_____	_____
For forward contracts used as a hedge—			
3. Determined that the documentation describes the following:			
a. The risk hedged	_____	_____	_____
b. How the hedge was consistent with the overall risk management strategy	_____	_____	_____
c. How the forward was expected to be effective in offsetting the exposure	_____	_____	_____
d. The approach in assessing the effectiveness of the hedge	_____	_____	_____

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
4. Determined that the following items were documented:			
a. The purpose(s) of the forward as a hedge	_____	_____	_____
b. The terms of the forward, the name of the counterparty, and the counterparty exposure amount	_____	_____	_____
c. The assets or liabilities (or portion thereof) that the forward hedged	_____	_____	_____
d. The specific forward contract used in the hedge	_____	_____	_____
e. Evidence that the forward continued to be an effective hedge	_____	_____	_____
f. Evidence that the forward was consistent with the insurance company's parameters, as specified in the DUP or applicable company policies and procedures, for entering into hedge transactions; for example, the notional amount or underlying	_____	_____	_____
If the forward was an exact offset of an outstanding forward—			
5. Read documentation indicating that the forward offset an outstanding forward previously purchased or sold by the insurance company and that the forward was an exact offset of the market risk of the forward being offset.	_____	_____	_____
For forwards used in a replication transaction—			
6. Determined that the documentation described the following:			
a. The investment type and characteristics replicated	_____	_____	_____
b. How the replication was consistent with the overall management investment strategy	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
c. How the forward was expected to be effective in replicating the investment characteristic of the replicated investment			
d. The approach for assessing the effectiveness of the replication transaction			
7. Determined that the following items were documented:			
a. The instruments used in the replication and the investment type and characteristics replicated			
b. The terms of the forward contract, the name of the counterparty, and the counterparty exposure amount			
For all selected forwards, including those that are a part of the replication transaction—			
8. Obtained a list of individuals, approved by the board of directors or a committee thereof who had the authority to authorize forward transactions. Compared the name of the individual who authorized the forward transaction with the names on the list and found the name of the individual on the list.			
9. Based on the details of the transaction identified in procedure 2 and company policy, compared the terms of the transaction with the insurance company's policy regarding the requirement for the board of directors or a committee thereof to authorize the specific transaction tested; for example, a transaction in which the notional amount exceeded a limit requiring additional approval. If the board of directors or a committee thereof was required to approve the transaction, read minutes of the board of directors or a committee thereof or other appropriate support and found evidence of approval of the transaction tested.			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	Findings: No Exception	Findings: Exception	Findings: N/A
10. Obtained a list of *qualified* and *nonqualified* counterparties, approved by the board of directors or a committee thereof. Compared the name of the counterparty involved in the forward transaction with names on the list and found the name of the counterparty on the respective qualified or nonqualified list.			
11. Determined that the counterparty was listed as qualified or nonqualified in the analysis used for monitoring the insurance company's limitations on counterparty exposure consistent with the classification in the listing obtained in procedure 10.			
12. Obtained a list of individuals authorized by the board of directors or committee thereof to trade forward contracts. Compared the name of the individual who executed the purchase or sale of the forward with the names on the list and found the name of the individual on the list.			
13. Obtained a list of individuals authorized to approve settlements or payments related to forward contracts. For the purchase and any transaction subsequent to purchase, compared the name of the individual who approved any payment or settlement of funds in connection with the forward contract with the names on the list and found the name of the individual on the list.			
14. Compared the name of the individual who approved any settlement or payment relating to the forward with the name of the individual who approved entering into the contract and found that the names were different.			
15. Compared the name of the individual who received cash or other consideration in connection with the forward with the name of the individual who entered into the contract and found that the names of the individuals were different.			

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
16. Obtained the deal ticket and confirmation for the purchase or sale of the forward contract and found that the purchase or sale was confirmed by the counterparty.			
17. Compared the name of the individual who received the deal ticket and confirmation with the names on a list of individuals authorized to trade forwards and found that the name was not on the list.			
18. Compared the terms of the forward contract, as stated on the deal ticket and confirmation, with the terms of the forward contract recorded in the insurance company's accounting records and found them to be in agreement.			
19. Obtained documentation for one reporting period, (for example, monthly or quarterly), that the insurance company determined that its accounting records for forwards, tested in procedure 18, agreed with or reconciled to the related control account, (for example, the subsidiary ledger to the general ledger).			
20. Obtained the accounting record documenting modifications, if any, to the forward contract. Compared the name of the individual who approved the modification with a list of individuals authorized to approve modifications and found the name of the individual who approved the modification on the list.			
21. For one reporting period, (for example, monthly or quarterly), obtained the insurance company's documentation of the existence of the forward contract and found that the insurance company either (*a*) obtained a statement from the custodian confirming the existence of the forward contract, (*b*) physically inventoried the forward contract, or (*c*) obtained a statement from the counterparty acknowledging the existence of the forward contract.			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
22. Using the list of authorized traders obtained in procedure 12, compared the name of the individual who had custody or access to the forward with the names of individuals authorized to execute purchases and sales of forwards and found that the name was not on the list.			
23. Compared information regarding the forward, such as type of derivative, notional amount, and fair value, with the comparable information included in the report to the board of directors or appropriate committee thereof and found them to be in agreement.			
24. If the forward should have been included in the monitoring analysis separately tested in step 10 within section 1, "All Derivative Types," compared information regarding the forward, such as type of derivative, notional amount, and fair value, with the comparable information in the monitoring analysis and found them to be in agreement.			
Effectiveness of Forward Contracts Used As Hedges and in Replication Transactions			
25. Read the insurance company's documentation of effectiveness and found that the insurance company evaluated the effectiveness of the forward as a hedge or replication in accordance with the policies regarding effectiveness.			
26. If the forward was no longer effective as a hedge or replication, compared the action taken by the insurance company with the action required by the accounting policies and procedures and found that the action taken was consistent with the accounting policy.			

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Legal Review			
27. Read documentation indicating that the legal department reviewed the forward contract to assess contract compliance with the DUP and enforceability.	_____	_____	_____
28. Read documentation indicating that the legal department updated its assessment of contract enforceability at least annually.	_____	_____	_____
Valuation			
29. Obtained the insurance company's policies and procedures for valuing forwards and found that the insurance company determined the fair value of the forward in accordance with the policy described in the insurance company's procedures for valuation of forwards.	_____	_____	_____
30. Read documentation supporting the fair value of the forward contract and found that the fair value was either (*a*) obtained from an independent source, (*b*) checked against an independent source, or (*c*) calculated internally by an authorized individual.	_____	_____	_____

Description of Exceptions if Any

Procedure Number	*Description of Exception*

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 6—Futures Contracts

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Performed the following procedures on selected futures contracts to test internal control over futures transactions. Selected five percent of each type of futures transaction, with the selections distributed throughout the year. These are purchases, sales, and cash settlements (closeouts of a position). If five percent of a given type of transaction exceeded 40, the number of items selected for that type of transaction was limited to 40. If five percent of a type of transaction resulted in less than four items, selected four or fewer items that represented all of the transactions of that type.			
Reporting			
1. Read the insurance company's derivative use plan (DUP) and any amendments thereto and found that the DUP permits the insurance company to trade futures.	_____	_____	_____
2. For each futures transaction selected for testing, read management's documentation describing the intended use of the futures and performed the following procedures, as applicable.	_____	_____	_____
For futures used as a hedge—			
3. Determined that the documentation describes the following:			
a. The risk hedged	_____	_____	_____
b. How the hedge was consistent with the overall risk management strategy	_____	_____	_____
c. How the futures position was expected to be effective in offsetting the exposure	_____	_____	_____
d. The approach in assessing the effectiveness of the hedge	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
4. Determined that the following items were documented:			
a. The purpose(s) of the futures as a hedge	_____	_____	_____
b. The terms of the futures transaction and the name of the exchange and firm(s) handling the trade	_____	_____	_____
c. The assets or liabilities (or portion thereof) that the futures transaction hedged	_____	_____	_____
d. Evidence that the futures contract continued to be an effective hedge	_____	_____	_____
e. Evidence that the futures position was consistent with the insurance company's parameters, as specified in the DUP or applicable company policies and procedures for futures transactions; for example, the notional amount or underlying	_____	_____	_____
For futures transactions that were an exact offset of an outstanding futures transaction—			
5. Read documentation indicating that the futures transaction offset an outstanding futures position previously purchased or sold by the insurer and that the futures transaction was an exact offset of the market risk of the futures position being offset.	_____	_____	_____
For futures used in a replication transaction—			
6. Determined that the documentation described the following:			
a. The investment type and characteristics replicated	_____	_____	_____
b. How the replication was consistent with the overall management investment strategy	_____	_____	_____
c. How the futures position was expected to be effective in replicating the investment characteristics of the replicated investment	_____	_____	_____
d. The approach in assessing the effectiveness of the replication transaction	_____	_____	_____

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
7. Determined that the following items were documented:			
a. The instruments used in the replication and the investment type and characteristics replicated	_____	_____	_____
b. The terms of the futures transaction and the name of the exchange and the firm(s) handling the trade	_____	_____	_____
c. The specific futures contract used in the replication	_____	_____	_____
For all selected futures including those that are a part of the replication transaction—			
8. Obtained a list of individuals, approved by the board of directors or a committee thereof, who had the authority to authorize futures trades. Compared the name of the individual who authorized the futures transaction with the names on the list and found the name of the individual on the list.	_____	_____	_____
9. Based on the details of the transaction identified in procedure 2 and company policy, compared the terms of the transaction with the insurance company's policy regarding the requirement for the board of directors or a committee thereof to authorize the specific transaction tested; for example, a transaction in which the notional amount exceeded a limit requiring additional approval. If the board of directors or a committee thereof was required to approve the transaction, read minutes of the board of directors or a committee thereof or other appropriate support and found evidence of approval of the transaction tested.	_____	_____	_____
10. Obtained a list of individuals authorized by the board of directors or committee thereof to trade futures contracts. Compared the name of the individual who executed the purchase or sale of the futures contract with the names on the list and found the name of the individual on the list.	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
11. Obtained a list of individuals authorized to approve settlements or disbursements related to futures transactions. For purchases and transactions subsequent to purchase or sale of the futures contract, compared the name of the individual who approved any settlement of funds relating to the futures with the names on the list and found the name of the individual on the list.			
12. Compared the name of the individual who approved any payment relating to the futures with the name of the individual who approved entering into the contract and found that the names were different.			
13. Compared the name of the individual who received cash or other consideration in connection with the futures with the name of the individual who entered into the contract and found that the names of the individuals were different.			
14. Obtained the deal ticket and confirmation for the purchase, expiration, or sale of the futures contracts and found that the purchase, sale, or expiration of the futures contract was confirmed by the deal ticket and confirmation.			
15. Compared the terms of the futures transaction, as stated on the deal ticket and confirmation, with the terms of the transaction recorded in the insurance company's accounting records and found them to be in agreement.			
16. Obtained documentation for one reporting period, (for example, monthly or quarterly), that the insurance company determined that its accounting records for futures, tested in procedure 15, agreed with or reconciled to the related control account, (for example, the subsidiary ledger to the general ledger).			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
17. For one reporting period, (for example, monthly or quarterly), obtained the insurance company's documentation of the existence of the futures contracts and found that the insurance company obtained statements from the futures counterparty(ies) or broker(s) confirming the futures transactions and positions.	_____	_____	_____
18. Compared information regarding the futures contract, such as type of derivative, notional amount, and fair value, with the comparable information included in the report to the board of directors or appropriate committee thereof and found them to be in agreement.	_____	_____	_____
19. If the futures position should have been included in the monitoring analysis separately tested in procedure 10 within section 1, " All Derivative Types," compared information regarding the futures contract, such as type of derivative, notional amount, and fair value, with the comparable information in the monitoring analysis and found them to be in agreement.	_____	_____	_____
Effectiveness of Futures Used As Hedges and in Replication Transactions			
20. Read the insurance company's documentation of effectiveness and found that the insurance company evaluated the effectiveness of the futures position as a hedge or replication in accordance with the policies regarding effectiveness.	_____	_____	_____
21. If the futures position was no longer effective as a hedge or replication, compared the action taken by the insurance company with the action required by the company policies and procedures and found that the action taken was consistent with the accounting policy.	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Valuation			
22. Obtained the insurance company's policies and procedures for valuing positions and found that the insurance company determined the valuation of the futures contract in accordance with the policy described in the insurance company's procedures for valuation of futures.	_____	_____	_____
23. Read documentation supporting the market price of the futures contract and found that the market price was obtained from an independent source.	_____	_____	_____

Description of Exceptions if Any

Procedure Number	*Description of Exception*

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 7—Option Contracts

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Performed the following procedures on selected option contracts to test internal control over option transactions. Selected five percent of each type of option transaction (that is, purchases, sales, expirations, and exercises), with the selections distributed throughout the year. If five percent of a given type of transaction exceeded 40, the number of items selected for that type of transaction was limited to 40. If five percent of a type of transaction resulted in less than four items, selected four or fewer items that represented all of the transactions of that type.			
Reporting			
1. Read the insurance company's derivative use plan (DUP) and any amendments thereto and found that the DUP permits the insurance company to trade or enter into option contracts.	_____	_____	_____
2. For each option selected for testing, read management's documentation describing the intended use of the option and performed the following procedures, as applicable.	_____	_____	_____
For options used as a hedge—			
3. Determined that the documentation described the following:			
a. The risk hedged	_____	_____	_____
b. How the hedge was consistent with the overall risk management strategy	_____	_____	_____
c. How the option was expected to be effective in offsetting the exposure	_____	_____	_____
d. The approach in assessing the effectiveness of the hedge	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
4. Determined that the following items were documented:			
a. The purpose(s) of the option as a hedge	_____	_____	_____
b. For over-the-counter (OTC) options, the terms of the option, the name of the counterparty, and the counterparty exposure amount	_____	_____	_____
c. For exchange-traded options, the term of the option, the name of the exchange, and the name of the firm(s) handling the trade	_____	_____	_____
d. The assets or liabilities (or portion thereof) that the option hedged	_____	_____	_____
e. For OTC and exchange-traded options, the specific option used in the hedge	_____	_____	_____
f. Evidence that the option continued to be an effective hedge	_____	_____	_____
g. Evidence that the option was consistent with the insurance company's parameters, as specified in the DUP or applicable company policies and procedures, for entering into hedge transactions; for example, the notional amount, or underlying	_____	_____	_____
If the option transaction was (*a*) for income generation and was for the sale of a call option on securities or (*b*) an exact offset to an outstanding option—			
5. Read the documentation supporting the transaction which indicated that the insurance company was holding or could immediately acquire through the exercise of options, warrants, or conversion rights already owned, the underlying securities during the entire period the option was outstanding.	_____	_____	_____
6. Read documentation indicating that the option offset an outstanding option previously purchased or sold by the insurance company and that the option was an exact offset to the market risk of the option being offset.	_____	_____	_____

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
For options used in a replication transaction—			
7. Determined that the documentation described the following:			
a. The investment type and characteristics replicated	_____	_____	_____
b. How the replication was consistent with the overall management investment strategy	_____	_____	_____
c. How the option was expected to be effective in replicating the investment characteristics of the replicated investment	_____	_____	_____
d. The approach in assessing the effectiveness of the replication transaction	_____	_____	_____
8. Determined that the following items were documented:			
a. The instruments used in the replication and the investment type and characteristics replicated	_____	_____	_____
b. The specific option used in the replication	_____	_____	_____
c. For OTC options, the terms of the option, the name of the counterparty, and the counterparty exposure amount	_____	_____	_____
d. For exchange-traded options, the name of the exchange and the firm(s) handling the trade	_____	_____	_____
For all selected options, including those that are a part of a replication transaction—			
9. Obtained a list of individuals, approved by the board of directors or a committee thereof, who had the authority to authorize option transactions. Compared the name of the individual who authorized the option transaction with the names on the list and found the name of the individual on the list.	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
10. Based on the details of the transaction identified in procedure 2 and company policy, compared the terms of the transaction with the insurance company's policy regarding the requirement for the board of directors or a committee thereof to authorize the specific transaction tested; for example, a transaction in which the notional amount exceeded a limit requiring additional approval. If the board of directors or a committee thereof was required to approve the transaction, read minutes of the board of directors or a committee thereof or other appropriate support and found evidence of approval of the transaction tested.			
11. Obtained a list of *qualified* and *nonqualified* counterparties, approved by the board of directors or a committee thereof. Compared the name of the counterparty involved in the option transaction with names on the list and found the name of the counterparty on the respective qualified or nonqualified list.			
12. For OTC options, determined that the counterparty was listed as qualified or nonqualified in the analysis used for monitoring the insurance company's limitations on counterparty exposure consistent with the classification in the listing obtained in procedure 11.			
13. Obtained a list of individuals authorized by the board of directors or committee thereof to trade option contracts. Compared the name of the individual who executed the purchase, sale, or exercise of the option with the names on the list and found the name of the individual on the list.			
14. Obtained a list of individuals authorized to approve payments relating to options contracts. Compared the name of the individual who approved any payment relating to the option with the names on the list and found the name of the individual on the list.			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	Findings: No Exception	Findings: Exception	Findings: N/A
15. Compared the name of the individual who approved any payment relating to the option with the name of the individual who approved entering into the contract and found that the names were different.			
16. Compared the name of the individual who received cash or other consideration in connection with the option with the name of the individual who entered into the contract and found that the names of the individuals were different.			
17. Obtained the deal ticket and confirmation for the purchase, sale, or exercise of the option and found that the purchase, sale, or exercise of the option was confirmed by the counterparty or firm handling the transaction.			
18. Compared the name of the individual who received the deal ticket and confirmation with the names on a list of individuals authorized to trade options and found that the name was not on the list.			
19. Compared the terms of the option contract, as stated on the deal ticket and confirmation, with the terms of the option contract recorded in the insurance company's accounting records and found them to be in agreement.			
20. Obtained documentation for one reporting period, (for example, monthly or quarterly), indicating that the insurance company determined whether its accounting records for options, tested in procedure 19, agreed with or reconciled to the related control account, (for example, the subsidiary ledger to the general ledger).			
21. Obtained the accounting record documenting modifications, if any, to the option transaction. Compared the name of the individual who approved the modification with a list of individuals authorized to approve modifications and found the name of the individual who approved the modification on the list.			

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
22. Obtained documentation for one reporting period, (for example, monthly or quarterly), indicating that the insurance company obtained a statement from the counterparty confirming the existence of the option position.			
23. Using the list of authorized traders obtained in procedure 13, compared the name of the individual who had custody of or access to the option documentation with the names of individuals authorized to purchase, sell, or exercise the option and found that the name was not on the list.			
24. Compared information regarding the option, such as type of derivative, notional amount, and fair value, with the comparable information included in the report to the board of directors or appropriate committee thereof and found them to be in agreement.			
25. If the option should have been included in the monitoring analysis separately tested in procedure 10 within section 1, "All Derivative Types," compared information regarding the option, such as type of derivative, notional amount, and fair value, with the comparable information in the monitoring analysis and found them to be in agreement.			
Effectiveness of Options Used As Hedges and in Replication Transactions			
26. Read the insurance company's documentation of effectiveness and found that the insurance company evaluated the effectiveness of the option as a hedge or replication in accordance with the policies regarding effectiveness.			
27. If the option was no longer effective as a hedge or replication, compared the action taken by the insurance company with the action required by the accounting policies and procedures and found that the action taken was consistent with the accounting policy.			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Legal Review			
28. Read documentation indicating that the legal department reviewed the option agreement to assess contract compliance with the DUP and enforceability.	_____	_____	_____
29. Read documentation indicating that the legal department updated its assessment of legal enforceability of the OTC option agreement at least annually.	_____	_____	_____
Valuation			
30. Obtained the insurance company's policies and procedures for valuing options and found that the insurance company determined the fair value of OTC options and the market price of exchange-traded options, in accordance with the policy described in the insurance company's procedures for the valuation of options.	_____	_____	_____
31. Read documentation supporting the fair value for OTC options and the market price of exchange-traded options and found that the fair value or market value was either (*a*) obtained from an independent source, (*b*) checked against an independent source, or (*c*) calculated internally by an authorized individual.	_____	_____	_____

Description of Exceptions if Any

Procedure Number	*Description of Exception*

Section 8—Swap Contracts

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Performed the following procedures on selected swap contracts to test internal control over swap transactions. Selected five percent of each type of swap transaction (that is, executions [purchases] and closeouts [sales]), with the selections distributed throughout the year. If five percent of a given type of transaction exceeded 40, the number of items selected for that type of transaction was limited to 40. If five percent of a type of transaction resulted in fewer than four items, selected four or fewer items that represented all the transactions of that type.			
Reporting			
1. Read the insurance company's derivative use plan (DUP) and any amendments thereto and found that the DUP permits the insurance company to enter into swap agreements.	_____	_____	_____
2. For each swap agreement selected for testing, read management's documentation describing the intended use of the swap agreement and performed the following procedures, as applicable.	_____	_____	_____
For swaps used as a hedge—			
3. Determined that the documentation describes the following:			
a. The risk hedged	_____	_____	_____
b. How the hedge was consistent with the overall risk management strategy	_____	_____	_____
c. How the swap was expected to be effective in offsetting the exposure	_____	_____	_____
d. The approach in assessing the effectiveness of the hedge	_____	_____	_____

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
4. Determined that the following items were documented:			
a. The purpose(s) of the swap as a hedge	_____	_____	_____
b. The terms of the swap, the name of the counterparty, and the counterparty exposure amount	_____	_____	_____
c. The assets or liabilities (or portion thereof) that the swap hedged	_____	_____	_____
d. Evidence that the swap continued to be an effective hedge	_____	_____	_____
e. Evidence that the swap was consistent with the insurance company's parameters, as specified in the DUP or applicable policies and procedures, for entering into swap agreements; for example, the notional amount or underlying	_____	_____	_____
For swaps that were an exact offset of an outstanding swap—			
5. Read documentation that indicated that the swap offset a swap previously purchased or sold, and that the swap was an exact offset to the market risk of the swap being offset.	_____	_____	_____
For swaps used in a replication transaction—			
6. Determined that the documentation described the following:			
a. The investment type and characteristics replicated	_____	_____	_____
b. How the replication was consistent with the overall management investment strategy	_____	_____	_____
c. How the swap was expected to be effective in replicating the investment characteristic of the replicated investment	_____	_____	_____
d. The approach in assessing the effectiveness of the replication transaction	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
7. Determined that the following items were documented:			
a. The instruments used in the replication and the investment type and characteristics replicated	_____	_____	_____
b. The terms of the swap, the name of the counterparty, and the counterparty exposure amount	_____	_____	_____
For all selected swaps including those that are a part of a replication transaction—			
8. Obtained a list of individuals, approved by the board of directors or a committee thereof who had the authority to authorize swap transactions. Compared the name of the individual who authorized the swap transaction with the names on the list and found the name of the individual on the list.	_____	_____	_____
9. Based on the details of the transaction identified in procedure 2 and company policy, compared the terms of the transaction with the insurance company's policy regarding the requirement for the board of directors or a committee thereof to authorize the specific transactions tested; for example, a transaction in which the notional amount exceeded a limit requiring additional approval. If the board of directors or a committee thereof was required to approve the transaction, read minutes of the board of directors or a committee thereof or other appropriate support and found evidence of approval of the transaction tested.	_____	_____	_____
10. Obtained a list of *qualified* and *nonqualified* counterparties, approved by the board of directors or a committee thereof. Compared the name of the counterparty involved in the swap agreement with names on the list and found the name of the counterparty on the respective qualified or nonqualified list.	_____	_____	_____

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
11. Determined that the counterparty was listed as qualified or nonqualified in the analysis used for monitoring the insurance company's limitations on counterparty exposure consistent with the classification in the listing obtained in procedure 10.	_____	_____	_____
12. Obtained a list of individuals authorized by the board of directors or committee thereof to trade swap contracts. Compared the name of the individual who executed the swap with the names on the list and found the name of the individual on the list.	_____	_____	_____
13. Obtained a list of individuals authorized to approve settlements or disbursements related to swaps. For purchases and any interim settlements or closeouts of the swap subsequent to purchase, compared the name of the individual who approved any settlement of funds relating to the swap with the names on the list and found the name of the individual on the list.	_____	_____	_____
14. Compared the name of the individual who approved any payment relating to the swap with the name of the individual who approved entering into the contract and found that the names were different.	_____	_____	_____
15. Compared the name of the individual who received cash or other consideration in connection with the swap with the name of the individual who entered into the contract and found that the names of the individuals were different.	_____	_____	_____
16. Obtained the deal ticket and confirmation for the purchase, execution, or closeout of the swap and found that the purchase, execution, or closeout of the swap was confirmed by the counterparty.	_____	_____	_____
17. Compared the name of the individual who received the deal ticket and confirmation with the names on a list of individuals authorized to trade swaps and found that the name was not on the list.	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
18. Compared the terms of the swap contract, as stated on the deal ticket and confirmation, with the terms of the swap contract recorded in the insurance company's accounting records and found them to be in agreement.			
19. Obtained documentation for one reporting period (for example, monthly, or quarterly), that the insurance company determined whether its accounting records for swaps, tested in procedure 18, agreed with or reconciled to the related control account, (for example, the subsidiary ledger to the general ledger).			
20. Obtained the accounting record documenting modifications, if any, to the swap agreement. Compared the name of the individual who approved the modification with a list of individuals authorized to approve modifications and found the name of the individual who approved the modification on the list.			
21. Compared the terms of the swap agreement recorded in the insurance company's accounting records with the terms shown in the executed copy of the swap agreement and found them to be in agreement.			
22. Using the list of authorized traders obtained in procedure 12, compared the name of the individual who had custody or access to the swap agreement with the names of individuals authorized to execute swap agreements and found that the name was not on the list.			
23. Compared information regarding the swap, such as type of derivative, notional amount, and fair value, with the comparable information included in the report to the board of directors or appropriate committee thereof and found them to be in agreement.			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
24. If the swap should have been included in the monitoring analysis separately tested in procedure 10 within section 1, "All Derivative Types," compared information regarding the swap, such as type of derivative, notional amount, and fair value, with the comparable information in the monitoring analysis and found them to be in agreement.	_____	_____	_____
25. Read accounting documentation indicating that the insurance company monitored periodic cash settlements related to swap transactions, meaning, the insurance company had controls in place to determine that periodic cash settlements, if any, were received.	_____	_____	_____
Effectiveness of Swaps Used As Hedges and in Replication Transactions			
26. Read the insurance company's documentation of effectiveness and found that the insurance company evaluated the effectiveness of the swap as a hedge or replication in accordance with the policies regarding effectiveness.	_____	_____	_____
27. If the swap was no longer effective as a hedge or replication, compared the action taken by the insurance company with the action required by the accounting policies and procedures and found that the action taken was consistent with the accounting policy.	_____	_____	_____
Legal Review			
28. Read documentation indicating that the legal department reviewed the swap agreement to assess contract compliance with the DUP and enforceability.	_____	_____	_____
29. Read documentation indicating that the legal department updated its assessment of the enforceability of the swap agreement at least annually.	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Valuation			
30. Obtained the insurance company's policies and procedures for valuing swaps and found that the insurance company determined the fair value of the swap in accordance with the policy described in the insurance company's procedures for valuation of swaps.	_____	_____	_____
31. Read documentation supporting the fair value of the swap and found that the fair value was either (*a*) obtained from an independent source, (*b*) checked against an independent source, or (*c*) calculated internally by an authorized individual.	_____	_____	_____

Description of Exceptions if Any

Procedure Number	*Description of Exception*

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 9—Swaption Contracts

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Performed the following procedures on selected swaption contracts to test internal control over swaption transactions. Selected five percent of each type of swaption transaction with the selections distributed throughout the year. These are executions (purchases) and closeouts (sales). If five percent of a given type of transaction exceeded 40, the number of items selected for that type of transaction was limited to 40. If five percent of a type of transaction resulted in less than four items, selected four or fewer items that represented all the transactions of that type.			
Reporting			
1. Read the insurance company's derivative use plan (DUP) and any amendments thereto and found that the DUP permits the insurance company to buy or sell swaptions.	_____	_____	_____
2. For each swaption contract selected for testing, read management's documentation describing the intended use of the swaption and performed the following procedures, as applicable.	_____	_____	_____
For swaptions used as a hedge—			
3. Determined that the documentation describes the following:			
a. The risk hedged	_____	_____	_____
b. How the hedge was consistent with the overall risk management strategy	_____	_____	_____
c. How the swaption was expected to be effective in offsetting the exposure	_____	_____	_____
d. The approach in assessing the effectiveness of the hedge	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
4. Determined that the following items were documented:			
a. The purpose(s) of the swaption as a hedge	_____	_____	_____
b. The terms of the swaption, the name of the counterparty, and the counterparty exposure amount	_____	_____	_____
c. The assets or liabilities (or portion thereof) that the swaption hedged	_____	_____	_____
d. Evidence that the swaption continued to be an effective hedge	_____	_____	_____
e. Evidence that the swaption was consistent with the insurance company's parameters, as specified in the DUP or applicable policies and procedures, for entering into swaption agreements; for example, the notional amount or underlying	_____	_____	_____
For swaptions that were an exact offset of an outstanding swaption—			
5. Read documentation indicating that the swaption offset an outstanding swaption and that the swaption was an exact offset of the market risk of the swaption being offset.	_____	_____	_____
For swaptions used in a replication transaction—			
6. Determined that the documentation described the following:			
a. The investment type and characteristics replicated	_____	_____	_____
b. How the replication was consistent with the overall management investment strategy	_____	_____	_____
c. How the swaption was expected to be effective in replicating the investment characteristic of the replicated investment	_____	_____	_____
d. The approach in assessing the effectiveness of the replication transaction	_____	_____	_____

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
7. Determined that the following items were documented:			
a. The instruments used in the replication and the investment type and characteristics replicated	_____	_____	_____
b. The terms of the swaption, the name of the counterparty, and the counterparty exposure amount	_____	_____	_____
For all selected swaptions including those that are a part of a replication transaction—			
8. Obtained a list of individuals, approved by the board of directors or a committee thereof, who had the authority to authorize swaptions. Compared the name of the individual who authorized the swaption transaction with the names on the list and found the name of the individual on the list.	_____	_____	_____
9. Based on the details of the transaction identified in procedure 2 and company policy, compared the terms of the transaction with the insurance company's policy regarding the requirement for the board of directors or a committee thereof to authorize the specific transactions tested; for example, a transaction in which the notional amount exceeded a limit requiring additional approval. If the board of directors or a committee thereof was required to approve the transaction, read minutes of the board of directors or a committee thereof or other appropriate support and found evidence of approval of the transaction tested.	_____	_____	_____
10. Obtained a list of qualified and nonqualified counterparties, approved by the board of directors or a committee thereof. Compared the name of the counterparty involved in the swaption transaction with names on the list and found the name of the counterparty on the respective qualified or nonqualified list.	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
11. Determined that the counterparty was listed as qualified or nonqualified in the analysis used for monitoring the insurance company's limitations on counterparty exposure consistent with the classification in the listing obtained in procedure 10.	_____	_____	_____
12. Obtained a list of individuals authorized by the board of directors or committee thereof to trade swaption contracts. Compared the name of the individual who executed the swaption with the names on the list and found the name of the individual on the list.	_____	_____	_____
13. Obtained a list of individuals authorized to approve settlements or disbursements related to swaption agreements. Compared the name of the individual who approved settlements and disbursements relating to the swaption with the names on the list and found the name on the list.	_____	_____	_____
14. Compared the name of the individual who approved any payment relating to the swaption with the name of the individual who approved entering into the contract and found that the names were different.	_____	_____	_____
15. Compared the name of the individual who received cash or other consideration in connection with the swaption with the name of the individual who entered into the contract and found that the names of the individuals were different.	_____	_____	_____
16. Obtained the deal ticket and confirmation for the purchase, sale, modification, or closeout of the swaption and found that the purchase, sale, modification, or closeout was confirmed by the counterparty.	_____	_____	_____
17. Compared the name of the individual who received the deal ticket and confirmation with the names on a list of individuals authorized to trade swaptions and found that the name was not on the list.	_____	_____	_____

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
18. Compared the terms of the swaption contract, as stated on the deal ticket and confirmation, with the terms of the swaption contract recorded in the insurance company's accounting records and found them to be in agreement.			
19. Obtained documentation for one reporting period (for example, monthly or quarterly), that the insurance company determined whether its accounting records for swaptions, tested in procedure 18, agreed with or reconciled to the related control account, (for example, the subsidiary ledger to the general ledger).			
20. Obtained the accounting record documenting modifications, if any, to the swaption agreement. Compared the name of the individual who approved the modification with a list of individuals authorized to approve modifications and found the name of the individual who approved the modification on the list.			
21. Compared the terms of the swaption agreement recorded in the insurance company's accounting records with the terms shown in the executed copy of the swaption agreement and found them to be in agreement.			
22. Using the list of authorized traders obtained in procedure 12, compared the name of the individual who had custody or access to the swaption agreement with the names of individuals authorized to execute swaption agreements and found that the name was not on the list.			
23. Compared information regarding the swaption, such as type of derivative, notional amount, and fair value, with the comparable information included in the report to the board of directors or appropriate committee thereof and found them to be in agreement.			

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
24. If the swaption should have been included in the monitoring analysis separately tested in procedure 10 within section 1, "All Derivative Types," compared information regarding the swaption, such as type of derivative, notional amount, and fair value, with the comparable information in the monitoring analysis and found them to be in agreement.			
Effectiveness of Swaptions Used As Hedges and in Replication Transactions			
25. Read the insurance company's documentation of effectiveness and found that the insurance company evaluated the effectiveness of the swaption as a hedge or replication in accordance with the policies regarding effectiveness.			
26. If the swaption was no longer effective as a hedge or replication, compared the action taken by the insurance company with the action required by the accounting policies and procedures and found that the action taken was consistent with the accounting policy.			
Legal Review			
27. Read documentation indicating that the legal department reviewed the swaption agreement to assess contract compliance with the DUP and enforceability.			
28. Read documentation indicating that the legal department updated its assessment of the enforceability of the swaption agreement at least annually.			
Valuation			
29. Obtained the insurance company's policies and procedures for valuing swaptions and found that the insurance company determined the fair value of the swaption in accordance with the policy described in the insurance company's procedures for valuation of swaptions.			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
30. Read documentation supporting the fair value of the swaption and found that the fair value was either (*a*) obtained from an independent source, (*b*) checked against an independent source, or (*c*) calculated internally by an authorized individual.	_____	_____	_____

Description of Exceptions if Any

Procedure Number	*Description of Exception*

Section 10—Warrant Contracts

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Performed the following procedures on selected warrant contracts to test internal control over warrant transactions. Selected five percent of each type of warrant transaction (that is, purchases, sales, expirations, and exercises), with the selections distributed throughout the year. If five percent of a given type of transaction exceeded 40, the number of items selected for that type of transaction was limited to 40. If five percent of a type of transaction resulted in less than four items, selected four or fewer items that represented all of the transactions of that type.			
Reporting			
1. Read the insurance company's derivative use plan (DUP) and any amendments thereto and found that the DUP permits the insurance company to trade or enter into warrant contracts.	_____	_____	_____
2. For each warrant selected for testing, read management's documentation describing the intended use of the warrant and performed the following procedures, as applicable.	_____	_____	_____
For warrants used as a hedge—			
3. Determined that the documentation described the following:			
a. The risk hedged	_____	_____	_____
b. How the hedge was consistent with the overall risk management strategy	_____	_____	_____
c. How the warrant was expected to be effective in offsetting the exposure	_____	_____	_____
d. The approach in assessing the effectiveness of the hedge	_____	_____	_____

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
4. Determined that the following items were documented:			
a. The purpose(s) of the warrant as a hedge	_____	_____	_____
b. For exchange-traded warrants, the term of the warrant, the name of the exchange, and the name of the firm(s) handling the trade	_____	_____	_____
c. For over-the-counter (OTC) warrants, the terms of the warrant, the name of the counterparty, and the counterparty exposure amount	_____	_____	_____
d. The assets or liabilities (or portion thereof) that the warrant hedged	_____	_____	_____
e. Evidence that the warrant continued to be an effective hedge	_____	_____	_____
f. Evidence that the warrant was consistent with the insurance company's parameters, as specified in the DUP or applicable company policies and procedures for entering into hedge transactions; for example, the notional amount or underlying	_____	_____	_____
If the warrant transaction was an exact offset of an outstanding warrant—			
5. Read documentation indicating that the warrant transaction offset an outstanding warrant previously purchased or sold by the insurance company and that the warrant was an exact offset of the market risk of the warrant being offset	_____	_____	_____
For warrants used in a replication transaction—			
6. Determined that the documentation described the following:			
a. The investment type and characteristics replicated	_____	_____	_____
b. How the replication was consistent with the overall management investment strategy	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
c. How the warrant was expected to be effective in replicating the investment characteristics of the replicated investment			
d. The approach in assessing the effectiveness of the replication transaction			
7. Determined that the following items were documented:			
a. The instruments used in the replication and the investment type and characteristics replicated			
b. The specific warrant used in the replication			
c. For exchange-traded warrants, the name of the exchange and the firm(s) handling the trade			
d. For OTC warrants, the terms of the warrant, the name of the counterparty, and the counterparty exposure amount			
For all selected warrants including those that are part of a replication transaction—			
8. Obtained a list of individuals, approved by the board of directors or a committee thereof who had the authority to authorize warrant transactions. Compared the name of the individual who authorized the warrant transaction with the names on the list and found the name of the individual on the list.			
9. Based on the details of the transaction identified in procedure 2 and company policy, compared the terms of the transaction with the insurance company's policy regarding the requirement for the board of directors or a committee thereof to authorize the specific transaction tested; for example, a transaction in which the notional amount exceeded a limit requiring additional approval. If the board of directors or a committee thereof was required to approve the transaction, read minutes of the board of directors or a committee thereof or other appropriate support, and found evidence of approval of the transaction tested			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
10. Obtained a list of *qualified* and *nonqualified* counterparties, approved by the board of directors or a committee thereof. Compared the name of the counterparty involved in the warrant transaction with names on the list, and found the name of the counterparty on the respective qualified or nonqualified list.	_____	_____	_____
11. For OTC warrants, determined that the counterparty was listed as qualified or nonqualified in the analysis used for monitoring the insurance company's limitations on counterparty exposure, consistent with the classification in the listing obtained in procedure 10.	_____	_____	_____
12. Obtained a list of individuals authorized by the board of directors or committee thereof to trade warrant contracts. Compared the name of the individual who executed the purchase, sale, or exercise of the warrant with the names on the list and found the name of the individual on the list.	_____	_____	_____
13. Obtained a list of individuals authorized to approve payments related to warrant contracts. Compared the name of the individual who approved any payment relating to the warrant with the names on the list, and found the name of the individual on the list.	_____	_____	_____
14. Compared the name of the individual who approved any payment relating to the warrant with the name of the individual who approved entering into the contract and found that the names were different.	_____	_____	_____
15. Compared the name of the individual who received cash or other consideration in connection with the warrant with the name of the individual who entered into the contract and found that the names of the individuals were different.	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
16. Obtained the deal ticket and confirmation for the purchase, sale, or exercise of an exchange-traded warrant and found that the purchase, sale, or exercise was confirmed by the firm handling the transaction.			
17. Compared the name of the individual who received the deal ticket and confirmation with the names on a list of individuals authorized to trade warrants and found that the name was not on the list.			
18. Compared the terms of the warrant contract, as stated on the deal ticket and confirmation, with the terms of the warrant contract recorded in the insurance company's accounting records and found them to be in agreement.			
19. Obtained documentation for one reporting period, (for example, monthly or quarterly), that the insurance company determined whether its accounting records for warrants, tested in procedure 18, agreed with or reconciled to the related control account, (for example, the subsidiary ledger to the general ledger).			
20. Obtained the accounting record documenting modifications, if any, to the warrant transaction. Compared the name of the individual who approved the modification with a list of individuals authorized to approve modifications and found the name of the individual who approved the modification on the list.			
21. For one reporting period, (for example, monthly or quarterly), obtained the insurance company's documentation of the existence of the warrant contract and found that the insurance company either (*a*) obtained statements from the custodian confirming the existence of the warrant contracts or (*b*) physically inventoried the warrant contracts.			

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
22. Using the list of authorized traders obtained in procedure 12, compared the name of the individual who had custody of or access to the warrant contracts with the names of individuals authorized to execute purchases, sales, or exercises of warrants and found that the name was not on the list.			
23. Compared information regarding the warrant, such as type of derivative, notional amount, and fair value, with the comparable information included in the report to the board of directors or appropriate committee thereof and found them to be in agreement.			
24. If the warrant position should have been included in the monitoring analysis separately tested in procedure10 of section 1,"All Derivative Types," compared information regarding the warrant, such as type of derivative, notional amount, and fair value, with the comparable information in the monitoring analysis and found them to be in agreement.			
Effectiveness of Warrants Used As Hedges and in Replication Transactions			
25. Read the insurance company's documentation of effectiveness and found that the insurance company evaluated the effectiveness of the warrant as a hedge or replication in accordance with the policies regarding effectiveness.			
26. If the warrant was no longer effective as a hedge or replication, compared the action taken by the insurance company with the action required by the accounting policies and procedures and found that the action taken was consistent with the accounting policy.			

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
Legal Review			
27. Read documentation indicating that the legal department reviewed a nonexchange traded warrant agreement to assess contract compliance with the DUP and enforceability.	_____	_____	_____
28. Read documentation indicating that the legal department updated its assessment of enforceability of the nonexchange traded warrant agreement at least annually.	_____	_____	_____
Valuation			
29. Obtained the insurance company's policies and procedures for valuing warrants and found that the insurance company determined the fair value of the warrant in accordance with the policy described in the insurance company's procedures for the valuation of warrants	_____	_____	_____
30. Read documentation supporting the fair value of warrants and found that the fair value was either (*a*) obtained from an independent source, (*b*) checked against an independent source, or (*c*) calculated internally by an authorized individual.	_____	_____	_____

Description of Exceptions if Any

Procedure Number	*Description of Exception*

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.38

Appendix C

Illustrative Management Representation Letter

[*Responsible Party's Letterhead*]

[*Date*]

[*CPA Firm's Name and Address*]

In connection with your engagement to apply the agreed-upon procedures enumerated in the American Institute of Certified Public Accountants' Statement of Position 01-03, *Performing Agreed-Upon Procedures Engagements that Address Internal Control Over Derivative Transactions as Required by the New York State Insurance Law*, which were agreed to by management of ABC Insurance Company, solely to assist us in complying with the requirements of Section 1410(b)(5) of the New York State Insurance Law, as amended (the Law), which addresses the assessment of internal control over derivative transactions as defined in Section 1401(a) of the Law and Section 178.6 of Regulation No. 163 during the year ended December 31, 20XX, we confirm, to the best of our knowledge and belief, the following representations made to you during your engagement:

1. We are responsible for establishing and maintaining effective internal control over derivative transactions in accordance with the Law.
2. During the year ended December 31, 20XX, the internal control over derivative transactions was functioning in accordance with the policies and procedures set forth in the Company's derivative use plan (DUP) and related accounting policies and procedures. There have been no errors or fraud that would indicate a weakness in the internal control over derivative transactions.
3. We have disclosed to you all significant deficiencies in the design or operation of the internal control over derivative transactions that would adversely affect the Company's ability to function in accordance with the Company's DUP.
4. There have been no communications from regulatory agencies, internal auditors, or other practitioners or consultants relating to the internal control over derivative transactions, including communications received between December 31, 20XX and the date of this letter.
5. We have made available to you all information that we believe is relevant to the internal control over derivative transactions.
6. We have responded fully to all inquiries made to us by you during the engagement.

To the best of our knowledge and belief, no events have occurred subsequent to December 31, 20XX and through the date of this letter that would require adjustment to or modification of the findings of the agreed-upon procedures.

[*Signature*]

[*Title*]

[*Signature*]

[*Title*]

Reporting on Controls Over Derivative Transactions at Insurance Entities Task Force

ALBERT J. REZNICEK, *Chair*
EDWARD F. BADER
DARRYL BRILEY
BEN B. KORBLY
EDWARD J. METZGER
DAVID A. NACHMAN
PAULA C. PANIK
ROBERT M. SOLITRO
MARY TODD STOCKER
DEBORAH H.WHITMORE

The AICPA is grateful to Jean Connolly, James S. Gerson, Laurel A. Hammer, Jay Matalon, and James M. Yanosy for their technical assistance with this document and also to Michael Moriarty of the New York State Department of Insurance for reviewing this document and providing recommendations.

AICPA Staff

CHARLES E. LANDES
Director
Audit and Attest Standards

JUDITH M. SHERINSKY
Technical Manager
Audit and Attest Standards

[The next page is 31,571.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 14,380

Statement of Position 01-4 Reporting Pursuant to the Association for Investment Management and Research Performance Presentation Standards

November 13, 2001

NOTE

This Statement of Position represents the recommendations of the AICPA's Investment Performance Statistics Task Force regarding the application of Statements on Standards for Attestation Engagements to engagements to report pursuant to the Association for Investment Management and Research Performance Presentation Standards. The Auditing Standards Board has found the recommendations in this Statement of Position to be consistent with existing standards covered by Rule 202 of the AICPA Code of Professional Conduct. AICPA members should be prepared to justify departures from the recommendations of this Statement of Position.

Introduction and Background

.01 The investment management industry is composed of a diverse group of financial entities, including registered investment companies, investment partnerships (such as venture capital funds and hedge funds), registered and nonregistered investment advisers, commodity pool operators and trading advisers, commercial and investment banks, and trust companies. Despite diverse financial structures and regulatory environments, these entities share the common goal of maximizing the rate of return on assets being managed. A presentation of an investment firm's past performance in managing proprietary or client funds can be a powerful tool for attracting new clients and maintaining the firm's client base. In recent years, market forces, including rapid industry growth, significant consolidation, fierce competition, and increased scrutiny from regulators and investors, have resulted in an increased focus on these types of presentations.

.02 To promote fair representation, full disclosure, and greater comparability in investment performance presentations, the Association for Investment Management and Research (AIMR) has developed the AIMR Performance Presentation Standards (AIMR-PPS® standards).[1] Although compliance with the AIMR-PPS standards is voluntary, an investment firm's

[1] The term "Association for Investment Management and Research Performance Presentation Standards" is abbreviated in this Statement of Position either as the AIMR-PPS standards or the standards. For information on the appropriate use of the AIMR-PPS registered trademark ®, see the AIMR Web site http://www.aimr.org.

claim of compliance with the AIMR-PPS standards is widely regarded as providing a competitive advantage. The AIMR-PPS standards include both required and recommended guidelines for composite construction, calculation methodology, presentation of results, and disclosure. First introduced in 1987, the AIMR-PPS standards represent suitable criteria[2] on which investment managers can base their investment return calculations and present their results. AIMR's Performance Presentation Standards Implementation Committee and Investment Performance Council oversee the continuing development of the AIMR-PPS standards and the Global Investment Performance Standards (GIPS® standards).

.03 In February 1999, AIMR issued the GIPS standards to provide a basis for readily accepted and comparable presentations of investment performance without regard to geographic location. At that time AIMR also took the first step in moving the AIMR-PPS standards toward a global investment performance standard by adding new requirements to bring them in line with the GIPS standards.

.04 In May 2001, AIMR took the next step in converging the AIMR-PPS standards with the GIPS standards by adopting and publishing on its Web site redrafted AIMR-PPS standards, the U.S. and Canadian version of GIPS. Because the GIPS standards are fundamentally based on the AIMR-PPS standards, the redraft of the AIMR-PPS standards was primarily a reorganization of the existing provisions. The AIMR-PPS standards indicate that investment firms already compliant with the standards will need to perform minimal additional work to continue to comply with the AIMR-PPS standards. The AIMR-PPS standards incorporate all the requirements and recommendations of the GIPS standards. All references to the AIMR-PPS standards in this Statement of Position (SOP) refer to the redrafted AIMR-PPS standards, the U.S. and Canadian version of GIPS.

.05 The AIMR-PPS standards recommend that firms obtain independent third-party verification of an investment firm's claim of compliance with the AIMR-PPS standards. Verification under the AIMR-PPS standards had previously consisted of two levels: Level I (firmwide verification) and Level II (verification of a specific composite). To encourage convergence of the AIMR-PPS standards and the GIPS standards, as of January 1, 2003, verification will only consist of the Level I procedures.[3] In addition, an investment management firm may choose to have a more extensive, specifically focused performance examination of a specific composite presentation. It should be noted that AIMR's emphasis is on *firmwide* verification, which a firm *must* obtain concurrent with, or prior to, obtaining a performance examination of the performance results of any specific composite.

.06 The AIMR-PPS standards specify that Level I verifications and performance examinations (Level II) must be performed by an independent third-party "verifier."

---

[2] The AIMR-PPS standards provide suitable criteria, as defined in Chapter 1, "Attest Engagements," of Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 2, AT sec. 101), for composite construction, calculation methodology, presentation of results, and disclosure. The criteria are available to users, as defined in Chapter 1 of SSAE No. 10, as they are posted to the AIMR Web site. The AIMR Web site also provides additional guidance on interpreting and applying the AIMR-PPS standards through a variety of means, including questions and answers, guidance statements, and subcommittee reports.

[3] The requirements for a Level I verification under the AIMR-PPS standards are the same as those under the GIPS standards.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Scope

.07 This SOP provides guidance to practitioners for engagements to examine and report on aspects of an investment firm's compliance with the AIMR-PPS standards (a Level I verification engagement). It also provides guidance on engagements to examine and report on the performance results of specific composites in conformity with the AIMR-PPS standards (a performance examination [Level II]). Such examination engagements should be performed pursuant to Chapter 1, "Attest Engagements," of Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 2, AT sec. 101). As described herein, the AIMR-PPS standards require that such engagements use the criteria they set forth; consequently, users of this SOP should be familiar with the AIMR-PPS standards and interpretative guidance.

.08 This SOP supersedes two AICPA Notices to Practitioners: *Examination Engagements to Report on Investment Performance Statistics Based on Established or Stated Criteria*, issued by the AICPA's Investment Companies Committee in November 1995; and *Engagements to Report on Performance Presentation Standards of the Association for Investment Management and Research*, issued by the AICPA Auditing Standards Division in July 1993. This SOP also supersedes paragraphs 11.18 through 11.22 of the AICPA Audit and Accounting Guide *Audits of Investment Companies*, Chapter 11, "Independent Auditor's Reports and Management Representations."

Overview of the AIMR-PPS Standards

Firmwide Compliance With the AIMR-PPS Standards

.09 For an investment firm to claim compliance with the AIMR-PPS standards, the firm must meet *all* of the required elements of the AIMR-PPS standards on a *firmwide* basis. Firms are prohibited from claiming compliance "except for" one or more of the required standards. Firms that have met all of the required elements may include the following statement in performance presentations to clients:

> [*Insert name of firm*] has prepared and presented this report in compliance with the Performance Presentation Standards of the Association for Investment Management and Research (AIMR-PPS®), the U.S. and Canadian version of the Global Investment Performance Standards (GIPS®). AIMR has not been involved in the preparation or review of this report.

.10 The AIMR-PPS standards must be applied on a firmwide basis. The AIMR-PPS standards state:

A firm may define itself as

a. an entity registered with the appropriate national regulatory authority overseeing the entity's investment management activities; *or*

b. an investment firm, subsidiary, or division held out to clients or potential clients as a distinct business unit (e.g., a subsidiary firm or distinct business unit managing private client assets may claim compliance for itself without its parent organization being in compliance);

c. (until January 1, 2005), all assets managed to one or more base currencies (for firms managing global assets).

When presenting investment performance in compliance with the AIMR-PPS standards, an investment management firm must state how it defines itself as a "firm."

.11 The AIMR-PPS standards establish both requirements and recommendations for investment firms to follow in preparing investment performance presentations. To claim firmwide compliance, an investment firm must adhere to the required standards. Adherence to the recommended standards is encouraged. The AIMR-PPS standards are divided into five sections that reflect the basic elements involved in presenting performance information:

Input Data: Consistency of input data is critical to effective compliance with the AIMR-PPS standards and establishes the foundation for full, fair, and comparable investment performance presentations. The standards provide the blueprint for a firm to follow in constructing this foundation.

Calculation Methodology: Achieving comparability among investment management firms' performance presentations requires uniformity in methods used to calculate returns. The standards mandate the use of certain calculation methodologies (e.g., performance must be calculated using a time-weighted total rate of return method).

Composite Construction: A composite is an aggregation of a number of portfolios into a single group that represents a particular investment objective or strategy. The composite return is the asset-weighted average of the performance results of all the portfolios in the composite. Creating meaningful, asset-weighted composites is critical to the fair presentation, consistency, and comparability of results over time and among firms.

Disclosure: Disclosures allow firms to elaborate on the raw numbers provided in the presentation and give the end user of the presentation the proper context in which to understand the performance results. To comply with the AIMR-PPS standards, firms must disclose certain information about their performance presentation and the calculation methodology adopted by the firm. Although some disclosures are required of all firms, others are specific to certain circumstances, and thus may not be applicable to all situations.

Presentation and Reporting: After constructing the composites, gathering the input data, calculating the returns and determining the necessary disclosures, the firms must incorporate this information in presentations based on the guidelines set out in the AIMR-PPS standards for presenting the investment performance results. No finite set of guidelines can cover all potential situations or anticipate future developments in investment industry structure, technology, products, or practices. When appropriate, firms have the responsibility to include in AIMR-compliant presentations information not covered by the Standards.

.12 The AIMR-PPS standards also include four additional sections that address the calculation and presentation of performance for alternative asset categories (for example, real estate, venture and private placements, wrap-fee accounts, and after-tax returns).

.13 Practitioners who perform a Level I verification or a performance examination (Level II) pursuant to the AIMR-PPS standards should be familiar with those standards and the interpretative guidance, which are available on AIMR's Web site.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Firmwide Verification and Performance Examination

Level I or Firmwide Verification

.14 A Level I verification tests:

a. Whether the investment firm has complied with all the composite construction requirements of the AIMR-PPS standards on a firmwide basis; and

b. Whether the investment firm's processes and procedures are designed to calculate and present performance results in compliance with the AIMR-PPS standards.

.15 Level I verification is considered to be the primary level of verification because it tests the validity of a firm's claim of compliance on a *firmwide* basis rather than testing the claim for only one or more composites. Under Level I, a single verification report is issued with respect to the whole firm. The AIMR-PPS standards specify procedures that practitioners should perform for a Level I verification (see Section III and appendix D of the AIMR-PPS standards; those procedures are reproduced in appendix A [paragraph .39] of this SOP).

.16 According to the AIMR-PPS standards, when an investment firm has obtained a Level I verification, the firm may state that it is "Level I verified." This claim may or may not be accompanied by a presentation of performance history for a specific composite. A Level I verification, however, does *not* imply that the verifiers have examined the accuracy of the performance results of any particular composite presentation(s) that may accompany the verification report. (See paragraph .37.)

Performance Examination (Level II)

.17 In addition to a Level I verification, an investment firm may choose to have a more extensive, specifically focused examination of a specific composite presentation. Such an examination, for the purposes of the AIMR-PPS standards, is referred to as a performance examination (Level II). The AIMR-PPS standards identify objectives and suggested procedures for a performance examination (Level II) (see appendix B [paragraph .40] of this SOP). A performance examination (Level II) also requires a Level I verification to be performed prior to or concurrent with *any* performance examination (Level II).

Examination Engagement

Engagement Objectives

.18 To satisfy the required procedures set forth by the AIMR-PPS standards, practitioners should conduct an examination engagement pursuant to Chapter 1 of SSAE No. 10. For a Level I engagement, the practitioner's objective is to express an opinion on whether, in all material respects:

a. The investment firm has complied with all the composite construction requirements of the AIMR-PPS standards on a firmwide basis; and

b. The investment firm's processes and procedures are designed to calculate and present performance results in compliance with the AIMR-PPS standards.

.19 For a performance examination (Level II), the practitioner's objectives include (*a*) expressing an opinion on a Level I engagement (see paragraph .18), and (*b*) expressing an opinion on whether the performance results of a specific composite are presented, in all material respects, in conformity with the AIMR-PPS standards.

Planning the Engagement

.20 SSAE No. 10 states that planning an attest engagement involves developing an overall strategy for the expected conduct and scope of the engagement. To develop such a strategy, practitioners need to have sufficient knowledge of the investment management industry and of the AIMR-PPS standards and interpretive guidance to enable them to understand adequately the events, transactions, and practices that, in their judgment, have a significant effect on the subject matter of the assertions.

.21 The examination should be conducted in accordance with attestation standards established by the AICPA. The engagement also should be conducted in accordance with the procedures set forth in the AIMR-PPS standards. This SOP is not intended to provide all the required and recommended procedures set forth in the AIMR-PPS standards or all the applicable attestation standards established by the AICPA.

Establishing an Understanding With the Client

.22 The practitioner should establish an understanding with the client regarding the services to be performed to reduce the risk that either the practitioner or the client may misinterpret the needs or expectations of the other party. The understanding should include the objectives of the engagement, management's responsibilities, the practitioner's responsibilities, limitations of the engagement, and any other limitations on the use of the practitioner's name and report. The understanding should include a statement that, if the client intends to use the practitioner's report on the examination, or refer to the practitioner, in connection with any sales or advertising literature, a draft of such literature should be provided to the practitioner for his or her review and comment prior to issuance.

.23 The practitioner should document the understanding in the working papers, preferably through a written communication with the client, such as an engagement letter (see appendix C [paragraph .41] of this SOP for a sample engagement letter).

Obtaining Sufficient Evidence

.24 In conducting an attest examination, the practitioner accumulates sufficient evidence to restrict attestation risk[4] to a level that is, in the practitioner's professional judgment, appropriately low for the high level of assurance that may be imparted by his or her report. A practitioner should select from all available procedures—that is, procedures that assess inherent and control risk and restrict detection risk—any combination that can restrict attestation risk to such an appropriately low level.

.25 As noted previously, the AIMR-PPS standards specify procedures that practitioners should perform for a Level I verification in Section III and

[4] See SSAE No. 10, Chapter 1, paragraph 1.45, footnote 9, for the definition of *attestation risk*.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

appendix D of the AIMR-PPS standards; those procedures are reproduced in appendix A [paragraph .39] of this SOP. Since a performance examination (Level II) requires a Level I verification, the practitioner should perform those procedures required for a Level I verification in *any* examination of a firm's investment performance prepared pursuant to AIMR-PPS standards. At a minimum, practitioners should follow the procedures required by the AIMR-PPS standards.

.26 In addition, practitioners who are engaged to conduct a performance examination (Level II) of one or more specific composite presentations should consider the objectives specified in appendix D of the AIMR-PPS standards in conducting a performance examination and should select from all available procedures any combination that can limit the risk of errors occurring and not being detected during the examination to an appropriately low level (see appendix B [paragraph .40] of this SOP for objectives and suggested procedures identified by the AIMR-PPS standards).

.27 Regardless of the scope of the engagement, the practitioner should obtain sufficient evidence to provide a reasonable basis for the opinion expressed in the report (see the second standard of fieldwork in Chapter 1 of SSAE No. 10).

.28 When the practitioner is engaged to conduct a performance examination (Level II) of one or more composites subsequent to the performance and issuance of a report on a Level I verification engagement, the practitioner should update his or her understanding of relevant controls and inquire about any other changes that may affect the planning and conduct of the performance examination (Level II).

.29 The AIMR-PPS standards require that investment firms report, at a minimum, 10 years of investment performance (or performance since inception of the firm/composite if the period since inception is less than 10 years) to claim compliance with the standards. During a composite-specific performance examination, the practitioner should be alert for circumstances and events that affect prior period performance results presented or the adequacy of disclosures concerning those prior period performance results. In updating his or her report on the performance results for prior periods, the practitioner should consider the effects of any such circumstances or events coming to his or her attention. An updated report on performance results for a prior period should be distinguished from a reissuance of a previous report, since the practitioner, in issuing an updated report, considers information that he or she has become aware of during the examination of the current period performance results and because an updated report is issued in conjunction with the practitioner's report on the performance results for the current period. Although the investment firm must present 10 years of investment performance results, a Level I verification or a performance examination (Level II) can cover any time period.

Representation Letter

.30 As part of a Level I verification, AIMR requires the practitioner to obtain a representation letter from the client firm confirming major policies and any other specific representations made to the practitioner during the engagement. The practitioner also ordinarily should obtain a representation letter as part of a performance examination (Level II). Examples of matters that might appear in a representation letter include the following:

a. A statement acknowledging management's responsibility for their assertions and, where applicable, for the preparation of specific statements of performance results.

b. A statement acknowledging responsibility for selecting the criteria (SSAE No. 10, paragraph 1.60).

c. A statement acknowledging responsibility for determining that such criteria (AIMR-PPS standards) are appropriate for its purposes, where the responsible party is the client (SSAE No. 10, paragraph 1.60).

d. Management's assertions about (*1*) compliance with all the composite construction requirements of the AIMR-PPS standards on a firmwide basis, (*2*) the processes and procedures designed to calculate and present performance results in compliance with the AIMR-PPS standards, and (*3*) where applicable, a statement that the specific composite statements of performance results are presented in conformity with the AIMR-PPS standards. Management's assertions should address the same periods to be covered by the practitioner's examination report.

e. A statement that all known matters contradicting the assertions and any communication from regulatory agencies affecting the subject matter or the assertions have been disclosed to the practitioner.

f. A statement that there has been no (*1*) fraud involving management or employees who have significant roles in the company's processes and procedures relating to compliance with the AIMR-PPS standards or (*2*) fraud involving others that could have a material effect on the company's compliance with the AIMR-PPS standards.

g. Availability of all records relevant to the examination.

h. A statement that management is responsible for maintaining sufficient books and records to substantiate performance as required under Rule 204 of the Investment Advisers Act of 1940 and that management has maintained such records to comply with those requirements.

i. A statement that any known events subsequent to the period (or point in time) of the subject matter being reported on that would have a material effect on the subject matter or the assertions have been disclosed to the practitioner.

j. Other matters as the practitioner deems appropriate.

Appendix D [paragraph .42] of this SOP contains a sample management representation letter, including additional representations that may be appropriate for a performance examination (Level II). Management's refusal to furnish all appropriate written representations constitutes a limitation on the scope of the examination sufficient to preclude rendering an opinion (see paragraph .32 of this SOP). Further, the practitioner should consider the effects of management's refusal on his or her ability to rely on other management representations.

Reporting

.31 SSAE No. 10 permits the practitioner to report either on the assertions or directly on the subject matter to which the assertions relate. The illustrative reports in Appendixes E [paragraph .43] and F [paragraph .44] present both reporting options.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.32 After conducting the procedures for a Level I verification, the practitioner may conclude that the investment firm is not in compliance with the standards or that the records of the firm cannot support a complete verification. Practitioners should be aware that the AIMR-PPS standards state that "the AIMR-PPS Claim of Compliance statement can only be made on a presentation that fully adheres to the requirements of the AIMR-PPS standards." In such situations, the practitioner should issue a statement to the investment firm clarifying why it was not possible to issue a verification report; issuance of a qualified (except for) opinion is not permitted.

.33 According to Chapter 1 of SSAE No. 10, when the practitioner is reporting on management's assertion, the practitioner's examination report should include an identification of the assertion and the responsible party. (When the assertion does not accompany the practitioner's report, the first paragraph of the report should also contain a statement of the assertion.)

.34 The AIMR-PPS standards require that the report clearly indicate whether a Level I verification or a performance examination (Level II) has been performed. The AIMR-PPS standards also require that the report state the time period covered.

.35 Appendix E [paragraph .43] presents illustrative reports for a Level I verification. Appendix F [paragraph .44] presents illustrative reports for a performance examination (Level II). The reports in appendixes E [paragraph .43] and F [paragraph .44] also illustrate how the reference to a Level I verification or a performance examination (Level II), required by the AIMR-PPS standards, may be incorporated into the attest report.

.36 The AIMR-PPS standards specify that conducting a Level I verification is a condition of conducting a performance examination (Level II); the examination report on the Level I verification may be issued prior to or concurrent with the performance examination report (Level II). Practitioners who conduct performance examinations (Level II) should report both on management's assertions about the subject matter of a Level I engagement and on the performance results of the specific composites that are the subject matter of the performance examination (Level II). The AIMR-PPS standards require that composite presentations that are the subject of a performance examination (Level II) report be attached to the report.

.37 To avoid confusion to users of the report, the practitioner should add a paragraph to a Level I report disclaiming an opinion on the performance results of any specific composites that may accompany the report (see the Level I report in appendix E [paragraph .43]). This recognizes that the practitioner cannot control whether the Level I verification report may be distributed by the investment firm as part of an AIMR-PPS standards-compliant composite presentation that has not also had a performance examination (Level II) conducted.

SOP Effective Date

.38 This SOP is effective for engagements to examine and report on aspects of an investment firm's compliance with, and/or examining and reporting on specific composite results in conformity with, the redrafted AIMR-PPS standards, the U.S. and Canadian version of GIPS. The SOP may not be applied to engagements in which the investment firm has not yet adopted the redrafted AIMR-PPS standards.

Appendix A

AIMR-PPS Guidance for a Level I Verification

[*Source: AIMR-PPS standards, Section III; www.aimr.org*]

Level I verification under the AIMR-PPS standards is equivalent to GIPS verification. Therefore, all references to "the standards" below relate interchangeably to AIMR-PPS or GIPS standards. The following are the **minimum** procedures that verifiers must follow when verifying an investment firm's claim of compliance with the standards. Verifiers must follow these procedures prior to issuing a verification report to the firm:

1. **Pre-verification Procedures**

   A. *Knowledge of the Firm.* Verifiers must obtain selected samples of the firm's investment performance reports, and other available information regarding the firm, to ensure appropriate knowledge of the firm.

   B. *Knowledge of the standards.* Verifiers must understand the requirements and recommendations of the standards, including any updates, reports, or clarifications of the standards published by AIMR or the Investment Performance Council, the AIMR-sponsored body responsible for oversight of the GIPS.

   C. *Knowledge of the Performance Standards.* Verifiers must be knowledgeable of country-specific performance standards, laws, and regulations applicable to the firm, and must determine any differences between the standards and the country-specific standards, laws and regulations.

   D. *Knowledge of Firm Policies.* Verifiers must determine the firm's assumptions and policies for establishing and maintaining compliance with all applicable requirements of the standards. At minimum, verifiers must determine the following policies and procedures of the firm:

      i. Policy with regard to investment discretion. The verifier must receive from the firm, in writing, the firm's definition of investment discretion and the firm's guidelines for determining whether accounts are fully discretionary.

      ii. Policy with regard to the definition of composites according to investment strategy; the verifier must obtain the firm's list of composite definitions with written criteria for including accounts in each composite.

      iii. Policy with regard to the timing of inclusion of new accounts in the composites.

      iv. Policy with regard to timing of exclusion of closed accounts in the composites.

      v. Policy with regard to the accrual of interest and dividend income.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

vi. Policy with regard to the market valuation of investment securities.

vii. Method for computing time-weighted portfolio return.

viii. Assumptions on the timing of capital inflows/outflows.

ix. Method for computing composite returns.

x. Policy with regard to the presentation of composite returns.

xi. Policies regarding timing of implied taxes due on income and realized capital gains for reporting performance on an after-tax basis.

xii. Policies regarding use of securities/countries not included in a composite's benchmark.

xiii. Use of leverage and other derivatives.

xiv. Any other policies and procedures relevant to performance presentation.

E. *Knowledge of Valuation Basis for Performance Calculations.* Verifiers must ensure that they understand the methods and policies used to record valuation information for performance calculation purposes. In particular, verifiers must determine that:

i. the firm's policy on classifying fund flows (e.g., injections, disbursements, dividends, interest, fees, taxes, etc.) is consistent with the desired results, and will give rise to accurate returns;

ii. the firm's accounting treatment of income, interest, and dividend receipts is consistent with cash account and cash accruals definitions;

iii. the firm's treatment of taxes, tax reclaims, and tax accruals is correct, and the manner used is consistent with the desired method (i.e., gross- or net-of-tax return);

iv. the firm's policies on recognizing purchases, sales, and the opening and closing of other positions are internally consistent and will produce accurate results; and

v. the firm's accounting for investments and derivatives is consistent with the standards.

2. Verification Procedures

A. *Definition of the Firm.* Verifiers must determine that the firm is, and has been, appropriately defined.

B. *Composite Construction.* Verifiers must be satisfied that:

i. the firm has defined and maintained composites according to reasonable guidelines in compliance with the standards;

ii. all of the firm's actual discretionary fee-paying portfolios are included in a composite;

iii. the manager's definition of discretion has been consistently applied over time;

iv. at all times, all accounts are included in their respective composites and no accounts that belong in a particular composite have been excluded;

v. composite benchmarks are consistent with composite definitions and have been consistently applied over time;

vi. the firm's guidelines for creating and maintaining composites have been consistently applied; and

vii. the firm's list of composites is complete.

C. *Non-Discretionary Accounts.* Verifiers must obtain a listing of all firm portfolios and determine on a sampling basis whether the manager's classification of the account as discretionary or non-discretionary is appropriate by referring to the account agreement and the manager's written guidelines for determining investment discretion.

D. *Sample Account Selection.* Verifiers must obtain a listing of open and closed accounts for all composites for the years under examination. Verifiers may check compliance with the standards using a selected sample of a firm's accounts. Verifiers should consider the following criteria when selecting the sample accounts for examination:

i. number of composites at the firm;

ii. number of portfolios in each composite;

iii. nature of the composite;

iv. total assets under management;

v. internal control structure at the firm (system of checks and balances in place);

vi. number of years under examination; and

vii. computer applications, software used in the construction and maintenance of composites, the use of external performance measurers and the calculation of performance results.

This list is not all-inclusive and contains only the **minimum** criteria that should be used in the selection and evaluation of a sample for testing. For example, one potentially useful approach would be to choose a portfolio for the study sample that has the largest impact on composite performance because of its size or because of extremely good or bad performance. The lack of explicit record keeping, or the presence of errors, may warrant selecting a larger sample or applying additional verification procedures.

E. *Account Review.* For selected accounts, verifiers must determine:

i. whether the timing of the initial inclusion in the composite is in accordance with policies of the firm;

ii. whether the timing of exclusion from the composite is in accordance with policies of the firm for closed accounts;

iii. whether the objectives set forth in the account agreement are consistent with the manager's composite definition as indicated by the account agreement, portfolio summary, and composite definition;

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

iv. the existence of the accounts by tracing selected accounts from account agreements to the composites;

v. that all portfolios sharing the same guidelines are included in the same composite; and

vi. that shifts from one composite to another are consistent with the guidelines set forth by the specific account agreement or with documented guidelines of the firm's clients.

F. *Performance Measurement Calculation.* Verifiers must determine whether the firm has computed performance in accordance with the policies and assumptions adopted by the firm and disclosed in its presentations. In doing so, verifiers should:

i. recalculate rates of return for a sample of accounts in the firm using an acceptable return formula as prescribed by the standards (i.e., time-weighted rate of return); and

ii. take a reasonable sample of composite calculations to assure themselves of the accuracy of the asset weighting of returns, the geometric linking of returns to produce annual rates of returns, and the calculation of the dispersion of individual returns around the aggregate composite return.

G. *Disclosures.* Verifiers must review a sample of composite presentations to ensure that the presentations include the information and disclosures required by the standards.

H. *Maintenance of Records.* The verifier must maintain sufficient information to support the verification report. The verifier must obtain a representation letter from the client firm confirming major policies and any other specific representations made to the verifier during the examination.

Appendix B

AIMR-PPS Guidance for a Performance Examination (Level II)

[*Source: AIMR-PPS standards, Appendix D; www.aimr.org*]

With the goal to shift the focus of the industry to firmwide verification, the term "Level II verification," which was previously an accepted form of verification under the AIMR-PPS standards, will be phased out on January 1, 2003. At that time, firms will no longer be able to state that a specific composite has been "Level II verified." Instead, after January 1, 2003, the AIMR-PPS standards will allow firms that have received or are in the process of receiving a firmwide (Level I) verification report to have a further, more extensive performance examination or audit of a specific composite presentation. However, firms will not be able to make the claim that a particular composite has been "verified" but can claim that the composite returns have been examined or audited. The previous Level II verification procedures have been re-titled Performance Examination (Level II) and have been redrafted to focus on the need for the verifier to conduct and report a Level I verification in order to issue a Performance Examination (Level II) report. Once the term "Level II" verification is removed from the AIMR-PPS standards, "Level I" verification will simply be re-termed "verification."

A. Scope and Purpose of Performance Examinations (Level II)

1. A Performance Examination (Level II) requires that:
   - i. The verifier follow all the verification procedures outlined for a Level I Verification and report on a Level I verification, and
   - ii. Performance results of the specific composite being examined are presented in conformity with the AIMR-PPS standards.
2. A Performance Examination (Level II) Report is issued only with respect to the composite examined by the verifier and does not attest to the accuracy of a performance presentation for any other composite.
3. After performing the Performance Examination (Level II), the verifier may conclude that the presentation does not conform to the AIMR-PPS standards or that the records of the firm cannot support the composite presentation. In such situations, the verifier should communicate to the investment management firm the reason(s) why it was not possible to provide a Performance Examination report.
4. A principal verifier may accept the work of a local or previous verifier as part of the basis for the principal verifier's opinion.

B. Procedures for Performance Examinations (Level II)

Verifiers must conduct a Level I verification as outlined for a Level I (AIMR-PPS) verification (Section III) and issue a Level I verification report prior or concurrent to issuing a Performance Examination (Level II) report. A principal verifier may accept the work of a local

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

or previous verifier as part of the basis for satisfying that a firm has previously received a Level I (AIMR-PPS) verification report.

When conducting an audit of a specific composite presentation, the verifier should consider the following presumptions, bearing in mind that they are not mutually exclusive and may be subject to important exceptions:

- Evidence obtained from independent sources outside an entity provides greater assurance about the subject matter or the assertion than evidence secured solely from within the entity.
- Information obtained from the verifier's direct personal knowledge (such as through physical examination, observation, computation, operating tests, or inspection) is more persuasive than information obtained indirectly.
- The more effective the controls over the subject matter, the more assurance they provide about the subject matter or the assertion.

In performing a performance examination, the verifier's objective is to accumulate sufficient evidence to limit the risk of errors occurring and not being detected during the audit to a level that is, in the verifier's judgment, appropriately low. A verifier should select from all available procedures any combination that can limit the risk of errors occurring and not being detected during the audit to an appropriately low level.

The extent to which the examination or audit procedures will be performed should be based on the verifier's consideration of (*a*) the nature and materiality of the information to be tested to the subject matter or the assertion taken as a whole, (*b*) the likelihood of misstatements, (*c*) knowledge obtained during current and previous engagements, (*d*) the extent to which the information is affected by judgment, and (*e*) inadequacies in the underlying data.

When conducting a Performance Examination or audit of a specific composite presentation, the verifier must consider the following objectives.

1. *Cash Flows:* Verifiers should determine whether capital contributions and withdrawals are recorded in the proper accounts, at the right amounts and on a timely basis. The following procedures should be considered:
   i. On a test basis, agree cash flows to appropriate supporting documentation.
   ii. Test contributions or withdrawals of securities to ensure proper valuation and timely recording.
   iii. Consider the reasonableness and consistent application of the methods used to account for cash flows, contributions and withdrawals.
2. *Income and Expenses:* Verifiers should determine that income and expenses are recorded in the proper accounts, at the right amounts, and on a timely basis. The following procedures should be considered:
   i. Agree significant income and expenses to supporting documentation such as custody statements.

ii. Evaluate the reasonableness and consistent application of the methods used to record income and expenses.

3. *Portfolio Trade Processing:* Verifiers should determine that purchases and sales of securities have been recorded in the proper accounts at the correct amounts on the appropriate dates. The following procedures should be considered:

   i. On a test basis, agree significant trading activity to supporting documentation such as custody statements or trade tickets.

   ii. On a test basis, agree significant end-of-period portfolio positions to supporting documentation such as custody statements.

   iii. Evaluate the reasonableness of the portfolio trade processing system.

4. *Portfolio Valuation:* Verifiers should determine whether the end-of-period valuations of security positions are appropriate and that valuation policies are consistently applied. The following procedures should be considered:

   i. On a test basis, agree significant end-of-period security valuations to an independent pricing source.

   ii. On a test basis, agree significant foreign currency exchange rates to an independent pricing source.

   iii. Evaluate the reasonableness and consistent application of the portfolio valuation methodology.

5. *Performance Measurement Calculation:* Verifiers should determine that the performance measurement statistics have been computed in accordance with the requirements contained in the AIMR-PPS standards on a consistent basis. The following procedures should be considered:

   i. On a test basis, test the computations of account returns to ensure the use of appropriate time-weighted return calculations.

   ii. On a test basis, test the computations of composite returns to ensure the use of appropriate size-weighted return calculations.

   iii. Evaluate the reasonableness and consistent application of the performance measurement calculation.

6. *Other Disclosures:* Verifiers should determine whether all required disclosures have been properly presented in the performance presentation and that disclosures are appropriately supported by available documentation. The following procedures should be considered:

   i. Evaluate whether all of the required disclosure requirements have been adequately satisfied.

   ii. Perform tests of required disclosures as deemed necessary. These tests could involve agreeing to supporting documentation, analytical procedures, or inquiry as appropriate.

   iii. Evaluate the reasonableness and consistent application of the disclosures.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.41

Appendix C

Sample Engagement Letter: Level I Verification and Performance Examination (Level II)

The following is an illustration of a sample engagement letter that may be used for this kind of engagement.

[*CPA Firm Letterhead*]

[*Client's Name and Address*]

Dear _____:

This will confirm our understanding of the arrangements for our examination of management's assertions that (1) [*name of company*] has complied with all the composite construction requirements of the Association for Investment Management and Research Performance Presentation Standards (AIMR-PPS® standards) on a firmwide basis for the [*specify period*] ending [*date*] and (2) the Company's processes and procedures are designed to calculate and present performance results in compliance with the AIMR-PPS standards as of [*date*]; this is referred to as a Level I verification under the AIMR-PPS standards. We have also been engaged to conduct an examination (referred to as a performance examination (Level II) under the AIMR-PPS standards) on the composite returns of [*specify composites*] of the Company for the [*specify period*] ending [*date*].

Our examination of management's assertions will be conducted in accordance with the attestation standards of the American Institute of Certified Public Accountants and with the criteria set forth in the AIMR-PPS standards. The Company is responsible for selecting the AIMR-PPS standards as the criteria against which we will evaluate its assertions and for determining that the AIMR-PPS standards are appropriate criteria for its purposes. The Company is responsible for compliance with all applicable laws, regulations, contracts, and agreements, including the AIMR-PPS standards. The Company is also responsible for the design, implementation, and monitoring of the policies and procedures upon which compliance is based.[5] Our responsibility is to express an opinion based on our examination.

Should conditions not now anticipated preclude us from performing our examination procedures and issuing a report as contemplated by the preceding paragraph, we will advise you promptly and take such action as we deem appropriate.

Working papers that are prepared in connection with this engagement are our property. The working papers are prepared for the purpose of providing principal support for our report.

As you are aware, there are inherent limitations in the examination process, including, for example, selective testing and the possibility that collusion or forgery may preclude the detection of material errors, fraud, and illegal acts.

---

[5] The independent practitioner may wish to include an understanding with the client about any limitation or other arrangements regarding liability of the practitioner or the client in the engagement letter.

Our fees will be billed as work progresses and are based on the amount of time required at various levels of responsibility plus actual out-of-pocket expenses. Invoices are payable upon presentation. We will notify you immediately of any circumstances we encounter that could significantly affect our initial estimate of total fees. The quoted fees assume that you will provide an accumulation of data for the year to be tested and that the records provided to us are clear, concise, and accurate.

In the event we are requested or authorized by Management or are required by government regulation, subpoena, or other legal process to produce our documents or our personnel as witnesses with respect to our engagement, the Company will reimburse us for our professional time and expenses, as well as any fees and expenses of our counsel, incurred in responding to such requests.

If the Company intends to use our report on the examination of the composite returns in whole or in part, or refer to [*name of CPA firm*], in connection with any sales or advertising literature, a draft of such literature will be provided to us for review and comment prior to issuance.

Pursuant to our agreement as reflected in this letter, we will examine and report on the composites selected by you until either you or we terminate this agreement.

If these arrangements are acceptable, please sign one copy of this letter and return it to us. We appreciate the opportunity to serve you.

Very Truly yours,

[*Name of CPA Firm*]

Accepted and agreed to:

[*Client Representative's Signature*]

_____

[*Title*]

[*Date*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.42

Appendix D

Sample Management Representation Letter: Level I Verification and Performance Examination (Level II)

[*Date*]

[*Name of CPA Firm*]

We are providing this letter in connection with your examination(s) of the assertions of [*name of company*] that (1) the Company has complied with all the composite construction requirements of the Association for Investment Management and Research Performance Presentation Standards (AIMR-PPS® standards) on a firmwide basis for the 10-year period ended December 31, 20Y0, (2) the Company's processes and procedures were designed to calculate and present performance results in compliance with the AIMR-PPS standards as of December 31, 20Y0, and (3) the Performance Results for Composite(s) [*specify composite(s)*] for the 10-year period ended December 31, 20Y0, are presented in conformity with the AIMR-PPS standards.

We confirm, to the best of our knowledge and belief, the following representations made to you during your examination(s):

1. We are responsible for (*a*) compliance with all the composite construction requirements of the AIMR-PPS standards on a firmwide basis for the 10-year period ended December 31, 20Y0, and (*b*) the design of the Company's processes and procedures to calculate and present performance results in compliance with the AIMR-PPS standards and have complied with those requirements as of December 31, 20Y0. We further confirm that we are responsible for the selection of the AIMR-PPS standards as the criteria against which you are evaluating our assertions. Further we confirm that we are responsible for determining that the AIMR-PPS standards are appropriate criteria for our purposes.
2. We assert to you that (*a*) we have complied with all the composite construction requirements of the AIMR-PPS standards on a firmwide basis for the 10-year period ended December 31, 20Y0, and (*b*) the Company's processes and procedures are designed to calculate and present performance results in compliance with the AIMR-PPS standards as of December 31, 20Y0. We also assert that the Performance Results for ABC Composite for the 10-year period ended December 31, 20Y0, are presented in conformity with the AIMR-PPS standards.
3. We are not aware of any matters contradicting the assertions, nor have we received any communications from AIMR or regulatory agencies concerning (*a*) noncompliance with the AIMR-PPS standards or our assertions with regard thereto or (*b*) noncompliance with any other criteria relevant to investment performance statistics.
4. There has been no (*a*) fraud involving management or employees who have significant roles in the Company's processes and procedures relating to compliance with the AIMR-PPS standards or (*b*) fraud involving others that could have a material effect on the Company's compliance with the AIMR-PPS standards.

5. We have made available to you all records relevant to your examination of the aforementioned assertions.

6. We acknowledge responsibility for maintaining sufficient books and records as required under Rule 204 of the Investment Advisers Act of 1940 and we have maintained such records to comply with those requirements.

We are not aware of any events that occurred subsequent to the period being reported on and through the date of this letter that would have a material effect on the aforementioned assertions.

_____

[*Name of Chief Executive Officer and Title*]

_____

[*Name of Chief Financial Officer and Title*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.43

Appendix E

Illustrative Attest Reports: Level I Verification

Example 1: Reporting on Management's Assertions

Independent Accountant's Report

Ellerton Asset Management
1 Investors Square
Anywhere, USA

We have examined the accompanying management assertions of Ellerton Asset Management (the Company) for the 10-year period ended and as of December 31, 20Y0. These assertions are the responsibility of the Company's management. Our responsibility is to express an opinion on these assertions based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting management's assertions and performing the procedures for a Level I Verification set forth by the Association for Investment Management and Research Performance Presentation Standards (AIMR-PPS® standards)[6] and such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, management's assertions referred to above are fairly stated, in all material respects, based on the AIMR-PPS standards.

We did not examine the performance results of the Company's composites for any period through December 31, 20Y0, including any performance presentations that may accompany this report and, accordingly, we express no opinion on any such performance results.

[*Signature*]

September 1, 20Y1

Example 1A: Illustrative Management's Assertions for Report Example 1

Ellerton Asset Management
1 Investors Square
Anywhere, USA

We assert that (1) we have complied with all the composite construction requirements of the Association for Investment Management and Research Performance Presentation Standards on a firmwide basis for the 10-year period

[6] The requirements for a Level I verification under the AIMR-PPS standards are the same as those under the GIPS standards; therefore, the practitioner may refer to the GIPS standards in an examination report on a GIPS verification, if requested.

ended December 31, 20Y0, and (2) the Company's processes and procedures are designed to calculate and present performance results in compliance with the Association for Investment Management and Research Performance Presentation Standards as of December 31, 20Y0.

[*Signature*]
John Q. Smith
Chief Executive Officer
Ellerton Asset Management

Example 2: Reporting Directly on the Subject Matter

Independent Accountant's Report

Ellerton Asset Management
1 Investors Square
Anywhere, USA

We have examined whether Ellerton Asset Management (the Company) (1) complied with all the composite construction requirements of the Association for Investment Management and Research Performance Presentation Standards[7] (AIMR-PPS® standards) on a firmwide basis for the 10-year period ended December 31, 20Y0, and (2) designed its processes and procedures to calculate and present performance results in compliance with the AIMR-PPS standards as of December 31, 20Y0. The Company's management is responsible for compliance with the AIMR-PPS standards and the design of its processes and procedures. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence about the Company's compliance with the above-mentioned requirements, evaluating the design of the company's processes and procedures referred to above, and performing the procedures for a Level I verification set forth by the AIMR-PPS standards and such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, Ellerton Asset Management has, in all material respects:

- Complied with all the composite construction requirements of the AIMR-PPS standards on a firmwide basis for the 10-year period ended December 31, 20Y0, and
- Designed its processes and procedures to calculate and present performance results in compliance with the AIMR-PPS standards as of December 31, 20Y0.

We did not examine the performance results of the Company's composites for any period through December 31, 20Y0, including any performance presentations that may accompany this report and, accordingly, we express no opinion on any such performance results.

[*Signature*]

September 1, 20Y1

[7] The requirements for a Level I verification under the AIMR-PPS standards are the same as those under the GIPS standards; therefore, the practitioner may refer to the GIPS standards in an examination report on a GIPS verification, if requested.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.44

Appendix F

Illustrative Attest Reports: Level I Verification and Performance Examination (Level II)

Example I: Reporting on Management's Assertions

Independent Accountant's Report

Atlas Asset Management
10 Main Street
Anytown, USA

We have examined the accompanying management assertions of Atlas Asset Management (the Company) for the 10-year period ended and as of December 31, 20Y0. We have also examined management's assertion relating to the Company's ABC and XYZ Composites for the 10-year period ended December 31, 20Y0. These assertions are the responsibility of the Company's management. Our responsibility is to express an opinion on these assertions based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting management's assertions and performing the procedures for a Level I verification and a performance examination (Level II) set forth by the Association for Investment Management and Research Performance Presentation Standards (AIMR-PPS® standards) and such other procedures we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, management's assertions referred to above are fairly stated, in all material respects, based on the AIMR-PPS standards.

This report does not relate to any composite presentation of the Company other than the Company's ABC and XYZ Composites.

[*Signature*]

September 1, 20Y1

Example 1A: Illustrative Management's Assertions for Report Example 1

Atlas Asset Management
10 Main Street
Anytown, USA

We assert that (1) we have complied with all the composite construction requirements of the Association for Investment Management and Research Performance Presentation Standards on a firmwide basis for the 10-year period ended December 31, 20Y0, and (2) the Company's processes and procedures are designed to calculate and present performance results in compliance with the Association for Investment Management and Research Performance Presentation Standards as of December 31, 20Y0.

We also assert that the statements of performance results for the ABC and XYZ Composites for the 10-year period ended December 31, 20Y0, are presented in conformity with the Association for Investment Management and Research Performance Presentation Standards.

[*Signature*]
John Q. Jones
Chief Executive Officer,
Atlas Asset Management Company

Example 2: Reporting Directly on the Subject Matter (Level I and Performance Examination (Level II) Report)

Independent Accountant's Report

Atlas Asset Management
10 Main Street
Anytown, USA

We have examined whether Atlas Asset Management (the Company) (1) complied with all the composite construction requirements of the Association for Investment Research and Management Performance Presentation Standards (AIMR-PPS® standards) on a firmwide basis for the 10-year period ended December 31, 20Y0, and (2) designed its processes and procedures to calculate and present performance results in compliance with the AIMR-PPS standards as of December 31, 20Y0. We have also examined the accompanying [*refer to title of accompanying statement*] of the Company's XYZ Composite for the 10-year period ended December 31, 20Y0. The Company's management is responsible for compliance with the AIMR-PPS standards and the design of its processes and procedures and for the [*refer to title of accompanying statement*]. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence about the Company's compliance with the above-mentioned requirements, evaluating the design of the company's processes and procedures referred to above, and performing the procedures for a Level I verification and a performance examination (Level II) set forth by the AIMR-PPS standards and such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, Atlas Asset Management has, in all material respects:

- Complied with all the composite construction requirements of the AIMR-PPS standards on a firmwide basis for the 10-year period ended December 31, 20Y0, and
- Designed its processes and procedures to calculate and present performance results in compliance with the AIMR-PPS standards as of December 31, 20Y0.

Also, in our opinion, [*refer to title of accompanying statement*] of the Company's XYZ Composite for the 10-year period ended December 31, 20Y0, is presented, in all material respects, in conformity with the AIMR-PPS standards.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

This report does not relate to any composite presentation of the Company other than the Company's XYZ Composite.

[*Signature*]

September 1, 20Y1

Example 3: Reporting Directly on the Subject Matter (Performance Examination (Level II) Report With a Reference to a Separate Report on a Level I Verification)

Independent Accountant's Report

Atlas Asset Management
10 Main Street
Anytown, USA

We have examined the accompanying [*refer to title of accompanying statements*] of Atlas Asset Management's (the Company) ABC and XYZ Composites for the 10-year period ended December 31, 20Y0. The Company's management is responsible for these statements. Our responsibility is to express an opinion based on our examination. We previously conducted an examination (also referred to as a Level I verification) of (1) the Company's compliance with all the composite construction requirements of the Association for Investment Management and Research Performance Presentation Standards (AIMR-PPS® standards) on a firmwide basis for the 10-year period ended December 31, 20Y0, and (2) whether the Company's processes and procedures were designed to calculate and present performance results in compliance with the AIMR-PPS standards as of December 31, 20Y0; our report dated August 7, 20Y1, with respect thereto is attached.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included performing the procedures for a performance examination (Level II) set forth by the AIMR-PPS standards and such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, [*refer to title of accompanying statements*] of the Company's ABC and XYZ Composites for the 10-year period ended December 31, 20Y0, are presented, in all material respects, in conformity with the AIMR-PPS standards.

This report does not relate to any composite presentation of the Company other than the Company's ABC and XYZ Composites.

[*Signature*]

September 1, 20Y1

Investment Performance Statistics Task Force

JAMES S. GERSON, *Chair*
STEPHEN D. CALLAHAN
HERBERT M. CHAIN
MATT FORSTENHAUSLER
SEAN KEOGH
JESSICA MANN
PETER J. MCNAMARA
JOHN N. SPINNEY, JR.
KARYN VINCENT

AICPA Staff

CHARLES S. LANDES
Director
Audit and Attest Standards

JANE M. MANCINO
Technical Manager
Audit and Attest Standards

[The next page is 31,621.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 14,390

Statement of Position 02-1 Performing Agreed-Upon Procedures Engagements That Address Annual Claims Prompt Payment Reports as Required by the New Jersey Administrative Code

May 23, 2002

NOTE

This Statement of Position (SOP) represents the recommendations of the AICPA's New Jersey Annual Claims Prompt Payment Reports Task Force regarding the application of Statements on Standards for Attestation Engagements (SSAEs) to agreed-upon procedures engagements performed to comply with the requirements of New Jersey Administrative Code, Title 11, Chapter 22, Subchapter 1 (NJAC 11:22-1 or the Code), which establishes Department of Banking and Insurance (Department) standards for the payment of claims relating to health benefits plans and dental plans and contains requirements for carriers to file certain reports with the Department relating to the timeliness of claims payments and the reasons for denial and late payment of claims in a format prescribed by the Department. The Department has approved the use of the agreed-upon procedures outlined in this SOP to comply with the reporting requirements of the Code. The Auditing Standards Board has found the recommendations in this SOP to be consistent with existing standards covered by Rule 202 of the AICPA Code of Professional Conduct. AICPA members should be aware of and consider these recommendations. If the auditor does not apply these recommendations, the auditor should be prepared to explain how he or she complied with the SSAE provisions addressed by these recommendations.

Introduction and Background

.01 New Jersey Administrative Code, Title 11, Chapter 22, Subchapter 1 (NJAC 11:22-1 or the Code), establishes Department of Banking and Insurance (Department) standards for the payment of claims relating to health benefits plans and dental plans and contains requirements for carriers to file certain reports with the Department relating to the timeliness of claims payments and the reasons for denial and late payment of claims in a format prescribed by the Department.

.02 NJAC 11:22-1 applies to any insurance company, health service corporation, medical service corporation, hospital service corporation, health maintenance organization, dental service corporation, and dental plan organization

that issues health benefits plans or dental plans in the state of New Jersey and to any agent, employee, or other representative of such entity that processes claims for such entity.

.03 Among other things, the Code requires carriers to report:

- Quarterly to the Department on the timeliness of claims payments in the format set forth in Appendix A (claims payment exhibit report) of NJAC 11:22-1, and
- Quarterly and annually on late payments of claims and the reasons for any denials (claims prompt payment report) in the format set forth in Appendix B of NJAC 11:22-1.

.04 Furthermore, the Code requires that the annual claims prompt payment report, which is due to be filed with the Department on or before March 31, pursuant to NJAC 11:22-1.9(a), be accompanied by the report of a private auditing firm, which may be a Certified Public Accountant (CPA) or a firm of CPAs. However, for calendar year 2001, the report of the private auditing firm may be filed with the Department on or before July 1, 2002. The Department has specified, in Bulletin No. 02-07, that the work shall be conducted, and the report shall be prepared, in accordance with agreed-upon procedures acceptable to the Department.

Applicability

.05 This Statement of Position (SOP) was developed to provide practitioners with guidance on performing agreed-upon procedures engagements that address annual claims prompt payment reports as required by the New Jersey Administrative Code. Practitioners should note that the engagement described in this SOP is designed only to satisfy the requirements of the Code. The procedures, as set forth in this SOP, are not necessarily appropriate for use in any other engagement.

The Code

Definitions

.06 The following definitions are reprinted from the Code and are applicable when performing the agreed-upon procedures engagement described in this SOP.

Agent—Any entity, including a subsidiary of a carrier, or an organized delivery system as defined by N.J.S.A. 17:48H-1, with which a carrier has contracted to perform claims processing or claims payment services.

Carrier—An insurance company, health service corporation, hospital service corporation, medical service corporation or health maintenance organization authorized to issue health benefits plans in this State and a dental service corporation or dental plan organization authorized to issue dental plans in this State.

Claim—A request by a covered person, a participating health care provider, or a nonparticipating health care provider who has received an assignment of benefits from the covered person, for payment relating to health care services or supplies or dental services or supplies covered under a health benefits plan or dental plan issued by a carrier.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Clean claim—

1. The claim is for a service or supply covered by the health benefits plan or dental plan;
2. The claim is submitted with all the information requested by the carrier on the claim form or in other instructions distributed to the provider or covered person;
3. The person to whom the service or supply was provided was covered by the carrier's health benefits or dental plan on the date of service;
4. The carrier does not reasonably believe that the claim has been submitted fraudulently; and
5. The claim does not require special treatment. For the purposes of this subchapter, special treatment means that unusual claim processing is required to determine whether a service or supply is covered, such as claims involving experimental treatments or newly approved medications. The circumstances requiring special treatment should be documented in the claim file.

Covered person—A person on whose behalf a carrier offering the plan is obligated to pay benefits or provide services pursuant to the health benefits or dental plan.

Covered service or *supply*—A service or supply provided to a covered person under a health benefits or dental plan for which the carrier is obligated to pay benefits or provides services or supplies.

Dental plan—A benefits plan which pays dental expense benefits or provides dental services and supplies and is delivered or issued for delivery in this State by or through any carrier in this State.

Department—The Department of Banking and Insurance.

Health benefits plan—A benefits plan that pays hospital and medical expense benefits or provides hospital and medical services, and is delivered or issued for delivery in this State by or through a carrier. Health benefits plan includes, but is not limited to, Medicare supplement coverage and risk contracts to the extent not otherwise prohibited by Federal law. For the purposes of this chapter, health benefits plan shall not include the following plans, policies or contracts: accident only, credit, disability, long-term care, CHAMPUS supplement coverage, coverage arising out of a workers' compensation or similar law, automobile medical payment insurance, personal injury protection insurance issued pursuant to P.L. 1972, c.70 (N.J.S.A. 39:6A-1 et seq.) or hospital confinement indemnity coverage.

Health care provider or *provider*—An individual or entity which, acting within the scope of its license or certification, provides a covered service or supply as defined by the health benefits or dental plan. Health care provider includes, but is not limited to, a physician, dentist and other health care professional licensed pursuant to Title 45 of the Revised Statutes and a hospital and other health care facilities licensed pursuant to Title 26 of the Revised Statutes.

Reporting Requirements

.07 The Code requires a carrier and its agent to remit payment of clean claims pursuant to specified time frames. The Code further requires that if a

carrier or its agent denies or disputes a claim, in full or in part, the carrier or its agent must, within a specified time frame, notify both the covered person when he or she will have increased responsibility for payment, and the provider, of the basis for its decision to deny or dispute the claim.

.08 The Code requires a carrier to report to the Department quarterly on the timeliness of claims payments in the format prescribed in NJAC 11:22-1, Appendix A, "New Jersey Claims Payment Exhibit." This quarterly report is not required to be subjected to an agreed-upon procedures engagement, nor is an annual claims payment exhibit report required to be filed with the Department.

.09 The Code also requires a carrier to report to the Department on a quarterly and annual basis on the late payment of claims and the reasons for denial of claims in the format prescribed in NJAC 11:22-1, Appendix B, "Quarterly (Annual) Claims Prompt Payment Report." The Code requires that the annual claims prompt payment report be accompanied by a report of a private auditing firm, which may be a CPA or a firm of CPAs.

.10 The Department has indicated, in Bulletin No. 02-07, that an agreed-upon procedures engagement pursuant to this SOP may be used to satisfy the requirement that an annual claims prompt payment report be accompanied by the report of a private auditing firm. Furthermore, in Bulletin No. 02-12, issued in May 2002, the Department has indicated that it agrees to the sufficiency of the procedures included in this SOP for its purposes.

Related Professional Standards

Chapter 2, "Agreed-Upon Procedures Engagements," of Statement on Standards for Attestation Engagements No. 10 (AT Sec. 201)

.11 Agreed-upon procedures engagements performed to meet the requirements of the Code are to be performed in accordance with Chapter 2, "Agreed-Upon Procedures Engagements," of SSAE No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 201). As described in Chapter 2 of SSAE No. 10 (AT sec. 201.03), an agreed-upon procedures engagement is one in which a practitioner is engaged by a client to issue a report of findings based on specific procedures performed on the subject matter. Not all of the provisions of Chapter 2 of SSAE No. 10 are discussed herein. Rather, this SOP includes guidance to assist practitioners in the application of selected aspects of Chapter 2 of SSAE No. 10.

.12 Chapter 2 of SSAE No. 10 (AT sec. 201.06) states, in part, that the practitioner may perform an agreed-upon procedures engagement provided that, ". . . (*c*) the practitioner and the specified parties agree upon the procedures performed or to be performed by the practitioner; and (*d*) the specified parties take responsibility for the sufficiency of the agreed-upon procedures for their purposes."

.13 As previously stated, Bulletin No. 02-07 from the Department states that an agreed-upon procedures engagement may be used to meet the requirement for an independent private auditing firm to report on the annual claims prompt payment reports as required by the New Jersey Administrative Code. Furthermore, the Department has approved the use of the agreed-upon procedures outlined in this SOP to comply with the reporting requirements of the

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Code. Accordingly, practitioners should not eliminate any of the procedures presented in appendix B [paragraph .28], "Agreed-Upon Procedures That Address Annual Claims Prompt Payment Reports as Required by the New Jersey Administrative Code," of this SOP or reduce the extent of the tests. The Department or the carrier may request that additional procedures be performed and the practitioner may agree to perform such procedures. In those circumstances, it would be expected that the additional procedures would be performed in the context of a separate agreed-upon procedures engagement.

Procedures to Be Performed

.14 The agreed-upon procedures to be performed are applied to the carrier's annual claims prompt payment report, which reports on the late payment of claims and reasons for denial of claims in the format prescribed in NJAC 11:22-1, Appendix B.

.15 The procedures to be performed in the agreed-upon procedures engagement described in this SOP are presented in appendix B [paragraph .28] of this SOP. The procedures have been designed so that the findings resulting from the application of the procedures can be recorded in a tabular format. The findings for each procedure should be reported as *No Exception*, *Exception*, or *N/A* (not applicable). If a procedure is not applicable to a particular carrier, the procedure should be marked N/A rather than deleted from the report.

.16 If any portion of a procedure results in an exception, the findings for that entire procedure should be recorded as an exception and described in the section "Description of Exceptions If Any." The practitioner should provide a brief factual explanation for each exception that will enable the specified parties to understand the nature of the findings resulting in the exception. If management informs the practitioner that the condition giving rise to the exception was corrected by the date of the practitioner's report, the practitioner's explanation of the exception may include that information; for example, "Management has advised us that the condition resulting in the exception was corrected on Month X, 20XX. We have performed no procedures with respect to management's assertion."

.17 A practitioner may perform significant portions of the agreed-upon procedures engagement before the end of the period covered by the report. If, during that time, the practitioner identifies conditions that result in an exception in one or more agreed-upon procedures, he or she should report the exception in the findings section of the agreed-upon procedures report, even if management corrects the condition prior to the end of the period.

.18 Chapter 2 of SSAE No. 10 (AT sec. 201.40) states the following:

> The practitioner need not perform procedures beyond the agreed-upon procedures. However, in connection with the application of agreed-upon procedures, if matters come to the practitioner's attention by other means that significantly contradict the subject matter (or written assertion related thereto) referred to in the practitioner's report, the practitioner should include this matter in his or her report. For example, if, during the course of applying agreed-upon procedures regarding an entity's internal control, the practitioner becomes aware of a material weakness by means other than performance of the agreed-upon procedure, the practitioner should include this matter in his or her report.

.19 A practitioner has no obligation to perform procedures beyond the agreed-upon procedures included in appendix B [paragraph .28] of this SOP.

However, if information that contradicts the information in the carrier's annual claims prompt payment report comes to the practitioner's attention by other means, such information should be included in the practitioner's report. This also would apply to conditions or events occurring during the subsequent-events period (subsequent to the period covered by the practitioner's report but prior to the date of the practitioner's report) that either contradict the findings in the report or that would have resulted in the reporting of an exception by the practitioner if that condition or event had existed during the period covered by the report. However, the practitioner has no responsibility to perform any procedure to detect such conditions or events.

Establishing an Understanding With the Client

.20 In accordance with Chapter 2 of SSAE No. 10 (AT sec. 201.10), the practitioner should establish an understanding with the client regarding the services to be performed. Such an understanding reduces the risk that the client may misinterpret the objectives and limitations of an agreed-upon procedures engagement performed to meet the regulatory requirements of the Code. Such an understanding also reduces the risk that the client will misunderstand its responsibilities and the responsibilities of the practitioner. The practitioner should document the understanding in the working papers, preferably through a written communication with the client (an engagement letter). The communication should be addressed to the client. Matters that might be included in such an understanding are the following:

- A statement confirming that an agreed-upon procedures engagement is to be performed to meet the requirements of NJAC 11:22-1
- A statement identifying the procedures to be performed as those set forth in SOP 02-1, *Performing Agreed-Upon Procedures Engagements That Address Annual Claims Prompt Payment Reports as Required by the New Jersey Administrative Code*
- A statement identifying the client and the Department as the specified parties to the agreed-upon procedures report
- A statement acknowledging the client's responsibility for the sufficiency of the procedures in the SOP and referring to Bulletin No. 02-12, which acknowledges the Department's responsibility for the sufficiency of the procedures in the SOP
- A statement acknowledging that the practitioner makes no representation regarding the sufficiency of the procedures in the SOP
- A statement describing the responsibilities of the practitioner, including but not limited to the responsibility to perform the agreed-upon procedures and to provide the client with a report, and the circumstances under which the practitioner may decline to issue a report
- A statement indicating that the engagement will be conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA)
- A statement indicating that an agreed-upon procedures engagement does not constitute an examination, the objective of which would be the expression of an opinion on the carrier's compliance with the requirements of NJAC 11:22-1, and that if an examination were performed, other matters might come to the practitioner's attention

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- A statement indicating that the practitioner will not express an opinion or any other form of assurance
- A statement describing the client's responsibility to comply with the requirements of NJAC 11:22-1 and the client's responsibility for the information in the carrier's annual claims prompt payment report
- A statement describing the client's responsibility for providing accurate and complete information to the practitioner
- A statement indicating that the practitioner has no responsibility for the completeness or accuracy of the information provided to the practitioner
- A statement restricting the use of the report to the client and the Department
- A statement describing any arrangements to involve a specialist

Management Representations

.21 Although Chapter 2 of SSAE No. 10 does not require a practitioner to obtain a representation letter from management in an agreed-upon procedures engagement, it is recommended that the practitioner obtain such a letter when performing the engagement described in this SOP. The representation letter generally should be signed by the appropriate members of management including the highest-ranking officer responsible for the carrier's compliance with the requirements of NJAC 11:22-1. Management's refusal to furnish written representations that the practitioner has determined to be appropriate for the engagement constitutes a limitation on the performance of the engagement that requires either modification of the report or withdrawal from the engagement.

.22 The representations that a practitioner deems appropriate will depend on the specific nature of the engagement; however, the practitioner ordinarily would obtain the following representations from management:

- A statement acknowledging responsibility for compliance with the requirements of NJAC 11:22-1 and responsibility for the information in the carrier's annual claims prompt payment report
- A statement that there have been no errors or fraud that might indicate that the carrier is not in compliance with the requirements of NJAC 11:22-1 and that there are no known matters (or that management has disclosed to the practitioner all known matters) that contradict the information in the carrier's annual claims prompt payment report
- A statement that management has disclosed to the practitioner any communications from regulatory agencies relating to the carrier's annual claims prompt payment report
- A statement that management has made available to the practitioner all information it believes is relevant to the carrier's annual claims prompt payment report
- A statement that management has responded fully to all inquiries made by the practitioner during the engagement
- A statement that no events have occurred subsequent to the date as of which the procedures were applied that would require modification of the findings of the agreed-upon procedures

.23 An illustrative representation letter is presented in appendix C [paragraph .29], "Illustrative Management Representation Letter," of this SOP. For additional information regarding management's written representations in an agreed-upon procedures engagement, see Chapter 2 of SSAE No. 10 (AT sec. 201.37–.39).

Restriction on the Performance of Procedures

.24 As previously stated, a practitioner should not agree to eliminate any of the procedures presented in appendix B [paragraph .28] of this SOP. If circumstances impose restrictions on the performance of the agreed-upon procedures, the practitioner should attempt to obtain agreement from the specified users for modification of the agreed-upon procedures presented in appendix B [paragraph .28] of this SOP. When such agreement cannot be obtained, the practitioner should describe the restriction(s) on the performance of procedures in his or her report or withdraw from the engagement.

Dating the Report

.25 The date of completion of the agreed-upon procedures should be used as the date of the practitioner's report.

Effective Date

.26 This SOP is effective upon issuance and is applicable only to agreed-upon procedures engagements that report on annual claims prompt payment reports as required by the NJAC.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.27

Appendix A

Illustrative Agreed-Upon Procedures Report

The following is an illustrative agreed-upon procedures report based on the guidance in Chapter 2, "Agreed-Upon Procedures Engagements," of Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards,* vol. 1, AT sec. 201).

Independent Accountant's Report
on Applying Agreed-Upon Procedures

To the Management of ABC Carrier:

We have performed the applicable procedures enumerated in the American Institute of Certified Public Accountants' Statement of Position (SOP) 02-1, *Performing Agreed-Upon Procedures Engagements That Address Annual Claims Prompt Payment Reports as Required by the New Jersey Administrative Code*, which were agreed to by ABC Carrier and the New Jersey Department of Banking and Insurance (the Department), solely to assist you in complying with the reporting requirements of New Jersey Administrative Code, Title 11, Chapter 22, Subchapter 1.9 (NJAC 11:22-1.9) for Appendix B 20XX Annual Report (Exhibit I) for the year ended December 31, 20XX. Management of ABC Carrier is responsible for compliance with the requirements of NJAC 11:22-1. This agreed-upon procedures engagement was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. The sufficiency of these procedures is solely the responsibility of ABC Carrier and the Department. Consequently, we make no representation regarding the sufficiency of the procedures described in the attached Appendix either for the purpose for which this report has been requested or for any other purpose.

The procedures performed and the findings are included in the attached Appendix.

We were not engaged to and did not conduct an examination, the objective of which would be the expression of an opinion on ABC Carrier's compliance with the requirements of NJAC 11:22-1 for the year ended December 31, 20XX. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

This report is intended solely for the information and use of the management of ABC Carrier and the State of New Jersey Department of Banking and Insurance, and is not intended to be and should not be used by anyone other than these specified parties.

[*Signature*]

[*Date*]

Appendix B

Agreed-Upon Procedures That Address Annual Claims Prompt Payment Reports as Required by the New Jersey Administrative Code

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
The following procedures were applied to the ABC Carrier's 20XX Appendix B annual claims prompt payment report.			
We obtained supporting documentation used by management to prepare the Annual New Jersey Prompt Payment Report, and for each of the five categories (physician, dental, other health care professional, hospital, or other health care facilities), where applicable, compared the number of claims and the amount of claims for each quarter and the annual period from the supporting documentation used by management to prepare the Annual New Jersey Prompt Payment Report to the following columns of the report:			
• Total claims	_____	_____	_____
• Denied ineligible	_____	_____	_____
• Denied document	_____	_____	_____
• Denied coding/enrollment	_____	_____	_____
• Denied for amount	_____	_____	_____
• Time limit special	_____	_____	_____
• Time limit other	_____	_____	_____
• Denied referred fraud	_____	_____	_____
• Interest paid	_____	_____	_____
• Interest amount paid	_____	_____	_____
• Total paid	_____	_____	_____

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
We selected 10 percent of the claims from ABC Carrier's supporting documentation used by management to prepare the Annual New Jersey Prompt Payment Report, with the selections distributed throughout the year. If 10 percent of the claims exceeded 50, then the number of items selected was limited to 50. If 10 percent of the claims resulted in less than 10 claims, then the number of items selected was 10, and for each item selected we:			
1. Compared the following information to ABC Carrier's claim payment system:			
• Paid amount	_____	_____	_____
• Claim finalization or payment date	_____	_____	_____
• Claim received date	_____	_____	_____
• Denial code	_____	_____	_____
• Claim category (physician, dental, other health care professional, hospital, or other health care facilities)	_____	_____	_____
2. Compared the following information to the original claim information submissions:			
• Date received	_____	_____	_____
• Amount billed	_____	_____	_____
• Category (physician, dental, other health care professional, hospital, or other health care facilities)	_____	_____	_____
3. Noted whether, per ABC Carrier's member records, original claim information submission, or both, the claim related to a policy issued in the state of New Jersey	_____	_____	_____
4. If a selected claim was denied, compared denial reason indicated in ABC Carrier's claims system records to supporting documentation used by management to prepare the Annual New Jersey Prompt Payment Report	_____	_____	_____

Procedures	*Findings* — *No Exception*	*Exception*	*N/A*
5. If a selected claim is a "clean claim," as defined in NJAC 11:22-1.2, and as determined by ABC Carrier, recalculated the amount of interest paid on the selected claim in accordance with the requirements of NJAC 11:22-1.5			
We selected 10 claims from ABC Carrier's primary claims system, with the selections distributed throughout the year, and for each item selected, traced the selected claims covered under New Jersey contracts to the supporting documentation used by management to prepare the Annual New Jersey Prompt Payment Report.			
We proved the arithmetic accuracy of ABC Carrier's 20XX Appendix B annual claims prompt payment report.			

Description of Exceptions if Any

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.29

Appendix C

Illustrative Management Representation Letter

[*ABC Carrier's Letterhead*]

[*Date*]

[*CPA Firm's Name and Address*]

In connection with your engagement to apply the agreed-upon procedures enumerated in the American Institute of Certified Public Accountants' Statement of Position (SOP) 02-1, *Performing Agreed-Upon Procedures Engagements That Address Annual Claims Prompt Payment Reports as Required by the New Jersey Administrative Code,* which were agreed to by ABC Carrier and the New Jersey Department of Banking and Insurance, solely to assist us in complying with the requirements of New Jersey Administrative Code, Title 11, Chapter 22, Subchapter 1 (NJAC 11:22-1.9), for Appendix B 20XX Annual Report (Exhibit I) for the period from January 1, 20XX through December 31, 20XX, we confirm, to the best of our knowledge and belief, the following representations made to you during your engagement:

1. We are responsible for compliance with the requirements of NJAC 11:22-1 and for the information in ABC Carrier's annual claims prompt payment report.

2. During the year ended December 31, 20XX, there have been no errors or fraud that would indicate that ABC Carrier is not in compliance with the requirements of NJAC 11:22-1.

3. We have disclosed to you all known matters contradicting the information in ABC Carrier's annual claims prompt payment report.

4. There have been no communications from regulatory agencies relating to ABC Carrier's annual claims prompt payment report, including communications received between December 31, 20XX, and the date of this letter.

5. We have made available to you all information that we believe is relevant to ABC Carrier's annual claims prompt payment report.

6. We have responded fully to all inquiries made to us by you during the engagement.

To the best of our knowledge and belief, no events have occurred subsequent to December 31, 20XX, and through the date of this letter that would require adjustment to or modification of the findings of the agreed-upon procedures.

[*Signature*]

[*Title*]

[*Signature*]

[*Title*]

New Jersey Annual Claims Prompt Payment Reports Task Force

JEFF MUZIO, *Chair*
CRAIG C. ANDERSON
JOHN D. HARRIS
JOHN LANGIONE
NANCY LOFREDO
KIM RAIMONDI
CHRIS SCUDELLARI

AICPA Staff

CHARLES E. LANDES
Director
Audit and Attest Standards

SUSAN S. JONES
Senior Technical Manager
Audit and Attest Standards

The AICPA is grateful to Jean Connolly, James S. Gerson, and Kim Hekker, for their technical assistance with this document.

[The next page is 31,651.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 14,400

Statement of Position 03-2 Attest Engagements on Greenhouse Gas Emissions Information

September 22, 2003

NOTE

This Statement of Position (SOP) represents the recommendations of the Joint Task Force of the AICPA and CICA on Sustainability Reporting regarding the application of Statements on Standards for Attestation Engagements (SSAEs) to attest engagements on greenhouse gas emissions information. The Auditing Standards Board has found the recommendations of this SOP to be consistent with existing standards covered by Rule 202 of the AICPA Code of Professional Conduct. If an AICPA member does not apply the attest guidance included in this SOP, he or she should be prepared to explain how he or she complied with the SSAE provisions addressed by such attest guidance.

Background and Introduction

Climate Change and Greenhouse Gases

.01 Many scientists believe that global temperatures are increasing and that the increase is due to a buildup of so-called greenhouse gases (GHGs) in the atmosphere. Certain atmospheric gases (methane, carbon dioxide, nitrous oxide, water vapor, and others) are called greenhouse gases because they are believed to help trap some of the outgoing energy, retaining heat somewhat like the glass panels of a greenhouse. Atmospheric concentrations of carbon dioxide, methane, and nitrous oxide are believed to have increased by over 31 percent, 151 percent, and 17 percent, respectively, since the late 19th century.[1] Over the same period, many scientists have noted an increase of approximately 1 degree Fahrenheit in the average global temperature.

.02 Fossil fuel use and other human activities have added significant amounts of GHGs to the atmosphere. GHG emissions are also produced by agriculture, animal husbandry, and various industrial processes. Many scientists believe the release of GHGs into the atmosphere to be the cause of the increase in global temperatures. This has led to a number of global and national initiatives to reduce GHG emissions; one such initiative is the Kyoto Protocol (see paragraphs .04 through .07). Since a significant portion of GHG emissions is closely tied to fossil fuel use, achieving the reductions envisioned by those various initiatives would require reduced consumption of coal, oil, natural gas, and other fuels. Such reductions would clearly affect consumers and industry in the United States and elsewhere.

---

[1] Source: Intergovernmental Panel on Climate Change (IPCC) Third Assessment Report: *Climate Change 2001 Summary for Policy Makers*, p. 34, Table SPM-1. www.ipcc.ch/pub/reports.htm.

.03 However, there is no universal agreement on the science behind global warming. Some scientists and policy makers oppose initiatives and regulations to reduce GHG emissions because they dispute how much of the global warming trend can be attributed to human activity, arguing that natural forces are also at work. As a result, some are reluctant to make the changes required to reduce GHG emissions while, in their view, the causes, consequences, and severity of climate change remain in doubt.

The Kyoto Protocol

.04 At the 1992 Earth Summit in Rio de Janeiro, a voluntary agreement to reduce global concentrations of "man-made greenhouse gases," the United Nations Framework Convention on Climate Change (UNFCCC), was adopted and ratified by the United States and a majority of the world's developed countries. When the voluntary targets outlined in the UNFCCC did little to reduce global concentrations of GHGs, the United Nations (UN) initiated an annual negotiation process known as the Conference of the Parties (COP) to set mandatory reduction targets. In 1997, during the third round of negotiations in Kyoto, Japan, the COP reached an agreement on a mandatory mechanism to reduce global GHG emissions; that agreement is now referred to as the Kyoto Protocol.

.05 The Kyoto Protocol set targets for each of 38 developed countries, which would have to reduce emissions by a certain percentage below their 1990 emissions baseline. To be legally binding, the Kyoto Protocol must be ratified by at least 55 countries, including developed countries responsible for at least 55 percent of the emissions in 1990.

.06 To give countries more options for achieving their emission reduction targets, the Kyoto Protocol incorporated a number of "flexibility mechanisms," namely emissions trading, clean development mechanism (CDM), and joint implementation (JI). Whether trading systems established under the Kyoto Protocol will allow trades with external parties (that is, those that have not signed the Kyoto Protocol) is still being debated among the signatory countries. GHG emission credits may also be traded outside the Kyoto Protocol processes through independent, voluntary markets such as the Chicago Climate Exchange, or by contracts between two or more companies. It is unclear whether GHG emissions credit trading from these latter two mechanisms can be used to meet targets related to the Kyoto Protocol.

GHGs to Be Regulated by the Kyoto Protocol

.07 The Kyoto Protocol would regulate emissions of the following six GHGs:

- Carbon dioxide (CO_2)
- Methane (CH_4)
- Nitrous oxide (N_2O)
- Perfluorocarbons (PFCs)
- Hydrofluorocarbons (HFCs)
- Sulphur hexafluoride (SF_6)

Why U.S. Companies Are Considering Strategies to Address Their GHG Emissions

.08 U.S. companies with operations in countries that have ratified the Kyoto Protocol may have to meet emission reduction targets in those countries

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

once the Kyoto Protocol becomes effective. Consideration of alternative strategies and related costs will enable those companies to find the lowest-cost alternative before triggering the imposition of requirements and any related fines. Emissions trading is considered to be an effective, cost-efficient way to meet limits imposed by regulators, especially toward the end of a compliance period.

.09 In addition, there is a sense among many companies that even though they will not be subject to the Kyoto Protocol in the United States, at some point a regulatory framework that places a limit on GHG emissions may be adopted. These companies take the view that it would be wise to start planning and preparing for a "carbon-constrained" future and eventually take advantage of the potential opportunities that GHG emissions trading presents.

GHG Emissions Trading Programs and GHG Registries in the United States

.10 There are a number of initiatives to establish GHG emissions trading programs or GHG emission registries in the United States, most of which are in various stages of development. One program currently in development is the Chicago Climate Exchange (CCX) (www.chicagoclimateX.com).

.11 The CCX is a voluntary *cap-and-trade program* for reducing and trading GHG emissions. Entities that agree to become members of the CCX must, upon becoming members, enter into a legally binding commitment to reduce their emissions of GHGs by 4 percent below the average of their 1998 through 2001 baseline by 2006, the last year of the pilot program. CCX will enable participants to buy and sell credits to find the most cost-effective way of achieving reductions. Trading is targeted to begin in the fourth quarter of 2003.

.12 Some trading schemes involve trading of CO_2 only, while others permit trading of the six GHGs identified in the Kyoto Protocol (see paragraph .07 of this Statement of Position [SOP]). The CCX plans to enable trading in the six GHGs described in the Kyoto Protocol. Those non-CO_2 GHGs can be translated into tons of CO_2 equivalent using the Intergovernmental Panel on Climate Change's (IPCC) Global Warming Potentials (GWP) (www.ipcc.ch).

.13 The California Climate Action Registry (www.climateregistry.org) will enable entities operating within the State of California to voluntarily record their annual GHG emissions inventories. In turn, the State of California has stated that it will use its best efforts to ensure that entities voluntarily inventorying their emissions will receive appropriate credit for early action (that is, action before regulation of GHG emissions) under any future international, federal, or state regulatory regimes relating to GHG emissions. Third-party certification[2] of the baseline and emission reductions is a key component of the California Climate Action Registry. An entity can register emissions (*a*) only for the units in California or (*b*) for all units within the United States.

Terms and Definitions Used by Registries and Regulatory Frameworks

.14 Different registries and regulatory frameworks may use different terms and definitions for similar services. A *validation* is a service that would

[2] See paragraph .14 of this Statement of Position (SOP) for a definition of the term *certification*.

provide assurance on the feasibility of the design of an emission reduction project, typically before inception of the project; an entity would typically engage an engineering or a consulting firm to provide such a service. This SOP does not provide guidance on validation services. A *verification* is the objective and independent assessment of whether the reported GHG inventory properly reflects the GHG impact of the entity in conformance with preestablished GHG accounting and reporting standards. The California Climate Action Registry's Certification Protocol (October 2002) defines a *certification* as "the process used to ensure that a given participant's *GHG emissions inventory* (either the baseline or the annual result) has met a minimum quality standard and complied with the Registry's procedures and protocols for calculating and reporting GHG emissions." A certification may be viewed by some as providing absolute, not reasonable, assurance. Practitioners should be aware that various GHG registries and regulatory frameworks may not define these terms in exactly the same way; thus the practitioner should obtain the official definitions of such terms under the registry or regulatory framework relevant to the engagement. However, practitioners should not use such terms in their attest reports on GHG emissions.

Scope of SOP

.15 This SOP provides guidance to practitioners for the following:

- Engagements to examine and report on a schedule or an assertion relating to information about a GHG emissions inventory (GHG emissions for a compliance period, such as a year) or a baseline GHG inventory
- Engagements to examine and report on a schedule on or an assertion relating to information about a GHG emission reduction in connection with (*a*) the recording of the reduction with a registry or (*b*) a trade of that reduction or credit

Such examination engagements should be performed pursuant to Chapter 1, "Attest Engagements," of Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101), as amended.

.16 While a review-level service relating to an entity's GHG inventory is permissible under existing attestation standards, it is most likely that the market will ultimately demand an examination-level service. Accordingly, this SOP provides guidance only on an examination-level service.

Engagement Acceptance Considerations

.17 Before accepting the engagement, the practitioner should consider guidance on engagement acceptance within Chapter 1 of SSAE No. 10, as amended. The following are examples of specific matters that should be considered:

- Independence (see paragraphs .18 through .20 of this SOP).
- Whether the practitioner has adequate technical knowledge of the subject matter to perform the engagement, including evaluation of the work of any specialists involved in the engagement (see paragraphs .21 through .26 of this SOP).
- Considerations in selecting and using the work of a specialist, when applicable (paragraphs .27 through .29 of this SOP).

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- Existence of suitable criteria (see paragraphs .30 through .36 of this SOP).
- Materiality considerations (see paragraph .37 of this SOP).
- Expectations of users of the GHG inventory or reduction information and the practitioner's report thereon.
- Whether the client is likely to have adequate information systems and controls to provide reliable GHG information.
- Whether sufficient evidence is likely to exist when the entity has changed measurement methods for GHG emissions from one period to the next (see paragraphs .39 and .65 of this SOP).
- The scope of the entity's GHG inventory (see paragraph .40 of this SOP for a discussion of boundaries and paragraphs .41 through .44 of this SOP for a discussion of direct and indirect emissions for a GHG inventory).
- Availability of historical data. The practitioner should consider the risk that historical data for the base year may not be available if the practitioner is engaged to perform the attest service at a date considerably later than the base year. (See paragraph .45 of this SOP for a discussion of baselines.)

Independence

.18 The practitioner performing an attest engagement should be *independent* pursuant to Rule 101, *Independence*, of the Code of Professional Conduct (AICPA, *Professional Standards,* vol. 2, ET sec. 101.01).[3]

.19 According to section 201 of the Sarbanes-Oxley Act (the Act),[4] it is unlawful for a public accounting firm registered with the Public Company Accounting Oversight Board that performs an audit of a public company to provide, contemporaneously with the audit, certain nonaudit services; those prohibited services do not include attest engagements on GHG emissions information. A registered public accounting firm may engage in any nonaudit service that is not on the prohibited list for a public company audit client only if the activity is approved in advance by the company's audit committee. The Act does not place any limitations on public accounting firms in providing nonaudit services to public companies that they do not audit or to any nonpublic companies.

.20 Certain GHG registries or regulatory frameworks set rules that prohibit professionals who provide assurance on GHG inventories or reductions from providing other services to the entity for a period of time (for example, California Climate Action Registry). The practitioner should consider whether the relevant scheme or registry sets independence requirements beyond those of the AICPA or sets other limitations on the scope of services.[5]

---

[3] For guidance on independence when engaged to issue an attest report that is restricted as to use, see Interpretation No. 11, "Modified Application of Rule 101 for Certain Engagements to Issue Restricted-Use Reports Under the Statements on Standards for Attestation Engagements," of Rule 101, *Independence* (AICPA, *Professional Standards*, vol. 2, ET sec. 101.13).

[4] See also subsections (g) through (l) of Section 10A of the Securities Exchange Act of 1934.

[5] For example, a greenhouse gas (GHG) framework or registry may set independence requirements that specifically prohibit a practitioner who has performed a financial statement audit or other specified service for an entity from also providing a verification (examination) of an entity's GHG emission inventory for a certain period of time.

Adequate Knowledge of Subject Matter and Use of a Specialist

.21 The second general attestation standard states, "The engagement shall be performed by a practitioner having adequate knowledge of the subject matter." Chapter 1 of SSAE No. 10 (AT sec. 101.22), as amended, states that "this knowledge requirement may be met, in part, through the use of one or more specialists on a particular attest engagement if the practitioner has sufficient knowledge of the subject matter (*a*) to communicate to the specialist the objectives of the work and (*b*) to evaluate the specialist's work to determine if the objectives were achieved." Before accepting an attest engagement on GHG emissions information, the practitioner should consider whether his or her involvement in the engagement and understanding of the subject matter are sufficient to enable the practitioner to discharge his or her responsibilities. The practitioner should accept an attest engagement on GHG emissions information only if the practitioner is satisfied that those persons who are to perform the engagement collectively possess the necessary professional competencies.

.22 In most attest engagements on GHG emissions, the nature of the entity's operations, emissions, or the emissions measurement methodology in general requires specialized skill or technical knowledge in a particular field other than accounting or auditing. As a result, the practitioner should possess adequate technical knowledge of the subject matter to understand how GHG emissions information might be misstated and to evaluate the work of a specialist and the specialist's conclusion, when applicable. A practitioner may obtain adequate knowledge of the subject matter through formal or continuing education, including self-study, or through practical experience. The practitioner should read the criteria selected by the responsible party to understand what is involved in the measurements in determining whether the practitioner has adequate technical knowledge.

.23 Since most attest engagements on GHG emissions will require specialized skill or technical knowledge in a particular field other than accounting or auditing, the practitioner may use the work of a specialist, such as an environmental engineer or consultant. If the client is a service entity whose GHG emissions are limited to the use of purchased electricity and natural gas or oil, the practitioner may be able to use published factors to convert the electricity, gas, or oil used to GHGs emitted. Under those circumstances, the practitioner may not need to use a specialist, provided that the practitioner possesses sufficient technical knowledge regarding the published factors, including an understanding of the nature of each factor and distinctions between alternatives. If the client has significant industrial operations with numerous sources of emissions, however, it is more likely that the practitioner will need to use a specialist.

.24 If specialized skills are needed to supplement the practitioner's technical knowledge, the practitioner should seek the assistance of a professional possessing such skills, who may be either a member of the engagement team or an outside professional. The practitioner should possess adequate technical knowledge to direct, supervise, and review the specialist's work in the former situation and to understand and evaluate the specialist's work in the latter situation.

.25 When the specialist is not a member of the practitioner's staff, the practitioner should consider the magnitude of the specialist's work in relation to the overall engagement to determine whether the practitioner will be performing a sufficient portion of the engagement to assume overall responsibility.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.26 When the responsible party employs an in-house specialist to develop evidence that is used to support the assertion or presentation, the practitioner should consider whether the practitioner or another member of the engagement team possesses adequate technical knowledge to understand, test, and evaluate the in-house specialist's work or whether the practitioner should seek the assistance from an outside specialist. The practitioner should follow the guidance in Statement on Auditing Standards (SAS) No. 73, *Using the Work of a Specialist* (AICPA, *Professional Standards*, vol. 1, AU sec. 336), in evaluating the competence and objectivity of the responsible party's in-house specialist.

.27 Considerations in selecting a specialist, or using the work of a specialist engaged by the responsible party, include:

a. The specialist's expertise and competence in the subject matter

b. The relevance of the specialist's expertise to the practitioner's objectives in the attest engagement

c. The objectivity of the specialist

d. The nature and extent of the anticipated use of the specialist

.28 If the specialist is employed by the practitioner's firm, the practitioner should follow the guidance in this SOP and the relevant guidance in SAS No. 22, *Planning and Supervision* (AICPA, *Professional Standards*, vol. 1, AU sec. 311). If an outside specialist is engaged, the practitioner should follow the guidance in this SOP and the relevant guidance in SAS No. 73. When the practitioner is considering using the work of a specialist engaged by the responsible party, the practitioner should follow the guidance contained in this SOP and the relevant guidance in SAS No. 73, including evaluating the relationship of the specialist to the responsible party.

.29 Examples of types of matters that ordinarily may require the practitioner to consider using the work of a specialist or having a specialist participate in the GHG engagement include:

- Review of the quality of client-provided data (for example, appropriateness and accuracy)
  - *a.* Determination of whether it is necessary or appropriate to use a derived emissions factor versus a published emissions factor
  - *b.* Determination of the population and selection of appropriate published emissions factors
  - *c.* Assessment of the methodology used to calculate the specific GHG emissions (see paragraphs .39 and .65 of this SOP)
- Review of the work of the client's in-house or external specialist (for example, to assess whether the assumptions underlying the methodology are reasonable)

Criteria

.30 The third general attestation standard states, "The practitioner shall perform the engagement only if he or she has reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users."

.31 Criteria that are established or developed by groups composed of experts that follow due process procedures, including exposure of the proposed criteria for public comment, ordinarily should be considered suitable.

.32 Different industries, regulatory organizations, or organizations acting in a standard-setting role may have developed guidance on measurement relevant to an industry, regulated group, or GHG emissions in general. Alternatively, an entity may develop its own methodology or criteria for measurement of emissions.

.33 The practitioner should consider whether criteria described in paragraph .32 are suitable (see Chapter 1 of SSAE No. 10 [AT sec. 101.23–.32], as amended, for guidance). For guidance on availability of criteria, see Chapter 1 of SSAE No. 10 (AT sec. 101.33–.34), as amended.

.34 Most entities will need to select a framework and further refine measurement criteria, perhaps using software tools for measuring emissions in specific industries or using certain industrial processes, such as cement production or aluminum smelting. The practitioner should review the entity's measurement protocol and consider whether the entity's measurement methods are appropriate.[6]

Attributes to Be Met by GHG Emission Reductions

.35 Various registries and GHG emissions trading schemes have specified attributes to be met by an emission reduction for it to be registered or traded. Common attributes are identified and described below; however, definitions may vary by trading scheme. The practitioner should also be aware that, in the context of a specific registry or emissions trading scheme, there may be additional requirements to be met by the emission reduction.

a. *Ownership.* In many cases, ownership is clear. Examples of such cases include efficiency upgrades at a manufacturing facility or fuel-switching at a power plant. For some project types, however, particularly those with renewable energy and demand-side management projects that offset or displace fossil-fuel emissions, demonstrating ownership can be challenging. Ownership of the reductions may be open to dispute because the reductions do not occur on the site of the project, but rather on the site of a fossil-fueled facility whose power was displaced. These are known as indirect emission reductions because the reductions occur at facilities other than the one where the project has been undertaken. The possibility that the direct source of emissions would claim title to the same reductions claimed by the project developer or that the joint venture partners would claim title to the same reductions of their joint venture (referred to as double-counting) represents a risk that buyers prefer to avoid. It is possible that multiple claimants, such as the owner of the emitting source, technology vendors, and the entity installing the technology, could claim ownership of these reductions.

b. *Real.* An emission reduction is real if it is a reduction in actual emissions resulting from a specific and identifiable action or undertaking that is not a mere change in activity level (for example, due to typical business fluctuations) and net of any leakage to a third party

[6] For example, the WRI/WBCSD GHG Protocol (released on October 23, 2001), when supplemented by appropriate specified methodologies for calculating GHG emissions, may be suitable criteria for calculating an GHG emissions inventory. This is an emerging area; as a result, other suitable frameworks may be developed in the future. See Appendix B, "Sources for GHG Emission Protocols and Calculation Tools" [paragraph .81].

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

or jurisdiction. Leakage occurs when an emission reduction project causes emissions to increase beyond the project's boundaries. Entities entering into an emission reduction project typically must demonstrate that the emission reduction will not cause emissions to increase beyond the project's boundaries.

c. *Quantifiable or measurable.* An emission reduction is quantifiable or measurable if the total amount of the reduction can be determined and the reduction is calculated in an accurate and replicable manner.

d. *Surplus.* An emission reduction is surplus if the reduction is not otherwise required of a source by current regulations or a voluntary commitment to reduce emissions to a specified level.

e. *Establishment of a credible emissions baseline.* Many programs measure emission reductions by comparing a credible emissions baseline without the project to the emissions baseline with the project. To give meaning to a reduction quantity, it should be compared with a credible baseline (that is, a baseline compiled in accordance with the current protocol, using the same boundaries and scope).

f. *Unique.* Credits should be created and registered only once from a specific reduction activity and time.

.36 Some registries or trading schemes may have a requirement for *additionality*. Environmental additionality requires that the emission reductions achieved by the project would not have occurred in the absence of the project (the reduction must be additional to any required reductions; that is, if the entity has taken on a cap, the reduction must be additional to the cap). A credible emission baseline is crucial for an entity to demonstrate additionality. Practitioners should be aware that various GHG registries and regulatory frameworks may not define *additionality* and the terms referred to in paragraph .35 in exactly the same way; thus the practitioner should obtain the official definitions of such terms under the registry or regulatory framework relevant to the engagement.

Materiality

.37 The practitioner should be aware of the materiality guidance in Chapter 1 of SSAE No. 10 (AT sec. 101.67), as amended. The practitioner should also consider whether the applicable GHG registry or voluntary or regulatory framework sets specific materiality limits of which the practitioner should be aware. If a GHG registry or framework sets specific materiality requirements that are more stringent than those of SSAE No. 10, the practitioner should consider whether it is possible to meet such requirements before accepting the engagement.

Uncertainty[7] in the Measurement of GHG Emissions

.38 Uncertainty in emissions estimates can be due to inherent risk or control risk. The practitioner should consider the implications of uncertainty in emissions estimates. Examples of matters that may create or increase uncertainty in emissions estimates include the following:

[7] The term *uncertainty* as used in the field of GHG emissions refers to variability in the measurement of GHG emissions rather than the term *uncertainty* as defined in the auditing literature.

- Use of factors that are poorly researched or uncertain (for example, factors for CH_4 and N_2O from combustion processes)
- Use of average case factors not perfectly matched to specific and varying circumstances (for example, miles per gallon, average $kgCO_2/MWh$ generated)
- Deliberate estimation to compensate for missing data (for example, nonreporting facilities or missing fuel bills)
- Assumptions that simplify calculation of emissions from highly complex processes
- Imprecise measurement of emissions-producing activity (for example, miles traveled in airplanes or rental vehicles, hours per year specific equipment is used)
- Insufficient frequency of measurement to account for natural variability
- Poor calibration of measuring instruments

Consistency

.39 Measurement of the GHG inventory requires consistent application of measurement methods. If the entity has changed measurement methods from one period to the next, the practitioner should consider the implications on the engagement (for example, whether it is essential that the same methods be used because either comparative information is presented or a reduction is being calculated and, if so, whether the entity has restated the prior period's results using the same measurement method as the current period). (See paragraphs .40, .45, .65 and .72 of this SOP.)

Boundaries

.40 It is important for the entity to draw clear *organizational boundaries*. This is particularly salient when accounting for GHG emissions from partially owned entities or facilities. The criteria framework selected by the entity may provide guidance on how to set organizational boundaries. Once organizational boundaries have been set, the entity must set its *operational boundaries*. Leakage may affect the choice of operational boundaries. In planning the engagement, the practitioner needs to understand the boundaries that have been set by the entity to plan the engagement and the potential for leakage. If leakage has occurred, the entity may account for it by adjusting its baseline or by changing its boundaries.

Scopes for Reporting GHG Emissions: Direct and Indirect Emissions

.41 GHG reporting and emission reductions may encompass one or more of the following three scopes of emissions:

- Scope 1: *Direct GHG Emissions.* These are emissions associated with the following:
  - *a.* Production of electricity, heat, or steam
  - *b.* Physical or chemical processing

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

c. Transportation by the entity of, for example, materials, products, waste, and employees
d. Fugitive emissions

- Scope 2: *Indirect GHG Emissions From the Generation of Imported or Purchased Electricity, Heat, or Steam*
- Scope 3: *Other Indirect Emissions,* including the following:
  a. Employee business travel
  b. Outsourced activities, contract manufacturing, and franchises
  c. Transportation by the vendor or contractor of, for example, materials, products, waste, and employees
  d. Emissions from product use and end of life
  e. Employee commuting
  f. Production of imported materials

.42 In the United States there is a focus on both actual emissions and *emissions intensity* (that is, emissions per unit of production). For example, national GHG reduction policy focuses on emission intensity while emissions trading organizations (for example, the Chicago Climate Exchange) trade in emission reduction credits, usually expressed as an annual rate (for example, tons of GHGs per year).

.43 The practitioner should consider whether the proposed scope of the engagement is appropriate, whether it covers (*a*) direct GHG emissions; (*b*) indirect GHG emissions associated with the generation of purchased electricity, heat, or steam; and (*c*) other indirect emissions.

.44 Some reporting schemes may classify these emissions sources differently than those noted in paragraph .41 of this SOP. The practitioner should evaluate the potential for double-counting of emissions and reductions, especially in instances of indirect emissions and shared ownership or control. If the practitioner has been engaged to provide assurance on an entity's indirect emissions, especially those emissions for a supplier not under the direct control of the entity, the practitioner should consider whether he or she can obtain a written assertion from the responsible party and obtain sufficient evidence to form an opinion; the practitioner also should consider the availability or existence of data for emitting sources not under the direct control of the entity.

Baselines

.45 A *baseline* is the amount of the entity's emissions for a specified base year against which any future changes in emissions are evaluated. The baseline should be recalculated, however, for changes in scope and boundaries, subsequent acquisitions, and sales or closing of emitting sources. If the practitioner is engaged to perform the attest service at a date considerably later than the base year, the practitioner should also consider potential differences in the quality of the data and consistency of methodology between the base year and the current year.

Examination Engagement: GHG Inventory

Objective of the Engagement

.46 The criteria selected determine the specific subject matter of the examination engagement and what is to be presented. It is anticipated that appropriate disclosures will be included in the presentation, not just the quantity

of GHG emissions for a period of time, and that the presentation may include or be accompanied by other information, such as the discussion of the responsible party's commitment and strategy, projections, and targets related to its GHG emissions. Therefore, the form of opinion will vary depending upon the information presented under the selected criteria.

.47 The practitioner's objective typically is to express an opinion about whether:

a. The entity's schedule of greenhouse gas emissions (GHG inventory)[8] information is presented, in all material respects, in conformity with the criteria selected by management (see paragraphs .30 through .36 of this SOP); or

b. The responsible party's written assertion about the schedule of greenhouse gas emissions information is fairly stated, in all material respects, based on the criteria selected by management.

Written Assertion by the Responsible Party

.48 A written assertion by a responsible party[9] may be presented to a practitioner in a number of ways, such as in a narrative description, within a schedule, or as part of a representation letter appropriately identifying what is being presented and the point in time or period of time covered. An example of a written assertion on a GHG inventory follows: "XYZ Company asserts that its schedule of GHG emissions information for the year ended December 31, 20XX, is fairly stated, in all material respects, based on [*identify criteria selected by management*]."

Examination Engagement: GHG Emission Reduction Information

Objective of the Engagement

.49 The practitioner's objective is to express an opinion about whether:

a. The entity's GHG emission reduction information related to a specific project or on an entity-wide basis is presented, in all material respects, in conformity with the criteria selected by management; or

b. The responsible party's written assertion about the GHG emission reduction information related to a specific project or on an entity-wide basis is fairly stated, in all material respects, based on the criteria selected by management.

Written Assertion by the Responsible Party

.50 A written assertion may be presented to a practitioner in a number of ways, such as in a narrative description, within a schedule, or as part of a representation letter appropriately identifying what is being presented and the point in time or period of time covered. An example of a written assertion on a

---

[8] An entity's emissions of GHGs for a specified period, typically a year or a series of years, are often referred to as the entity's *GHG inventory*.

[9] The responsible party is defined in Chapter 1, "Attest Engagements," of Statement on Standards for Attestation Engagements No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101.11), as the person or persons, either as individuals or representatives of the entity, responsible for the subject matter.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

GHG emission reduction project follows: "XYZ Company reduced GHG emissions in connection with project ABC by 50,000 tons of CO_2 equivalents for the year ended December 31, 20XX, based on [*identify criteria selected by management*]."

Examples of GHG Emission Reduction Projects

.51 Examples of GHG emission reduction projects include but are not limited to the following:

- Use of renewable energy systems such as wind, solar, and other low emission technologies
- Change in processes to increase energy efficiency/installation and use of more energy efficient equipment
- Carbon sequestration: no-till farming; agricultural grass and tree plantings
- Change from more GHG-intensive fuels to less GHG-intensive fuels (for example, from coal to natural gas or nuclear power)
- Recovery and use of agricultural and landfill methane
- Improvement in the fuel efficiency of vehicle fleets
- Reduction in venting or flaring on offshore oil production platforms (installation of zero flare systems; rapid response to unplanned events)
- Cessation of operations at noneconomical plants
- Demand-side management projects

Prerequisite for an Examination of GHG Emission Reduction Information

.52 As a prerequisite to providing examination-level assurance on GHG emission reduction information, the practitioner should perform procedures on the entity's GHG emissions for the period in which the project took effect sufficient to form an opinion on the GHG emission reduction information.

.53 If one practitioner has examined and reported on an entity's GHG inventory but another practitioner is engaged to examine and report on the entity's GHG emission reduction information, the practitioner engaged to examine and report on the GHG emission reduction information should consider the guidance in SAS No. 1, section 543, *Part of Audit Performed by Other Independent Auditors* (AICPA, *Professional Standards*, vol. 1, AU sec. 543), in deciding whether he or she may rely on the work of the other practitioner. The practitioner also should consider the consistency of the assumptions and methods for measuring the GHG emission reduction to that used in measuring the GHG inventory reported on by the other practitioner. See paragraphs .39 and .65 of this SOP.

.54 Members of professions other than public accounting are subject to their own professional requirements; those requirements may differ from those of the public accounting profession. When a non-CPA has provided verification or certification services (see paragraph .14 of this SOP) with respect to an entity's GHG inventory and the practitioner is engaged to provide assurance on an entity's GHG reduction, the practitioner should perform examination procedures to obtain sufficient evidence with respect to the entity's GHG inventory

as part of examining the entity's GHG emission reduction (for example, the practitioner should consider the appropriateness of the methodology and any emission factors used, and whether the base year emissions were adjusted if needed). The practitioner should consider certain aspects of the specialist's work in accordance with SAS No. 73.

Engagement Performance

Planning the Examination Engagement

.55 The examination should be performed in accordance with attestation standards established by the AICPA (see Chapter 1 of SSAE No. 10). This SOP is not intended to provide all the guidance set forth in the applicable standards established by the AICPA.

.56 The practitioner should establish an understanding with the client regarding the services to be performed. The understanding should include the objectives of the engagement, management's responsibilities, the practitioner's responsibilities, and the limitations of the engagement. The practitioner should document the understanding in the working papers, preferably through a written communication with the client, such as an engagement letter.

.57 Other considerations in planning the examination engagement include the following:

Applicable to GHG Inventories and Reductions

a. Obtain an understanding of the entity's business and ascertain whether the entity has operations, and therefore GHG emission sources, in multiple locations and ascertain the types of GHG emissions produced.

b. Ascertain the organizational and operational boundaries used for the emissions inventory.

c. Ascertain whether there have been any mergers, acquisitions, divestitures, sales of emitting sources, or outsourcing of functions with significant emissions that may require adjustment of the entity's baseline.

d. Ascertain whether all significant sources of emissions have been identified by the entity.

e. Evaluate the potential for double-counting of emissions and, if applicable, reductions.

f. When applicable, obtain an understanding of any regulatory framework(s) (for example, state- or country-specific regulations, permits, or operating licenses governing emissions where the client has operations; the Kyoto Protocol) or any requirements relevant to a voluntary commitment to register or reduce GHG emissions.

g. Obtain a description of how GHG emissions have been calculated and reported, including emissions factors and their justification, and any assumptions on which estimates are based.

h. Obtain an understanding of the internal control over gathering and reporting GHG emissions data, including data assembly and data retention. Effective internal control may reduce the likelihood of material misstatement of an entity's GHG inventory.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

i. Ascertain which protocols were used for measurement of emissions; also ascertain whether they were used in a consistent manner throughout the entity over the period under examination.

j. Consider the use of a specialist.

k. Consider whether a legal letter should be obtained.

Applicable to GHG Reductions Only

l. Ascertain type(s) of emission reduction(s); for instance, switch in fuel type or change in production process (see paragraph .39 of this SOP).

m. Under some registries or regulatory frameworks, the emitting entity is required to engage an outside specialist to evaluate the scientific or engineering basis for the proposed reduction project (sometimes referred to as a validation); those rules may further specify that the party evaluating the science cannot be the same party as the verifier. Where applicable, ascertain whether another reputable party has evaluated the science and found it to be acceptable. Obtain a copy of the related report and consider implications of findings reported.

n. Ascertain whether there are any ownership issues relating to the GHG emission reduction credits to be sold. (For example, in the case of a landfill, does the seller own the landfill or have ownership rights over the emission reduction by virtue of a contract?)

Part of Attest Engagement Performed by Other Practitioners

.58 If another practitioner is providing assurance on the GHG inventory for a subsidiary of the entity, that practitioner also should follow the guidance in this SOP. The practitioner who is engaged to provide assurance for the entity as a whole (hereafter referred to as the principal practitioner) should consider whether the practitioner for the subsidiary has the skill and knowledge required to conduct the engagement. SAS No. 1, section 543, provides guidance on the professional judgments the independent auditor makes in deciding whether he or she may serve as principal auditor and use the work and reports of other independent auditors who have audited the financial statements of one or more subsidiaries, divisions, branches, components, or investments included in the financial statements presented. The principal practitioner may find that guidance helpful when performing an attest engagement on GHG emissions and another practitioner is providing assurance with respect to the GHG emissions of a subsidiary or other component of the client entity. The practitioner for the subsidiary should inquire about whether the subsidiary is using the same protocol, scope of reporting, and boundaries as the parent entity.

Attestation Risk

.59 Attestation risk is the risk that the practitioner may unknowingly fail to appropriately modify his or her attest report on the subject matter or assertion that is materially misstated. It consists of (*a*) the risk (consisting of *inherent risk* and *control risk*) that the subject matter or assertion contains deviations or misstatements that could be material and (*b*) the risk that the practitioner will not detect such deviations or misstatements. The degree of reliability between methods of measurement of emissions varies (inherent risk). For example, the degree of reliability from a stack test may be greater than that from the use of emissions factors. The reliability of the information also depends on the source of the GHGs and the measurement systems in place.

.60 Examples of causes of possible misstatements of GHG inventory or GHG emission reduction information include the following:

- Human error in calculations
- Use of incorrect emissions factors
- Omission from the inventory of emissions from one or more emitting sources
- Omission from the inventory of one or more GHG emissions (for example, omission of methane emissions)
- Failure to properly account for leakage (for example, when the entity has outsourced a major function that accounted for a significant part of its GHG emissions baseline but has not adjusted its baseline to reflect such change)
- Failure to appropriately adjust the baseline for events such as sales or acquisitions of emitting sources
- Existence of one or more significant deficiencies in the entity's internal control over reporting of emissions information
- Double counting of an emission source within the entity

Obtaining Sufficient Evidence

.61 In conducting an attest engagement, the practitioner accumulates sufficient evidence to restrict attestation risk to a level that is, in the practitioner's professional judgment, appropriately low for the high level of assurance that may be imparted by his or her report. A practitioner should select from all available procedures—that is, procedures that assess inherent and control risk and restrict detection risk—any combination that can restrict attestation risk to such an appropriately low level. (See Chapter 1 of SSAE No. 10 [AT sec. 101.51–.53], as amended.)

.62 In an examination engagement of a GHG inventory or an emission reduction, the practitioner should select from the following procedures, among others:

a. Obtain evidence of how emissions were calculated and any underlying methodologies, emission factors, and assumptions.

b. Evaluate techniques used by the client to calculate the emissions or emission reduction, including how completeness and uncertainty are addressed in those calculations. Reductions are calculated by comparing the amount of emissions from one period to another. For clients reporting on a facility basis, this will usually be done annually. For clients reporting on a project basis, the period may vary depending on the nature of the project. Measurement techniques include, but are not limited to, the use of mass balance equations (MBE), emissions factors, stack tests, and direct measurement of emissions, including continuous emission monitors (CEMs). For reductions calculated in comparison to a base year, evaluate adjustments to the base year based on structural changes with the client's organization and on changes in ownership/control of the emitting source(s). (Mergers, acquisitions, sales of emitting sources, outsourcing of certain functions, and joint ventures [practitioners should ascertain how the entity accounts

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

for joint ventures] may cause leakage and would likely require adjustment of the baseline.) Note that adjustments based on organic growth or decline are generally not appropriate.

c. Ascertain whether there have been any changes in the protocol(s) used to calculate emissions. Where applicable, ascertain whether the subsidiary uses the same protocol.

d. Conduct site visits as considered appropriate.

e. Inquire about the business purpose or reason behind such measurements or emission reductions.

f. Ascertain whether there have been any changes in baselines, such as sales or acquisitions of operational facilities or subsidiaries.

g. Where applicable, obtain information about the frequency of meter readings and calibration and maintenance of meters.

h. Examine relevant contracts.

i. Obtain an understanding of the internal control over the subject matter of the contracts and contractual aspects.

j. Trace information to supporting documents.

k. Inquire about the nature of significant judgments and estimates made by management and any uncertainties regarding measurements; the practitioner should consider management's process for and internal control over developing those estimates, inquire about key factors and assumptions underlying those estimates, and evaluate the reasonableness thereof.

l. Where applicable, trace emissions factors used to recognized sources.

m. Ascertain whether emissions factors have been properly applied and whether the underlying assumptions are documented; consider whether those assumptions have a reasonable basis.

n. Perform analytical procedures (for example, change in amounts from the previous year, fluctuations in amounts during the present year, variation from an independent expectation developed by the practitioner).

o. Where applicable, compare emission data to number of units sold for the period.

p. Where applicable, confirm details of the transaction(s) (for example, quantity of methane sold or purchased) with the other party to the transaction.

q. Inquire about whether there have been any changes in production levels (lower emissions due to a drop in production level might not be permanent); obtain evidence supporting production levels.

r. Inquire about whether there have been any communications from regulators concerning emission levels or noncompliance with permits or regulatory schemes.

s. Obtain supporting evidence for any emission reduction credits that are banked, purchased from, or sold to a third party (such information may be included in a public report on a GHG inventory).

t. Obtain and read environmental (or Environmental, Health and Safety [EH&S]) internal audit reports and minutes of audit committee meetings (or other relevant board committees to which the environmental/EH&S internal auditors report).

u. Inquire about whether there have been any subsequent events that would affect the subject matter or the assertion.

v. Obtain a legal letter when considered appropriate (for example, to address (1) noncompliance with regulatory schemes [emissions exceed permitted amount], (2) ownership of credits, or (3) the existence of any unasserted claims).

w. Obtain written representations from management.

.63 In an examination engagement of GHG emission reduction information, the practitioner should also select from the following additional procedures, among others:

a. Obtain evidence of significant changes in the production process, switches from one fuel type to another, or other changes resulting in the emission reduction.

b. Evaluate techniques used by the client to calculate the emission reduction. Reductions are calculated by comparing the amount of emissions from one period to another, typically a year. Measurement techniques include but are not limited to the use of MBEs, stack tests, and metering of gases or effluents, including CEMs.

c. Inquire about the reason or business purpose for the reduction and consider the possible implications with respect thereto. Consider obtaining from management a written representation regarding the reason for the reduction project (See paragraph .36 of this SOP on additionality.)

d. Inquire whether there are any permits applicable to the facility and, if so, examine the permit for factors that may have a bearing on the reduction project (for example, reductions that meet other requirements cannot be transferred).

e. Where applicable, examine reports prepared by the seller for purposes other than the sale of the GHG credit (for example, an emission report filed with a regulatory agency) and check for consistency of information related to the sale.

f. Where applicable, confirm details of emission reduction credits with the relevant GHG registry.

Consideration of Subsequent Events

.64 Events or transactions sometimes occur subsequent to the point in time or period of time of the subject matter being tested but before the date of the practitioner's report that have a material effect on the subject matter and therefore require adjustment or disclosure in the presentation of the subject matter or the assertion. These occurrences are referred to as *subsequent events*. In performing an attest engagement, the practitioner should consider information about subsequent events that comes to his or her attention. While the practitioner has no responsibility to detect subsequent events, the practitioner should inquire of the responsible party (and his or her client if the client is not the responsible party) about whether they are aware of any subsequent events, through the date of the practitioner's report, that would have a material effect on the subject matter or the assertion. If the practitioner has decided to obtain a representation letter from the responsible party, the letter ordinarily would include a representation concerning subsequent events. (Chapter 1 of SSAE No. 10

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

[AT sec. 101.95–.99], as amended, provides additional guidance on the consideration of subsequent events in an attest engagement.) Types of events that may represent a subsequent event in the context of an attest engagement on GHG emissions include the following:

- Changes in baseline emissions due to events such as acquisition or disposition of facilities, change in number of shifts at a facility, or change in production levels
- Destruction of the facility to which an emission reduction relates
- In the case of a GHG emission reduction, unplanned or accidental release of sequestered carbon

Adequacy of Disclosure

.65 When the entity has changed its boundaries or emissions calculation methodologies, and when mergers, divestitures, acquisitions, or closures occur, the practitioner should consider whether those changes are likely to be significant to the users of the report. If so, the practitioner should determine whether the criteria are clearly stated or described for each of the dates or periods, and whether the changes have been adequately disclosed. (See Chapter 1 of SSAE No. 10 [AT sec. 101.70 and .76–.77].) See paragraph .72 of this SOP for reporting guidance.

Representation Letter

.66 In an examination engagement, a practitioner should consider obtaining a representation letter from the responsible party. Written representations from the responsible party ordinarily confirm representations explicitly or implicitly given to the practitioner, indicate and document the continuing appropriateness of such representations, and reduce the possibility of misunderstanding concerning the matters that are the subject of the representations. Examples of matters that might appear in such a representation letter include the following:

a. A statement acknowledging responsibility for the subject matter and, when applicable, the assertion

b. A statement acknowledging responsibility for selecting the criteria, where applicable

c. A statement acknowledging responsibility for determining that such criteria are appropriate for its purposes, where the responsible party is the client

d. Management's assertion about the subject matter based on the criteria selected

e. A statement acknowledging ownership of the emissions or emission reductions

f. A statement that all known matters contradicting the assertion or presentation and any communication from regulatory agencies affecting the subject matter or the assertion have been disclosed to the practitioner

g. A statement that management (responsible party) has disclosed to the practitioner all significant deficiencies in the design or operation of internal control over its GHG inventory

h. A statement regarding the availability of all records relevant to the subject matter

i. A statement that management has responded fully to all inquiries made by the practitioner during the engagement

j. A statement that any known events subsequent to the period (or point in time) of the subject matter being reported on that would have a material effect on the subject matter (or, if applicable, the assertion) have been disclosed to the practitioner

k. Other matters as the practitioner deems appropriate

l. Relevant to an emission reduction, a statement regarding the business purpose of the emission reduction project

m. Relevant to an emission reduction, a statement that the reduction is both real and additional to any requirements

Appendix C [paragraph .82] includes an illustrative management representation letter.

.67 When the client is not the responsible party, the practitioner should consider obtaining a letter of written representations from the client as part of the attest engagement. Examples of matters that might appear in such a representation letter include the following:

a. A statement regarding whether the client is aware of any matters that might contradict the subject matter or the assertion

b. A statement that all known events subsequent to the period (or point in time) of the subject matter being reported on that would have a material effect on the subject matter (or, if applicable, the assertion) have been disclosed to the practitioner

c. A statement acknowledging the client's responsibility for selecting the criteria, where applicable

d. A statement acknowledging the client's responsibility for determining that such criteria are appropriate for its purposes

e. Other matters as the practitioner deems appropriate

.68 If the responsible party or the client refuses to furnish all written representations that the practitioner deems necessary, the practitioner should consider the effects of such a refusal on his or her ability to express an opinion about the subject matter. If the practitioner believes that the representation letter is necessary to obtain sufficient evidence to express an opinion, the responsible party's or the client's refusal to furnish such evidence in the form of written representations constitutes a limitation on the scope of an examination sufficient to preclude an unqualified opinion and is ordinarily sufficient to cause the practitioner to disclaim an opinion or withdraw from an examination engagement. However, based on the nature of the representations not obtained or the circumstances of the refusal, the practitioner may conclude, in an examination engagement, that a qualified opinion is not appropriate. Further, the practitioner should consider the effects of the refusal on his or her ability to rely on other representations.

Reporting

.69 SSAE No. 10, as amended, permits the practitioner to report either on the written assertion or directly on the subject matter to which the assertion relates. However, as stated in Chapter 1 of SSAE No. 10 (AT sec. 101.66), as

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

amended, if conditions exist that, individually or in combination, result in one or more material misstatements or deviations from the criteria, the practitioner should modify the report and, to most effectively communicate with the readers of the report, should ordinarily express his or her opinion directly on the subject matter, not on the assertion.

.70 The report should contain language describing inherent limitations, such as the following:

> Environmental and energy use data are subject to inherent limitations, given the nature and the methods used for determining such data. The selection of different but acceptable measurement techniques can result in materially different measurements. The precision of different measurement techniques may also vary.

.71 The precision of different measurement techniques may vary; for example, stack tests would provide more precise measurements than the use of published emission factors.

.72 When the measurement methods and the application thereof have not been consistent from period to period, the practitioner's report should be modified. The form of the modification depends on whether the presentation or management's assertion appropriately disclose those facts or whether prior periods, if presented or used in the calculation of a reduction, are restated. If the responsible party (that is, in most cases, the client) does not appropriately restate the baseline and prior period(s) inventory for the change, the practitioner should include an explanatory paragraph in the practitioner's report describing the lack of consistency and should express a qualified or an adverse opinion due to a departure from the criteria. If the responsible party does appropriately restate, the practitioner should include an explanatory paragraph (following the opinion paragraph) in his or her report that refers to the change in the measurement methods or application.

.73 When the trading scheme or GHG registry contains specific materiality requirements that are more stringent than those of Chapter 1 of SSAE No. 10, as amended, the practitioner may wish to consider including a reference to those requirements in the attest report.

.74 Chapter 1 of SSAE No. 10, as amended, requires the report on an attest examination engagement to contain a statement of management's responsibility for the subject matter or the assertion. The statement of management's responsibility may also address management's responsibility for selecting and adhering to the criteria used.

.75 Appendix D [paragraph .83] presents illustrative reports for the examination of an entity's GHG emissions information for a period of time. Appendix E [paragraph .84] presents illustrative reports for the examination of an entity's GHG emission reduction information.

.76 The practitioner, in his or her attest report, may wish to refer to the report of another practitioner under the following circumstances:

- When reporting on an attest engagement on GHG emissions and another practitioner is providing assurance with respect to the GHG emissions of a subsidiary or other component of the client entity
- When reporting on an attest engagement on an emission reduction and another practitioner has examined and reported on the entity's emissions inventory

See Appendix D [paragraph .83], Example 3, for an example examination report that refers to the report of another practitioner.

.77 The practitioner reporting on the emission reduction would only be able to divide responsibility with the practitioner reporting on the GHG inventory information if both practitioners are reporting on emissions information for the same emission source(s) addressed by the reduction project. For example, if practitioner A reported on a GHG inventory for Plant X for which practitioner B is reporting on the emission reduction, practitioner B may divide responsibility by referring in his or her report to the work of practitioner A. However, if practitioner A reported on the company's GHG inventory for its nationwide operations taken as a whole, practitioner B, who is reporting only on the reduction project at Plant X, would need to perform sufficient additional procedures on the GHG inventory at Plant X and should not refer in his or her report to the work of practitioner A.

Attest Documentation

.78 SSAE No. 11, *Attest Documentation* (AICPA, *Professional Standards*, vol. 1, AT sec. 101.100–.107), sets documentation requirements. The practitioner should be aware that the GHG registry or regulatory scheme relevant to the attest engagement may have set additional documentation requirements for those providing assurance on GHG emissions inventories or reductions (sometimes referred to as *verifiers*).

Effective Date

.79 This SOP is effective for reports on attest engagements on GHG emissions information issued on or after December 15, 2003. Early implementation is permitted.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.80

Appendix A

Glossary

Additionality. A project is *additional* if it would not have happened but for the incentive provided by the credit trading program (for example, Clean Development Mechanism [CDM] or Joint Implementation [JI]). The Kyoto Protocol specifies that only projects that provide emission reductions that are *additional* to any that would occur in the absence of the project activity shall be awarded certified emission reductions (CERs) in the case of CDM projects or emission reduction units (ERUs) in the case of JI projects. This is often referred to as environmental additionality. Financial additionality is the notion that a project is made commercially viable through its ability to generate value in the form of certified emission reductions. Various greenhouse gas (GHG) registries or regulatory frameworks may define these terms differently.

Allowance. An allowance is the unit of trade under a trading system. In a closed trading system, trading of allowances is permitted only between parties subject to the scheme or regulatory system. Allowances grant the holder the right to emit a specific quantity (for example, one ton) of emissions once. The total quantity of allowances issued by regulators dictates the total quantity of emissions possible under the system. Allowances are typically granted to emitters by governmental entities or agencies either for free or for a fee. At the end of each compliance period each source must surrender sufficient allowances to cover its emissions during that period. In an open trading system, trades can be made between parties within the system and parties outside the system.

Baseline. A baseline refers to the level of emissions during some specified period, often referred to as a "baseline year." Emission reductions targets are often expressed as a percent reduction from the baseline emission level.

Boundaries. There are two types of boundaries: organizational and operational. When accounting for GHG emissions from partially owned entities, it is important to draw clear organizational boundaries, which should be consistent with the organizational boundaries that have been drawn up for financial reporting purposes. After the entity has determined its organizational boundaries in terms of the entities it owns or controls, it must then set operational boundaries with respect to direct and indirect emissions. The WRI/WBCSD Greenhouse Gas Protocol provides additional guidance on setting organizational and operational boundaries with respect to GHG emissions.

Certification. The process used to ensure that a given participant's GHG inventory (either the baseline or the annual result) has met a minimum quality standard and complied with a specific registry's procedures and protocols for calculating and reporting GHG emissions is often referred to as a certification. Many perceive that a certification would be required to provide a higher level of assurance than a verification or a practitioner's examination report.

Closed trading system. In a closed trading system, trading of allowances is permitted only between parties subject to the scheme or regulatory system. (See also "Open trading system.")

Credit. The term *credit* is used in a number of contexts, most commonly in relation to emission reductions that have been achieved in excess of the required amount for one of the following:

- The Kyoto Protocol's Joint Implementation (JI), also known as emission reduction units (ERUs)
- The Kyoto Protocol's Clean Development Mechanism (CDM), specifically known as Certified Emission Reductions (CERs)
- The Kyoto-related and voluntary trading schemes

Data assembly. Data assembly is the process the client uses to "roll-up" individual site or process level information to a facility- or corporate-level report. For example, the entity may choose to have a manufacturing unit report only the number of widgets it produced each year and have corporate level environmental staff apply the appropriate emission factors to calculate the resultant emissions. Alternatively, the entity may choose to have all calculations done at the operational level and assign only quality control responsibilities to the corporate staff.

Direct GHG emissions. Direct GHG emissions, or Scope 1 reporting under the WRI/WBCSD Greenhouse Gas Protocol, represent emissions associated with the following:

- Production of electricity, heat, or steam
- Physical or chemical processing
- Transportation by the entity of, for example, materials, products, waste, and employees
- Fugitive emissions

GHG inventory. An entity's GHG emissions for a compliance period, such as a year, is referred to as its GHG inventory.

Indirect GHG emissions. Indirect emissions, or Scope 2 reporting under the WRI/WBCSD Greenhouse Gas Protocol, represent emissions from the generation of imported or purchased electricity, heat, or steam. Other indirect emissions, or Scope 3 reporting under the GHG Protocol, include the following:

- Employee business travel
- Outsourced activities, contract manufacturing, and franchises
- Transportation by the vendor or contractor of, for example, materials, products, waste, and employees
- Emissions from product use and end of life
- Employee commuting
- Production of imported materials

Inventory. See "GHG inventory."

Leakage. Leakage occurs when an emission reduction project causes emissions to increase beyond the project's boundaries. Entities entering into an emission reduction project typically must demonstrate that the emission reduction will not cause emissions to increase beyond the project's boundaries.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Offset. Offsets are created when a source makes voluntary, permanent emission reductions that are in surplus to any required reductions. Entities that create offsets can trade them to other entities to cover growth or relocation. Regulators may be required to approve each trade. Regulators normally require a portion of the offsets to be retired to ensure an overall reduction in emissions. Offsets are an open system (an open system is one in which trades can be made between parties within the system and parties outside the system). One offset is an emission reduction that a pollution source has achieved in excess of permitted levels and/or required reductions. The excess amount is the credit and can be sold on the market.

Open trading system. In an open trading system, trades can be made between parties within the system and parties outside the system. (See "Closed trading system.")

Permit. Permits are certificates of operation that allow holders to operate a facility provided they do not exceed a specified rate (kilograms/tons per day). Permits are often designated as an upper limit. Because few systems operate at 100 percent of capacity at all times, actual emissions are usually a fraction of the theoretical upper limit of allowed emissions. However, as new permits become harder to obtain, existing operations are motivated to increase their level of operations under their existing permits (for example, by adding a second shift, thereby legally increasing the overall quantity of emissions). Allowances (see "Allowances") are transferable, while the permit itself is attached to a specific installation or site.

Validation. The process used to ensure that a given project, if implemented, can achieve the projected reduction results. The entity may validate the feasibility of the design of an emission reduction project internally, or the entity may engage an outside party (typically an engineering or a consulting firm) to perform the validation.

Verification. A *verification* is the objective and independent assessment of whether the reported GHG inventory properly reflects the GHG impact of the entity in conformance with pre-established GHG accounting and reporting standards.

Verified emission reductions (VERs). VERs are created, in the absence of government rules, by project-based activities that are defined by the buyer and seller and verified by a third party.

Emissions Trading Programs

Baseline-and-credit program. In a baseline-and-credit program (that is, credit- or project-based trading), each participant is provided a baseline against which its performance is measured. If an action is taken to reduce emissions, the difference between the baseline and the actual emissions, where actual emissions are less than the baseline, can be credited and traded. The baseline established for crediting purposes can be fixed or dynamic, decreasing or increasing over time. The key distinction between a cap-and-trade program and a baseline-and-credit program is that in the former, regulated sources' emissions are required to remain under an emissions cap, which is a fixed quantity. Such a limit is not necessarily imposed in a baseline-and-credit program. The Kyoto Protocol's Clean Development Mechanism (CDM), for example, would operate as a baseline-and-credit program.[10]

---

[10] Adapted from Richard Rosenzweig and Josef Janssen, *The Emerging International Greenhouse Gas Market* (Arlington, Va.: Pew Center on Global Climate Change, 2002).

Cap-and-trade program. In a cap-and-trade program (that is, allowance-based trading), the maximum level of emissions that can be released from sources is set by the control authority. This level is the cap. All sources are required to have allowances to emit. The allowances are freely transferable; they can be bought or sold. The control authority issues exactly the number of allowances needed to produce the desired emission level. The largest example of this kind of system, and the most comprehensive trading program to date, is Title IV of the U.S. Clean Air Act Amendments of 1990, under which allowances of SO_2 can be traded to comply with an emissions cap.[11]

[11] See footnote 1.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.81

Appendix B

Sources for GHG Emission Protocols and Calculation Tools

These tools are included solely as informational resources. They are not, however, endorsed by the AICPA.

World Resource Institute/World Business Council for Sustainable Development (WRI/WBCSD) Greenhouse Gas Protocol	www.ghgprotocol.org/standard/standard.htm	
GHG Calculation Tools (cross-sector and sector specific tools)	www.ghgprotocol.org/standard/tools.htm	This Web site contains tools for the following: • Calculating N_2O emissions from the production of adipic acid • Calculating CO_2 and PFC emissions from the production of aluminum • Calculating CO_2 emissions from the production of ammonia • Calculating CO_2 emissions from the production of cement • Calculating HFC-23 emissions from the production of HCFC-22 • Calculating CO_2 emissions from the production of iron and steel • Calculating CO_2 emissions from the production of lime • Calculating N_2O emissions from the production of nitric acid • Calculating CO_2 emissions from mobile combustion • Calculating GHG emissions from office-based organizations • Calculating GHG emissions from pulp and paper mills

(continued)

		• Calculating PFC emissions from the production of semiconductor wafers • Calculating CO_2 emissions from stationary combustion
California Climate Action Registry	www.climateregistry.org	• Certification Protocol (Committee report) June 2002 • General Reporting Protocol (Committee report) June 2002

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.82

Appendix C

Illustrative Management Representation Letter

[*Date*]

[*Name of CPA Firm*]

We are providing this letter in connection with your examination of our assertion(s) that [*describe assertion(s), for example, the accompanying schedule of greenhouse gas (GHG) emissions information for XYZ Company for the year ended December 31, 20XX, is presented in conformity with (identify criteria)*].

We are responsible for [*describe assertions and subject matter*]. We further confirm that we are responsible for the selection of [*identify criteria used, for example the World Resource Institute / World Business Council for Sustainable Development Greenhouse Gas Protocol*] as the criteria against which you are evaluating our assertion(s). Further we confirm that we are responsible for determining that [*identify criteria*] represent appropriate criteria for our purposes.

We confirm, to the best of our knowledge and belief, the following representations made to you during your examination:

1. We are not aware of any matters contradicting the assertion(s), nor have we received any communications from regulatory agencies or [*identify organizations to which the company reports GHG emissions*] affecting the subject matter or our assertion(s) on such subject matter.
2. We have disclosed to you all significant emission sources. There are no material emissions that have not been recorded in the greenhouse gas (GHG) emission records underlying our assertion referred to above.
3. There has been no (*a*) fraud involving management or employees who have significant roles in the Company's processes and procedures relating to measurements of emissions in conformity with the criteria specified above or (*b*) fraud involving others that could have a material effect on measurements of emissions in conformity with the selected criteria.
4. There are no significant deficiencies in the design or operation of the Company's internal control over its GHG inventory.
5. We have made available to you all records relevant to your examination of the aforementioned subject matter or assertion(s).
6. We have responded fully to all inquiries made by you during the engagement.
7. [*Add additional representations as deemed appropriate.*]

We are not aware of any events that occurred subsequent to the period being reported on and through the date of this letter that would have a material effect on the aforementioned subject matter or assertion(s).

[*Name of chief executive officer and title*]

[*Name of corporate environmental officer and title*]

[*The following illustrates an example of a written assertion and additional representations that should be obtained in connection with GHG emission reductions:*]

Example assertion in connection with an emission reduction:

XYZ Company reduced GHG emissions in connection with project ABC by 50,000 tons of CO_2 equivalents for the year ended December 31, 20XX, based on [*identify criteria selected by management*].

Additional representations:

The GHG emission reduction project was undertaken for the purpose of [*describe business purpose*]. The GHG emission reductions were achieved as a direct result of the project and not as a result of any changes in activity level. The GHG emission reductions related to the project are both real and additional to any requirements. Further, we have satisfactory title to all GHG emission reduction credits related to the project, and there are no liens or encumbrances on such GHG emission reduction credits, nor have any GHG emission reduction credits been pledged as collateral.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.83

Appendix D

Illustrative Examination Reports on GHG Emissions Information

The report examples illustrated herein are for general use; see Chapter 1, "Attest Engagements," of Statement on Standards for Attestation Engagement No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101.78–.83), as amended, for requirements and guidance on restricting the use of an attest report.

Example 1—Reporting on Subject Matter

Independent Accountant's Report

We have examined the accompanying schedule of greenhouse gas emissions information of XYZ Company (the Company) for [*identify period; for example, the year ended December 31, 20XX*]. XYZ Company's management is responsible for the schedule of greenhouse gas emissions information. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included obtaining an understanding of the nature of the Company's greenhouse gas emissions and its internal control over greenhouse gas emissions information, examining, on a test basis, evidence supporting the Company's schedule of greenhouse gas emissions information and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Environmental and energy use data are subject to inherent limitations, given the nature and the methods used for determining such data. The selection of different but acceptable measurement techniques can result in materially different measurements. The precision of different measurement techniques may also vary.

In our opinion, the schedule referred to above presents, in all material respects, the greenhouse gas emissions information of XYZ Company for [*identify period; for example, the year ended December 31, 20XX*] in conformity with [*identify criteria*].

[*Signature*]

[*Date*]

Example 2—Reporting on Management's Assertion

Independent Accountant's Report

We have examined management's assertion that [*identify the assertion—for example, the accompanying schedule of greenhouse gas emissions information for XYZ Company for the year ended December 31, 20XX, is presented in conformity with (identify criteria)*]. XYZ Company's management is responsible for the assertion. Our responsibility is to express an opinion on the assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included obtaining an understanding of the nature of the Company's greenhouse gas emissions and its internal control over greenhouse gas emissions information, examining, on a test basis, evidence supporting management's assertion and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Environmental and energy use data are subject to inherent limitations, given the nature and the methods used for determining such data. The selection of different but acceptable measurement techniques can result in materially different measurements. The precision of different measurement techniques may also vary.

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on [*identify criteria*].

[*Signature*]

[*Date*]

Example 3—Reporting on Subject Matter; Includes Reference to the Report of Another Practitioner

Independent Accountant's Report

We have examined the accompanying schedule of greenhouse gas emissions information of XYZ Company and subsidiaries (the Company) for the year ended December 31, 20XX. XYZ Company's management is responsible for the schedule of greenhouse gas emissions information. Our responsibility is to express an opinion based on our examination. We did not examine the schedule of greenhouse gas emissions information for B Company, a wholly owned subsidiary, which reflected 20 percent of the related consolidated emissions. This schedule was examined by other accountants, whose report has been furnished to us and our opinion, insofar as it relates to the amounts included for B Company, is based solely on the report of the other accountants.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included obtaining an understanding of the nature of the Company's greenhouse gas emissions and its internal control over greenhouse gas emissions information, examining, on a test basis, evidence supporting the Company's schedule of greenhouse gas emissions information and performing such other procedures as we considered necessary in the circumstances. We believe that our examination and the report of the other accountants provide a reasonable basis for our opinion.

Environmental and energy use data are subject to inherent limitations, given the nature and the methods used for determining such data. The selection of different but acceptable measurement techniques can result in materially different measurements. The precision of different measurement techniques may also vary.

In our opinion, based on our examination and the report of the other accountants, the schedule referred to above presents, in all material respects, the greenhouse gas emissions information of XYZ Company for the year ended December 31, 20XX, in conformity with [*identify criteria*].

[*Signature*]

[*Date*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.84

Appendix E

Illustrative Examination Reports on GHG Emission Reduction Information

The report examples illustrated herein are for general use; see Chapter 1, "Attest Engagements," of Statement on Standards for Attestation Engagements No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101.78-.83), as amended, for requirements and guidance on restricting the use of an attest report.

Example 1—Reporting on Subject Matter

Independent Accountant's Report

We have examined the schedule of greenhouse gas emission reduction information of XYZ Company related to the ABC project for the year ended December 31, 20XX. XYZ Company's management is responsible for the greenhouse gas emission reduction information. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included obtaining an understanding of the nature of the Company's greenhouse gas emissions and its internal control over greenhouse gas emission reduction information, examining, on a test basis, evidence supporting the greenhouse gas emission reduction information and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Environmental and energy use data are subject to inherent limitations, given the nature and the methods used for determining such data. The selection of different but acceptable measurement techniques can result in materially different measurements. The precision of different measurement techniques may also vary.

Our engagement related to the specific project identified above. We were not engaged to, and did not, examine XYZ Company's entity-wide greenhouse gas emissions inventory or whether the entity has reduced its entity-wide greenhouse gas emissions inventory. Accordingly, we do not express an opinion or any other form of assurance on its entity-wide greenhouse gas emissions inventory or changes from prior periods.

In our opinion, the schedule of greenhouse gas emission reduction information of XYZ Company related to ABC project for the year ended December 31, 20XX is presented, in all material respects, in conformity with [*identify criteria*].

[*Signature*]

[*Date*]

Example 2—Reporting on Management's Assertion

Independent Accountant's Report

We have examined management's assertion that [*identify the assertion; for example, XYZ Company reduced GHG emissions in connection with project ABC by 50,000 tons of CO_2 equivalents for the year ended December 31, 20XX*] based on [*identify criteria selected by management*]. XYZ Company's management is responsible for the assertion. Our responsibility is to express an opinion on the assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included obtaining an understanding of the nature of the Company's greenhouse gas emissions and its internal control over greenhouse gas emission reduction information, examining, on a test basis, evidence supporting management's assertion and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Environmental and energy use data are subject to inherent limitations, given the nature and the methods used for determining such data. The selection of different but acceptable measurement techniques can result in materially different measurements. The precision of different measurement techniques may also vary.

Our engagement related to the specific project identified above. We were not engaged to, and did not, examine XYZ Company's entity-wide greenhouse gas emissions inventory or whether the entity has reduced its entity-wide greenhouse gas emissions inventory. Accordingly, we do not express an opinion or any other form of assurance on its entity-wide greenhouse gas emissions inventory or changes from prior periods.

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the [*identify criteria*].

[*Signature*]

[*Date*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Joint Task Force of the AICPA and CICA on Sustainability Reporting

BETH A. SCHNEIDER, *Chair*
RON BERGIN
DENNIS R. JENNINGS
ERIC ISRAEL
JOHN L. PAYNE, P.E.
EMIL RAGONES
ALAN WILLIS

AICPA Staff

CHARLES E. LANDES
Director
Audit and Attest Standards

JANE M. MANCINO
Technical Manager
Audit and Attest Standards

J. LOUIS MATHERNE
Director
Business Assurance and Advisory Services

CICA Staff

GREGORY P. SHIELDS, CA
Director
Assurance Services Development

The Joint Task Force of the AICPA and CICA on Sustainability Reporting gratefully acknowledges the contributions of Michael J. Radcliffe in the development of this SOP.

[The next page is 31,701.]

Section 14,410

Statement of Position 04-1
Auditing the Statement of Social Insurance

November 22, 2004

NOTE

This Statement of Position (SOP) represents the recommendations of the AICPA's Social Insurance Task Force (task force) regarding the application of Statements on Auditing Standards to audits of statements of social insurance prepared in accordance with the standards of the Federal Accounting Standards Advisory Board (FASAB). Audits of federal government agencies are also governed by *Government Auditing Standards* ("the Yellow Book") and applicable Office of Management and Budget (OMB) guidance.

The Auditing Standards Board has found the recommendations in this SOP to be consistent with existing standards covered by Rule 202 of the AICPA Code of Professional Conduct. AICPA members should be aware that they may have to justify departures from the recommendations in this SOP if the quality of their work is questioned.

Financial reporting for social insurance programs and auditing of statements of social insurance are developing areas of practice. As auditors gain additional experience in implementing this SOP, the task force will monitor and consider feedback from auditors and users of statements of social insurance, and will determine whether additional or revised guidance on this subject is needed.

Introduction

.01 The Federal Accounting Standards Advisory Board (FASAB) establishes accounting standards for reporting information about the following social insurance programs:

a. Old-Age Survivors and Disability Insurance (OASDI or Social Security)

b. Medicare (Hospital Insurance [HI] and Medicare Supplementary Medical Insurance [SMI])

c. Railroad Retirement benefits

d. Black Lung benefits

e. Unemployment Insurance

.02 FASAB standards require the financial statements of the federal agencies responsible for the Social Security, Medicare, Railroad Retirement, and Black Lung programs and the financial statements of the federal government-wide entity to present a statement of social insurance as a basic financial statement. FASAB standards require these agencies and the government-wide entity to report:

a. The estimated present value of the income to be received from or on behalf of the following groups during a projection[1] period sufficient to illustrate the long-term sustainability of the social insurance programs:

(1) Current participants who have not yet attained retirement age

(2) Current participants who have attained retirement age

(3) Individuals expected to become participants

b. The estimated present value of the benefit payments to be made during that same period to or on behalf of the groups listed in item *a*

c. The estimated net present value of the cash flows during the projection period (the income described in item *a* over the expenditures described in item *b*, or the expenditures described in item *b* over the income described in item *a*)

d. In notes to the statement of social insurance:

(1) The accumulated excess of all past cash receipts, including interest on investments, over all past cash disbursements within the social insurance program represented by the fund balance at the valuation date

(2) An explanation of how the net present value referred to in item *c* above is calculated for the closed group[2] (Paragraph 27(3)(i) of Statement of Federal Financial Accounting Standards [SFFAS] No. 17, *Accounting for Social Insurance*, identifies the information to be included in this explanation.)

(3) Comparative financial information for items *a*, *b*, *c*, and *d*(1) for the current year and for each of the four preceding years

(4) The significant assumptions used in preparing the estimates

.03 The income, expenditures, and net present value of cash flows recognized in the statement of social insurance differ from traditional concepts of income and expenditures for retirement and health benefit programs. Financial reporting for social insurance programs includes estimates of income and expenditures not only for current program participants but also for individuals expected to become participants in social insurance programs in the future. In paragraphs 26 through 28 of the basis for conclusions section of SFFAS No. 25, *Reclassification of Stewardship Responsibilities and Eliminating the Current Services Assessment*, FASAB acknowledges this difference and explains why the recognition of such amounts is essential to the fair presentation of federal financial statements:

> 26. The Board believes that the SOSI [statement of social insurance] should be treated as a basic financial statement because it is essential to fair presentation and is important to achieve the objectives of federal financial repor-ting. The related stewardship objectives include helping users to assess the impact

---

[1] The AICPA *Guide for Prospective Financial Information* (Guide) defines the term *projection* and differentiates it from the term *forecast*. In this Statement of Position (SOP), the term projection is used in its generic sense, as it is used in standards issued by the Financial Accounting Standards Advisory Board (FASAB) and the federal agencies that administer social insurance programs. The use of the term *projection* in this SOP is not intended to suggest that information presented in the statement of social insurance is a projection as defined in the Guide or that the provisions of the Guide would apply to the audit of the statement of social insurance.

[2] The *closed group* is defined as those persons who, as of a valuation date, are participants in a social insurance program as beneficiaries, covered workers, or payers of earmarked taxes or premiums.

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

on the country of the Government's activities, determine whether the Government's financial position improved or deteriorated over the period, and predict whether future budgetary resources will likely be sufficient to sustain public services and meet obligations as they come due. In that regard, the multi-trillion dollar obligations associated with Social Insurance over the next 75 years could significantly exceed the largest liabilities currently recognized in the U.S. Government Balance Sheet.

27. The Board acknowledges that there is great uncertainty inherent in long term projections, but believes that if the uncertainty is suitably disclosed—as is required by SFFAS 17—it need not preclude designating the information as a basic financial statement, essential for fair presentation in conformity with GAAP . . .

28. Even within the context of historical financial reporting, the Board notes that accrual-basis "historical" financial statements include many measurements that involve assumptions about the future. The distinction between reporting on the financial effects of events that have occurred and the effects of future events depends, obviously, upon the definition of the event. The information required by SFFAS 17 reports on the financial effects of existing law and demographic conditions and assumptions, just as the pension obligation at a point in time is based on existing conditions. In that sense, Social Insurance information can be viewed as reflecting events that have occurred and, therefore, as "historical."

Applicability

.04 This Statement of Position (SOP) provides guidance to auditors in auditing the statement of social insurance for the following social insurance programs:

a. Old-Age Survivors and Disability Insurance (OASDI or Social Security)

b. Medicare (Hospital Insurance [HI] and Medicare Supplementary Medical Insurance [SMI])

c. Railroad Retirement benefits

d. Black Lung benefits

As permitted by Statement on Auditing Standards (SAS) No. 1, section 543, *Part of Audit Performed by Other Independent Auditors* (AICPA, *Professional Standards*, vol. 1, AU sec. 543), as amended, a principal auditor may fulfill the requirements of this SOP by using work that other independent auditors have performed in conformity with the provisions of this SOP. For example, for the OASDI program, the auditor of the federal government-wide financial statements may use the work and report of the auditor of the Social Security Administration's statement of social insurance.

Management's Responsibilities

.05 The agency's management (management) is responsible for preparing the statement of social insurance and the estimates underlying it in conformity with generally accepted accounting principles. In doing so, management must determine its best estimate[3] of the economic and demographic conditions that

[3] Paragraph 25 of FASAB Statement of Federal Financial Accounting Standards (SFFAS) No. 17, *Accounting for Social Insurance*, states, in part, "The projections and estimates used should be based on the entity's best estimates of demographic and economic assumptions, taking each factor individually and incorporating future changes mandated by current law." Certain agencies prepare social insurance information using assumptions prepared by a board of trustees. Auditors should consider such assumptions to represent the agency's "best estimates" if the trustees have characterized them as such, and agency management has determined them to be reasonable. With respect to these assumptions, the auditor should perform audit procedures that are consistent with the guidance in paragraphs .09 through .36 of this SOP.

will exist in the future. Because estimates in the statement of social insurance are based on subjective as well as objective factors, management must use judgment to estimate amounts included in the statement of social insurance. Management's judgment ordinarily is based on its knowledge and experience about past and current events and its assumptions about conditions it expects to exist. Management is responsible for the accuracy and completeness of the statement of social insurance.

Preparing Social Insurance Estimates

.06 Management is responsible for preparing the estimates underlying the statement of social insurance. That process ordinarily consists of:

a. Identifying the relevant factors that may affect the estimates

b. Developing assumptions that represent management's best estimate of circumstances and events with respect to the relevant factors

c. Accumulating relevant, sufficient, and reliable data on which to base the estimates

d. Determining the estimated amounts based on assumptions and other relevant factors

e. Determining that the estimates are presented in conformity with generally accepted accounting principles and that disclosure is adequate

Conceptual Model

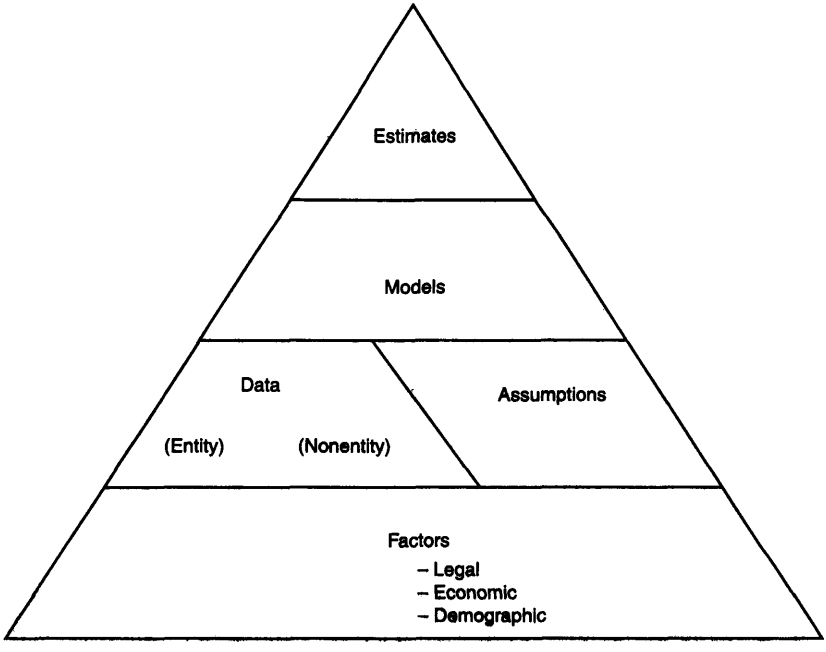


Figure 1: Elements of the Process of Developing Social Insurance Estimates

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

.07 Figure 1, "Elements of the Process of Developing Social Insurance Estimates," is a conceptual model depicting the elements of the process that results in the statement of social insurance. It is not intended to depict the[4] actual process used by an organization to develop the statement of social insurance. With the assistance of internal and external specialists, management considers, identifies, and documents factors, assumptions, and data that serve as input to a model for developing estimates. When auditing the statement of social insurance, the auditor should be aware that the factors, data, assumptions, and models used to develop the statement of social insurance are closely interrelated and may not be separable. Following are definitions of the terms used in Figure 1:

a. *Factors.* The elements or variables that affect income or expenditures for a program and for which data must be gathered and assumptions must be generated, for example, legal, economic, and demographic factors. An example of a factor is the number of individuals reaching age 65 in a specific year.

b. *Assumptions.* Expectations about what will happen in the future. An example of an assumption is that there will be a 1 percent increase in the number of women working outside the home in each of the next five years. An assumption is expressed as a value or direction assigned to a factor.

c. *Data.* Organized factual information used for analysis or to make decisions. An example is census data and classifications of that data, such as the population classified by sex or age. Data may be developed within the entity that prepares the statement of social insurance or it may come from sources outside the entity.

d. *Models.* Methods or formulas for mathematically expressing how the assumptions and data relate to each other. For example, a model might indicate that a 1 percent decline in the birth rate in a given year will result in a 0.2 percent decrease in social insurance income and benefit payments 10 years later. A model is a set of coded instructions, rules, or procedures used to perform a desired sequence of events or to obtain a result. Typically, models are developed by using various computer applications.

e. *Estimates.* The amounts or valuations that result after processing the factors, data, and assumptions in a model. These estimates will be used in preparing the statement of social insurance.

Designing and Implementing Internal Control Related to Estimates

.08 To help ensure the accuracy and completeness of the statement of social insurance, management should design and implement controls consistent with *Standards for Internal Control in the Federal Government* issued by the Government Accountability Office (GAO; formerly the General Accounting Office). An entity's internal control may reduce the likelihood of material misstatements of estimates. Among the aspects of internal control that are relevant to the process of developing estimates are the following:

---

[4] Office of Management and Budget (OMB) Circular No. A-123, *Management Accountability and Control*, Section II "Establishing Management Controls," states, in part, "... documentation for transactions, management controls, and other significant events must be clear and readily available for examination."

a. Management communication of the need for proper estimates

b. Accumulation of relevant, sufficient, and reliable data on which to base accounting estimates

c. Preparation of the estimates by qualified personnel

d. Adequate review and approval of the estimates by appropriate levels of authority, for example:

(1) Review of the sources of the relevant factors

(2) Review of the process used to develop assumptions

(3) Review of the reasonableness of the assumptions and resulting estimates

(4) Consideration of the need to use the work of specialists

(5) Consideration of changes in previously established methods for developing estimates

e. Comparison of prior estimates with actual subsequent results to assess the reliability of the process and models used to develop the estimates

f. Appropriate general and application controls related to computer-based models used in the calculation of estimates included in the statement of social insurance

The Auditor's Responsibility

.09 SAS No. 57, *Auditing Accounting Estimates* (AICPA, *Professional Standards*, vol. 1, AU sec. 342.10), states that the auditor should obtain an understanding of how management developed the estimate. Based on that understanding, the auditor should use one or a combination of the following approaches to evaluate the reasonableness of an estimate:

a. Review and test the process used by management to develop the estimate.

b. Develop an independent expectation of the estimate to corroborate the reasonableness of management's estimate.

c. Review subsequent events or transactions occurring prior to the completion of fieldwork.

In auditing the statement of social insurance, if controls over the estimation process are effective, the most practicable and efficient approach may be to review and test the process used by management. However, if the auditor finds that controls over the estimation process are ineffective, the auditor should consider whether it is practicable to:

- Develop an independent expectation of the estimate, or portions of the estimate, to corroborate management's estimate

or

- Obtain competent evidence from outside the audited agency's process that would be sufficient to support the assertions in the statement of social insurance.

If it is not practicable to mitigate the effects of the ineffective controls through substantive procedures such as these, the auditor's report on the statement of social insurance should be modified.

.10 The auditor's objective when auditing the statement of social insurance is to obtain sufficient, competent, evidential matter to provide reasonable assurance that:

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

a. The estimates presented in the statement of social insurance are reasonable in the circumstances.

b. The statement of social insurance is presented fairly, in all material respects, in conformity with generally accepted accounting principles, including adequate disclosure.

To achieve this objective, the auditor carries out the audit as described in paragraphs .11 through .40. As discussed in footnote 9 of paragraph .18, if the auditor does not possess the level of competence in actuarial science to qualify as an actuary, it is necessary for the auditor to obtain the services of an independent actuary[5] to assist the auditor in planning and performing auditing procedures. Generally, the auditor will need the assistance of an independent actuary in performing various procedures during all phases of the audit and related to all elements of the estimates.

Planning the Audit

.11 In planning the audit of the statement of social insurance, the auditor should:

a. Obtain knowledge about the following matters:

(1) The agency's program and its operations including relevant laws and regulations governing the program that have a direct and material effect on the statement of social insurance (paragraphs .12 and .13)

(2) The agency's process for developing, evaluating, and incorporating estimates in the statement of social insurance (paragraph .14)

(3) The work performed by the agency's actuary (paragraphs .15 through .19)

(4) The work performed and findings reported by any external review groups that have been commissioned by the agency, an appropriate advisory board, or the trustees[6] (paragraph .20)

b. Consider materiality (paragraphs .21 and .22)

---

[5] The actuary can either be under contract with the audit firm or employed by the audit firm. In either case, the actuary performing services for the audit firm would need to meet the independence standards of generally accepted governmental auditing standards (GAGAS), which are applicable to audits of statements of social insurance. For example, for actuaries under contract with the audit firm, the auditor should determine whether the actuary's firm is independent of the agency being audited and then assess the actuary's ability to impartially perform the work and report results. In conducting this assessment, the auditor should provide the actuary with the GAGAS independence requirements and obtain representations from the actuary regarding his or her independence from the audited entity. For actuaries employed by the audit firm, the independence requirements are the same as those for auditors. Paragraphs 3.06 through 3.18 of Chapter 3, "General Standards,"*Government Auditing Standards: 2003 Revision* (GAO-03-673G) describe applicable independence requirements.

[6] Certain social insurance programs are overseen by a board of trustees. For example, the Social Security Act establishes a board of trustees to oversee the financial operations of the Federal Old-Age and Survivors Insurance Trust Fund and the Federal Disability Insurance Trust Fund. The board is composed of six members, four of whom serve automatically by virtue of their positions in the federal government: the Secretary of the Treasury (the managing trustee), the Secretary of Labor, the Secretary of Health and Human Services, and the Commissioner of Social Security. The other two members are appointed by the President and confirmed by the Senate to serve as public representatives.

c. Obtain an understanding of the agency's internal control as it relates to the preparation of the statement of social insurance (paragraphs .23 through .26).

d. Assess control risk (paragraphs .27 through .31).[7]

Obtaining Knowledge About the Agency's Program and Its Operations

.12 The auditor should obtain knowledge about the program and its operations including:

a. The nature of the program's activities

b. The source of its funding

c. Who the beneficiaries are

.13 An important aspect of the program and its operations are the laws and regulations governing the program that may have a direct and material effect on amounts reported as social insurance income and expenditures. Auditors should obtain from agency management the laws and regulations governing the operation of the social insurance program, and make inquiries about the laws and regulations that significantly affect the determination of amounts included in the statement of social insurance. Auditors also should consider changes to laws and new regulations published in final form and how management has given effect to such changes in its determination of future social insurance income and expenditures.

Obtaining Knowledge About the Agency's Process for Developing, Evaluating, and Incorporating Estimates in the Statement of Social Insurance

.14 The auditor should obtain knowledge about the agency's process for developing, evaluating, and incorporating estimates in the statement of social insurance. To obtain that knowledge, the auditor:

a. Makes inquiries of management; individuals responsible for initiating, processing, or recording estimates; and internal and external specialists with expertise in relevant subject matter, such as actuarial science, economics, and law.

b. Reads entity or nonentity documents and records used to prepare the statement of social insurance, as well as the agency's documentation of the process for preparing the statement of social insurance.

c. Observes entity activities and operations used to prepare the statement of social insurance, such as transferring data from a tabulation report to a computerized application.

Obtaining Knowledge About the Work Performed by the Agency's Actuary

.15 Information presented in the statement of social insurance ordinarily is determined on the basis of an actuarial valuation of the program performed

[7] The auditor generally would conclude that inherent risk is high for assertions about estimates in the statement of social insurance because of the complexity of such estimates and the need for significant judgment in preparing them. Other factors that may affect inherent risk in auditing the statement of social insurance include the political climate surrounding social insurance programs, budget limitations, and economic conditions.

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

or reviewed by the agency's actuary, using data received from sources inside and outside the agency, and actuarial techniques. SAS No. 73, *Using the Work of a Specialist* (AICPA, *Professional Standards*, vol. 1, AU sec. 336.12), states:

> The auditor should (*a*) obtain an understanding of the methods and assumptions used by the specialist, (*b*) make appropriate tests of data provided to the specialist, taking into account the auditor's assessment of control risk, and (*c*) evaluate whether the specialist's findings support the related assertions in the financial statements.

.16 The auditor's qualifications do not encompass actuarial science or the complexities of probability and longevity associated with social insurance income and expenditures. The auditor may have a general awareness and understanding of actuarial concepts and practices; however, he or she does not purport to act in the capacity of an actuary. The auditor, therefore, should follow the guidance in SAS No. 73 to obtain assurance regarding the work of an actuary on such matters as program income and benefit payments.

.17 An audit of the statement of social insurance requires cooperation and coordination between the auditor and the actuary. The auditor uses the work of the actuary as an audit procedure to obtain competent evidential matter; the auditor does not merely rely on the report of an actuary. Although the appropriateness and reasonableness of the methods and assumptions used, as well as their application, are within the expertise of the actuary, the auditor does not divide responsibility with the actuary for his or her opinion on the financial statements taken as a whole. Thus, the auditor should satisfy himself or herself as to the professional qualifications and reputation of the actuary as well as the actuary's objectivity, and should obtain an understanding of the actuary's methods and assumptions, test data provided to the actuary, and consider whether the actuary's findings support the related representations in the financial statements.

.18 If the actuary who has prepared or reviewed the actuarial valuation of the social insurance program was engaged by the agency administering that program, it is necessary for the auditor to obtain the services of an independent actuary[8] to assist the auditor in performing auditing procedures that assess the agency actuary's methods, assumptions, and estimates, and aid the auditor in determining whether the agency actuary's findings are not unreasonable in the circumstances.[9] Government Auditing Standards, which are applicable to audits of statements of social insurance, provide independence requirements and examples of personal, external, and organizational impairments to independence.

.19 The auditor should document (*a*) the specific audit procedures that were performed with the assistance of an independent actuary, and the related findings and conclusions, (*b*) the relationship between the procedures performed with the assistance of an independent actuary and the auditor's assessments of audit risk and materiality, and (*c*) all other significant matters related

---

[8] See footnote 5.

[9] Although SAS No. 73, *Using the Work of a Specialist* (AICPA, *Professional Standards*, vol. 1, AU sec. 336.12), does not preclude the auditor from using the work of a specialist who is related to the client, because of the significance of the estimates of income and expenditures to the statement of social insurance, and the complexity and subjectivity involved in developing such estimates, auditing estimates in the statement of social insurance requires the use of an outside actuary, that is, an actuary who is not employed or managed by the agency. If the auditor has the requisite knowledge and experience in actuarial science, the auditor may serve as the actuary. If the auditor does not possess the level of competence in actuarial science to qualify as an actuary, the auditor should use the work of an independent outside actuary.

to the objectives and scope of the independent actuary's work, including any limitations on the independent actuary's procedures.

Obtaining Knowledge About the Work Performed by External Review Groups

.20 In some cases, the agency responsible for the preparation of the statement of social insurance or the program's trustees may commission the services of an external review group comprising technical experts in relevant fields to review the factors, assumptions, data, estimates, and models used to prepare the statement of social insurance. In many instances, individuals assigned to perform these reviews are recognized authorities in their respective fields of study. Because of the nature of these external review groups and the qualifications of the individuals typically assigned to them, the auditor should consider their work in an audit of the statement of social insurance. The auditor should obtain an understanding of the work performed by the external review group, how its findings are communicated to the agency, and how the agency has responded to these findings.[10] See paragraph A-18c of the appendix of this SOP, entitled "Illustrative Controls and Audit Procedures," [paragraph .42] for examples of inquiries the auditor makes of management to obtain knowledge about the work performed by external review groups.

Considering Materiality

.21 Auditors use judgment in determining the appropriate element of the financial statements to use as a materiality base. Auditors generally consider materiality in the context of the financial statements taken as a whole, taking into account both quantitative as well as qualitative attributes of the financial statements. Auditors should exercise due professional care when setting the materiality base, carefully assessing the information gained during the planning phase of the audit and the needs of a reasonable person relying on the financial statements.

.22 For certain federal agencies, amounts reported in the statement of social insurance may vary significantly from the amounts reported in the other basic financial statements, or may differ significantly on a qualitative basis. In such cases, it may not be appropriate to establish a single materiality threshold for the entire set of financial statements. Instead, the auditor should consider using a separate materiality level when planning and performing the audit of the statement of social insurance and related disclosures.

Obtaining an Understanding of the Agency's Internal Control

.23 SAS No. 55, *Consideration of Internal Control in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 319), as amended, defines internal control, describes the objectives and components of internal control, and explains how the auditor should consider internal control in planning and performing an audit.

.24 In auditing the statement of social insurance, the auditor should obtain an understanding of the design of the agency's controls relevant to an audit of the statement of social insurance and should determine whether those controls have been placed in operation. In planning the audit, this knowledge is used to:

---

[10] Although reviews by external review groups may not be conducted annually, in auditing the statement of social insurance the auditor should obtain and review the most recent report of such external review groups.

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

a. Identify risks of potential misstatements.

b. Consider factors that affect the risk of material misstatement.

c. Design tests of controls, when applicable.

d. Design substantive tests.

.25 SAS No. 55 as amended defines internal control as a process—effected by an entity's board of directors, management, and other personnel—designed to provide reasonable assurance regarding the achievement of the objectives of (*a*) reliability of financial reporting, (*b*) effectiveness and efficiency of operations, and (*c*) compliance with applicable laws and regulations.

.26 Internal control consists of the following five interrelated components:

a. *Control environment* sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

b. *Risk assessment* is the entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks should be managed.

c. *Control activities* are the policies and procedures that help ensure that management directives are carried out.

d. *Information and communication systems* support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.

e. *Monitoring* is a process that assesses the quality of internal control performance over time.

Generally, controls that are relevant to an audit pertain to the entity's objective of reliable financial reporting.

Assessing Control Risk

.27 After obtaining an understanding of the design of controls relevant to the statement of social insurance and determining whether those controls have been placed in operation, the auditor assesses control risk for assertions in the statement of social insurance. Control risk is the risk that a material misstatement that could occur in an assertion will not be prevented or detected on a timely basis by the entity's internal control. Assessing control risk is the process of evaluating the effectiveness of an entity's internal control in preventing or detecting material misstatements in the financial statements. Control risk should be assessed in terms of financial statement assertions. The assessed level of control risk is used to determine the nature, timing, and extent of substantive procedures to be performed for financial statement assertions.

.28 The auditor may determine that assessing control risk below the maximum level for certain assertions would be effective and more efficient than performing only substantive tests. Also, the auditor may conclude that it is not practical or possible to restrict detection risk to an acceptable level by performing only substantive tests. In such circumstances, the auditor should obtain evidential matter about the effectiveness of both the design and operation of controls to reduce the assessed level of control risk.

.29 SAS No. 55 as amended (AU sec. 319.04), indicates that the auditor has the option of assessing control risk at the maximum level if he or she believes controls are unlikely to pertain to an assertion or are unlikely to be effective, or because evaluating the effectiveness of controls would be inefficient. However, when auditing the statement of social insurance, the complexity and subjectivity of the estimates, the volume of data involved, and the importance of controls ordinarily would make performing only substantive tests an ineffective strategy.[11]

.30 For certain assertions, the auditor may desire to further reduce the assessed level of control risk. In such cases, the auditor considers whether evidential matter sufficient to support a further reduction is likely to be available and whether performing additional tests of controls to obtain such evidential matter would be efficient.

.31 The risk of material misstatement of estimates ordinarily varies with the complexity and subjectivity of the process, the availability and reliability of the relevant data, the number and significance of assumptions that are made, and the degree of uncertainty associated with the assumptions.

Performing Audit Procedures

.32 As indicated in paragraph .09 of this SOP, in evaluating the reasonableness of the estimates in the statement of social insurance, the auditor primarily reviews and tests the process used by management. The appendix of this SOP [paragraph .42] contains examples of:

a. Procedures the auditor performs to obtain knowledge about the agency's process for developing, evaluating, and incorporating estimates in the statement of social insurance

b. Controls that are relevant to an agency's preparation of the statement of social insurance (The auditor should obtain an understanding of the design of such controls and determine whether they have been placed in operation.)

c. Procedures the auditor performs to test controls, assess control risk, and test assertions in the statement of social insurance

Testing the Work of the Agency's Actuary

.33 When auditing estimates and considering the related factors, assumptions, data, and models, the auditor should obtain the services of an actuary in accordance with SAS No. 73.[12]

.34 With respect to the actuarial present value of amounts reported in the statement of social insurance, the auditor, in following the guidance in SAS No. 73, should:

a. Read the agency actuary's actuarial report.

b. Obtain satisfaction regarding the professional qualifications, competence, and objectivity of the agency's actuary. Examples of factors

---

[11] OMB Bulletin No. 01-02 states that "For those internal controls that have been properly designed and placed in operation, the auditor shall perform sufficient tests to support a low assessed level of control risk."

[12] See footnote 9.

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

to consider are the actuary's membership in a recognized professional organization and the opinion of other actuaries, whom the auditor knows to be qualified, regarding the actuary's professional qualifications.

c. Obtain an understanding of the actuary's objectives, scope of work, methods, and assumptions, and their consistency of application. The auditor should ascertain whether the methods and assumptions used in the valuation of the social insurance program are consistent with relevant Actuarial Standards of Practice adopted by the Actuarial Standards Board.[13] Management, not the actuary, is responsible for the assumptions made and methods used.

d. Inquire whether the actuarial valuation considers all pertinent provisions of laws and regulations governing program operations, including any changes to laws or regulations affecting the actuarial calculations since the date of the latest statement of social insurance.

e. Test the reliability and completeness of the data provided by the agency and used by the actuary in the actuarial valuation. (See paragraphs A-11 through A-14 in the appendix to this SOP [paragraph .42].) In the event that data provided to the actuary are significantly incomplete, the auditor should inquire of the actuary about the treatment of the incomplete data and should determine whether the method used by the actuary to give effect to the missing data in his or her valuation is reasonable in the circumstances.

f. Assess the nature and significance of any reservations concerning assumptions or data that the actuary has stated in his or her report.

Testing the Fund Balance

.35 Paragraph 27(3)(h) of SFFAS No. 17 requires the agency to report "the accumulated excess of all past cash receipts, including interest on investments, over all past cash disbursements within the social insurance program represented by the fund balance at the valuation date." As noted in paragraph 26 of SFFAS No. 17, the valuation date for the statement of social insurance may differ from the valuation date for the other financial statements. Accordingly, the auditor should conduct appropriate testing of the accumulated cash receipts over the accumulated cash disbursements, as of the social insurance valuation date. The nature and extent of testing is a matter of professional judgment. Examples of procedures the auditor may perform are confirmation testing or roll-forward testing.

Obtaining Management's Representations

.36 SAS No. 85, *Management Representations* (AICPA, *Professional Standards*, vol. 1, AU sec. 333), as amended, requires the auditor to obtain a representation letter from management confirming representations given to the auditor during the engagement, for example, a representation regarding the completeness of the information provided to the auditor. In an audit of the statement of social insurance, the representation letter should include, as applicable, the following representations:

---

[13] Relevant standards include Actuarial Standards of Practice No. 21, *The Actuary's Responsibility to the Auditor*, No. 23, *Data Quality*, and No. 32, *Social Insurance*.

a. The actuarial assumptions and methods used to measure amounts in the statement of social insurance for financial accounting and disclosure purposes represent management's best estimates regarding future events based on demographic and economic assumptions, and future changes mandated by law.

b. There were no material omissions from the data provided to the agency's actuary for the purpose of determining the actuarial present value of the estimated future income to be received, and estimated future expenditures to be paid during a projection period sufficient to illustrate the long-term sustainability of the [*name of the social insurance program*] as of [*dates of statements of social insurance presented*].

c. Management is responsible for the assumptions and methods used in the preparation of the statement of social insurance. Management of the agency agrees with the actuarial methods and assumptions used by the agency's actuary and has no knowledge or belief that would make such methods or assumptions inappropriate in the circumstances. Management did not give any instructions, nor cause any instructions to be given to the agency's actuary with respect to values or amounts derived, and is not aware of any matters that have affected the objectivity of the agency's actuary. Management believes that the actuarial assumptions and methods used to measure amounts in the statement of social insurance for financial accounting purposes are appropriate in the circumstances.

d. The statement of social insurance covers a projection period sufficient to illustrate long-term sustainability of the social insurance program.

e. Management has provided the auditor with all the reports developed by external review groups appointed by the agency or the program's trustees related to estimates in the statement of social insurance.

f. The following matters relating to the statement of social insurance have been disclosed properly in the notes to the financial statements:

(1) The accumulated excess of all past cash receipts, including interest on investments, over all past cash disbursements within the social insurance program represented by the fund balance at the valuation date

(2) An explanation of how the net present value is calculated for the closed group[14] (Paragraph 27(3)(i) of SFFAS No. 17 identifies the information to be included in this explanation.)

(3) Comparative financial information for the items in paragraphs .02a, .02b, .02c, and .02d(1) of this SOP, for the current year and for each of the four preceding years

(4) Significant assumptions used in preparing the estimates

g. There have been no changes in [*or*, Changes in the following have been properly recorded or disclosed in the financial statements]:

---

[14] The *closed group* is defined as those persons who, as of a valuation date, are participants in a social insurance program as beneficiaries, covered workers, or payers of earmarked taxes or premiums.

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

(1) The actuarial methods or assumptions used to calculate amounts recorded or disclosed in the financial statements between the valuation dates (that is, January 1, 20X8, and January 1, 20X7) or changes in the method of collecting data.

(2) The actuarial methods or assumptions used to calculate amounts recorded or disclosed in the financial statements between the valuation date and the financial reporting date (that is, January 1, 20X8, and September 30, 20X8) or changes in the method of collecting data.

h. There have been no changes in [*or*, Changes in the following have been properly recorded or disclosed in the financial statements]:

(1) Laws and regulations affecting social insurance program income and benefits between the valuation dates (January 1, 20X8, and January 1, 20X7).

(2) Laws and regulations affecting social insurance program income and benefits between the valuation date and the financial reporting date (that is, January 1, 20X8, and September 30, 20X8).

i. Accounting estimates applicable to the financial information of the agency included in the statement of social insurance are based on management's best estimate, after considering past and current events and assumptions about future events.

Reporting

.37 Since FASAB has defined the statement of social insurance as a basic financial statement, the auditor reports on it as a part of his or her report on the other basic financial statements. In addition to following the requirements of SAS No. 58, *Reports on Audited Financial Statements* (AICPA, *Professional Standards*, vol. 1, AU sec. 508), as amended, the auditor's report on a federal agency's financial statements that present a statement of social insurance should include the following elements:

a. An opinion as to whether the statement of social insurance presents fairly, in all material respects, the financial condition[15] of the agency's social insurance program(s) as of the valuation date in conformity with generally accepted accounting principles.

b. An explanatory paragraph following the opinion paragraph, describing that (i) the statement of social insurance presents the actuarial

---

[15] In Statement of Federal Financial Accounting Concepts No. 1, *Objectives of Federal Financial Reporting*, the FASAB articulates a concept of *financial condition*, as distinct from *financial position*. Financial condition is broader and more forward-looking than financial position. Presenting information on financial condition is consistent with FASAB's financial reporting objective of stewardship. In illustrating how the stewardship objective aligns with the needs of users of federal financial statements, FASAB observes that,

> All users need information on earmarked revenues recorded in trust funds. They want to know, for example, whether the Social Security Trust funds are likely, in the foreseeable future, to need infusions of new taxes to pay benefits. Citizens need to know the implications of investing trust fund revenues in government securities.

In reporting the actuarial present value of the estimated future income to be received, estimated future expenditures to be paid, and excess of income over expenditures during a projection period sufficient to illustrate the long-term sustainability of an agency's social insurance programs, and in disclosing in the notes to the financial statements comparative financial information for the five most recent years, the statement of social insurance presents the financial condition of the programs. Thus, in reporting on the statement of social insurance, the auditor refers to the financial condition of the agency's social insurance programs.

present value of the agency's estimated future income to be received from or on behalf of the participants and estimated future expenditures to be paid to or on behalf of participants during a projection period sufficient to illustrate long-term sustainability of the social insurance program; (ii) in preparing the statement of social insurance, management considers and selects assumptions and data that it believes provide a reasonable basis for the assertions in the statement; and (iii) because of the large number of factors that affect the statement of social insurance and the fact that future events and circumstances cannot be known with certainty, there will be differences between the estimates in the statement of social insurance and the actual results, and those differences may be material.

c. Reference to any standards or regulations in addition to generally accepted auditing standards, such as *Government Auditing Standards*, that apply to audits of federal financial statements and any additional elements of the auditor's report that those standards or regulations require.

.38 The following is an illustrative auditor's report for a statement of social insurance.

Independent Auditor's Report[16]

We have audited the accompanying consolidated balance sheets of XYZ Social Insurance Agency, as of September 30, 20X8 and 20X7, the related consolidated statements of net cost, of changes in net position and of financing; the combined statements of budgetary resources for the years then ended; and statements of social insurance as of January 1, 20X8, 20X7, 20X6, 20X5, and 20X4.[17] These financial statements are the responsibility of XYZ Social Insurance Agency's management. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements*. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of XYZ Social Insurance Agency as of

---

[16] SAS No. 58, *Reports on Audited Financial Statements* (AICPA, *Professional Standards*, vol. 1, AU sec. 508.65–.74) provides guidance on reporting on comparative financial statements, including guidance on reporting when there has been a change in auditors.

[17] The auditor's report on the statement of social insurance covers a period of five years (see paragraph 27(3)(j) of SFFAS No. 17); whereas, the auditor's report on the other financial statements covers a period of two years. In the first year's audit of the statement of social insurance, the auditor would only express an opinion on one year; in year two, the auditor would express an opinion on two years, and so on, until all five years were covered.

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

September 30, 20X8 and 20X7; its net cost of operations; changes in net position, budgetary resources, and financing for the year then ended; and the financial condition of its social insurance programs as of January 1, 20X8, 20X7, 20X6, 20X5, and 20X4, in conformity with accounting principles generally accepted in the United States of America.

As discussed in Note X to the financial statements, the statements of social insurance present the actuarial present value of the Agency's estimated future income to be received from or on behalf of the participants and estimated future expenditures to be paid to or on behalf of participants during a projection period sufficient to illustrate long-term sustainability of the social insurance program. In preparing the statements of social insurance, management considers and selects assumptions and data that it believes provide a reasonable basis for the assertions in the statements. However, because of the large number of factors that affect the statement of social insurance and the fact that future events and circumstances cannot be known with certainty, there will be differences between the estimates in the statement of social insurance and the actual results, and those differences may be material.

Management's Discussion and Analysis (MD&A) and the Required Supplementary Information (RSI) are not required parts of the financial statements but are supplementary information required by the Federal Accounting Standards Advisory Board and OMB Bulletin No. 01-09, *Form and Content of Agency Financial Statements*. We have applied certain limited procedures, which consisted principally of inquiries of management regarding the methods of measurement and presentation of the MD&A and the RSI. However, we did not audit this information and express no opinion on it.

In accordance with *Government Auditing Standards*, we have also issued a report dated [*report date*] on our consideration of the agency's internal control and a report dated [*report date*] on its compliance with laws and regulations. Those reports are an integral part of an audit performed in accordance with *Government Auditing Standards* and should be read in conjunction with this report in considering the results of our audit.

[*Signature*]

[*Date*]

.39 The statement of social insurance does not articulate with the other basic financial statements. For that reason, the portion of the auditor's report that addresses the statement of social insurance ordinarily will not affect the auditor's report on the balance sheet or the statements of net costs, changes in net position, financing, or budgetary resources. The following illustrates a report in which the auditor disclaims an opinion on the statement of social insurance but expresses an unqualified opinion on the other financial statements.

Independent Auditor's Report

We have audited the accompanying consolidated balance sheets of XYZ Social Insurance Agency, as of September 30, 20X8 and 20X7, the related consolidated statements of net cost, of changes in net position and of financing, and the combined statements of budgetary resources for the years then ended, and we were engaged to audit the statements of social insurance as of January 1, 20X8, 20X7, 20X6, 20X5, and 20X4. These financial statements are the responsibility of XYZ Social Insurance Agency's management. Our responsibility is to express an opinion on these financial statements based on our audits.

Except as explained in the following paragraph, we conducted our audits in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements*. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

[*Insert paragraph describing limitation on scope of the audits of the statements of social insurance.*]

Because of the matter discussed in the preceding paragraph, the scope of our work was not sufficient to enable us to express, and we do not express, an opinion on the statements of social insurance as of January 1, 20X8, 20X7, 20X6, 20X5, and 20X4.

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of XYZ Social Insurance Agency as of September 30, 20X8 and 20X7, its net cost of operations, changes in net position, budgetary resources, and financing for the year then ended in conformity with accounting principles generally accepted in the United States of America.

[*Omit explanatory paragraph required by paragraph .37b of this SOP.*]

[*Modify the paragraph reporting on Management's Discussion and Analysis and Required Supplementary Information for the effects of the scope limitations regarding the statement of social insurance on that information, considering the guidance in SAS No. 42,* Reporting on Condensed Financial Statements and Selected Financial Data *(AICPA,* Professional Standards, *vol. 1, AU sec. 552), as amended, and SAS No. 29,* Reporting on Information Accompanying the Basic Financial Statements in Auditor-Submitted Documents *(AICPA,* Professional Standards, *vol. 1, AU sec. 551), as amended.*]

[*Reference to reports on internal control and compliance with laws and regulations in accordance with the Government Auditing Standards is the same as in the illustration in paragraph .38 of this SOP.*]

[*Signature*]

[*Date*]

.40 If the agency that operates a social insurance program issues financial statements that purport to present financial position, net cost of operations, changes in net position, budgetary resources, and financing for the years then ended, but omits the related statements of social insurance, the auditor ordinarily will conclude that the omission requires qualification of the auditor's opinion in the following manner.

Independent Auditor's Report

We have audited the accompanying consolidated balance sheets of XYZ Social Insurance Agency, as of September 30, 20X8 and 20X7, the related consolidated statements of net cost, of changes in net position and of financing, and the combined statements of budgetary resources for the years then ended. These financial statements are the responsibility of XYZ Social Insurance Agency's management. Our responsibility is to express an opinion on these financial statements based on our audits.

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

[*Same second paragraph as the standard report*]

The agency declined to present statements of social insurance as of January 1, 20X8, 20X7, 20X6, 20X5, and 20X4. Presentation of such statements describing the financial condition of its social insurance programs is required by accounting principles generally accepted in the United States of America.

In our opinion, except that the omission of the statements of social insurance results in an incomplete presentation as explained in the preceding paragraph, the financial statements referred to above present fairly, in all material respects, the financial position of XYZ Social Insurance Agency as of September 30, 20X8 and 20X7; its net cost of operations; and changes in net position, budgetary resources, and financing for the year then ended in conformity with accounting principles generally accepted in the United States of America.

[*Omit explanatory paragraph required by paragraph .37b of this SOP.*]

[*Modify, in accordance with the guidance in AU Section 558,* Required Supplementary Information *(AICPA,* Professional Standards, *vol. 1, AU sec. 558.08), the paragraph regarding Management's Discussion and Analysis and the Required Supplementary Information (RSI) for the omission of the RSI.*]

[*Reference to reports on internal control and compliance with laws and regulations in accordance with* Government Auditing Standards *is the same as in the illustration in paragraph .38 of this SOP.*]

[*Signature*]

[*Date*]

Effective Date and Transition

.41 This SOP is effective for audits of statements of social insurance for periods beginning after September 30, 2005. SFFAS No. 17 (subparagraph 27(3)(a-h)) requires disclosure of the information for the current year and for each of the four preceding years. Comparative information in the statement of social insurance that has not been audited should be marked as unaudited. Earlier implementation of the provisions of this SOP is permitted.

Appendix

Illustrative Controls and Audit Procedures

A-1. This appendix contains examples of:

a. Procedures the auditor performs to obtain knowledge about the agency's process for developing, evaluating, and incorporating estimates in the statement of social insurance

b. Controls that are relevant to the agency's preparation of the statement of social insurance (The auditor should obtain an understanding of the design of such controls and determine whether they have been placed in operation.)

c. Procedures the auditor performs to tests controls and assertions in the statement of social insurance

A-2. The appendix is divided into the following five sections:

a. Factors (paragraphs A-3–A-5)

b. Assumptions (paragraphs A-6–A-10)

c. Data (paragraphs A-11–A-14)

d. Models (paragraphs A-15–A-17)

e. Estimates (paragraphs A-18–A-20)

Each of these sections includes examples of the items described in paragraph A-1. The procedures and controls included in this appendix are illustrative and do not represent a complete list of procedures and controls.

Factors

A-3. In evaluating the reasonableness of an accounting estimate, the auditor ordinarily concentrates on key factors that are significant to the estimate, sensitive to variation, deviations from historical patterns, and subjective and susceptible to misstatement and bias. The following are examples of procedures the auditor performs to obtain knowledge about how the agency generates, evaluates, selects, and reviews factors to be included in estimates in the statement of social insurance:

a. Identifying the individuals involved in generating, evaluating, selecting, and reviewing factors to be included in estimates in the statement of social insurance

b. Determining how factors affecting social insurance estimates are generated, evaluated, selected, and reviewed, and how that process is documented[1]

c. Reading documentation of the process for generating, evaluating, selecting, and reviewing estimates to be included in the statement of social insurance

---

[1] Office of Management and Budget (OMB) Circular No. A-123, *Management and Accountability Control*, and No. A-127, *Financial Management Systems*, outline documentation requirements for manual and automated financial related transactions and systems.

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

A-4. In all audits, the auditor should obtain an understanding of internal control sufficient to plan the audit by determining whether applicable controls are suitably designed and placed in operation. The following are examples of controls related to factors:

a. Management's process for monitoring the environment to determine the effect that change in the environment (for example, legal, political, health, immigration) might have on the factors considered

b. Procedures to prevent and detect the inadvertent omission of factors that should be considered in developing the estimate (An example of such a control would be comparing factors considered and selected in the current period with those of prior periods.)

c. Hiring procedures to ensure that individuals responsible for generating, evaluating, selecting, and reviewing factors have the appropriate education and experience

A-5. The following are examples of procedures the auditor performs to test controls and financial statement assertions related to factors:

a. Reviewing documentation of the factors considered in developing the estimate

b. Evaluating whether the factors that have been considered are relevant and sufficient for the purpose of preparing the statement of social insurance

c. Considering whether there are additional key factors that management has not addressed

Assumptions

A-6. In evaluating the reasonableness of an accounting estimate, the auditor ordinarily concentrates on assumptions that are significant to the accounting estimate, sensitive to variation, deviations from historical patterns, and subjective and susceptible to misstatement and bias.

A-7. The following are examples of matters the auditor inquires about in discussions with management and other knowledgeable personnel to determine how the agency generates, evaluates, selects, and reviews assumptions to be included in estimates in the statement of social insurance:

a. The source of the assumptions for significant estimates[2]

b. How the assumptions underlying the estimates are documented

[2] For some agencies, the assumptions are established by an external board of trustees and provided to the agency. For example, for the Social Security program, the Social Security Act establishes a board of trustees to oversee the financial operations of the Federal Old-Age and Survivors Insurance Trust Fund and the Federal Disability Insurance Trust Fund. The board is composed of six members, four of whom serve automatically by virtue of their positions in the federal government. They are the Secretary of the Treasury (the managing trustee), the Secretary of Labor, the Secretary of Health and Human Services, and the Commissioner of Social Security. The other two members are appointed by the President and confirmed by the Senate to serve as public representatives. In such circumstances, the auditor's procedures generally would focus on testing the work performed by the agency's actuary in reviewing the assumptions developed by the board of trustees. The agency's actuary reports on whether (*a*) the techniques and methodology used to evaluate the financial and actuarial status of the program is based upon sound principles of actuarial practice and are generally accepted within the actuarial profession; and (*b*) the assumptions used and the resulting actuarial estimates are, individually and in the aggregate, reasonable for the purpose of evaluating the financial and actuarial status of the trust funds, taking into consideration the past experience and future expectations for the population, the economy, and the program.

c. The process for determining the best estimate (for example, intermediate) assumptions (possible outcomes)

d. How management considers and determines the effect that variation in the underlying assumptions will have on the estimates

A-8. The following are examples of controls related to assumptions:

a. The agency's documentation of the process used to generate, evaluate, select, and review assumptions

b. How management monitors the environment for possible changes that might affect the assumptions used to develop estimates, for example, the need to consider alternative assumptions

c. Comparing assumptions made in the current period with those of prior periods and reconciling differences

d. Hiring procedures to ensure that personnel have the appropriate education and experience to meet job description requirements

A-9. The following are examples of procedures the auditor performs to test controls and financial statement assertions related to assumptions:

a. Identifying the assumptions used and evaluating the reasonableness of those assumptions

b. Determining whether data and other related information support the assumptions

c. Evaluating whether interrelated assumptions are consistent with each other

d. Comparing assumptions made by the entity to the range of assumptions made by entities in other industries, for example, insurance companies, financial institutions, or other government agencies, and evaluating the implications of significant differences

e. Considering whether there are alternative assumptions about the factors

f. Evaluating whether the assumptions selected are consistent with supporting data, relevant historical data, and industry data

g. Reviewing available documentation of the assumptions used in developing the estimates

h. Evaluating whether facts and informed judgment about past and future events or circumstances support the underlying assumptions

i. Evaluating whether any of the significant assumptions are so subjective that no reasonably objective basis could exist to support the use of the assumption

j. Inquiring of program managers regarding the reasonableness of assumptions that are related to the manager's realm of responsibility

k. Evaluating whether the assumptions appear to be complete, that is, whether assumptions have been developed for each key factor

l. Considering whether the assumptions appear to be relatively objective, that is, are not unduly optimistic or pessimistic

m. Evaluating whether the assumptions are consistent with the laws and regulations governing the program

n. Evaluating whether the assumptions, individually and in the aggregate, make sense in the context of the statement of social insurance taken as a whole

o. Evaluating whether significant assumptions are appropriately disclosed in the statement of social insurance

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

A-10. Assumptions that have no material effect on the statement of social insurance may not have to be individually evaluated; however, the aggregate effect of individually insignificant assumptions should be considered in making an overall evaluation of whether the assumptions underlying the reported amounts are reasonable.

Data

A-11. The following are examples of matters the auditor inquires about in discussions with management and other knowledgeable personnel, and reads about in agency documentation to determine how the agency generates, evaluates, selects, and reviews data to be included in estimates in the statement of social insurance:

a. The source of the data for significant estimates and whether the data are developed internally or by outside parties

b. How data are collected, maintained, processed, and updated

c. How the data underlying the estimates are documented

A-12. The following are examples of controls related to data:

a. Controls over the accuracy and completeness of internally prepared data, for example, review of the data for reasonableness and consistency with other data, and general and application controls over the data such as edit checks and batch totals

b. Controls that prevent and detect errors in the collection, maintenance, processing, and updating of the data, for example, manual controls to ensure that data are accurately entered and uploaded to a computerized system

c. Controls over the reliability of external sources of data, for example, confirming and verifying data by tracing and agreeing it to census information in reports prepared by the United States Census Bureau

d. Procedures to identify and document authorized users of the system and to restrict access to the system, for example, the use of unique user passwords and periodic changes to those passwords

e. Preparation and review of a risk assessment on a regular basis or when a significant change occurs in either the internal or external physical environment

f. Preventive maintenance agreements or procedures for key system hardware components

g. On a regular basis, backing up software and data that are stored offsite

h. Restricting access to utility programs that can read, add, change, or delete data or programs to authorized individuals

i. Establishing procedures to ensure that original source documents are retained or are reproducible by the agency for an adequate amount of time to facilitate the retrieval or reconstruction of data

A-13. The following are examples of procedures the auditor performs to test controls and financial statement assertions related to data:

a. Evaluating whether the data used to develop the estimates are relevant, reliable, and sufficient for the purpose

b. Identifying the source of the data, that is, whether the data were developed by the agency or by an outside entity

c. Reviewing documentation of the data used to develop estimates

d. Determining whether data used to develop estimates are consistent with supporting data, historical data, and other related information. An example would be determining whether a positive or negative correlation exists between sets of data if such a correlation would be expected to exist.

e. Evaluating the accuracy and completeness of internally prepared data

f. Tracing and agreeing internally prepared data to system output reports generated by the agency

A-14. In determining the extent of the procedures to be performed on data obtained from an external source, a factor to consider is whether the data are widely disseminated and used, or whether the data were developed for limited use. An example of data that are widely disseminated and used is a report prepared by the U.S. Census Bureau. For such data, the auditor may trace and agree the information to reports prepared by the U.S. Census Bureau. If management has made adjustments to data obtained from a widely disseminated and used external source, the auditor should evaluate:

a. Management's reason for adjusting the data

b. The accuracy and completeness of the adjustments to the externally obtained data

c. Management's documentation supporting the adjustment

For data meant for limited use, all other factors being equal, the auditor should confirm or otherwise verify data obtained from other federal agencies and other external sources that were used in the actuarial valuation. If management has made adjustments to data developed for limited use, the auditor should evaluate:

a. Management's reason for adjusting the data

b. The accuracy and completeness of the adjustments to the externally obtained data

c. Management's documentation supporting the adjustment

Models

A-15. The following are examples of procedures the auditor performs to obtain knowledge about how the agency generates, evaluates, selects, and reviews models used to develop estimates included in the statement of social insurance:

a. Inquiring of management and other knowledgeable personnel about how they design or select the model used for the development of estimates and how they document that model

b. Inquiring of management and other knowledgeable personnel about how they determine the effect that variations in the underlying assumptions have on the estimates

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

A-16. The following are examples of controls related to models:

a. General and application controls related to the model, such as controls over input to the model and processing of that input

b. Controls that prevent and detect errors in the development and processing of the model

c. Controls that prevent or detect unauthorized access or changes to the model, for example, an access control table that is a component of the system and prohibits unauthorized users from accessing and changing the model. An example of a detective control is an audit log that tracks any changes made to the model

d. Controls designed to ensure that the information contained in the statement of social insurance and related disclosures conforms to generally accepted accounting principles

e. Designating responsibility for significant information resources within the agency (for example, data and programs) and establishing and maintaining security over such resources

f. Comparing existing system security features to documented system security requirements

g. Assigning responsibility to individuals in a manner that ensures that no single individual has the authority to read, add, change, or delete information without an independent review of that activity

h. Subjecting hardware and software acquisitions and implementations to extensive testing prior to acceptance in production

A-17. The following are examples of procedures the auditor performs to test controls and financial statement assertions related to models:

a. Reviewing documentation that describes the instructions, rules, or procedures used in the model to calculate estimates

b. Reperforming calculations used in the model to translate the assumptions, data, and factors into the estimate

c. Reviewing management's documentation of its sensitivity analysis and considering whether the results are consistent with the auditor's expectations

d. If available, comparing the results of the model with the results of models used by other organizations for reasonableness

Estimates

A-18. The following are examples of matters the auditor inquires about in discussions with management and other knowledgeable personnel to determine how the agency generates, evaluates, selects, and reviews estimates to be included in the statement of social insurance:

a. How management obtains the expertise to develop and evaluate estimates in the statement of social insurance, including hiring procedures, professional development activities, and procedures for engaging outside specialists

b. Who has final authority for reviewing and approving estimates

c. The work performed by external review groups, their findings, and how those findings are used by the agency, for example:

(1) The scope and timing of the work performed by external review groups

(2) The composition of external review groups and the qualifications of the members

(3) Whether the external review groups are independent of the agency

(4) Whether the external review groups issued formal reports including findings or recommendations

A-19. The following are examples of controls related to estimates:

a. Procedures related to the review and implementation of recommendations developed by external review groups

b. General and application controls related to estimates, such as evidence of supervisory and management review of estimates and supporting documentation

c. Controls intended to ensure that the information contained in the statement of social insurance and related notes conforms to Federal Accounting Standards Advisory Board (FASAB) guidance

d. Controls related to the supervision of individuals who develop estimates, and the review of those estimates and supporting documentation

e. Controls to regularly verify that personnel developing estimates are qualified to perform those tasks based on their education, training, and experience, as required

A-20. The following are examples of procedures the auditor performs to test controls and financial statement assertions related to estimates:

a. Developing a trend analysis in which one period is compared to the next period

b. Determining whether the information in the statement of social insurance, including related disclosure, is supported by sufficient, competent evidential matter

c. Comparing the estimated future expenditures predicted by the actuarial model to actual expenditures for the previous fiscal year

d. Evaluating the reasonableness of the time period covered by the statement of social insurance. FASAB standards require that the statement of social insurance cover a projection period sufficient to illustrate long-term sustainability of the social insurance program.

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

Auditing Standards Board 2004

JOHN A. FOGARTY, *Chair*
HAROLD L. MONK, Vice Chair
BARTON W. BALDWIN
GERALD W. BURNS
CRAIG W. CRAWFORD
GEORGE P. FRITZ
JAMES W. GOAD
DAN L. GOLDWASSER
LYNFORD GRAHAM
AUSTON G. JOHNSON
JAMES E. LEE
WANDA LORENZ
SUSAN L. MENELAIDES
WILLIAM F. MESSIER
DANIEL D. MONTGOMERY
DIANE M. RUBIN
MARK K. SCOLES
SCOTT A. SEASOCK
MICHAEL T. UMSCHEID

Social Insurance Task Force

PATRICK L. MCNAMEE, *Chair*
SHIRLEY L. ABEL
BEN W. CARMICHAEL, JR.
WALTER F. FENNELL
DANIEL L. KOVLAK
ELLIOT P. LEWIS
JOHN C. WARNER

AICPA Staff

CHARLES E. LANDES
Director
Audit and Attest Standards

JUDITH M. SHERINSKY
Technical Manager
Audit and Attest Standards

[The next page is 50,741.]

PA Section 16,000
PRACTICE ALERTS

TABLE OF CONTENTS

Section		*Paragraph*
16,010	Dealing With Audit Differences (PA 94-1)	.01-.09
	Introduction	.01
	Evaluating Audit Differences	.02-.06
	Communicating Audit Differences	.07-.09
16,020	Auditing Inventories—Physical Observations (PA 94-2)	.01-.18
	Introduction	.01-.02
	Inventory Fraud Schemes/Techniques	.03
	Planning Considerations	.04-.08
	The Actual Physical Count	.09
	Multiple Locations	.10-.11
	Inventories Held for or by Others	.12-.13
	Use of Specialists	.14
	Post-Observation Matters	.15-.16
	Conclusion	.17-.18
[16,030]	Acceptance and Continuance of Audit Clients (PA 94-3) [Superseded by PA 03-3, *Acceptance and Continuance of Clients and Engagements*]	
[16,040]	Revenue Recognition Issues (PA 95-1) [Superseded by PA 98-3, *Revenue Recognition Issues*]	
[16,050]	Auditing Related Parties and Related-Party Transactions (PA 95-3) [Superseded by *Accounting and Auditing for Related Parties and Related Party Transactions—A Toolkit for Accountants and Auditors*]	
16,060	The Private Securities Litigation Reform Act of 1995 (PA 96-1)	.01-.15
	Introduction	.01
	Fraud Detection and Disclosure	.02-.03
	Private Securities Reform Act of 1995	.04-.06
	Safe Harbor for Forward Looking Statements	.07-.13
	Effective Date of Provisions	.14-.15
16,070	Members in Public Accounting Firms (PA 97-1)	.01-.04
	Financial Statements on the Internet	.01-.04

Section		Paragraph
16,080	Audits of Employee Benefit Plans (PA 97-2)	.01-.13
	Introduction	.01-.02
	Governmental Oversight of Employee Benefit Plans	.03
	Financial Accounting and Reporting Standards	.04-.05
	Common Deficiencies	.06-.07
	Best Practices	.08
	Recent Developments	.09-.10
	Service Organizations	.11
	Year 2000 Issues	.12-.13
16,090	Changes in Auditors and Related Topics (PA 97-3)	.01-.23
	Introduction	.01-.03
	Review of Audit Documentation	.04-.05
	Opening Balances	.06-.09
	Requests to Reissue Reports	.10-.18
	Use of Indemnification Clauses When Reissuing Reports	.19-.20
	Audits of Financial Statements Previously Audited	.21
	Reporting as Successor Auditor When Prior-Period Audited Financial Statements Were Audited by a Predecessor Auditor Who Has Ceased Operations	.22-.23
16,100	The Auditor's Use of Analytical Procedures (PA 98-1)	.01-.39
	Introduction	.01-.03
	Substantive Analytical Procedures—Key Concepts and Discussion	.04-.05
	Expectations	.06-.21
	Level of Assurance	.22-.25
	Difficulties in Applying Substantive Analytical Procedures and Ways to Avoid Them	.26-.35
	Analytical Procedures and Fraud Detection	.36-.39
16,110	Professional Skepticism and Related Topics (PA 98-2)	.01-.11
	Introduction	.01-.03
	The Auditor's Review of Non-Standard Journal Entries	.04-.08
	The Auditor's Review of Original and Final Source Documents	.09-.11
16,120	Responding to the Risk of Improper Revenue Recognition (PA 98-3)	.01-.22
	Introduction	.01-.02
	Required Risk Assessment	.03-.04
	Improper, Aggressive or Unusual Revenue Recognition Practices	.05
	Audit Planning Considerations	.06-.09
	Brainstorming	.10-.12
	Audit Response	.13

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Section		Paragraph
16,120	Responding to the Risk of Improper Revenue Recognition (PA 98-3)—continued	
	Confirmations and Management Representations	.14-.16
	Accounting Considerations	.17-.19
	Communications with Board of Directors/Audit Committees	.20-.21
	Conclusion	.22
16,130	Guidance for Independence Discussions With Audit Committees (PA 99-1)	.01-.28
	Firm Policies and Procedures	.06
	Determination of Matters to Be Communicated	.07-.08
	Engaging the Audit Committee	.09-.10
	Threats to Objectivity and Related Safeguards	.11-.13
	Form of Communication	.14-.19
	Timing of Discussions with Audit Committees	.20-.22
	Other Matters	.23-.28
	Initial Public Offerings	.23
	Initial Year of Application	.24
	Prospective Clients	.25
	Failure to Comply with the Standard	.26-.28
16,140	How the Use of a Service Organization Affects Internal Control Considerations (PA 99-2)	.01-.28
	Introduction	.01-.02
	Factors to Consider in Planning an Audit	.03
	When the User Auditor's Planning Should Consider the Guidance in SAS No. 70	.04
	Nature and Materiality of the Transactions	.05-.06
	Degree of Interaction	.07-.11
	Factors to Consider in Assessing Control Risk	.12-.17
	SAS No. 70 Reports	.18-.26
	Types of Reports	.18
	What Is Included in the Reports	.19
	Considerations in Using the Reports	.20-.24
	Timing Considerations in Using the Reports	.25-.26
	Conclusion	.27-.28
16,150	Accounting for Certain Equity Transactions (PA 00-1)	.01-.31
	Stock Issued for Goods and Services	.02-.12
	Stock Issued to an Owner for Expertise or Intellectual Capital Contributed to Business	.13-.15
	Employee Stock Options	.16-.22
	Retroactive Earnings per Share Adjustment for Cheap Stock	.23-.26
	Extinguishment of Related Party Debt	.27-.28
	Other Accounting Literature Addressing Equity Transactions	.29-.30
	Summary	.31

Section		*Paragraph*
16,160	Guidance for Communication With Audit Committees Regarding Alternative Treatments of Financial Information Within Generally Accepted Accounting Principles (PA 00-2)	.01-.12
	Introduction	.01-.04
	Recommendation to Meet the Objectives of SAS No. 61 and the Sarbanes-Oxley Act of 2002	.05-.06
	Discussion of Quality, Not Acceptability or Preferability, of Accounting Principles and Judgments	.07
	Discussion of Aggressiveness vs. Conservatism in Financial Reporting	.08-.11
	Summary	.12
16,170	Auditing Construction Contracts (PA 00-3)	.01-.06
	Introduction	.01-.03
	Best Practices	.04-.06
[16,180]	Quarterly Review Procedures for Public Companies (PA 00-4) [Superseded by Statement on Auditing Standards No. 100, *Interim Financial Information*]	
16,190	Common Peer Review Recommendations (PA 01-1)	.01-.13
	Introduction	.01-.03
	Implementation of New Professional Standards or Pronouncements	.04-.06
	Equity Transactions	.07
	Revenue Recognition	.08
	Documentation	.09
	Miscellaneous	.10-.11
	Annual Reviewers' Alert	.12
	Summary	.13
16,200	Audit Considerations in Times of Economic Uncertainty (PA 01-2)	.01-.22
	Introduction	.01-.02
	Professional Skepticism	.03-.08
	Inventory	.09-.10
	Accounts Receivable	.11
	Investments	.12
	Long-Lived Assets, Including Goodwill and Intangibles	.13-.15
	Deferred Taxes and Other Deferred Charges	.16
	Accounts Payable	.17
	Debt	.18-.19
	Going Concern	.20
	Other Considerations	.21
	Summary	.22

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Section		Paragraph
[16,210]	Communications With the Securities and Exchange Commission (PA 02-1) [Superseded due to the issuance of the SEC document entitled, "Guidance for Consulting on Accounting Matters with the Office of the Chief Accountant"]	
16,220	Use of Specialists (PA 02-2)	.01-.24
	Introduction	.01-.02
	Decision to Use a Specialist	.03
	Use of a Specialist Engaged or Employed by the Audit Client	.04-.13
	Use of Specialists Engaged or Employed by the Audit Firm	.14-.17
	Introduction Examples of Specific Types of Specialists to Be Utilized	.18-.24
	Information Technology ("IT") Specialists	.18-.23
	Business Valuation Specialists	.24
16,230	Reauditing Financial Statements (PA 02-3)	.01-.32
	Introduction	.01-.03
	Client/Engagement Acceptance Procedures and Considerations	.04-.08
	Planning the Reaudit	.09-.12
	Understanding the Client's Business	.13
	Understanding of Internal Control, Assessment of Control Risk and Tests of Controls	.14-.15
	Substantive Audit Procedures	.16-.25
	Inventory	.18
	Confirmations With Third Parties	.19-.21
	Opening Balances and Consistency of Application of Accounting Principles	.22-.24
	Uncorrected Financial Statement Misstatements	.25
	Representation Letters	.26-.27
	Reporting Implications	.28-.29
	Other Audit Issues	.30-.31
	Internal Inspection	.32
16,240	Audit Confirmations (PA 03-1)	.01-.37
	Introduction	.01-.02
	General Confirmation Guidance	.03-.23
	Improving Confirmation Response Rates	.04-.06
	Negative vs. Positive Confirmation Requests	.07-.09

Section		Paragraph
16,240	Audit Confirmations (PA 03-1)—continued	
	Nonresponses to Positive Confirmations	.10
	Responses to Positive Confirmation Requests Indicating Exceptions	.11-.12
	Confirmations Received Via Fax or Electronically	.13
	Management Requests to Not Confirm	.14-.17
	Alternative Procedures	.18-.21
	Use of Client Personnel	.22-.23
	Confirmation Guidance With Respect to Specific Areas	.24-.36
	Confirmation of Accounts Receivable	.25-.29
	Confirmation of Terms of Unusual or Complex Agreements or Transactions	.30-.31
	Confirmation of Accounts Payable	.32-.35
	Confirmations of Related Party Transactions	.36
	Evolving Alternatives to Confirmation	.37
16,250	Journal Entries and Other Adjustments (PA 03-2)	.01-.26
	Introduction	.01-.05
	Obtaining an Understanding of the Entity's Financial Reporting Process and Its Controls Over Journal Entries and Other Adjustments	.06-.08
	Assessing the Risk of Material Misstatement Resulting From Journal Entries and Other Adjustments	.09-.11
	Inquiries of Individuals Involved in the Financial Reporting Process	.12
	Assessment of Completeness of Journal Entry and Other Adjustments Sources	.13
	Identification and Selection of Journal Entries and Other Adjustments for Testing	.14-.24
	Other Adjustments	.25
	Documentation	.26
16,260	Acceptance and Continuance of Clients and Engagements (PA 03-3)	.01-.50
	Introduction	.01-.02
	Acceptance of Clients and Engagements	.03-.06
	Continuance of Clients and Engagements	.07-.10
	The Client Acceptance and Continuance Process	.11
	Availability of Competent Personnel to Perform the Engagement	.12
	Communication With Predecessor Accountants or Auditors	.13-.20
	Assessment of Management's Commitment to the Appropriate Application of Generally Accepted Accounting Principles	.21

Copyright © 2005, American Institute of Certified Public Accountants, Inc.

Section		Paragraph
16,260	Acceptance and Continuance of Clients and Engagements (PA 03-3)—continued	
	Assessment of Management's Commitment to Implementing and Maintaining Effective Internal Control	.22
	Assessment of the Entity's Financial Viability	.23-.24
	Independence and Objectivity	.25-.31
	Inquiry of Third Parties	.32
	Background Investigations	.33-.42
	Other Considerations	.43-.48
	Restrictions on Scope of Services	.44
	Entities Under Common Control	.45-.46
	One-Time Engagements	.47
	Business and Industry Environment	.48
	Timing Considerations	.49
	Documentation	.50
16,270	Illegal Acts (PA 04-1)	.01-.37
	Introduction	.01-.04
	The Auditor's Responsibility for Detection of Illegal Acts Having a Direct and Material Effect on the Financial Statements	.05-.06
	The Auditor's Responsibility for Detection of Illegal Acts Having an Indirect Effect on the Financial Statements	.07
	Audit Procedures in the Absence of Specific Information Indicating the Existence of Possible Illegal Acts	.08-.13
	Action on Discovery of Possible Illegal Acts	.14-.28
	Obtain an Understanding Regarding the Illegal Act	.17
	Determine Whether the Audit Committee Has Been Informed About the Illegal Act	.18
	Client Investigation of the Possible Illegal Act	.19-.26
	Material Illegal Acts	.27
	Immaterial Illegal Acts	.28
	Disclosure of Illegal Acts to Third Parties	.29-.30
	Reporting Considerations	.31-.36
	Scope Limitation	.32
	Departure From Generally Accepted Accounting Principles	.33
	Inability to Determine Materiality of an Illegal Act	.34
	Client Refusal to Accept Report	.35
	Audits Performed Under *Government Auditing Standards*	.36
	Documentation	.37

[The next page is 50,751.]

Section 16,010

Practice Alert 94-1
Dealing With Audit Differences

First issued
February, 1994;
Updated December, 1999

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits and is based on existing audit and accounting literature, the professional experience of the members of the AICPA SEC Practice Section Professional Issues Task Force (PITF) and information provided by the AICPA SEC Practice Section members firms to their own professional staff. The information in this Practice Alert represents the views of the members or the PITF and is not an official position of the AICPA. Official positions are determined through certain specific committee procedures, due process and deliberation. The information provided herein should be used by practitioners with the understanding that it be read in conjunction with the professional literature and only as a means of assisting them in meeting their professional responsibilities.

Introduction

.01 Auditors often identify potential adjustments to client accounts as a consequence of audit work performed. Although auditors recognize the importance of identifying and accumulating audit differences, experiences, including those from litigation and peer reviews, suggest that audits can be more effective if auditors pay closer attention to this identification and accumulation process. Specifically, auditors should be mindful that:

- The materiality of audit differences needs to be considered in light of various factors in addition to earnings and stockholders' equity, such as the impact on debt covenants, and analysts' earnings estimates.
- An agreement with management to waive "hard" debit audit differences, including errors, because they have identified offsetting "soft" credit differences can result in problems. Experience has shown that soft differences may not materialize, particularly when they are discovered by management at the last minute after being informed of "hard" differences.
- Numerous audit differences trending in the same direction might suggest bias on the part of management to achieve an earnings forecast. In the worst case, it could be a possible prelude to fraud.
- Accumulated unrecorded audit differences that are not material in the period of origin may be material to financial statements of subsequent periods or when considered in light of changed conditions, including

changes in an entity's management or ownership. This is particularly a consideration where the purchase price is based on book value or a multiple of earnings.

- Audit committees and outsiders (attorneys, regulators, other auditors, etc.) who become aware of waived audit differences sometimes question why those differences were not recorded, especially if they are marginally below materiality thresholds, are errors and/or are clear deviations from generally accepted accounting principles. Audit committees may become upset that they were not previously informed of these differences.

Evaluating Audit Differences

.02 Auditing standards require the auditor to consider whether aggregated uncorrected misstatements, in relation to individual amounts, subtotals or totals in the financial statements, materially misstate the financial statements taken as a whole. Experience indicates that auditors also may need to give closer consideration to the effects on compliance with debt covenants, widely used ratios, financial statement disclosures and whether they may be indicative of an irregularity or illegal act. (See Statement on Auditing Standards (SAS) No. 47, *Audit Risk and Materiality in Conducting an Audit*, as amended, paragraphs 34 through 40.) The internal control implications of identified audit differences should also be carefully considered.

.03 Auditors should exercise great care when netting "hard" debit differences and "soft" credit differences because the soft differences may never materialize. For example, the auditor should be careful if a client proposes to reduce inventory obsolescence reserves in order to offset proposed physical inventory test count differences that decrease inventory. Last-minute entries oftentimes need an even higher degree of audit challenge, particularly if they seem to offset unfavorable proposed audit differences.

.04 Also, even when individual accounting estimates included in the financial statements are within acceptable boundaries, the auditor should consider whether the trend of the differences between those estimates and the auditor's best estimates might suggest a possible bias on the part of management. In considering that possible bias, as well as aggregated unadjusted audit differences, the auditor is well advised to bear in mind that the financial statements still could be materially misstated due to differences that have not been detected.

.05 Audit differences are ordinarily accumulated in order to assess their effects on significant components of the financial statements. The accumulated audit differences should include both known differences (e.g., mathematical mistakes, omissions, errors in classifying or recording balances or transactions) and likely differences (e.g., projected total misstatements from sampling applications, differences between an estimate recorded by the client and the auditor's assessment of the closest reasonable amount).

.06 When assessing the materiality of audit differences for a public company, an auditor should consider Staff Accounting Bulletin 99 ("SAB 99"). SAB 99 addresses the concepts of materiality in financial statements. The SAB expresses the views of the SEC staff that "exclusive reliance on certain quantitative benchmarks to assess materiality in preparing financial statements

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

and performing audits of those financial statements is inappropriate." The SAB reminds auditors of the need to consider both "quantitative" and "qualitative" factors in assessing an item's materiality. In SAB 99, the SEC also expresses the view "A matter is material if there is a substantial likelihood that a reasonable person would consider it important." The SAB provides guidance on the qualitative assessment of materiality in the preparation and audit of financial statements, and reminds registrants of their obligation to maintain accounting records and internal accounting controls as required by the Securities Exchange Act of 1934.

Communicating Audit Differences

.07 Encouraging management to record audit differences, even if they are not material to the current year financial statements, sends a clear message about management's responsibility for the accounting records and financial statements. There is usually a much greater likelihood management will record appropriate adjustments when those adjustments are brought to their attention early in the audit process. Recording such differences assures that future financial statements will not be affected by an accumulation of unadjusted differences. An accumulation of immaterial unadjusted differences may take on increased significance if an entity or a business segment is sold, a new management team is appointed or if those differences become subject to scrutiny by third parties such as attorneys, regulators or other auditors. In the event that audit differences are not recorded and are assessed as immaterial, the auditor should work towards an agreed plan for management to record such items in the succeeding year.

.08 Finally, auditors are reminded of their obligation to inform the audit committee, or other formally designated oversight body, of recorded and unrecorded adjustments arising from the audit that could, in their judgment, have a significant effect on the entity's financial reporting process. (See SAS No. 61, *Communication With Audit Committees*, as amended, paragraph 9.)

.09 In early 2000, the Auditing Standards Board will issue SAS No. 89, *Audit Adjustments*, which increases the auditor's responsibilities for communicating passed audit differences to audit committees. Specifically, the auditor will be required to inform the audit committee about uncorrected misstatements aggregated by the auditor during the current engagement and pertaining to the latest period presented that were determined by management to be immaterial, both individually and in the aggregate, to the financial statements taken as a whole. The auditor also will be required to obtain a written representation from management acknowledging that it has considered these financial statement misstatements and concluded that any uncorrected misstatements are immaterial, both individually and in the aggregate, to the financial statements taken as a whole. The SAS will be effective for audits of financial statements for periods beginning on or after December 15, 1999.

[The next page is 50,761.]

Section 16,020

Practice Alert 94-2
Auditing Inventories—Physical Observations

First issued
July, 1994;
Updated July, 1999

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits. This document has been prepared by the SEC Practice Section Professional Issues Task Force and is based on the experiences of the individual members of the task force and matters arising from litigation and peer reviews. It has not been approved, disapproved or otherwise acted upon by any committee of the AICPA.

Introduction

.01 The inventories of most commercial entities, especially those of manufacturers or distributors, are material to their financial statements. By its nature, accounting for inventories is complex and generally involves a great deal of detail and is therefore susceptible to inadvertent errors. For similar reasons and the fact that auditors test only a portion of the inventories, there exists more than a low risk of manipulation when management is disposed toward financial statement fraud.

.02 This Alert discusses some ways in which inventory frauds have been perpetrated and presents information that might help prevent such frauds from going undetected. This Alert deals primarily with issues related to the physical existence of inventories. This Alert does not cover matters pertaining to inventory obsolescence, pricing or costing.

Inventory Fraud Schemes/Techniques

.03 Unfortunately, in many cases of inventory fraud, client personnel at various levels knowingly participated and assisted in the scheme. The following are examples of inventory frauds:

- Including inventory that is not what it is claimed to be or valuing nonexistent inventory. Examples are:
  - — Empty boxes or "hollow squares" in stacked goods.
  - — Mislabeled boxes containing scrap, obsolete items or lower value materials.
  - — Consigned inventory, inventory that is rented, or traded-in items for which credits have not been issued.
  - — Diluted inventory so it is less valuable (e.g., adding water to liquid substances).

- — Increasing or otherwise altering the inventory counts for those items the auditor did not test count.
- — Programming the computer to produce fraudulent physical quantity tabulations or priced inventory listings.
- — Manipulating the inventory counts/compilations for locations not visited by the auditor.
- — Double-counting inventory in transit between locations.
- — Physically moving inventory and counting it at two locations.
- — Including in inventory merchandise recorded as sold but not yet shipped to a customer ("bill and hold sales").
- — Arranging for false confirmations of inventory held by others.
- — Including inventory receipts for which corresponding payables had not been recorded.
- — Overstating the stage of completion of work-in-process.
- — Reconciling physical inventory amounts to falsified amounts in the general ledger.
- — Manipulating the "roll-forward" of an inventory taken before the financial statement date.

Planning Considerations

.04 Even though there are numerous ways inventory frauds can be orchestrated, a well planned audit—appropriately executed with professional skepticism—can thwart many inventory falsification schemes. The audit procedures to be applied stem from and are responsive to the auditor's assessment of risk (i.e., What could go wrong?). The use of analytical procedures (e.g., review of preliminary high-to-low inventory-value listings or comparison of year-to-year quantities) in planning the audit often helps identify inventory locations, areas or items for specific attention or greater scrutiny during and after the physical count.

.05 To plan an appropriate and effective inventory observation, it is important for the engagement team leaders to have an understanding of the client's business, its products, its computer processing applications and relevant controls before the physical count occurs, including knowledge of the physical inventory or cycle count procedures and the inventory summarization, pricing and cutoff procedures.

.06 When a client plans to count inventories at various dates or at a date other than that of the financial statements, the early consideration of its business, internal controls and their effectiveness, and cutoff procedures are especially important. Heightened risks or the lack of adequate internal controls may suggest that the inventory should be taken and observed at year end.

.07 An appropriate understanding of the client's business systems, relevant computer processing applications and inventory procedures helps determine the experience needed by the personnel assigned to observe the physical count and their individual responsibilities. Assigning junior personnel to observe the count at a complex manufacturing operation may or may not be prudent, depending on the extent of on-site supervision provided. Similarly, work-in-process inventory presents completion/valuation issues that may call for a more experienced auditor.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.08 When the observation requires the use of personnel from another office or another CPA firm, adequate planning also enables the auditor to provide clear, comprehensive instructions about the scope of the engagement, the important risk factors, the relevant controls, cutoff procedures, and the expected level of reliance to be placed on internal controls.

The Actual Physical Count

.09

- The risk of inclusion of duplicate or fictitious items is higher in areas and for items not test counted by the auditor. Testing some counts made by all count teams at locations visited and ensuring that hard-to-count items are test counted helps minimize the risk of misstatement.
- Applying analytical procedures to the final priced-out inventory detail can help identify inventory items that might require additional audit scrutiny.
- Although client personnel are often helpful to the auditor making test counts, making test counts of which client personnel are unaware provides added assurance. The auditor can also record the details of some quantities that the auditor did not actually count for comparison with the final inventory listing. Also, the auditor needs to maintain appropriate control over the audit work papers so the client is not aware of the details of the test counts.
- Because the description on a container may not always match the goods inside, it is a good idea to open some containers or packages. Checking for empty containers or "hollow squares" (i.e., spaces between stacks of boxes) and verifying the units of measure on tags or count sheets are meaningful procedures. When observing work-in-process inventory, the auditor also needs to consider the reasonableness of the recorded stage of completion.
- When incorrect counts are observed, the auditor considers the nature and significance of the errors and whether to increase the extent of test counts or expand other procedures. Recounts of particular areas or the work of particular count teams may be necessary.
- Scanning inventory tags or count sheets for unusual or unreasonable quantities and descriptions is a useful technique to verify their propriety. Subsequent to the physical count, it may be desirable to test large or unusual inventory quantities or items with large extended values that were not test counted during the observation.
- The need to monitor the client's control over the physical count tags or sheets used should not be downplayed or overlooked. Paying close attention to tag/count sheet control procedures helps avoid the inclusion of improper items and ensures appropriate items are included in the final inventory listing.

Multiple Locations

.10 Knowledge of all inventory locations is necessary to prevent the exclusion of any area(s) from audit consideration. Following are a few matters for auditors to consider related to multiple inventory locations.

.11 To help discourage the shifting of inventory from one location to another, the merits of taking the physical inventory at all significant locations at the same time should be considered. When the physical count at each significant location will not be observed, informing management that observations will be performed at some locations without advance notice might help discourage the manipulation of the quantity or quality of the inventory. For locations not visited, the auditor may perform alternative procedures to detect material misstatements. Comprehensive analytical procedures subsequently applied to priced-out inventory summarizations may be one such technique (e.g., the analysis of year-to-year inventories by location, the relationship of inventory to sales levels, etc.). However, the auditor needs to remember that analytical procedures may not always detect erroneous changes in inventory.

Inventories Held for or by Others

.12 Ascertaining whether all inventory items on hand are the property of the client can be difficult in some situations. A client's procedures for identifying, segregating and excluding from inventory goods held on consignment should be considered. Requesting information from selected suppliers about such goods helps in this regard. Once consignment goods have been identified, noting the descriptions, quantities, serial numbers and shipping advice numbers for some items will help the auditor determine whether those items were properly excluded from the client's inventory.

.13 When a client consigns inventory to others or stores merchandise at a third-party location, written confirmation of the goods held is ordinarily obtained directly from the custodian. If such goods are significant in amount, one or more of the procedures discussed in SAS No. 1, section 331, *Inventories*, as amended, paragraph 14, which include visits to such locations and observation of physical counts, may be appropriate.

Use of Specialists

.14 An auditor is not expected to possess the expertise of a specialist trained or qualified in another profession or occupation. Consequently, use of a specialist in certain situations to determine quantities (e.g., stockpiled materials, mineral reserves) or to value special-purpose inventory (e.g., high-technology materials or equipment, chemicals, works of art, precious gems) or to measure the stage of completion of long-term contracts may be appropriate. If the specialist used is affiliated or otherwise has a relationship with the client, the auditor will want to consider the need to perform procedures or otherwise test some or all of the specialist's assumptions, methods and findings. This will provide information about the reasonableness of the findings. Alternatively, the auditor could engage another specialist for this purpose.

Post-Observation Matters

.15 The extent of audit procedures required normally increases when the inventory observation is performed at a date other than the balance sheet date. The extent and nature of the increase depends on the nature of the client's business, the type of inventory, inventory turnover period, the records maintained, the strength of the related internal controls, and the time interval between the observation and the date of the balance sheet. Interim physical

 Copyright © 2001, American Institute of Certified Public Accountants, Inc.

inventories or the client's use of cycle count programs present different audit risks warranting careful assessment of controls, and by extension, different audit tests. This assessment of audit risks and key controls and the focused testing thereof, along with appropriate analytical procedures, are important audit procedures to consider in these circumstances. The guidance in SAS No. 45, *Omnibus Statement on Auditing Standards—1983*, "Substantive Tests Prior to the Balance Sheet Date," is relevant in these circumstances.

.16 Testing significant items in the reconciliation of the physical inventory to the general ledger helps identify inadvertent errors along with intentional misstatements. Significant reconciling items for those locations where the physical counts were not observed by the auditor generally merit scrutiny. Goods in-transit and inventory transfers between affiliates, locations or departments are tested to ascertain their existence and to determine the propriety of their inclusion or exclusion.

Conclusion

.17 Unfortunately, there are no foolproof methods for assuring that all inventory counts are free from inadvertent or intentional misstatement. No audit will necessarily detect all fraudulent activity, especially when collusion to mislead the auditors occurs among client personnel or with third parties. However, understanding the client's business, its count procedures and controls and a resulting careful assessment of where and how quantity error might occur helps reduce the risk of inadvertent or intentional misstatement. Appropriate planning for the physical inventory observation together with healthy audit skepticism can effectively reduce the incidence of inventory misstatements.

.18 This Practice Alert is not a complete list of all audit procedures, nor is every procedure discussed herein applicable in all circumstances. Additional information on this important subject is provided in the AICPA's Auditing Procedures Study, *Audits of Inventories* (Product No. 021045MJ). The AICPA Order Department may be reached at (888) 777-7077.

[The next page is 50,811.]

Section 16,060

Practice Alert 96-1
The Private Securities Litigation Reform Act of 1995

First issued
May, 1996;
Updated July, 1999

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits. This document has been prepared by the SEC Practice Section Professional Issues Task Force. It has not been approved, disapproved or otherwise acted upon by any committee of the AICPA.

Introduction

.01 As 1995 drew to a close, the Private Securities Reform Act of 1995 (the Act) became law. This Act provides welcome liability reform for both Securities and Exchange Commission (SEC) registrants and those who provide services to SEC registrants. The Act not only changes the way that plaintiffs may bring lawsuits, but also imposes certain obligations and requirements on SEC registrants and their auditors. This Practice Alert discusses two sections of the Act (Fraud Detection and Disclosure and the Safe Harbor for Forward-Looking Statements) and how they affect auditors in performing audits and other services.

Fraud Detection and Disclosure

.02 The Fraud Detection and Disclosure section of the Act reaffirms the independent accountant's responsibility regarding illegal acts as described in both Statement on Auditing Standards (SAS) No. 53, *The Auditor's Responsibility to Detect and Report Errors and Irregularities*, and SAS No. 54, *Illegal Acts by Clients*. The Act requires that audits of financial statements conducted pursuant to the Securities Exchange Act of 1934 include generally accepted auditing standards procedures designed to provide reasonable assurance of detecting illegal acts that would have a direct and material effect on the determination of financial statement amounts.

.03 An illegal act is defined as an "act or omission that violates any law, or any rule or regulation having the force of law." Under the Act, as under current practice, if the auditor "detects or otherwise becomes aware of information indicating that an illegal act (whether or not perceived to have a material effect on the financial statements of the issuer) has or may have occurred," the

auditor then (1) determines whether it is likely that an illegal act has occurred; (2) evaluates the possible effects of the illegal act on the issuer's financial statements; and (3) promptly informs the appropriate level of management and assures that the audit committee or board of directors is adequately informed with respect to the illegal act, unless it is clearly inconsequential.

Private Securities Reform Act of 1995

.04 The Act contains new reporting requirements that will come into play if the auditor:

- Determines that the audit committee or the board of directors is adequately informed with respect to illegal acts that "have been detected" or have otherwise come to the auditor's attention during the course of the audit, and
- Concludes that the illegal act has a material effect on the financial statements;
- Senior management has not taken, and the board has not caused it to take, "timely and appropriate remedial actions";[1] and
- The failure to take remedial action "is reasonably expected to warrant departure from a standard report of the auditor, when made, or warrant resignation from the audit engagement."

In that instance the auditor "shall, as soon as practicable," report its conclusions directly to the board.

.05 Under the new reporting requirements added by the Act, an issuer that receives the report described above must notify the SEC within one business day after receiving the report and must send a copy of that notice to the auditor. If the auditor does not receive the notice within the one day period, it must, whether or not it resigns, furnish a copy of its report (or documentation of an oral report) to the SEC within one business day after the failure of the issuer to give its required notice. Auditors are protected from liability in a private action "for any finding, conclusion, or statement" expressed in a report required of them under this provision. The SEC staff has stated that until the SEC adopts reporting requirements to implement this rule, any auditor faced with filing such a notice should contact the SEC staff at (202) 942-4400.

.06 The Fraud Detection and Disclosure section of the Act also reemphasizes the requirements that audits include:

- Procedures designed to identify related party transactions that are material to the financial statements or otherwise require disclosure therein. Note that appropriate procedures for identifying related parties and the related disclosure requirements are contained in SAS No. 45, *Omnibus Statement on Auditing Standards—1983*, "Related Parties," and Financial Accounting Standard No. 57, *Related Party Disclosures*. In addition, related party issues are discussed in Practice Alert 95-3, *Auditing Related Parties and Related Party Transactions* [section 16,050]; and

[1] "Remedial action" for this purpose may include: (1) taking appropriate disciplinary actions; (2) establishing policies, internal controls, and related monitoring procedures designed to safeguard against the recurrence of such illegal acts; and (3) as appropriate, reporting the effects of the illegal acts in the financial statements. SAS No. 54, paragraphs 17 and 18.

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

- An evaluation of whether there is substantial doubt about the ability of the issuer to continue as a going concern during the ensuing fiscal year. This provision of the Act is covered by SAS No. 59, *The Auditor's Consideration of an Entity's Ability to Continue as a Going Concern* (as amended by SAS No. 77, *Amendments to Statements on Auditing Standards No. 22*, Planning and Supervision, *No. 59*, The Auditor's Consideration of an Entity's Ability to Continue as a Going Concern, *and No. 62*, Special Reports).

Safe Harbor for Forward-Looking Statements

.07 The Act amends the Securities Act of 1933 and the Securities Exchange Act of 1934 by creating a new "safe harbor" for forward-looking statements made by an issuer, persons acting on behalf of the issuer, and any outside reviewer retained by the issuer to make a statement on the issuer's behalf. Under the Act, the term "forward-looking information" means:

a. A statement containing a projection of revenues, income, earnings per share, capital expenditures, dividends, capital structure, or other financial items;

b. A statement of management's plans and objectives for future operations, including plans or objectives relating to the issuer's products or services;

c. A statement of future economic performance, including any statement contained in management's discussion and analysis of financial condition or the results of operations included pursuant to SEC rules and regulations;

d. Any statement of the assumptions underlying or relating to any statement described in *a.*, *b.*, or *c.*;

e. Any report issued by an outside reviewer retained by the issuer, to the extent that the report assesses a forward-looking statement made by the issuer; or

f. A statement containing a projection or estimate of such other items as may be specified by SEC rules or regulations.

.08 However, the Act provides for certain exclusions to the safe harbor protection, most notably for forward-looking statements made in connection with an initial public offering or a tender offer, and forward-looking statements included in financial statements prepared in accordance with generally accepted accounting principles (historical financial statements). Additional exclusions are detailed in the Act.

.09 The safe harbor protection covers both written and oral forward-looking statements made by the registrant or those acting on the registrant's behalf. In addition, there is no requirement under the Act to update the forward-looking statements. To be protected by the Act, a written or oral forward-looking statement must:

1. Be identified as a forward-looking statement; and
2. Be accompanied by meaningful (not boilerplate) cautionary language identifying important factors that might cause the actual results to differ materially from those in the forward-looking statement.

If these conditions are not met, liability may be attached only if the plaintiff can prove that the forward-looking statement was made with actual knowledge that the statement was false or misleading.

.10 Oral forward-looking statements and cautionary language can satisfy the requirement of identifying important factors by making reference to a readily available written document, including a filing with the SEC.

.11 Companies may request that auditors advise them in the development and presentation of forward-looking statements, possibly extending to attesting to their assertions regarding such information. Other companies may only seek informal input in the process. Attempting to provide guidance for all situations is difficult, but the following should be helpful in relation to the level of service requested.

- *No substantive attention requested by the registrant*

  When no substantive work has been requested, the auditor's responsibility for forward-looking statements included in documents containing audited financial statements is discussed in SAS No. 8, *Other Information in Documents Containing Audited Financial Statements*, and SAS No. 37, *Filings under Federal Securities Statutes*. Basically, SAS No. 8 and SAS No. 37 require auditors to read other information, including any forward-looking statements, cautionary language, and important factors, and to consider whether such information, or the manner of its presentation, is materially inconsistent with the financial statement information or the manner of its presentation. This responsibility, of course, does not include opining on whether or not the disclosure meets the requirements of the safe harbor or any reasonableness or other review of the forecasted information. To assist client executives and directors in understanding this responsibility, auditors should discuss with them the auditor's responsibility for such information under generally accepted auditing standards as part of the required communications under SAS No. 61, *Communication with Audit Committees*, as amended, paragraph 10. The auditor may wish to add language to the engagement letter or other communications to clarify this understanding.

- *Substantive attention requested by the client, not leading to a report on such information*

  The company may engage the auditor to consult on the forward-looking statement, cautionary language, and important factors. Because of the subjective nature of this consultation, the extent of the auditor's involvement should be clarified with the company. In addition, documenting the discussions held and having an engagement letter are strongly encouraged. In any event, the auditor should be aware of the SEC's position that accountants who assist in the preparation of a forecast may not be independent from an SEC perspective and may not report on the forecast.

- *Substantive attention requested by the client, leading to a report on such information*

  The company may request the auditor to examine or perform agreed-upon procedures on the forward-looking statement, cautionary language, and important factors under Statements on Standards for Attestation Engagements, *Financial Forecasts and Projections*, and the 1993 *AICPA Guide for Prospective Financial Information*. The

 Copyright © 2001, American Institute of Certified Public Accountants, Inc.

auditors report on an *examination* of forward-looking statements can be issued to the public. The auditor should emphasize to the company, however, that any agreed-upon procedures report would be limited to client officials and the board of directors and that the company and others cannot refer to the report in public statements. If underwriters require comfort with respect to forward-looking information, the auditor should refer to SAS No. 72, *Letters for Underwriters and Certain Other Requesting Parties*, for guidance.

.12 Legal counsel has advised that auditor's reports with respect to forward-looking information are eligible for the statutory safe harbor. As long as the auditor is acting within the scope of the engagement (what the statute terms acting "on behalf of the issuer"), safe harbor protection is available for "any report issued by an outside reviewer retained by an issuer, to the extent that the report assesses a forward-looking statement made by the issuer." Thus, coverage would be available for an auditor's report on wholly prospective information (for example, a report on an issuer's projected financial results for the upcoming year) or for a report on information that is both prospective and historical, such as the MD&A (in which case the report would be protected only as it relates to the issuer's forward-looking statements). Because historical financial statements are exempt from the safe harbor, reports on those financial statements receive no safe harbor protection. (The statute does empower the SEC to issue rules extending safe harbor protection to financial statement information, but it is not clear whether the Commission will exercise this authority.) The auditor should consult with legal counsel in determining whether and to what extent a particular report meets the statutory requirements for safe harbor coverage.

.13 The SEC's previous efforts at encouraging the disclosure of forward-looking statements with safe harbor protection were not successful because of the uncertainty and perceived ineffectiveness of the previous safe harbor. The new safe harbor for forward-looking statements is intended to provide real protection to registrants and auditors that provide services in connection with such statements. As with the existing safe harbor (which remains in place), the ultimate effectiveness and extent of protection will be tested through practice and proven over time in the courts.

Effective Date of Provisions

.14 Most of the provisions of the Act, including the Safe Harbor for Forward-Looking Statements, became effective on Friday, December 22, 1995. However, the Fraud Detection and Disclosure provisions of the Act apply to annual reports for any period beginning on or after January 1, 1996, with respect to any registrant that is required to file selected quarterly financial data pursuant to SEC rules or regulations, and for any period beginning on or after January 1, 1997, with respect to any other registrant.

.15 This Practice Alert is not intended to represent a legal interpretation or description of the Act; auditors should seek advice from legal counsel for such information.

[The next page is 50,821.]

Section 16,070

Practice Alert 97-1
Members in Public Accounting Firms

First issued
January/February 1997;
Updated August, 1999

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits. This document has been prepared by the SEC Practice Section Professional Issues Task Force and is based on the experiences of the individual members of the task force and matters arising from litigation and peer reviews. It has not been approved, disapproved or otherwise acted upon by any committee of the AICPA.

Financial Statements on the Internet

.01 Generally accepted auditing standards (GAAS) provides guidance to independent auditors when clients publish documents that contain information (hereinafter "other information") in addition to audited financial statements and the independent auditor's report thereon. (See SAS No. 8, *Other Information in Documents Containing Audited Financial Statements.*) Examples of such documents include annual reports to shareholders, annual reports of not-for-profit organizations, and annual reports filed with regulatory authorities under the Securities Exchange Act of 1934.[1]

.02 Recent technology has changed the traditional means of disseminating information. Today, some entities are including their annual audited financial statements and related auditor's report on the Internet. The Internet is an interactive medium, where entities portray information in components referred to as "pages," which can be connected to other pages appearing elsewhere on the "Web site" through "hyperlinks." Thus, the commingling of data from various sources is controlled by the "reader" or "browser," rather than the traditional binding of tangible documents.

.03 The users of the new technology are different from the client personnel with whom the auditor most often interacts. Today, the technological frontier (the Internet) is largely a marketing arena, but those users are not limited to the familiar marketing tools. For example, an entity might decide to include (by embedding a hyperlink) marketing information in the revenue recognition section of their summary of significant accounting policies. Also, this marketing information might be updated weekly.

[1] SAS No. 8 is not applicable when financial statements and report appear in a registration statement filed under the Securities Act of 1933. See SAS No. 72, *Letters for Underwriters and Certain Other Requesting Parties*, as amended, and SAS No. 37, *Filings Under Federal Securities Statutes.*

.04 Auditors have recently asked questions regarding the dissemination of audit reports and the accompanying financial statements on the Internet, some of which are:

- Does an independent auditor have an obligation with respect to the ever-changing other information in an electronic site that contains audited financial statements and the related auditor's report?

  The Auditing Standards Board recently approved for issuance an interpretation to SAS No. 8 entitled "Other Information in Electronic Sites That Contain Audited Financial Statements," to address this question. The Interpretation advises that auditors do not have an obligation pursuant to SAS No. 8 to read or consider information included in an electronic site.

- How may a client ensure the security of information integrity when published on the Internet? Tales appear daily in the news media concerning hackers breaking into previously thought secure databases, and altering or deleting information.

  The auditor may wish to discuss these concerns with the client, so that the client may review the safeguards utilized to protect the data.

- Can a client who distributes its audited financial statements and auditor's report on the Internet set it up so that a user knows when they are hyper-linking to matters outside of that document?

  Yes, and at least one large organization has done so by creating distinct boundaries around its "annual report." Specifically, when users either enter or leave pages of the annual report, they are warned with a message. (Alternatively, entities might wish to clearly mark each page of the annual report information as being a part of the annual report.)

  Because of the way traditional documents are typically broken into much smaller "pages" for publishing on the Internet, it can be difficult for a user to locate a complete "document." Entities may wish to provide a facility on their site that would allow easy access to all parts of a document or the ability to download or print an entire document.

  Auditors may wish to discuss these matters with the client during the performance of the audit.

[The next page is 50,831.]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Section 16,080

Practice Alert 97-2
Audits of Employee Benefit Plans

First issued
May, 1997;
Updated April, 1999

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits. This document has been prepared by the SEC Practice Section Professional Issues Task Force (PITF) and is based on the experiences of the individual members of the task force and matters arising from litigation and peer reviews. It has not been approved, disapproved, or otherwise acted upon by any committee of the AICPA.

Introduction

.01 The AICPA Peer Review Program, the AICPA Professional Ethics Division, as well as the U.S. Department of Labor (DOL), continue to note a high rate of deficiencies on audits of employee benefit plans. These deficiencies primarily resulted from the auditor's failure to comply with professional auditing standards and DOL reporting requirements. Practitioners, whose work is considered deficient by the DOL's Pension and Welfare Benefit Administration (PWBA), are referred to state licensing boards and/or to the AICPA Professional Ethics Division, and could face severe consequences, including loss of license and loss of membership in the AICPA, if found to have performed deficient employee benefit plan audits. Plan administrators could face monetary civil penalties under ERISA section 502(c)(2) if found to have filed deficient audit reports.

.02 Employee benefit plans must meet a number of specialized financial, operational and regulatory requirements, and auditors have certain responsibilities for testing compliance with certain of those requirements. This Practice Alert is intended to assist auditors of employee benefit plans by providing an overview of the governmental oversight of employee benefit plans, the relevant financial accounting and reporting standards and the common deficiencies noted on such audits. This Practice Alert also includes best practices adopted by firms performing audits of employee benefit plans and an overview of current legislative developments which, if enacted, would significantly change the way employee benefit plan audits are conducted.

Governmental Oversight of Employee Benefit Plans

.03 The Employee Retirement Income Security Act of 1974 (ERISA) was enacted to protect the interests of workers who participate in employee benefit plans and their beneficiaries. To achieve this objective, ERISA requires financial

reporting to government agencies and disclosure to participants and beneficiaries, establishes standards of conduct for plan fiduciaries, and provides for appropriate remedies, sanctions, and access to the federal courts. ERISA also provides for substantial federal government oversight in the operating and reporting practices of employee benefit plans. The ERISA reporting requirements and the plans subject to those requirements are described in the AICPA Audit and Accounting Guide *Employee Benefit Plans*, with conforming changes as of May 1, 1999 (the AICPA Guide). This Practice Alert addresses employee benefit plans that are subject to ERISA.

Financial Accounting and Reporting Standards

.04 FASB Statement No. 35, *Accounting and Reporting by Defined Benefit Pension Plans*, established standards of financial accounting and reporting for financial statements of defined benefit pension plans, but did not establish standards for defined contribution plans or health and welfare benefit plans. The AICPA Guide provides comprehensive guidance, including the guidance prescribed by FASB Statement No. 35, on accounting, auditing, and reporting matters for defined benefit, defined contribution and health and welfare benefit plans.

.05 Employee benefit plans that are subject to ERISA are required to report certain information annually to federal government agencies—that is, the U.S. Department of Labor (DOL), Internal Revenue Service (IRS), and Pension Benefit Guaranty Corporation (PBGC) and to provide summarized information to plan participants. For many plans, the information is reported to the IRS on Form 5500, *Annual Return/Report of Employee Benefit Plan*, which includes financial statements and certain supplemental schedules (for example, plan investments and reportable transactions). Comments or questions on this Alert should be directed to the AICPA's SEC Practice Section at (201) 938-3022.

Common Deficiencies

.06 The PWBA has established an ongoing quality review program to enhance the quality of audit work performed by independent auditors in audits of plan financial statements that are required by ERISA. The AICPA, working with the PWBA, has made a concerted effort to improve the guidance available to auditors of employee benefit plans, and has incorporated such improvements in the AICPA Guide. The DOL strongly encourages the use of the AICPA Guide in meeting the requirements contained in ERISA. A complement to the AICPA Guide, the AICPA *Employee Benefit Plans Audit Risk Alert—1999*, (the AICPA Audit Risk Alert) provides an overview of recent economic, industry, regulatory, and professional developments. Both the AICPA Guide (Product No. 0123368QB) and the AICPA Audit Risk Alert (Product No. 022201QB) can be ordered from the AICPA Order Department at (888) 777-7077 by phone, or at (800) 362-5066 by fax.

.07 The PWBA, in their review of employee benefit plan audits, has noted the following common deficiencies:

a. Inadequate audit program or planning documentation. Such deficiencies included lack of a specific audit program tailored to the audit

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

of employee benefit plans, failure to obtain/review relevant plan documents, failure to understand the operations of the plan or current developments affecting the plan, and failure to address the area of prohibited transactions in the audit program. (Chapter 5 of the AICPA Guide provides guidance on audit planning, including the limited-scope audit exemption.)

b. *Inadequate documentation of the auditor's understanding of the plan's internal control.* Such deficiencies included either no work or significantly inadequate work with respect to obtaining a sufficient understanding of the plan's internal control. (Chapter 6 of the AICPA Guide provides guidance on internal control.)

c. *Inadequate documentation supporting the audit work performed and insufficient procedures performed.* Such deficiencies included failure to perform sufficient audit work related to participant data, benefit payments and/or plan obligations. (Chapters 9 and 10 of the AICPA Guide provide guidance in these areas.) Also, in certain instances, the auditor did not test the fair market valuations, investment transactions or authorizations for investment transactions. (Chapter 7 of the AICPA Guide provides guidance on investments.) In limited-scope engagements, the auditor did not obtain the proper certification from the bank or insurance company or the certification did not cover all of the plan assets. (Paragraphs 7.51 and 7.52 of the AICPA Guide provide guidance on limited-scope auditing procedures.) In audits of multi-employer plans, the auditor performed inadequate work relating to the contributions received from contributing employers. In certain participant-directed plans, the auditor did not agree the allocation of employee contributions to selected investment options. (Chapter 8 of the AICPA Guide provides guidance on contributions received and related receivables.)

d. *Deficiencies in the auditor's report.* Such deficiencies included failure to reflect a departure from generally accepted accounting principles, and failure to report on all the years presented. (Chapter 13 of the AICPA Guide provides guidance on, and examples of, auditor's reports.)

e. *Deficiencies in the note disclosures.* Such deficiencies included failure to disclose: the investments that represent 5 percent or more of the plan's net assets available for benefits (see paragraphs 2.26*g*, 3.28*g* and 4.57 of the AICPA Guide); information as to whether or not the plan has received a favorable tax determination ruling from the IRS (see paragraphs 2.26*f*, 3.28*f* and 4.57 of the AICPA Guide); the priorities of distribution of plan assets upon termination of the plan (see paragraphs 2.26*c*, 3.28*c* and 4.57 of the AICPA Guide); the funding policy of the plan (see paragraphs 2.26*d*, 3.28*d* and 4.57 of the AICPA Guide); information regarding the method and significant assumptions used to determine the actuarial present value of the plan's accumulated plan benefits as required by FASB Statement No. 35 (see paragraphs 2.20–2.24 of the AICPA Guide).

f. *Failure to comply with ERISA's or DOL's reporting and disclosure requirements.* The most common reporting and disclosure deficiencies were as follows: the auditor's report failed to extend to one or more of the required supplemental schedules (see paragraphs 13.09–13.18

of the AICPA Guide); the required supplemental schedules failed to include all the necessary information pursuant to ERISA and DOL regulations (see Appendix paragraphs A.51(b) and A.70–A.76 and Exhibit A-1 of the AICPA Guide); the plan administrator inappropriately invoked the limited-scope audit exemption when the financial institution holding the plan's assets did not qualify for such exemption because it was not a bank or similar institution or an insurance company (see Appendix paragraphs A.57–A.58 of the AICPA Guide); the statement of net assets was not presented in comparative form as required by DOL regulations (see Appendix paragraph A.51(*a*) of the AICPA Guide); the notes to the plan's financial statements failed to include certain information required by DOL regulations (for example, a note reconciling financial statement amounts to amounts reported in Form 5500 Series Annual Report) (see Appendix paragraph A.51(c) of the AICPA Guide); the audit was of the trust rather than of the plan (see Appendix paragraph A.55 of the AICPA Guide).

Best Practices

.08 To assist practitioners and CPA firms improve audit quality related to audits of employee benefit plans, and to reduce related enforcement and litigation risks, best practices used by firms in performing audits of employee benefit plans are noted below. These best practices were adapted from an article titled, "A Warning to CPAs on Employee Benefit Audits," by David M. Walker, CPA, in the June 1996 edition of the *Journal of Accountancy* (reprints may be obtained from the AICPA library at (888) 777-7077; available for AICPA members only). The best practices are as follows:

- Assign professionals trained in auditing employee benefit plans—preferably at the manager and/or senior level—to employee benefit plan audits, especially for higher-risk engagements. Factors that could be indicative of a high risk employee benefit plan audit include, among other things: plan sponsor financial difficulties; significant underfunding; volatile or non-readily marketable investments (for example, real estate and derivatives); plan amendments; changes in actuarial estimates or methods; plan merger, consolidation or termination; settlement of obligations or curtailment of accrual of benefits; initial audits; existence of prohibited transactions or unusual party-in-interest transactions; weak control environment (little or no direct plan sponsor involvement with plan administration); change in trustee, custodian or record keeper; report in accordance with Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, not available from trustee, custodian or third-party administrator; recent IRS or DOL investigation; and accounting changes.
- Perform second (concurring) partner reviews on higher-risk engagements (see above for factors that could be indicative of a high risk employee benefit plan audit). (Concurring partner reviews are required for members firms of the AICPA SEC Practice Section who audit plans that file Form 11-K.)
- Coordinate responsibility for employee benefit plan audits between audit and tax staff, so that qualified tax staff review the plan's tax status, transactions with parties-in-interest, and Form 5500.

 Copyright © 2001, American Institute of Certified Public Accountants, Inc.

- Ensure that engagement personnel have access to current guidance (see "Common Deficiencies" section above for a discussion of the AICPA Guide and the AICPA Audit Risk Alert). Ensure that engagement personnel have adequate training in employee benefit plan audits and any other related matters. (The AICPA sponsors an annual national conference on employee benefit plans, which provides hands-on interactive workshops in auditing, taxation, Form 5500 preparation, plan administration, and multi-employer plans; question and answer sessions with industry experts and government officials directly responsible for regulating employee benefit plans; and updates on all the recent and proposed employee benefit plan legislative and regulatory matters. The AICPA also offers the following self-study courses: Employee Benefit Plans I: Accounting Principles, Audits of Employee Benefit Plans, and Audits of 401(k) Plans. To obtain further information about the conference and the self-study courses, call (888) 777-7077.
- Use standardized engagement tools and documentation approaches. The AICPA has published checklists for defined benefit, defined contribution and health and welfare plans. The checklists include both industry specific and general disclosure requirements, and can be ordered from the AICPA Order Department at (888) 777-7077.
- Use the AICPA's publication, *Financial Statement Reporting and Disclosure Practice for Employee Benefit Plans* (Product No. 008725), which gives examples on required disclosure for employee benefit plan financial statements.
- Ensure that the CPA firm's internal inspection or monitoring program addresses employee benefit plan audit engagements and that engagement reviews are performed by qualified personnel.
- Use technical hotlines and support services provided by the AICPA and various state societies. The AICPA's Technical Information Division offers a hotline for accounting and auditing practice questions, and can be reached, free of charge to AICPA members, at (888) 777-7077. The AICPA's Tax Information Phone Service ("TIPS") offers a hotline for federal, state and local tax questions, and can be reached at (888) 777-7077, option 3, or members can submit questions through the AICPA Web site (see http://www.aicpa.org/feedback/index.htm). TIPS charges a fee of $3 per minute (with a $30 minimum) from January 15 to April 15 and $2 per minute (with no minimum) the rest of the year, whether the query is by phone or through the Web site. The fee is billed to the member's MasterCard, Visa or Discover credit card. Also, the PWBA encourages auditors and plan filers to call its Division of Accounting Services at (202) 219-8794 with ERISA-related accounting and auditing questions and questions regarding preparation of Form 5500. Questions concerning filing requirements should be directed to the PWBA's Division of Reporting Compliance at (202) 219-8770.
- Consider engaging the services of another CPA firm, experienced in employee benefit plan accounting, audit and ERISA matters, when necessary and appropriate.

Implementing these best practices can significantly improve audit quality and client service and reduce related enforcement and litigation risks.

Recent Developments

.09 In June 1998, the Financial Accounting Standards Board issued Statement No. 133, *Accounting for Derivative Instruments and Hedging Activities*. FASB No. 133 applies to employee benefit plans, although most plans do not hold such instruments. The AICPA's publication, *Employee Benefit Plans—1999 Audit Risk Alert*, describes the accounting effects of FASB No. 133 relating to employee benefit plans.

.10 There are currently two proposed Statements of Positions (SOPs) relating to employee benefit plans. The two SOPs would amend the Audit and Accounting Guide *Employee Benefit Plans*, SOP 92-6, *Accounting and Reporting by Health and Welfare Benefit Plans* [section 10,530], and SOP 94-4, *Reporting of Investment Contracts Held by Health and Welfare Benefit Plans and Defined-Contribution Plans* [section 10,620].

Service Organizations

.11 Many plans are now offering their participants on-line access to their 401(k) plans. In such circumstances, participants can review their accounts, and change their investment elections at any time, even from home. Because plan participants can change their investments daily, by telephone or via Intranet sites, daily valuations of such plans are becoming commonplace with virtually no record of the changes being maintained by the service provider of the plan. Additionally, more and more services are being "bundled" and provided by one service provider. These service providers execute transactions and maintain accountability on behalf of the plan administrator. For example, outside service organizations such as, bank trust departments, insurance companies, and benefits administrators may maintain records and process benefit payments. Often, the plan sponsor does not maintain independent accounting records of transactions executed by the service provider. In fact, many plan sponsors no longer maintain records such as participant enrollment forms detailing the contribution percentage and the allocation by fund option, and this amount can be changed by telephone or on-line without any record. In these situations, the auditor may be unable to obtain a sufficient understanding of internal controls relevant to transactions executed by the service organization in planning the audit and determining the nature, timing and extent of testing to be performed without considering those components maintained by the service organization. These circumstances require an understanding of the requirements of SAS No. 70, *Service Organizations*, and additional explanation is described in Practice Alert 99-2, *How the Use of a Service Organization Affects Internal Control Considerations* [section 16,140].

Year 2000 Issues*

.12 Generally, the Year 2000 issues are the entity's management's responsibility and not the auditor's. Management must assess and remediate the affects of the Year 2000 issue on an entity's system. Under generally accepted auditing standards, the auditor has the responsibility to plan and perform the audit to obtain reasonable assurance whether the financial statements are free of material misstatement. Thus, the auditor's responsibility relates to the detection of material misstatement of the financial statements being audited, whether caused by the Year 2000 issues or by some other cause.

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

.13 However, auditors should be aware of the auditing and accounting issues that arise from the Year 2000 issue, including audit planning, going-concern issues, establishing an understanding of the services to be provided to the client, impairment of revenue and expense recognition, and disclosure. A more comprehensive discussion of this topic can be found in AICPA's *1999 Audit Risk Alert*. Additional information on Year 2000 Issues can be found on the AICPA's website.

[The next page is 50,841.]

Section 16,090

Practice Alert 97-3
Changes in Auditors and Related Topics

First issued
November, 1997;
Updated August, 1999
and April, 2004

NOTICE TO READERS

This Practice Alert is intended to provide practitioners with information that may help them improve the effectiveness and efficiency of their engagements and practices and is based on existing professional literature, the experience of members of the Professional Issues Task Force ("PITF") and information provided by certain AICPA member firms to their own professional staff. This information represents the views of the members of the PITF and has not been approved by any senior technical committee of the AICPA. The auditing portion of this publication is an *Other Auditing Publication* as defined in Statement on Auditing Standards (SAS) No. 95, *Generally Accepted Auditing Standards. Other Auditing Publications* have no authoritative status; however, they may help the auditor understand and apply SASs. If an auditor applies the auditing guidance included in an *Other Auditing Publication*, the auditor should be satisfied that, in his or her judgment, it is both appropriate and relevant to the circumstances of the subject audit. This publication was reviewed by the AICPA Audit and Attest Standards staff and published by the AICPA, and is presumed to be appropriate.

Introduction

.01 The purpose of this Practice Alert is to provide practitioners with guidance regarding appropriate procedures after a successor auditor has accepted an engagement to audit financial statements.

.02 Practice Alert 03-3, *Acceptance and Continuance of Clients and Engagements* [section 16,260] provides practitioners and their firms with guidance regarding the establishment of policies and procedures for deciding whether to accept or continue a client relationship and whether to perform a specific engagement for that client. The alert provides guidance with respect to following elements of an effective client acceptance program:

- Availability of competent personnel to perform the engagement.
- Communication with predecessor accountants or auditors.
- Assessment of management's commitment to the appropriate application of generally accepted accounting principles.
- Assessment of management's commitment to implementing and maintaining effective internal control.
- Assessment of the entity's financial viability.
- Independence and objectivity, including how the firm can mitigate possible impairment threats from significant clients.

- Inquiry of third parties.
- Background investigations.

The alert is currently available on the AICPA's Web site at: http://www.aicpa.org/download/secps/pralert_03_03.pdf

.03 A predecessor auditor is an auditor who (*a*) has reported on the most recent audited financial statements or was engaged to perform but did not complete an audit of the financial statements and (*b*) has resigned, declined to stand for reappointment, or been notified that his or her services have been, or may be, terminated. Predecessor auditors must consider relevant issues when they are asked by a former client to reissue their reports on previously audited financial statements. Such issues include the need to decide whether to reestablish a client relationship, including consideration of the former client's intended use of the predecessor auditor's report. For example, a former client's request that a predecessor auditor reissue his or her report in connection with an initial public offering would expose the predecessor auditor to additional risk that was not contemplated at the time the original report was issued.

Review of Audit Documentation

.04 After accepting the engagement, the successor auditor should request the client to authorize the predecessor auditor to allow a review of the predecessor auditor's audit documentation. In such situations, the predecessor auditor may want to obtain written notification of such a request in an effort to reduce or avoid misunderstandings. Appendix A to SAS No. 84 provides an illustrative client consent and acknowledgment letter which the predecessor auditor may wish to send the former client. It is customary that the predecessor auditor make himself or herself available to the successor auditor as well as certain audit documentation for review. Pursuant to SAS No. 84, the predecessor auditor should ordinarily permit the successor auditor to review audit documentation including documentation of planning, internal control, audit results and other matters of continuing accounting and auditing significance.

.05 Before permitting access to the audit documentation, the predecessor auditor may wish to obtain a written communication from the successor auditor regarding the use of the audit documentation. Appendix B to SAS No. 84 includes an illustrative successor auditor acknowledgment letter. The purpose of the letter is to clarify the use of the audit documentation between the predecessor auditor and the successor auditor. This often provides the predecessor auditor more comfort in allowing unrestricted access to the audit documentation and may lead to a smoother transition.

Opening Balances

.06 The responsibility for the opening balances on the current year financial statements and consistency of accounting principles always rests solely with the client and the successor auditor. The successor auditor must obtain sufficient competent evidential matter to afford a reasonable basis for expressing an opinion on the financial statements under audit, including evaluating the consistency of the application of accounting principles. The nature of the tests to be performed and the extent of evidence obtained in auditing the opening balances on the current-year financial statements and consistency of accounting principles is a matter of professional judgment.

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

.07 Evidence that may be obtained that will help a successor auditor determine the nature, timing and extent of auditing procedures to be applied to opening balances may include the following:

1. The most recently audited financial statements and the predecessor auditor's opinion thereon. The successor auditor may also consider making inquiries about the professional reputation and standing of the predecessor auditor in forming his or her opinion on the opening balances. For example, a firm with a sound reputation in the business community and an unqualified peer review report would normally give the successor auditor more comfort with respect to opening balances than if the predecessor auditor was unknown and their peer review report was qualified. Peer review reports can be requested from the firm. In addition, peer review reports for member firms of the AICPA Center for Public Company Audit Firms and for members of the PCPS: the AICPA Alliance for Member Firms can be obtained from the following Web site: http://www.aicpa.org/centerprp/publicfile01.htm.
2. The results of inquiries made to predecessor auditors. For example, a successor auditor would normally have a greater degree of comfort based on responses from a predecessor auditor that there were no disagreements with respect to the application of accounting principles or auditing procedures. Also, a successor auditor should consider the impact on opening balances when the predecessor auditor informs the successor auditor that his or her response to questions and access to certain audit documentation was limited.
3. The results of the successor auditor's review of the predecessor auditor's audit documentation relating to the most recently completed audit may affect the nature, timing, and extent of the successor auditor's procedures. For example, upon reviewing a predecessor auditor's audit documentation with respect to contingencies at the beginning of the year, the successor auditor may conclude that the predecessor auditor's assessment of internal controls, substantive testing, and evaluation of misstatements is sufficient to preclude applying procedures to prior year transactions, and may take comfort from a current year attorney's letter or other procedures.
4. The results of audit procedures performed on the current period's transactions that may provide evidence about the opening balances or consistency. For example, evidence gathered during the current year's audit may provide information about the existence and valuation of receivables and inventory recorded at the beginning of the year.

.08 In those rare circumstances where a successor auditor is not allowed access to a predecessor auditor's audit documentation, the successor auditor should consider the implications on whether the successor auditor will be able to obtain sufficient competent evidential matter to afford a reasonable basis for expressing an opinion on the financial statements under audit. A successor auditor should not necessarily interpret a refusal for access to a predecessor auditor's audit documentation as a need to perform an audit of the previously audited financial statements.

.09 In all circumstances, the successor auditor should use professional judgment in determining the nature, timing, and extent of procedures to be performed on opening balances. Such procedures, as outlined in 1, 2 and 4 above, will assist the successor auditor in determining the need to perform an audit of the previously audited financial statements.

Requests to Reissue Reports

.10 Predecessor auditors may be asked to reissue their report on financial statements for a number of reasons, including requests made by a former client to include a predecessor auditor's report in a registration statement filed with the SEC. In such situations, the predecessor auditor is, in effect, being asked to reestablish a client relationship and should consider the ramifications of that decision.

.11 Before consenting to the inclusion of his or her report on previously audited financial statements, a predecessor auditor should perform procedures similar to its client acceptance and continuation procedures as required by Statement on Quality Control Standards No. 2, *System of Quality Control for a CPA Firm's Accounting and Auditing Practice* (QC section 20, paragraphs .14 through .16). In determining the nature and extent of client acceptance and continuation procedures as required by QC 20, an auditor might consider the guidance contained in Practice Alert 03-3, *Acceptance and Continuance of Clients and Engagements* [section 16,260]. That alert is currently available on the AICPA's Web site at: http://www.aicpa.org/download/secps/pralert_03_03.pdf.

.12 Such procedures would typically include an evaluation of whether specific events have occurred to determine whether a relationship with the former client should be reestablished, including a major change in one or more of the following: (1) management; (2) directors; (3) ownership; (4) legal counsel; (5) financial condition; (6) litigation status; (7) nature of the company's business; and (8) the scope of the engagement. Additionally, an auditor should determine whether he or she should be associated with a client that has selected, or may select, an underwriter that has been the subject of adverse publicity or that has matters reported on the underwriter's Form BD that raise questions or concerns about the underwriter. Similarly, an auditor should consider the professional reputation and experience of both the successor auditor and legal counsel who is or will be associated with subsequent years' financial statements.

.13 After consideration of the above, and other relevant factors, but before consenting to reissuance of his or her report, the predecessor auditor should consider whether that report is still appropriate in the circumstances. The auditor should perform procedures on events occurring subsequent to the date or period of the most recent financial statements. The nature and extent of the procedures will vary depending on the circumstances of the particular situation, but generally consist of the following (as per SAS No. 58, *Reports on Audited Financial Statements*, as amended):

If a successor auditor has audited the financial statements of the most recent period following the period audited by the predecessor auditor, subsequent events procedures may consist of the following:

- Reading the financial statements for the current period (or the entire registration statement if the financial statements are included in a filing with the SEC).
- Comparing the financial statements that were reported on by the predecessor auditor with the financial statements to be presented in the registration statement (or other document).
- Obtaining a letter from the successor auditor indicating whether their audit has disclosed any events or transactions subsequent to the period covered by the most recent statement of income (or

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

the date of the latest balance sheet) audited by the predecessor auditor that, in the successor auditor's opinion, would have a material effect on, or require disclosure in the financial statements reported on by the predecessor auditor.

.14 SAS No. 85, *Management Representations*, adds the additional requirement that a predecessor auditor obtain a representation letter from management of the former client in conjunction with reissuing his or her report on previously audited financial statements. This representation letter from management should state that nothing came to management's attention that would cause them to believe that any of their previous representations should be modified and whether any events have occurred subsequent to the balance sheet date of the latest prior period financial statements reported on by the predecessor auditor that would require adjustment to or disclosure in those financial statements. Appendix C to SAS No. 85 includes an illustrative management representation letter that might be obtained in these circumstances. In addition to the above described procedures, an auditor should consider the relevant guidance in SAS No. 1, section 543, *Part of Audit Performed by Other Independent Auditors*, as amended, paragraphs .10 through .12, which provides suggested procedures that may be performed when additional evidential matter might be necessary in the circumstances.

.15 If, after performing the procedures enumerated above and other procedures considered necessary in the circumstances, a predecessor auditor becomes aware of events or transactions occurring subsequent to the date of his previous report that may require an adjustment, additional disclosure, or reclassification to the financial statements previously reported on, the predecessor auditor should make inquiries and perform other procedures that are considered necessary in the circumstances.

.16 The extent of such procedures is a matter of professional judgment and will vary depending on the effect of the items on the financial statements previously issued. For example, reviewing the reclassification of a line of business as discontinued operations for comparative purposes with the subsequent year's treatment, resulting from a subsequent decision made by the company, would generally require less extensive procedures than those that may be required in connection with the correction of an error in previously issued financial statements. In such instances, the predecessor auditor might consider requesting a review of the audit documentation of the successor auditor in those areas related to the matter affecting the prior-period financial statements. Based on the evidence obtained, the predecessor auditor should then decide whether to revise the previously issued report. When reissuing his or her report on prior-period financial statements, a predecessor auditor should use the date of his or her previous report; if the financial statements are restated or the predecessor auditor revises the previous report, the report should be dual dated. If the predecessor auditor decides not to revise the previously issued report when the financial statements have been restated, the successor auditor should follow the guidance in SAS No. 58, paragraph 74, as amended.

.17 If successor auditors have not been engaged, or if engaged, have not performed an audit of the subsequent financial statements or sufficiently familiarized themselves with the accounting policies, control environment and other pertinent aspects of the company, the predecessor auditor's subsequent events review procedures might be the same as those performed by a continuing auditor in accordance with SAS No. 1, section 560, *Subsequent Events*, as amended.

.18 After considering the above or other relevant factors, an auditor may decide not to consent to the use of his or her previously issued report. The AICPA's

Code of Professional Conduct, Statements on Auditing Standards (SAS No. 58, as amended, paragraph 70) and the rules and regulations of the SEC do not require an independent certified public accountant who has performed a financial statement audit, to subsequently sign a consent for inclusion of that report in a registration statement filed with the SEC, or for any other reason. Additionally, SAS No. 58, as amended, does not require the predecessor auditor to communicate or disclose the reasons why that auditor decided not to reissue his or her audit report and there is no requirement for disclosure of those reasons to the entity or its audit committee, as a client relationship does not exist.

Use of Indemnification Clauses When Reissuing Reports

.19 In many instances, the risk of litigation that results from the inclusion of a predecessor auditor's report on financial statements of a former client may be such that a predecessor auditor might decide not to reissue his or her report unless the former client agrees to indemnify them for legal and other costs that might be incurred in defending itself, in the event of threatened or actual litigation, associated with knowing misrepresentations by management. In general, AICPA Ethics Ruling No. 94 (ET section 191.188–.189) allows obtaining such indemnification agreements. However, SEC rules related to independence prohibit indemnification agreements between auditors and current publicly-held clients.

.20 As a result of discussions between the AICPA and the SEC, the staff of the SEC agreed not to question a predecessor auditor's independence with respect to a former audit client if that former audit client agrees to indemnify the predecessor auditor for the payment of legal costs and expenses that the predecessor auditor might incur in defending itself against legal actions or proceedings that arise as a result of the consent of that predecessor auditor to the inclusion of its auditor's reports on the former audit client's prior year's financial statements in a new registration statement provided that: (1) Such indemnification letter would be void and any advanced funds would be returned to the former client if a court, after adjudication, found the former auditor liable for malpractice, and (2) The indemnification provision is entered into after a successor auditor has issued an audit report on the former client's most recent financial statements included in the registration statement of the former client.

Audits of Financial Statements Previously Audited

.21 In September 2002, the Professional Issues Task Force issued Practice Alert 02-3, *Reauditing Financial Statements* [section 16,230]. The Alert provides practitioners with information that may help them when they are engaged to reaudit and report on financial statements that have been previously audited by another auditor. The alert is currently available on the AICPA's Web site at: http://www.aicpa.org/members/div/secps/lit/practice/pralert_02_03.htm.

Reporting as Successor Auditor When Prior-Period Audited Financial Statements Were Audited by a Predecessor Auditor Who Has Ceased Operations

.22 In November 2002, the AICPA issued Auditing Interpretation No. 15 to SAS No. 58. The Interpretation provides guidance regarding the effect on the

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

successor auditor's report when the prior-period financial statements audited by a predecessor auditor who has ceased operations are presented for comparative purposes with current-period audited financial statements.

.23 The Interpretation is available using the following web address: http://www.aicpa.org/members/div/auditstd/announce/interpsas58.htm.

[The next page is 50,851.]

Section 16,100

Practice Alert 98-1
The Auditor's Use of Analytical Procedures

First issued
May, 1998;
Updated August, 1999

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits and is based on existing audit literature, the professional experience of the members of the Professional Issues Task Force (PITF) and information provided by SECPS member firms to their own professional staff. This information represents the views of the members of the PITF and is not an official position of the AICPA. Official positions are determined through certain specific committee procedures, due process and deliberation. The information provided herein should be used by practitioners with the understanding that it be read in conjunction with the professional literature and only as a means of assisting them in meeting their professional responsibilities.

Introduction

.01 Analytical procedures are defined by Statement on Auditing Standards (SAS) No. 56, *Analytical Procedures*, as "evaluations of financial information made by a study of plausible relationships among both financial and nonfinancial data." Analytical procedures are used in all three main phases of an audit: planning, substantive testing and overall review. The use of analytical procedures in the planning and overall review phases of an audit is required under generally accepted auditing standards and plays an important role in assisting the auditor in determining the nature, timing and extent of his or her substantive testing and in forming an overall opinion as to the reasonableness of recorded account balances.

.02 The use of analytical procedures in the substantive testing phase of the audit is a consideration left to the judgment of the auditor and may or may not be a preferred choice to traditional detail tests of transactions. However, the use of analytical procedures typically enables the auditor to perform substantive tests that provide sound audit evidence, assists the auditor in better understanding a client's business, and when performed properly, may result in a more efficient and effective means of testing an account balance.

.03 This Practice Alert provides guidance to practitioners on:

- Applying substantive analytical procedures through discussion of certain key concepts and definitions related to forming expectations of recorded balances,
- Difficulties noted in the performance of analytical procedures, and
- How analytical procedures can assist the auditor in evaluating the risk of fraud.

Substantive Analytical Procedures—Key Concepts and Discussion

.04 Developing analytical procedures is a four-step process that consists of: (1) the development of an expectation; (2) the identification of fluctuations; (3) the investigation of material fluctuations and (4) the evaluation of the likelihood of material misstatements being present in the financial statements.

.05 The following discussion focuses on definitions and concepts pertinent to an auditor's development of an expectation and how accurate that expectation should be based on the risk characteristics of a particular engagement and should be read in conjunction with SAS No. 56 and the AICPA Publication *Analytical Procedures—Auditing Practice Release* (the "APR").

Expectations

.06 Expectations are the auditor's prediction of what a recorded account balance or ratio *should* be. Auditors may be less likely to detect significant unexpected differences in the financial statements of a client when an expectation has not been properly developed. In forming an expectation, the auditor must determine that the relationship between the items used to develop the expectation and the recorded amount is plausible because the items might sometimes appear to be related when they are not, leading to erroneous conclusions. Plausible relationships are best defined as relationships expected to exist based on the auditor's understanding of the client and the industry in which the client operates.

.07 To gain this understanding the auditor might analyze forces external to the client's industry, the client's position within the industry and the processes the client has in place to achieve its objectives. The auditor might also consider the results of prior years audits, the client's budgeted and actual amounts, discussions held with client personnel responsible for the preparation of recorded account balances or ratios and financial and nonfinancial results of comparable entities operating in the industry.

.08 An expectation is typically developed using one or more of the following types of internally prepared data: prior year data adjusted for expected change; current period data; budgets or forecasts; and nonfinancial data from within the entity. These types of data might be considered independent and reliable if they are consistent with current business conditions and not subject to influence or manipulation by persons involved in the accounting functions related to the account balance being tested.

.09 Often, the account balance being tested can be estimated using data external to the entity. Sources of external information might include: government agencies (e.g., changes in tax rates); industry regulators, trade associations, industry surveys (e.g., bank interest rates); published financial information for companies of a similar size and/or with similar characteristics in the same industry; and securities exchanges.

.10 The auditor should consider the following factors which may limit or preclude the use of external information: industry statistics may be biased by the results of one or two major players within the industry; the client's activities may not match those that are covered by the information; industry statistics may only reflect prior year history; and the quality of industry statistics depends upon the degree of care taken by the industry participants in completing periodic returns.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.11 In assessing the relationship between data used and the account balance being tested, the auditor should give consideration to the following factors: data may exist for only a part of the account balance being tested (e.g., comparable industry data is only available for certain of the products sold by the company); the relationship is circular or deterministic (e.g., predicting sales balances from commissions when commissions are calculated as a percentage of sales); the effects of changes in relationships, seasonality and lags (e.g., the client may have discontinued a product line, sales are in peak seasons, or the item of audit interest may be related to data of a prior period, such as the collectibility of receivables may be based on sales that occurred in prior periods).

.12 The auditor should also bear in mind that relationships in income statement account balances tend to be more predictable than relationships involving only balance sheet accounts. Income statement account balances generally represent accumulations of similar transactions processed over a period of time and often have a predictable relationship with other data. Balance sheet items are the residual balance from transactions at specific points in time and are often more subject to management discretion.

.13 The level of disaggregation and reliability of the data used in forming an expectation determines, in part, the precision with which the auditor can estimate an account balance. The desired precision of the expectation can vary according to the purpose of the analytical procedure. For example, an auditor would typically want more precision in performing substantive-type analytical procedures than in performing preliminary analytical procedures during planning. Generally, the higher the level of disaggregation of the data, the more precise the expectation will be. The reliability of the data is influenced by whether the data is:

- Audited
- From independent sources outside the entity
- From sources within the entity that are independent from those responsible for the amount being tested
- Subject to a reliable system of internal controls

Research has shown that incorrect expectations have been formed by the use of unreliable data and have led to incorrect audit conclusions. The auditor should exercise professional skepticism in considering the reliability of data used in forming expectations.

.14 *Precision*—Precision is a measure of the closeness of the auditor's expectation to the actual amount (which may or may not be the recorded amount). Factors that affect the level of precision of an expectation include the basis upon which the expectation is developed (such as trend analysis, ratio analysis, reasonableness testing or regression analysis), the level of disaggregation of the data, the reliability of the data and the nature of the account balance being tested (e.g., income statement accounts might be less difficult to develop expectations for than balance sheet accounts).

.15 *Trend analysis*—Trend analysis is the analysis of change(s) in an account balance over time and is most appropriate when the account or relationship is fairly stable. Conversely, trend analysis is less effective in situations when the entity being audited has experienced significant operating or accounting changes. Trend analysis typically produces the most effective results and higher levels of assurance when performed on disaggregated data, because at an aggregate level it tends to be relatively imprecise.

.16 When using this type of analytical procedure, an auditor needs to gain a sufficient understanding of the environment and its associated volatility as it relates to the account being tested. Because trend analysis does not take into account changes in the business environment in which an entity operates, it is often suited for account balances where lower levels of assurance are necessary to reduce detection risk to acceptable levels. Trend analysis is often most useful to the auditor when used in conjunction with the planning and overall review stages of the audit. Refer to the upcoming APS for case study examples on the effective use of trend analysis.

.17 *Ratio Analysis*—Ratio analysis is the comparison of relationships between financial statement accounts (between two periods or over time), the comparison of an account to nonfinancial data, or the comparison of relationships between entities operating within an industry. Ratio analysis may be considered most appropriate when the relationship between accounts is fairly predictable and stable.

.18 Ratio analysis, like trend analysis, typically produces the most effective results and higher levels of assurance when performed on disaggregated data, because at an aggregate level it tends to be relatively imprecise. Refer to the APR for case study examples on the effective use of ratio analysis.

.19 *Reasonableness testing*—Reasonableness testing is the analysis of account balances or changes in account balances within an accounting period which involves the development of an expectation based on financial and/or nonfinancial data. Reasonableness tests rely on the auditor's knowledge of the entity and the environment in which it operates to develop expectations of an account balance. As an example of a reasonableness test, an auditor might consider using the number of employees hired and terminated, the timing of pay changes, and the effect of vacation and sick days to develop a model that could predict the change in payroll expense from the previous year to the current balance. Refer to the upcoming APS for case study examples on the effective use of reasonableness testing.

.20 *Regression analysis*—Regression analysis involves the use of statistical models to quantify the auditor's expectation(s) with measurable risk and precision levels. Regression analysis bears a resemblance to reasonableness testing in that it involves using the auditor's knowledge of the factors that affect the account balance in developing a model to predict it. Because regression analysis often involves the use of internally prepared data, it is most effective in assisting the auditor in detecting material misstatements in account balances when the data is disaggregated and is from an accounting system with good internal controls.

.21 For analytical procedures used as substantive tests, the precision of the expectation developed is the primary determinant of how much assurance the auditor may obtain from such tests. In other words, the more assurance an auditor needs to obtain from analytical procedures on account balances where the risk of misstatement is high, the more precise his or her expectation needs to be. Because it involves the development of an expectation based on relatively sophisticated models, regression analysis generally tends to give the auditor more precision than any of the previously mentioned methods. Refer to the upcoming APS for case study examples on the effective use of regression analysis.

Level of Assurance

.22 The level of assurance that must be obtained in any audit testing is the amount of assurance the auditor needs to reduce detection risk to an

 Copyright © 2000, American Institute of Certified Public Accountants, Inc.

acceptable level. The level of assurance an auditor actually receives from a substantive analytical procedure is the degree to which the analytical procedure actually reduces audit risk. As such, an auditor plans the level of assurance he or she wishes to achieve in performing analytical procedures based on risk assessment in the planning stages of the audit. As the level of assurance needed from an analytical procedure increases, the auditor should design the analytical procedure with a corresponding level of precision.

.23 *Confirmation of Accounts Receivable and the Use of Analytical Procedures*—In certain circumstances, auditors have concluded that it may be more effective to use analytical procedures as an alternative to confirmations when testing accounts receivable. Auditing standards presume that confirmation procedures are generally performed in conjunction with testing of accounts receivable.

.24 The decision to utilize alternative procedures may be reached only after the auditor has carefully concluded that one of the following three conditions are present (SAS No. 67, *The Confirmation Process*, paragraphs 34 and 35): (1) accounts receivable are immaterial to the financial statements; (2) the use of confirmations would be ineffective; or (3) the assessed level of inherent and control risk is low, and the assessed level, in conjunction with the evidence expected to be provided by analytical procedures or other substantive tests of details, is sufficient to reduce audit risk to an acceptably low level. The auditor's conclusions should be documented in the working papers.

.25 In the event that confirmations are not used when testing accounts receivable balances and the auditor decides to use analytical procedures as substantive tests, the analytical procedures should be designed with a high level of precision in order to gain a tolerable level of assurance.

Difficulties in Applying Substantive Analytical Procedures and Ways to Avoid Them

.26 While analytical procedures can potentially improve audit efficiency and effectiveness, they also require the use of significant audit judgment in identifying and investigating unexpected fluctuations. Some of the difficulties posed and ways to address them were discussed in an article that appeared in the Nov. 1997 *Journal of Accountancy* entitled "When Judgment Counts" (reprints may be obtained from the AICPA library at (888) 777-7077; available for AICPA members only). These issues are generally discussed below.

.27 *Using Unaudited Balances as a Starting Point*—Auditors should be careful not to use management's unaudited balance as a starting point in determining what a recorded balance should be without also looking to other predicative factors. For example, assume an auditor forms an expectation of what a recorded cost of sales balance should be based on a client's unaudited sales balance. In developing an expectation for what sales should be, the auditor used a trend analysis. It is unlikely that either result in this example has actually been audited in that the auditor has not developed an expectation on an independent basis using sufficiently reliable data. SAS No. 56 includes specific wording that instructs the auditor of his or her responsibility to develop an independent expectation using reliable data.

.28 While auditors should be careful not to let unaudited account balances unduly influence their development of expectations of an account balance they

should also be aware that unaudited information, independent of the accounting function, may provide reliable information to assist in developing an expectation.

.29 *Unusual Fluctuations Might Reflect a Pattern*—SAS No. 56 indicates that an auditor should evaluate significant differences between an expectation that he or she has developed and the amount recorded in the financial statements. In addition, an auditor should take care to recognize a pattern of fluctuations which may be necessary to correctly identify the cause of a fluctuation. Tendencies to examine each account without regard to combinations of financial discrepancies may result in problematic situations being overlooked.

.30 As an example, assume an auditor has developed an expectation related to sales that is significantly lower than the actual recorded balance. In addition, the results of positive confirmations in accounts receivable indicated a number of discrepancies. These two problems, in combination, might indicate to the auditor that the sales balance and related receivables balance are misstated. Should the auditor consider the discrepancies noted in each balance in isolation, there might be a tendency to "explain" each discrepancy away without seeing a potentially serious issue.

.31 *Placing Reliance on Management's Explanations*—Auditors should use discretion in using management as a first resource in explaining unexpected fluctuations as a client's explanation might limit the auditor's consideration of other likely causes. An explanation that is offered by management in situations where the auditor cannot readily explain the variance between his or her expectation and the recorded amount should be carefully evaluated as to both its reasonableness in explaining the variance noted and its effect(s) on other accounts.

.32 Information which may provide plausible explanations for fluctuations that should be considered by the auditor might include: an understanding of matters noted while performing audit work in other areas, particularly while performing audit work on the data used to develop an expectation; inquiries of client personnel unrelated to the preparation of the financial statements, analytical procedures performed in the planning stage of the audit; management and board reports containing explanations of variances between budgeted and actual results; and review of minutes of meetings.

.33 *Developing Expectations at the Appropriate Level of Disaggregation*—In addition to the issues identified in the *Journal of Accountancy* article, auditors should be careful while performing substantive analytical procedures to use data at an appropriate level of disaggregation. Use of data that is disaggregated at the appropriate level is important in allowing the auditor to assess the risk of material misstatement in the financial statements.

.34 For example, an auditor would have more information on which to base a conclusion on sales balances if that amount were considered on a monthly or quarterly basis than on an annualized basis. Generally, the more complex and non-routinely processed the amount to be tested is, the more difficult it is to develop an expectation that is sufficiently precise to provide adequate assurance that material misstatement does not exist.

.35 By not analyzing data at the appropriate level of disaggregation, an auditor may not be as likely to detect unusual fluctuations caused by significant non-routine journal entries in the final quarter of a client's fiscal year.

 Copyright © 2001, American Institute of Certified Public Accountants, Inc.

Unusual non-routine journal entries, if recorded consistently by the client over a period of years, would not necessarily be detected by the auditor when analyzing data on an aggregate level. Such fourth quarter adjustments might alert the auditor to an audit area requiring additional testing or even be indicative of the possibility of fraud.

Analytical Procedures and Fraud Detection

.36 The results of analytical procedures do not provide the auditor with the necessary evidence to determine if fraud has resulted in a material misstatement to the financial statements. However, analytical procedures, performed during the planning, substantive testing and overall review stages of the audit, do provide the auditor with a tool in determining if account balances might have an increased chance of having been subjected to fraud. Accordingly, analytical procedures can assist the auditor in fulfilling his or her responsibilities under paragraph 12 of SAS No. 82, *Fraud in a Financial Statement Audit*, which states, in part, that "The auditor should specifically assess the risk of material misstatement of the financial statements due to fraud and should consider that assessment in designing the audit procedures to be performed."

.37 SAS No. 82 requires that an auditor should specifically assess the risk of material misstatement of the financial statements due to fraud and consider that assessment in designing his or her audit procedures. Analytical procedures have the potential to detect the possible existence of fraud during the planning stage by directing the auditor's attention to unexpected fluctuations or relationships. By performing such procedures at the appropriate level of disaggregation, the auditor has the potential to detect where such fraud might be present.

.38 Even in situations where the auditor expects the client to adjust its trial balance after the completion of preliminary analytical procedures, he or she should consider whether some accounts, such as debt, might be less likely to be adjusted than others, such as expense accounts. In these situations, the auditor would still be able to analyze certain accounts in the planning stages and assess the likelihood that a material misstatement might exist.

.39 SAS No. 82 indicates that if certain risk factors are present that would indicate the likelihood of fraud, the auditor might respond by performing substantive analytical procedures at a more detailed level.

[The next page is 50,871.]

Section 16,110

Practice Alert 98-2
Professional Skepticism and Related Topics

First issued
September, 1998;
Updated August, 1999

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits and is based on existing audit literature, the professional experience of the members of the Professional Issues Task Force (PITF) and information provided by SECPS member firms to their own professional staff. This information represents the views of the members of the PITF and is not an official position of the AICPA. Official positions are determined through certain specific committee procedures, due process and deliberation. The information provided herein if used by practitioners should be used with the understanding that it is read in conjunction with the professional literature and only as a means of assisting them in meeting their professional responsibilities.

Introduction

.01 Generally accepted auditing standards requires the auditor to exercise due professional care in the planning and performance of the audit and in the preparation of the auditor's report. Due professional care requires the auditor to exercise professional skepticism, which can be best defined as an attitude that includes a questioning mind and working practices that encompass a critical assessment of audit evidence. Since evidence is gathered and evaluated throughout the audit, professional skepticism should be exercised throughout the entire audit process. In gathering and evaluating evidence, including obtaining management representations, the auditor should neither assume that management is dishonest nor assume unquestioned honesty. Exercising professional skepticism means that the auditor should not be satisfied with less than persuasive evidence. Although representations obtained from management are part of the evidential matter the independent auditor obtains, they are rarely by themselves sufficient evidence to afford a reasonable basis for an opinion regarding the financial statements taken as a whole.

.02 There have been a number of instances in the past when misstated audited financial statements have been issued when the auditor may not have exercised adequate professional skepticism during the audit. While it is not possible to list all sensitive areas where this might occur, experience suggests that the following areas should be among those subject to particular scrutiny:

- Management responses to questions resulting from analytical reviews.
- Representations regarding recoverability of assets or deferred charges.

- Accruals (or lack thereof), particularly for unusual events or transactions.
- Substance of large and unusual (particularly period-end) transactions.
- Vague contract terms or conditions.
- Non-standard journal entries and copies of original documents (see further discussion below).

.03 Regular reminders to members of the firm and professional staff of the need to exercise appropriate professional skepticism would be useful in avoiding potential problems. This Practice Alert provides guidance to practitioners in two areas which may warrant a relatively high level of professional skepticism and attention to audit evidence: (1) the review of non-standard journal entries, and (2) the review of original and final versions of source documents rather than photocopies or draft versions in these two areas. This Practice Alert also provides a comprehensive list of previously issued Practice Alerts.

The Auditor's Review of Non-Standard Journal Entries

.04 Statement on Auditing Standards (SAS) No. 55, *Consideration of Internal Control in a Financial Statement Audit*, as amended by SAS No. 78, *Consideration of Internal Control in a Financial Statement Audit: An Amendment to Statement on Auditing Standards No. 55* requires the auditor to obtain a sufficient understanding of the information system relevant to financial reporting to understand:

- The classes of transactions in the entity's operations that are significant to the financial statements.
- How those transactions are initiated (e.g., manual or computerized).
- The accounting records, supporting information, and specific accounts in the financial statements involved in the processing and reporting of transactions.
- The accounting processing involved from the initiation of a transaction to its inclusion in the financial statements, including electronic means used to transmit, process, maintain and access information.
- The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures.

SAS No. 78 also notes that such knowledge should be used to identify types of potential misstatements, consider factors that affect the risk of material misstatement, and design substantive tests.

.05 In today's complex computerized environments, reviewing the general ledger for non-standard journal entries has changed significantly from years ago when the general ledger could be manually scanned for evidence of non-standard journal entries. Standard journal entries include those journal entries processed in the normal course of business, such as sales, inventory purchases and cash disbursements. Non-standard journal entries are ones that are made outside the normal course of business, such as the provision for loan losses, provision for inventory obsolescence and cut-off or period-end adjustments. Non-standard journal entries may pose increased risk to the auditor in

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

that they might conceal attempts by management to manipulate earnings and can be recorded in practically any account.

.06 Auditors may find that certain accounts might contain transactions processed in the normal course of business and some that are not. As an example, consider accounts payable, which may contain routine postings from the accounts payable subsidiary ledger to the general ledger, but may also contain entries to reconcile the two ledgers. The accounts payable account balance may also include debits to the account with an offset entry intended to inflate earnings. Since accounts payable is often subject to a high volume of activity, such reconciling entries or miscellaneous debits, or non-standard journal entries, may be difficult for the auditor to detect.

.07 In order to determine which transactions are not subject to processing in the normal course of business, the auditor should consider whether the client has an established routine, or set of procedures, for processing a class of transactions on a recurring basis. Often, there will be an established routine whose recording is frequently recurring and is important to the day-to-day operation and management of the business. Routine processing does not necessarily or exclusively involve computer systems. Most processing involves a combination of manual and automated steps and procedures.

.08 Transactions processed in the normal course of business generally have less risk of misstatement than other transactions. In order to identify transactions processed outside the normal course of business, particularly in computerized environments, the auditor may need to use computer-assisted audit techniques, such as report writers, software or data-extraction tools, or other systems-based techniques. The functionality of the software and proper processing with the client data files is essential to produce credible evidence. Electronic evidence often requires extraction of the desired data by a knowledgeable auditor or a specialist. SAS No. 31, *Evidential Matter*, as amended by SAS No. 80, *Amendment to Statement on Auditing Standards No. 31*, Evidential Matter, provides guidance for auditors who have been engaged to audit the financial statements of an entity that transmits, processes, maintains or accesses significant information electronically. In addition, the AICPA published an Auditing Procedures Study, *The Information Technology Age: Evidential Matter in the Electronic Environment*, to provide auditors with non-authoritative guidance on applying SAS No. 80. Account balances which might be subject to misstatement may be identified by the auditor in assessing whether each significant account balance:

- Contains journal entries processed outside the normal course of business.
- Contains transactions that are complex or unusual in nature.
- Contains estimates and period-end adjustments.
- Contains journal entries indicative of potential problems with the accounting systems.
- Has been prone to client error in the past.
- Has not been reconciled on a timely basis or contains old reconciling items.
- Represents a particular risk specific to the client's industry.
- Represents account balances affecting the client's value and liquidity (e.g., account balances that are used in determining loan covenant ratios).

The Auditor's Review of Original and Final Source Documents

.09 During the course of an audit of financial statements, auditors are frequently provided with photocopies or draft versions of documents, rather than original and final source documents. Of course, photocopies can be made of virtually every type of audit evidence, including bank statements, invoices, legal agreements, etc., and by accepting photocopies or draft versions as audit evidence, the auditor risks that the photocopy may not conform to the original and final source document. Also, with the advances in modern technology, scanners can also be used to alter documents. As an example, consider that bank statements can be altered and photocopies to reflect higher cash balances, invoices can be falsified to reflect sales which did not take place and legal agreements can be amended so that the photocopy does not reflect the actual agreement in place.

.10 SAS No. 82, *Consideration of Fraud in a Financial Statement Audit*, states that the unavailability of other than photocopied documents when documents in original form are expected to exist may pose a risk of material misstatement due to fraud. When presented with photocopied documents, the auditor should exercise professional skepticism and consider the need to obtain the original source documents to ensure conformity to the photocopied documents.

.11 Also, when reviewing a document other than an original, there may be situations when an auditor receives a facsimile confirmation response rather than a written communication mailed directly to the auditor. A facsimile response may create some risk because it may be difficult to ascertain the source of the response. While the facsimile response may include the name and facsimile number of the entity sending the document, the auditor should assess the risk that the sender might have falsified that information. SAS No. 67, *The Confirmation Process*, states that to restrict the risk associated with facsimile responses and treat the confirmations as valid audit evidence, the auditor should consider taking certain precautions, such as verifying the source and contents of a facsimile response in a telephone call to the purported sender. In addition, the auditor should consider requesting the purported sender to mail the original confirmation directly to the auditor.

[The next page is 50,881.]

 Copyright © 2001, American Institute of Certified Public Accountants, Inc.

Section 16,120

Practice Alert 98-3 Responding to the Risk of Improper Revenue Recognition

First Issued November, 1998; Updated April, 2004

NOTICE TO READERS

This Practice Alert is intended to provide practitioners with information that may help them improve the effectiveness and efficiency of their engagements and practices and is based on existing professional literature, the experience of members of the Professional Issues Task Force (PITF) and information provided by certain AICPA member firms to their own professional staff. This information represents the views of the members of the PITF and has not been approved by any senior technical committee of the AICPA. The auditing portion of this publication is an *Other Auditing Publication* as defined in Statement on Auditing Standards (SAS) No. 95, *Generally Accepted Auditing Standards. Other Auditing Publications* have no authoritative status; however, they may help the auditor understand and apply SASs. If an auditor applies the auditing guidance included in an *Other Auditing Publication*, the auditor should be satisfied that, in his or her judgment, it is both appropriate and relevant to the circumstances of the subject audit. This publication was reviewed by the AICPA Audit and Attest Standards staff and published by the AICPA, and is presumed to be appropriate.

Introduction

.01 A substantial portion of litigation against accounting firms and a number of SEC Accounting and Auditing Enforcement Releases involve revenue recognition issues. Many of these issues result from alleged improper accounting treatment of sales recorded in the ordinary course of a client's business. Such improper accounting treatment ranges from allegedly stretching the accounting rules to falsifying sales in an effort to manage earnings. Therefore, auditors need to pay attention to warning signals that may indicate increased audit risk with respect to revenue recognition and respond with appropriate professional skepticism and additional audit procedures.

.02 This Practice Alert is intended to remind auditors of certain factors or conditions that can be indicative of increased audit risk of improper, aggressive or unusual revenue recognition practices, and suggests ways in which auditors may reduce the risk of failing to detect such practices. This Practice Alert also refers to professional guidance which addresses the accounting considerations for revenue recognition, and it reminds auditors of their responsibilities to communicate with the board of directors and audit committees.

Required Risk Assessment

.03 SAS No. 99, *Consideration of Fraud in a Financial Statement Audit,* requires the auditor to ordinarily presume that improper revenue recognition is a

fraud risk on all audit engagements. The key threshold is "should ordinarily". If the auditor does not identify improper revenue recognition as a risk of material misstatement due to fraud, the auditor should document the reasons supporting that conclusion.

.04 In addition, the Appendix to SAS No. 99 provides examples of fraud risk factors relating to fraudulent financial reporting, almost all of which may be relevant to revenue recognition.

Improper, Aggressive or Unusual Revenue Recognition Practices

.05 Auditors need to consider the possibility that client personnel at various levels may participate in schemes that result in the overstatement of revenue. In some cases, customers and suppliers may be involved in such schemes as well. Client officials may be aware they are overstating revenue or may simply believe they are reflecting economic substance from their perspective. Revenue recognition principles are sometimes difficult to apply and often vary by industry. A high level of care is always required in this area, but if the auditor becomes aware of certain factors or conditions, as outlined below, special consideration may be required.

Audit Planning Considerations

.06 To reduce the risk of improper revenue recognition, the audit needs to be planned and executed with an appropriate degree of professional skepticism. In planning the audit, the auditor should obtain a sufficient understanding of the client's industry and business, its products, its marketing and sales policies and strategies, its internal controls, and its accounting policies and procedures related to revenue recognition. During the planning phase of the audit, the auditor should seek to identify conditions that increase the risk of misstatement. Those conditions may include:

- A change in the company's revenue recognition policy.
- New product or service introductions or new sales arrangements.
- Sales terms that do not comply with the company's normal policies.
- Existence of longer than expected payment terms or installment receivables.
- Significant sales or volume of sales that are recorded at or near the end of the reporting period.
- Individually significant sales.
- Unusual or complex revenue transactions.
- Unusual volume of sales to distributors/ resellers (i.e., "channel stuffing").
- Sales billed to customers prior to the delivery of goods and held by the seller ("bill and hold" or "ship-in-place" sales).
- The use of non-standard contracts or contract clauses.
- The use of letters of authorization in lieu of signed contracts or agreements.
- Transactions with related parties.
- Transactions involving barters, swaps, "round-trip" or "back-to-back."

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

- The existence of "side-agreements."
- Multiple-element arrangements.
- Revenue recognition when right of return exists.
- Control environment considerations, such as:
  - — Aggressive accounting policies or practices.
  - — Pressure from senior management to increase revenues and earnings.
  - — Lack of involvement by the accounting/finance department in sales transactions or in the monitoring of arrangements with distributors.

.07 The auditor's understanding should include the procedures for receiving and accepting orders, shipping goods, relieving inventory, and billing and recording sales transactions. A sufficient understanding of a client's policies with respect to acceptable terms of sale and an evaluation of when revenue recognition is appropriate given those terms is essential. It is also essential that the auditor have an understanding of the computer applications and key documents (e.g., purchase orders, shipping reports, bills of lading, invoices, credit memos, etc.) used during the processing of revenue transactions.

.08 The auditor's knowledge base of the revenue recognition cycle provides a perspective or mindset for determining the nature, timing, and extent of audit procedures to be applied. For example, a company operating in a declining industry or one characterized by frequent business failures ordinarily will present different audit considerations and may require different or more extensive audit procedures than a company operating in a healthy industry. Similarly, the risk of management misrepresentation may be greater when management's compensation is based to a significant degree on reported earnings or when management places undue emphasis on meeting analysts' earnings projections. Even when additional revenues do not contribute much to earnings (e.g., immature companies operating at a loss), recognize that many of these companies are valued based on increased revenues. Risk also may be heightened when there are frequent disputes or disagreements with management concerning the aggressive application of accounting principles. A proper understanding of a client's business, its accounting policies and procedures, and the nature of its transactions with customers is also useful in assessing the extent of experience or supervision required of the personnel assigned to audit revenue transactions. Certain unusual or complex sales contracts may signal the need for more experienced engagement personnel.

.09 The performance of well-planned analytical procedures during the audit planning process and in executing the audit itself (such as, a comparison of sales and customer receivable cash collections to corresponding periods of the prior year and to budgeted amounts; a review of monthly and/or quarterly sales volume analyses; a review of sales credits and returns subsequent to year-end; and comparisons of agings of accounts receivable portfolios in the current and prior periods) may assist the auditor in identifying situations that warrant additional consideration. A company constantly increasing sales that "always meets or exceeds" budgeted sales targets and that result in the "build-up" of accounts receivable may warrant extra attention. When a substantial portion of the company's sales occur at the end of the accounting period, extra caution in auditing revenue transactions is appropriate. Also, individually significant revenue transactions, which could be designed to ease short-term profit concerns, may merit specific attention. Caution should also be

exercised when "bill and hold" sales exist. Auditors need to examine such transactions and obtain an understanding of the transaction's business purpose to evaluate whether revenue recognition is appropriate.

Brainstorming

.10 SAS No. 99 requires that engagement teams conduct a brainstorming session as part of the planning process. One of the main objectives of the brainstorming session is to set the "tone at the top" by challenging any preconceived assumptions and bias that the engagement team members may have regarding the client and to remind the engagement team members to exercise professional skepticism during the course of the audit. The brainstorming session will also allow the team to exchange ideas about how and where they believe the entity's financial statements might be susceptible to material misstatements due to fraud, how that fraud might be concealed, and how the auditor might respond.

.11 Knowledge of common frauds related to improper revenue recognition can help engagement teams conduct more effective brainstorming sessions. Typical revenue recognition frauds include:

- Sales in which evidence indicates the customer's obligation to pay for the merchandise depends on:
  - — receipt of financing from another (third) party;
  - — resale to another (third) party (i.e., sale to distributor, consignment sale); or
  - — fulfillment by the seller of material unsatisfied conditions.
- Sales of merchandise that are shipped in advance of the scheduled shipment date without evidence of the customer's agreement or consent.
- Pre-invoicing of goods that are in the process of being assembled or invoicing prior to, or in the absence of, actual shipments.
- Shipments are made after the end of the period (i.e., books kept open to record revenue for products shipped after the period end).
- Sales are not based on actual (firm) orders to buy.
- Shipments are made on canceled or duplicate orders.
- Shipments are made to a warehouse or other intermediary location without the instruction of the customer.
- Shipments that are sent to and held by freight forwarders pending return to the company for required customer modifications.
- Altered dates on contracts or shipping documents.

.12 Many fraud schemes are designed to accelerate the recognition of revenue; however, the auditor should be alert for conditions that may motivate management to delay revenue recognition. For example, when sales estimates for a subsequent year are soft and management has met their earnings target for the current year, they may be tempted to improperly delay revenues into the next year. Additionally, an owner of a privately held entity may be motivated to improperly delay revenue recognition as a means of minimizing taxable income.

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Audit Response

.13 If there is an identified risk of material misstatement due to fraud that involves improper revenue recognition, the auditor may want to consider:

- Performing substantive analytical procedures related to revenue using disaggregated data, for example, comparing revenue reported by month and by product line or business segment during the current reporting period with comparable prior periods. Computer-assisted audit techniques may be useful in identifying unusual or unexpected revenue relationships or transactions.
- Confirming with customers certain relevant contract terms and the absence of side agreements, because the appropriate accounting often is influenced by such terms or agreements. For example, acceptance criteria, delivery and payment terms, the absence of future or continuing vendor obligations, the right to return the product, guaranteed resale amounts, and cancellation or refund provisions often are relevant in such circumstances.
- Inquiring of the entity's sales and marketing personnel or in-house legal counsel regarding sales or shipments near the end of the period and their knowledge of any unusual terms or conditions associated with these transactions.
- Being physically present at one or more locations at period end to observe goods being shipped or being readied for shipment (or returns awaiting processing) and performing other appropriate sales and inventory cutoff procedures.
- For those situations for which revenue transactions are electronically initiated, processed, and recorded, testing controls to determine whether they provide assurance that recorded revenue transactions occurred and are properly recorded.
- Examining inventory reports or other correspondence from distributors and reconciling that information with the company's records.
- Vouching all large or unusual sales made at quarter-end and year-end to original source documents.
- Performing a detailed review of the entity's quarter-end and year-end adjusting journal entries and investigating any that appear unusual as to nature or amount.
- Scanning the general ledger, accounts receivable subledger, and sales journal for unusual activity.
- Checking the clerical accuracy of the revenue journal or similar record and tracing the postings of the totals to the appropriate account in the general ledger.
- Checking the reconciliation of revenue journals during the audit period to the general ledger control account, or checking the postings to the general ledger control account from sources other than the revenue journal for unusual or unexpected activity.
- Analyzing and reviewing deferred revenue accounts at the end of the period for propriety of deferral.
- Analyzing and reviewing credit memos and other accounts receivable adjustments for the period subsequent to the balance sheet date.

- Scanning the general ledger or subsidiary ledgers, as appropriate, for a period subsequent to year-end for reversals of sales or large sales returns.
- Reviewing significant year-end contracts for unusual pricing, billing, delivery, return, exchange, or acceptance clauses. Performing post-year-end specific review for contract revisions or cancellations and for refunds or credits issued.
- As part of the accounts receivable confirmation effort, confirming with customers the terms of sales agreements, including the absence of right of return and terms that might preclude immediate revenue recognition.
- Comparing operating cash flow to sales; analyze by salesperson, location or period.

Confirmations and Management Representations

.14 In January 2003, the PITF issued Practice Alert 03-1, *Audit Confirmations* [section 16,240], to emphasize the importance of the confirmation process. Additionally, the Alert focuses practitioners on the other benefits of confirming accounts besides confirmation of balances and discourages performing alternative procedures in lieu of confirming balances and information. The Alert also provides practical guidance regarding non-responses to positive confirmation requests, confirmations received via fax or electronically, and use of client personnel in the confirmation process.

.15 The Alert can be downloaded using the following web address: http://www.aicpa.org/download/secps/pralert_03_01.pdf.

.16 SAS No. 85, *Management Representations*, requires the auditor to obtain written representations from management relating to the following: financial statements; completeness of information; recognition, measurement and disclosure; and subsequent events. Although representations from management are not a substitute for application of audit procedures designed to afford a reasonable basis for an opinion on the financial statements, the auditor may consider it useful to obtain written representations concerning specific revenue recognition issues, such as the terms and conditions of unusual or complex sales agreements. Such representations may include confirmation that there are no contingencies that affect the obligation of customers to pay for merchandise purchased, and may also include confirmation regarding the existence of side agreements. This is particularly important when it is common industry practice to provide customers with certain rights of return or other privileges (e.g., in high-technology enterprises). In addition to obtaining representations from management, auditors should consider making inquiries of others familiar with the transactions (e.g., sales personnel), aside from the accounting and finance personnel, and consider whether there is a need to also obtain written representations from those individuals.

Accounting Considerations

.17 Revenue is defined in FASB Concept Statement No. 6, *Elements of Financial Statements*, paragraph 78, as follows:

> "Revenues are inflows or other enhancements of assets of an entity or settlements of its liabilities (or a combination of both) from delivering or producing goods, rendering services, or other activities that constitute the entity's ongoing major or central operations."

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Further, FASB Concepts Statement No. 5, *Recognition and Measurement in Financial Statements of Business Enterprises*, paragraph 83 states that the recognition of revenue involves consideration of two factors:

- Being realized or realizable and
- Being earned.

.18 Paragraph 84(a) of FASB Concepts Statement No. 5 states that revenues from manufacturing and selling activities are commonly recognized at the time of the sale, usually meaning delivery.

.19 The auditor should be aware that many pronouncements have been issued with respect to revenue recognition. The auditor should consider those pronouncements that are relevant to the client's industry and the types of transactions in which the client engages when performing the audit.

Communications With Board of Directors/Audit Committees

.20 Shareholders rely on the board of directors and its audit committee to monitor company performance and make decisions that serve the best interests of the company and its shareholders. SAS No. 61, *Communication With Audit Committees*, requires the auditor to ensure that the audit committee (defined as those parties who have oversight of the financial reporting process) receives additional information regarding the scope and results of the audit that may assist the audit committee in overseeing the financial reporting and disclosure process for which management is responsible. Certain matters are required to be communicated, as follows: the auditor's responsibility under generally accepted auditing standards; significant accounting policies; management judgments and accounting estimates; audit adjustments; auditor's judgments about the quality of an entity's accounting principles; other information in documents containing audited financial statements; disagreements with management; consultation with other accountants; major issues discussed with management prior to retention; and difficulties encountered in performing the audit.

.21 The communication by the auditor to the board of directors/audit committee should include a discussion related to revenue recognition practices of the company, including matters such as a change in the company's revenue recognition policy, a lack of involvement by the accounting/finance department in sales transactions or in the monitoring of arrangements with distributors, significant sales or volume of sales that are recorded at or near the end of the reporting period, sales terms that do not comply with the company's normal policies, etc.

Conclusion

.22 No audit can be designed to provide absolute assurance that all revenue recorded by the client is appropriate or that fraudulent financial reporting is discovered. However, an awareness of conditions that increase audit risk, along with an appropriate skeptical response to issues identified during the planning process and during the performance of field work, can help auditors increase the likelihood that either inadvertent or intentional material misstatements of revenue will be detected.

[The next page is 50,891.]

Section 16,130

Practice Alert 99-1
Guidance for Independence Discussions With Audit Committees

May, 1999

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits and is based on existing audit literature, the professional experience of the members of the AICPA SEC Practice Section Professional Issues Task Force (PITF) and information provided by AICPA SEC Practice Section member firms to their own professional staff. The information in this Practice Alert represents the views of the members of the PITF and is not an official position of the AICPA. Official positions are determined through certain specific committee procedures, due process and deliberation. The information provided herein should be used by practitioners with the understanding that it be read in conjunction with the professional literature and only as a means of assisting them in meeting their professional responsibilities.

.01 In January 1999, the Independence Standards Board (ISB) adopted Independence Standard No. 1, *Independence Discussions with Audit Committees* (the "Standard"). The Standard states that it applies to any auditor intending to be considered an independent accountant within the meaning of the Securities Acts administered by the Securities and Exchange Commission (SEC). This should be considered to include an auditor with respect to any entity for which his or her engagement is required to comply with SEC Regulation S-X.[1] The Standard requires annual written and oral communications between the auditor and the audit committee (or the board of directors if there is no audit committee) of a public company client regarding relationships that, in the auditor's professional judgment, may reasonably be thought to bear on independence, as well as written confirmation that the auditor is independent of the company within the meaning of the Securities Acts. Such communications are required with respect to audits of entities with fiscal years ending after July 15, 1999, with earlier application encouraged.

.02 The Standard can be obtained from the ISB website at www.cpaindependence.org. The ISB has expressed its belief that the Standard will improve corporate governance by affording to audit committees a mandated opportunity to deepen their understanding of auditor independence issues. The ISB believes the Standard will assist directors in satisfying themselves that the

[1] The Standard applies to auditors of domestic and foreign registrants. The Standard would also apply where a regulatory agency (such as the Office of the Comptroller of the Currency (OCC)) undertakes to have auditors of entities under its jurisdiction comply with SEC Independence Rules. It is noted that an auditor might contractually obligate himself or herself to follow Regulation S-X. An example might be a private company intending to have a public offering in the future and the desire of management to have the auditor meet all SEC requirements.

company has engaged "independent" accountants as required by the Securities Acts. The ISB also believes that a mandate that audit firms describe and discuss the judgmental matters that might impact on independence will bring more focus within the firms on this important issue.

.03 Additionally, *The Report and Recommendations of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees* (the "Blue Ribbon Committee Report"), issued in February 1999, included a recommendation that the listing rules for both the New York Stock Exchange and the National Association of Securities Dealers require audit committee charters to specify that the audit committee is responsible for ensuring receipt of the communication required by the Standard.

.04 This recommendation also indicated the charter should specify that the audit committee is responsible for actively engaging in a dialogue with the auditors relating to the disclosure of any relationships or services that may impact the objectivity and independence of the auditor and should take appropriate action, if necessary, to ensure the continued independence of the auditor. To address implementation issues relative to the Standard, the Professional Issues Task Force of the AICPA SEC Practice Section (PITF) has been asked to develop initial guidance for CPA firms. The guidance in this PITF Alert is designed to assist firms in evaluating and enhancing their policies and procedures for identifying and communicating with audit committees those judgmental matters that may reasonably be thought to bear on the auditor's independence.

.05 These communications in turn should serve to assist audit committees/boards of directors in fulfilling certain of their responsibilities relative to corporate governance. These communications also will assist auditors in fulfilling their responsibilities to serve the interests of the public and strengthen the public's confidence in audited financial information reported by registrants. The following discussion is in the context of communications between the auditor and the audit committee/board of directors. This should not be construed as precluding the auditor from having similar communications with senior management. Indeed, the PITF encourages such communications.

Firm Policies and Procedures

.06 Firms should establish policies and procedures relating to independence communications with audit committees. These policies and procedures should be distributed to all professional staff to enhance their awareness of independence issues and reaffirm professional standards. The following information may be a useful framework for developing these policies and procedures.

Determination of Matters to Be Communicated

.07 The Standard requires auditors to communicate, in writing, at least annually all relationships between the auditor and the company that, in the auditor's professional judgment, may reasonably be thought to bear on independence. In determining which relationships to discuss, the auditor should not conclude that a relationship need not be disclosed solely because he or she has concluded that independence is not impaired. The auditor should consider whether the audit committee, which, as stated in the Blue Ribbon Committee Report, may be viewed as a "guardian of investor interests and corporate accountability," would consider the disclosure and discussion of the relationship beneficial to further its understanding of auditor independence in the company's specific circumstances. While the decision regarding the matters to

 Copyright © 2001, American Institute of Certified Public Accountants, Inc.

be communicated will vary in each circumstance, and that decision is ultimately the auditor's, consideration should be given to communicating and discussing with the audit committee all non-audit services that the auditor has agreed to perform for the client.

.08 Exhibit A provides examples of certain relationships that, depending on the specific facts and circumstances, may commonly be thought to bear on the auditor's independence. Exhibit A also includes relevant safeguards to ensure the auditor's continued independence.

Exhibit A

Consideration of Relationships and Other Matters That May Bear on Independence

This Exhibit provides examples of relationships that, depending on the specific facts and circumstances, may reasonably be thought to bear on independence, along with typical safeguards that, if in place, may mitigate threats to the auditor's independence. The information that follows may be used as a guide in determining the types of relationships that may be disclosed by the auditor. These examples should not be considered all-inclusive, nor should it be construed that the example relationships would be required to be disclosed by all auditors in all cases.

Employment:[2]

Disclosure of Relationship: The former audit engagement partner joined the audit client as Vice President and Chief Financial Officer.

Safeguards: The accounting firm conducted a review of all services for this client that were performed by the former partner for an appropriate period preceding the employment offer and did not note any matters which would cause the firm to believe the former partner and the firm were not independent of the company. The accounting firm performed a review of the appropriateness of the assignments of the succeeding engagement partner and concurring review partner and considered the need for involvement of other partners with appropriate experience and stature to ensure an appropriate level of professional skepticism is maintained.

In addition, the accounting firm and the former partner have severed all relationships, including settlement of the former partner's capital account and settlement of retirement benefits to the extent required by the SEC's independence rules.

Disclosure of Relationship: The former audit engagement manager joined the audit client as Controller.

Safeguards: The accounting firm conducted a review of all services for this client that were performed by the former manager for an appropriate period preceding the employment offer and did not note any matters which would cause the firm to believe the former manager and the firm were not independent of the company. The accounting firm performed a review of the appropriateness of the assignment of the remaining engagement team to ensure that an appropriate level of professional skepticism is maintained.

Disclosure of Relationship: The office managing partner in the local office of the accounting firm accepted a position with the audit client as Chief Operating Officer. Such partner provided no professional services to the company prior to his/her employment.

Safeguards: The accounting firm performed a review of the appropriateness of the assignments of engagement partner and concurring review partner and considered the need for involvement of other partners with appropriate experience and stature to ensure an appropriate level of professional

(*continued*)

[2] On March 12, 1999, the ISB issued a Discussion Memorandum, *Employment with Audit Clients*, to seek comments on a variety of independence issues when audit firm personnel accept employment with audit clients. Practitioners should be alert for developments in this area.

 Copyright © 2000, American Institute of Certified Public Accountants, Inc.

Exhibit A—continued

skepticism is maintained. In addition, the accounting firm and the former partner have severed all relationships, including settlement of the former partner's capital account and settlement of retirement benefits to the extent required by the SEC's independence rules.

Family Relationships:

Disclosure of Relationship: The audit client's Controller is the wife of a manager in the accounting firm's [city] office.

Safeguards: The accounting firm's manager will be restricted from performing any work for the audit client and his office will not participate in a significant portion of the audit engagement. All of the work on the engagement for the audit client will be performed by the accounting firm's office in [other city].

Disclosure of Relationship: One of the accounting firm's partners has a brother who is a director of the audit client.

Safeguards: Neither the partner nor the office to which he is assigned has any involvement in the accounting firm's engagement for the audit client. Further, the partner and his office are adequately geographically separated from both the residence of his brother and the office of the accounting firm performing the work on the engagement.

Non-audit Services:

Disclosure of Relationship: The accounting firm has been engaged to perform the following non-audit services:

- Extended audit services by outsourcing the internal audit function. Annual fees for this engagement are approximately [amount of fees].
- Assistance in the implementation of an accounting system [describe the system implemented]. Fees for this engagement were approximately [amount of fees].

Safeguards: In each case, management of the audit client has sufficient expertise to take responsibility for all management decisions that will be made and the accounting firm will not assume the role of an employee or of management of the audit client.

Other Separate Business Arrangements Involving Mutual Clients:

Disclosure of Relationship: The accounting firm and the audit client entered into separate business arrangements to provide advisory and consulting services which dealt with [describe nature of accounting firm's services] to a mutual third party. Fees for such services totaled approximately [amount of accounting firm's fees].

Safeguards: We believe this engagement does not constitute doing business with the client. In proposing for the services, the role of the accounting firm and the audit client were clearly defined through the use of separate proposals indicating the services for which each party was responsible. The third party has contracted separately with the accounting firm and the audit client such that neither party is dependent on the other party's performance and each party's liability and contractual obligations are separate.

Engaging the Audit Committee

.09 While the auditor must make the decision as to what is reported to the audit committee, engaging the audit committee chair in discussions regarding his or her views on relationships that may reasonably be thought to bear on independence may be a worthwhile approach to begin the process. If this approach is used, the audit committee chair should be asked by the auditor to express his or her views and concerns regarding the types of relationships that may reasonably be thought to bear on independence and, accordingly, would be expected to be disclosed. It is reasonable to assume that expectations may vary from company to company and the level of sensitivity as to independence issues may vary as well. These discussions should foster an open channel of communication between the parties relative to independence and other matters and should assist the auditor in understanding the audit committee's expectations regarding the types of relationships to be discussed.

.10 While the PITF believes these discussions are worthwhile and should facilitate a meaningful discussion with the audit committee, in the final analysis, it is the auditor's judgment that must prevail with respect to the matters that get reported and discussed with the audit committee. Exhibit B provides the form of a sample letter to the audit committee chair that could be used to initiate these discussions.

 Copyright © 2000, American Institute of Certified Public Accountants, Inc.

Exhibit B

Sample Letter to Audit Committee Chair

July 15, 19x9
Mr. [or Ms.] Smith
Audit Committee Chair
Blank Company
Main Street
City, State Zip Code

Dear Mr. [or Ms.] Smith:

In January 1999, the Independence Standards Board adopted Independence Standard No. 1, Independence Discussions with Audit Committees (the "Standard"). The Standard requires annual written and oral communications between our Firm and the Audit Committee of Blank Company regarding relationships that in our professional judgment may reasonably be thought to bear on our independence. Additionally, The Report and Recommendations of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees issued in February 1999 included a recommendation that the listing rules for both the New York Stock Exchange and the National Association of Securities Dealers require audit committee charters to specify that the audit committee is responsible for ensuring receipt of the communication required by the Standard. This recommendation also indicated the charter should specify that the audit committee is responsible for actively engaging in a dialogue with the auditors relating to the disclosure of any relationships or services that may reasonably be thought by the auditor to bear on independence and should take appropriate action, if necessary, to ensure the continued independence of the auditor.

In order to facilitate our independence discussions with the Audit Committee, I would like to meet with you to obtain an understanding of the expectations of you and the Audit Committee with respect to the types of matters and relationships between our Firm and Blank Company that you believe may bear on our independence. These may include specific areas of interest to you and the Audit Committee, as well as matters the Audit Committee and senior management believe should be considered because they may be of interest to the Audit Committee as a representative of Blank Company's investors.

I would be pleased to meet with you at your convenience to discuss your thoughts and views on auditor independence and related matters.

Yours truly,

Threats to Objectivity and Related Safeguards

.11 To assist audit committees in expanding their understanding of auditor independence issues, auditors are encouraged to periodically discuss emerging independence issues and new or revised independence standards.

.12 To further assist these discussions, auditors also may consider providing the audit committee with an overview of common threats to auditor objectivity. While independence standards are designed to preclude relationships that may appear to impair an auditor's objectivity, additional safeguards have been developed by firms and the profession, and other external factors exist, that further mitigate threats to actual loss of objectivity.

.13 Exhibit C provides a summary of common threats to auditor objectivity and related safeguards that mitigate these threats.

 Copyright © 2000, American Institute of Certified Public Accountants, Inc.

Exhibit C

Common Threats to Auditor Objectivity and Related Safeguards Often Employed to Mitigate These Threats

Common Threats to Auditor Objectivity:

- Self-Interest: The threat to the auditor's objectivity due to financial or other self-interests.
- Self-Review: The threat to the auditor's objectivity caused by a self-review of services performed by the auditor or the auditor's firm during the audit.
- Advocacy: The threat to the auditor's objectivity if the auditor becomes an advocate for (or against) the client's position.
- Familiarity or Trust: The threat of the auditor becoming too trusting of the client and therefore not maintaining appropriate professional skepticism.
- Intimidation: The threat of the auditor becoming intimidated or threatened by an overbearing or dominating member(s) of management.

Related Safeguards Often Employed to Mitigate These Threats:

Instilling Professional Values:

- Training
- Firm Policies on Independence
- Monitoring Investments
- Annual Confirmations of Compliance with Firm Independence Policies

Communication:

- Audit Team Disagreement Resolution Process
- Consultation Requirements
- Separate National Consultation Function

Internal Accountability:

- Partner Rotation
- Concurring Partner Reviews
- Internal Inspection/Monitoring Programs
- Analysis of Regulatory and Litigation Experience
- Internal Disciplinary Actions
- Partner and Staff Evaluation and Compensation Methods

Risk Management:

- Client Acceptance and Retention Policies
- New Service Line Acceptance Policies

External Factors:

- Peer Review
- Quality Control Inquiry Committee (QCIC) Review
- Ethics Investigations (by the AICPA, state societies and state boards)
- SEC Enforcement Division
- Litigation Threat
- Reputational Threat

Form of Communication

.14 Communications from the auditor to the audit committee should disclose the relationships identified that may reasonably be thought to bear on independence. Disclosure should not be construed to imply that the auditor's independence has been impaired. In fact, it is presumed that the auditor has concluded that independence has not been impaired. Rather, disclosure of the relationships is a tool to foster discussion between the auditor and the audit committee regarding the nature of the relationship.

.15 The Standard requires that written communications summarize the relationship(s) identified. The auditor may wish to include in its written communications the relevant safeguards employed by the firm (see Exhibit A) to ensure the auditor's continued independence. Oral communications should include an open candid discussion relating to the relationship and a discussion of the relevant safeguards.

.16 The Standard also requires that the written communication include a confirmation that, in the auditor's professional judgment, the auditor is independent of the company within the meaning of the Securities Acts.

.17 Exhibit D provides the form of a sample letter relating to annual independence discussions with audit committees and confirmation that the auditor is independent of the company within the meaning of the Securities Acts.

 Copyright © 2000, American Institute of Certified Public Accountants, Inc.

Exhibit D

Sample Letter Relating to Annual Independence Discussions With Audit Committees

September 15, 19x9
The Audit Committee [or the Board of Directors]
Blank Company
Main Street
City, State Zip Code

Dear Audit Committee Members:

We have been engaged to audit the consolidated financial statements of Blank Company (the "Company") for the year ending December 31, 19x9.

Our professional standards require that we communicate at least annually with you regarding all relationships between our Firm and the Company that, in our professional judgment, may reasonably be thought to bear on our independence. [We have previously communicated with Mr./Ms. Smith, Chair of the Audit Committee, to obtain his/her views as to the nature of the matters that should be reported to the Audit Committee.] We have prepared the following comments to facilitate our discussion with you regarding independence matters. [After the initial year, this last sentence might be revised to read: "We have prepared the following comments to facilitate our discussion with you regarding independence matters arising since September 15, 19x9, the date of our last letter."]

We are aware of the following relationships between our Firm and the Company that, in our professional judgment, may reasonably be thought to bear on our independence. The following relationships represent matters that have occurred during 19x9, the initial year of adoption, through September 15, 19x9.

[Describe any significant relationships or matters bearing on the Firm's independence, and also discuss the appropriate safeguards in place. See Exhibit A for examples.]

[OR]

We are not aware of any relationships between our Firm and the Company that, in our professional judgment, may reasonably be thought to bear on our independence which have occurred during 19x9, the initial year of adoption, through September 15, 19x9.

We hereby confirm that as of September 15, 19x9, we are independent accountants with respect to the Company, within the meaning of the Securities Acts administered by the Securities and Exchange Commission and the requirements of the Independence Standards Board.

This report is intended solely for the use of the Audit Committee, the Board of Directors, management, and others within the Company and should not be used for any other purposes.

We look forward to discussing with you the matters addressed in this letter as well as other matters that may be of interest to you at our upcoming meeting on September 30, 19x9. We will be prepared to answer any questions you may have regarding our independence as well as other matters.

Yours truly,

.18 While this Alert focuses on the Standard, it is recognized that communications with audit committees, whether written or oral, are broader than independence. For example, membership requirements of the AICPA SEC Practice Section require annual communication of the nature of and the amount of fees billed for management advisory [consulting] services. Generally accepted auditing standards require communications of matters regarding internal control, including material weaknesses identified, and various other matters.

.19 The recently issued Blue Ribbon Committee Report contains recommendations that will likely result in additional required discussions with audit committees, including dialogue on accounting principles. Without in any way reducing the importance of the independence discussion, the auditor may choose a more comprehensive form of communication to cover some or all of these other matters.

Timing of Discussions with Audit Committees

.20 Annually, the auditor should meet with the audit committee to discuss all applicable relationships (actual and, preferably, proposed) between the company and the auditor. It may be beneficial to establish a schedule of regular meetings to discuss independence matters with the audit committee, including the timing for the annual independence confirmation. To enhance the effectiveness of the process, early communication to the audit committee of significant new matters might be considered at the time the relationship is established or the matter is first identified, rather than waiting until the meeting.

.21 The annual meeting desirably should be conducted as early as possible in the audit cycle. However, it should be noted that the ISB intentionally left the timing flexible as long as the communication is done annually. It is entirely acceptable to have the communication at any time, preferably prior to the issuance of the auditor's report. If the formal communication takes place early in the audit cycle, the auditor and the audit committee should establish a protocol to update the audit committee for any new or proposed relationships requiring communication that may have occurred since the initial communication.

.22 If the formal communication takes place near the end of the audit cycle, it may be desirable to combine the independence discussions with other required communications.

Other Matters

Initial Public Offerings

.23 Auditors and audit committees of first time registrants must comply with the Standard prior to the company's initial public offering. These communications are required for all audits of financial statements with fiscal years ending after July 15, 1999, and included in the registration statement in the company's initial public offering. Thus, this may require involvement of both the current auditor and a predecessor auditor, if there has been a change of auditors during this period. Early communication between the auditor and the audit committee is encouraged to proactively identify and resolve any potential issues regarding the auditor's independence early in the offering process.

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Initial Year of Application

.24 The Standard requires annual discussion between the auditor and the audit committee. For existing registrants in the initial year of application, these discussions are only required to cover relationships that exist in the current year. Thus, where a change of auditor has occurred, the discussions would only require involvement of the current auditor.

Prospective Clients

.25 Auditors are encouraged to discuss relationships that may exist with prospective clients during the proposal process. Discussion should include identification of the relationship, a discussion of safeguards that may mitigate these threats and, where necessary, identification of the methods to resolve potential impairments of independence prior to commencement of the audit.

Failure to Comply with the Standard

.26 The ISB recognized the possibility that there might be occasions where the required communications are not completed. This could occur for a variety of reasons, including unexpected cancellation of a scheduled meeting with the audit committee, or the inadvertent failure to schedule and complete the meeting or the auditor's failure to issue a written confirmation of its independence with respect to the company.

.27 The ISB did not intend that an isolated and inadvertent violation of the Standard's requirements would constitute a per se impairment of the auditor's independence, provided that the auditor is in compliance with all other independence rules. The ISB specifically recognized that in such circumstances, the violation could be "cured" through the prompt completion of the procedures. In the unlikely event that the auditor encounters difficulty in completing these procedures either initially or at the time a "cure" is attempted, prompt communication with the audit committee and the board of directors should be undertaken to highlight the effect of the failure to comply with the Standard on the company.

.28 The ISB also recognized that the auditor could, but is not required to, withhold his or her audit report until such discussion with the audit committee took place.

[The next page is 50,911.]

Section 16,140

Practice Alert 99-2
How the Use of a Service Organization Affects Internal Control Considerations

July/August 1999

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits and is based on existing audit literature, the professional experience of the members of the Professional Issues Task Force (PITF) and information provided by SEC Practice Section member firms to their own professional staff. This information represents the views of the members of the PITF and is not an official position of the AICPA. Official positions are determined through certain specific committee procedures, due process and deliberation. The information provided herein should be used only with the understanding that it is to be read in conjunction with the professional literature and that it is only a means of assisting auditors in meeting their professional responsibilities.

Introduction

.01 Obtaining a Statement on Auditing Standards (SAS) No. 70 report may be an efficient means of satisfying the requirements of generally accepted auditing standards (GAAS) with respect to service organizations. There have been recent examples of situations where a user organization's auditor did not obtain a SAS No. 70 report and did not employ alternative approaches to obtaining the necessary information. There also have been recent examples where a SAS No. 70 report was obtained but the report was not sufficient for the user auditor's purposes or was not needed. This may result from the user auditor not having a sufficient understanding of SAS No. 70, *Service Organizations*, or the different types of SAS No. 70 reports that are issued (i.e., Type 1 and Type 2 reports). Today, more and more companies are outsourcing activities to service organizations. In doing so, there often is a belief by the user organization that the service organization can be totally relied upon and that the user organization needs only to provide very limited, if any, controls. It is in these situations that it is critical for the user auditor to consider the guidance in SAS No. 70 and the implications the service organization may have to his/her audit.

.02 Many companies and organizations use outside service organizations to provide services ranging from performing specific tasks (such as maintaining custody of marketable securities) to replacing entire departments (such as performing all computer processing). They generally use such organizations because they do not have the internal expertise or skills to perform the services or it is cost effective to outsource the service. Examples of service organizations are:

- Data processing service organizations that perform such services as payroll, billing, general ledger accounting and other administrative functions.
- Trust departments of financial service companies.
- Mortgage loan servicers.
- Organizations providing services for employee benefit plans, such as providing investment management, custody of investments, record keeping of employee or participant data, processing employee benefit claims, and other accounting or administrative functions.

Factors to Consider in Planning an Audit

.03 Professional standards require that the auditor obtain an understanding of an entity's internal controls sufficient to plan the audit. The understanding is obtained by performing procedures to gain knowledge about the design of the controls relevant to the audit of the financial statements and whether they have been placed in operation. The requirement to understand internal control may extend beyond the controls in place at the entity's physical environment and may extend to other organizations who perform services on behalf of the entity to assist it in the recording, processing, summarizing and reporting of information in its financial statements. SAS No. 70 provides guidance for auditing an entity when a service organization's services are part of the user organization's information system.

When the User Auditor's Planning Should Consider the Guidance in SAS No. 70

.04 A user auditor should consider the guidance in SAS No. 70 whenever a service organization's services are part of the user organization's information system. A service organization's services would meet that criterion if they affect:

- How the user organization's transactions are initiated.
- The accounting records, supporting information, and specific accounts in the financial statements involved in the processing and reporting of the user organization's transactions.
- The accounting processing involved from the initiation of the transactions to their inclusion in the financial statements.
- The financial reporting process used to prepare the user organization's financial statements, including significant accounting estimates and disclosures.
- The guidance in SAS No. 70 does not relate to an entity that obtains a service from another organization that is limited to executing a client's transactions that are authorized by the client. Examples of such services are when a bank processes checking account transactions and when a broker processes securities transactions that are initiated by the client.
- The significance of the service organization's controls depends primarily on the nature and materiality of the transactions it processes for

 Copyright © 2001, American Institute of Certified Public Accountants, Inc.

the user organization and the degree of interaction between the internal controls at the user organization and the controls at the service organization.

Nature and Materiality of the Transactions

.05 If the transactions processed or accounts affected by the service organization are material to the user organization's financial statements, the user auditor may need to obtain an understanding of the controls at the service organization. In certain situations, the transactions processed and accounts affected may not appear to be material to the user organization's financial statements, but the nature of the transactions processed may require that the user auditor obtain an understanding of those controls. Such a situation might exist when a service organization provides third-party administration services to self-insured organizations providing health insurance benefits to employees. Although transactions processed and accounts affected may not appear to be material to the user organization's financial statements, the user auditor may need to gain an understanding of the controls at the third-party administrator because improper processing may result in a material understatement of the liability for unpaid claims.

.06 Information about the nature of the service provided by a service organization may be available from a variety of sources, such as SAS No. 70 reports by service auditors, user manuals, system overviews, technical manuals, the contract between the user organization and the service organization, and reports by internal auditors, or regulatory authorities on the service organization's controls.

Degree of Interaction

.07 The degree of interaction relates to the extent to which a user organization is able to and decides to implement effective internal controls over the processing performed by the service organization and on the nature of the services provided by the service organization.

.08 If the user organization implements highly effective internal controls over the processing of transactions at the service organization, the user auditor may not need to gain an understanding of the controls at the service organization in order to plan the audit. For example, if the user organization has such controls, the user auditor could obtain an understanding of the controls by performing a walkthrough at his/her client.

.09 If the user organization has a low degree of interaction and has not placed into operation effective internal controls over the activities of the service organization, the user auditor would most likely need to gain an understanding of the relevant controls at the service organization in order to plan the audit in accordance with GAAS.

.10 If the user organization relies on controls at the service organization to prevent or detect errors that would have an impact on its financial statements, the user auditor must understand those controls.

.11 The understanding of the service organization should include an understanding of the control environment, risk assessment, control activities,

information and communication and monitoring relevant to the audit of the client's financial statements. The understanding should include knowledge about the design of the controls and whether they have been placed in operation. The understanding of the controls should enable the user auditor to:

- Identify the types of potential misstatements that could occur in the client financial statements.
- Consider the factors that affect the risk of misstatement.
- Design substantive tests.

Failure to obtain such an understanding from either the client or the service organization may cause the user auditor to consider whether a scope limitation on the audit has occurred.

Factors to Consider in Assessing Control Risk

.12 After the user auditor obtains an understanding of the relevant controls at both the user organization and the service organization and considers the factors that affect the risk of material misstatement, he or she should assess control risk for the financial statement assertions. As previously stated, if the user organization has implemented certain controls over the service organization's activities that effectively operate to prevent or detect material misstatements in its financial statements, the user auditor may be able to perform the audit without identifying and testing controls at the service organization.

.13 Generally, the user auditor can identify relevant controls at a service organization by reading the service auditor's report, either a Type 1 or Type 2 report. Information about the operating effectiveness of the controls at the service organization are only included in a Type 2 report. Control risk can only be assessed below the maximum, if evidential matter is obtained using one or a combination of the following ways:

- By testing the user organization's controls over the activities of the service organization.
- By obtaining a service auditor's report (Type 2) on controls placed in operation and tests of operating effectiveness, or a report on the application of agreed-upon procedures that describes relevant tests of controls.
- By the user auditor performing appropriate tests of controls at the service organization.

Following is a further discussion of when each of these activities may apply.

.14 The user organization may establish effective controls over the service organization's activities that may be tested and that may enable the user auditor to reduce the assessed level of control risk below the maximum for some or all of the related assertions. For example, if a user organization uses an EDP service center to process payroll transactions, the user organization may establish controls over input and output data to prevent or detect material misstatements. The user organization might recalculate the service organization's payroll computations on a test basis. In this situation, the user auditor may perform tests of the user organization's controls over data processing that would provide a basis for assessing control risk below the maximum for the assertions related to payroll transactions. The user auditor may decide that obtaining evidence of the operating effectiveness of the service organization's controls, such as those over changes in payroll programs, is not necessary or efficient.

 Copyright © 2000, American Institute of Certified Public Accountants, Inc.

.15 The user auditor may find that controls relevant to assessing control risk below the maximum for the particular assertions are applied only at the service organization. If the user auditor plans to assess control risk below the maximum for specified assertions, the user auditor should obtain evidence of the operating effectiveness of these controls by obtaining and evaluating a service auditor's report that describes the results of the service auditor's tests of those controls, or by performing tests of controls at the service organization.

.16 If the user auditor decides to use a service auditor's report, the user auditor should consider the extent of the evidence provided by the report concerning the effectiveness of controls intended to prevent or detect material misstatements regarding the particular assertions. The user auditor remains responsible for evaluating the evidence presented by the service auditor and for determining the effect of this evidence on the assessment of control risk at the user organization.

.17 Because SAS No. 70 reports may be intended to satisfy the needs of several different user auditors, a user auditor should determine whether the specific tests of controls and results in the service auditor's reports are relevant to assertions that are significant in the user organization's financial statements. For those tests of controls and results that are relevant, a user auditor should consider whether the nature, timing and extent of such tests of controls and results provide sufficient evidence about the effectiveness of the controls to support the user auditor's desired assessment of the level of control risk. In evaluating these factors, the user auditor should also keep in mind that the shorter the time period covered by the tests of controls and the longer the time elapsed since the performance of the tests, the less support for control risk reduction the tests may provide.

SAS No. 70 Reports

Types of Reports

.18 There are two types of SAS No. 70 reports:

- Reports on controls placed in operation (Type 1). Such a report may provide a user auditor with an understanding of the controls in operation at a service organization and whether they are suitably designed to achieve specific control objectives. A Type 1 report may be useful in providing the user auditor with an understanding of controls necessary to plan the audit and to design effective tests of controls and substantive tests at the user organization, but it is not intended to provide the user auditor with a basis for reducing his/her assessment of control risk below the maximum.
- Reports on controls placed in operation and tests of operating effectiveness (Type 2). Such a report may provide the user auditor with an understanding of controls in operation at a service organization and whether they are suitably designed to achieve specific control objectives. Also, a Type 2 report indicates whether the controls that were tested were operating with sufficient effectiveness to provide reasonable assurance that the control objectives were achieved. This report may provide the user auditor with an understanding of controls necessary to plan the audit and may also provide a basis for reducing his/her assessment of control risk below the maximum.

What Is Included in the Reports

.19 A SAS No. 70 report typically includes the following items:

- Service organization's description of controls placed in operation as of a specific date.
- Service organization's description of the specified control objectives.
- Auditor's opinion on whether the description presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specified date.
- Auditor's opinion on whether the controls were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if those controls were complied with satisfactorily.
- Auditor's opinion as to whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in the report were achieved during the specified period (Type 2 reports only).

Considerations in Using the Reports

.20 After determining the need for a SAS No. 70 report, some auditors have a tendency to simply obtain the report and place it in the audit working papers. This clearly does not satisfy the requirements of GAAS.

.21 In considering whether the service auditor's report is satisfactory for his/her purposes, the user auditor should make inquiries concerning the service auditor's professional reputation as discussed in SAS No. 1, section 543, as amended.

.22 The user auditor may want to consider reading the report to determine whether the service auditor demonstrates an understanding of the subject matter. If the user auditor believes that the service auditor's report may not be sufficient to meet his/her objectives, the user auditor may consider supplementing his/her understanding of the service auditor's procedures and conclusions by discussing with the service auditor the scope and results of the service auditor's work.

.23 Also, if necessary, the user auditor may contact the service organization to perform additional testing (this is usually arranged by the user organization). This additional testing can be performed by the service auditor (e.g., by applying agreed-upon procedures at the request of the user auditor) or by the user auditor.

.24 The user auditor should not make reference to the report of the service auditor as a basis, in part, for his/her opinion on the user organization's financial statements. The service auditor's report is used in the audit, but the service auditor is not responsible for examining any portion of the user organization's financial statements as of any date or for any period. Thus, there cannot be a division of responsibility for the audit of the user organization's financial statements.

Timing Considerations in Using the Reports

.25 A service organization's description of controls is as of a specified date for both a Type 1 and Type 2 report. Accordingly, the service auditor issues a report on whether the description presents fairly, in all material respects, the

 Copyright © 2001, American Institute of Certified Public Accountants, Inc.

relevant aspects of the service organization's controls at a specified date. Such information may be used to plan the audit of a user organization's financial statements in the same way that an auditor's understanding of internal controls at a specified date is used to plan the audit of the financial statements of an entity that does not use a service organization.

.26 A report on controls placed in operation that is as of a date outside the reporting period of a user organization may be useful in providing a user auditor with a preliminary understanding of the controls placed in operation at the service organization, if the report is supplemented by additional current information from other sources. If the service organization's description is as of a date that precedes the beginning of the period under audit, the user auditor should consider updating the information in the description to determine whether there have been any changes in the service organization's controls relevant to the processing of the user organization's transactions. Procedures to update the information in a service auditor's report may include:

- Discussions with user organization personnel who would be in a position to know about changes at the service organization.
- A review of current documentation and correspondence issued by the service organization.
- Discussion with service organization personnel or with the service auditor.

If the user auditor determines that there have been significant changes in the service organization's controls, the user auditor should attempt to gain an understanding of the changes and consider the effect of those changes on his/her audit.

Conclusion

.27 SAS No. 70 provides guidance on factors an independent auditor should consider when auditing the financial statements of an entity that uses a service organization. This Alert clarifies and highlights factors an auditor should consider in those audits. SAS No. 70 also provides guidance for independent auditors who issue reports on the processing of transactions by a service organization for use by other auditors, but this Alert does not address those circumstances. This Alert should be read as a complement to SAS No. 70. Terms such as user auditor and service auditor are defined in SAS No. 70.

.28 The AICPA recently issued an updated version of the Auditing Practice Release, *Service Organizations: Applying SAS No. 70.* This publication (AICPA Publication Number 060457-CLD7) provides extensive guidance to auditors performing (1) an audit of a user organization's financial statements and (2) procedures at a service organization that will enable them to issue a service auditors report on a service organization's controls that may affect user organizations. This publication can be purchased by calling (888) 777-7077.

[The next page is 50,931.]

Section 16,150

Practice Alert 00-1
Accounting for Certain Equity Transactions

January, 2000

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits and is based on existing professional literature, the professional experience of the members of the Professional Issues Task Force (PITF) and information provided by SEC Practice Section member firms to their own professional staff. This information represents the views of the members of the PITF and is not an official position of the AICPA. Official positions are determined through certain specific committee procedures, due process and deliberation. The information provided herein should be used only with the understanding that it is to be read in conjunction with the professional literature and that it is only a means of assisting auditors in meeting their professional responsibilities.

.01 Equity or capital transactions are often complex and should involve close scrutiny by auditors. As highlighted at the conclusion of this Alert, substantial additional guidance is available addressing differing forms of equity or capital transactions. In this Alert, the Professional Issues Task Force (PITF) will provide some of the more common examples which require careful consideration to determine the appropriate accounting treatment.

Stock Issued for Goods and Services

.02 Start-up companies commonly issue stock in exchange for property, services, or any other form of asset other than cash. The general rule to be applied when equity instruments are issued to non-employees for property or services other than cash is that the transaction should be recorded at the fair value of the consideration received or the fair value of the equity instruments issued, whichever is more reliably measurable.

.03 An example of the above is as follows:

> ABC Manufacturing Inc. purchased inventory from their vendor XYZ & Co. In lieu of cash, ABC issued 1,000 shares of common stock to XYZ. ABC is a closely held company and the value of its stock has no readily determinable market value.

In the above example, ABC should determine the fair value of the inventory they are purchasing and assign that value to the inventory. Assuming the fair value of the inventory was estimated at $2,500, the accounting entry would be to record inventory at the fair value ($2,500) with the corresponding credits being recorded to common stock and additional paid-in capital.

.04 Similarly, if ABC issued stock to compensate XYZ for services performed, the services would generally be valued at the estimated fair value of the services, because the services are generally more reliably measurable than the fair value of the securities issued. The manner in which the services are recorded (e.g., capitalize versus expense) will depend on the nature of the services and their treatment under generally accepted accounting principles.

.05 An example of this scenario follows:

> Mr. Baylor, a consultant who is not considered a founder or an insider of ABC, performs 1,000 hours of services for 10,000 shares of ABC's common stock. The stock has no readily determinable market value. Mr. Baylor typically charges his clients $100 an hour.

In this instance the most reliable measurable value would appear to be Mr. Baylor's services valued at 1,000 hours multiplied by $100 an hour, or $100,000. Thus, the ABC would record an expense for $100,000 and credits to common stock and paid-in capital for $100,000.

.06 In circumstances where the stock issued has no readily determinable market value and the goods and or services received cannot be measured objectively and reliably, a company generally should record the asset or service at a nominal value.

.07 Another example of the above concepts follows:

> Mr. Smith, who is not an insider or founder of the company, contributes raw land to a start-up company that will be used to build its manufacturing facility. The land was willed to Mr. Smith 20 years ago and has never been appraised. In exchange for the land, the company issues Mr. Smith 500,000 shares of the company's convertible preferred stock. The company's convertible preferred stock has no active trading, but a valuation was performed by a consultant six months before the land was donated. Mr. Smith is the consultant's uncle. The question is how do you value this transaction.

The above example demonstrates the complexities of equity transactions. First, the valuation of the company's stock by Mr. Smith's nephew would probably not be considered to be a reliable measure due to the fact that they are related parties. If practical, an appraisal of the land by an independent, qualified person may be a reliable measure. However, if an independent, qualified person performed the appraisal of the company's stock, this value may also be a reliable measure. If neither can be reliably measurable, the asset should be recorded at a nominal value.

.08 The use of the book, par, or stated value of the stock as a basis for valuation is not appropriate. Similarly the contractual value assigned to goods, services or other assets received does not represent an appropriate surrogate measure of their value. The company should be able to furnish evidence to outside parties as to how the fair value of the goods, services or other assets was determined, as in the example cited above involving the transaction with Mr. Baylor. In that example, Mr. Baylor kept time records for his consulting services.

.09 Emerging Issues Task Force (EITF) 96-18, *Accounting for Equity Instruments That Are Issued to Other Than Employees for Acquiring, or in Conjunction with Selling, Goods or Services*, provides numerous examples of situations where (1) the fair value of the equity instrument is more reliably measurable than the fair value of the goods or services received and (2) the counterparty receives shares of stock, stock options or other equity instruments in settlement of all or a part of a transaction.

 Copyright © 2001, American Institute of Certified Public Accountants, Inc.

.10 EITF 96-18 also addresses the measurement date for accounting for equity instruments that are issued to other than employees in exchange for goods and services. The EITF reached a consensus that the issuer should measure the fair value of the equity instruments using the stock price and other measurement assumptions at the earlier of either of the following:

1. The date at which a commitment for performance by the counterparty to earn the equity instrument is reached (referred to as a "performance commitment"), or
2. The date at which the counterparty's performance is complete.

.11 Examples 1–3 of Exhibit 96-18A of EITF 96-18, describe transactions in which a performance commitment exists prior to the time that the counterparty's performance is complete. Examples 4–7 describe transactions in which a performance commitment does not exist prior to the time the counterparty's performance is complete.

.12 EITF 96-18 is extremely complex. This very brief summary should not be relied upon without a complete reading and understanding of the pronouncement itself. It is mentioned only as a reminder of an important source of authoritative literature on accounting for equity transactions.

Stock Issued to an Owner for Expertise or Intellectual Capital Contributed to Business

.13 Companies sometimes issue stock to an owner for expertise contributed to a business, such as a patent or other intellectual capital. Such circumstances are most common immediately prior to an initial public offering (IPO). The question is what value should the company place on the asset acquired.

.14 The Securities and Exchange Commission (SEC) states in Staff Accounting Bulletin (SAB) Topic 5-G, *Acquisition of Assets from Promoters and Shareholders in Exchange for Common Stock*, that "transfers of nonmonetary assets to a company by its promoters or shareholders in exchange for stock prior to or at the time of the company's initial public offering normally should be recorded at the transferor's historical cost basis determined under generally accepted accounting principles".

.15 The following is an example applying the above principle:

> Mr. Norton, a founder of ABC Industries, Inc., contributes a patent to ABC in exchange for stock immediately prior to ABC's IPO. The patent was obtained by Mr. Norton at a cost of $1,000 (filing fees). The remainder of the costs associated with the patent relate to Mr. Norton's own time developing the intellectual property. If Mr. Norton maintained books in accordance with generally accepted accounting principles, the patent would be recorded on those books at $1,000. Therefore, when the patent is contributed, ABC should record the patent at $1,000 with corresponding credits to common stock and additional paid-in capital.

Employee Stock Options

.16 The financial accounting and reporting standards for stock-based employee compensation plans are contained in the Financial Accounting Standards Board's (FASB) Statement No. 123, *Accounting for Stock-Based*

Compensation, and the Accounting Principles Board's (APB) Opinion 25, *Accounting for Stock Issued to Employees*. These pronouncements cover all arrangements by which employees receive shares of stock or other equity instruments of the employer or the employer incurs liabilities to employees in amounts based on the price of the employer's stock. Examples are stock purchase plans, stock options, restricted stock, and stock appreciation rights.

.17 FASB Statement No. 123 prescribes a *fair value method* of accounting for an employee stock option or similar equity instrument and encourages all *entities* to adopt that method of accounting for all of their employee stock compensation plans. However, FASB Statement No. 123 also permits an entity to continue to measure compensation cost for those plans using the *intrinsic value method* of accounting prescribed by APB Opinion 25. Where entities elect to continue using the accounting in APB Opinion 25, they are required to make pro forma disclosures of net income and, if presented, earnings per share, as if the fair value method of FASB Statement No. 123 had been applied.

.18 Under the fair value method, compensation cost is measured at the grant date based on the value of the award and is recognized over the service period, which is usually the vesting period. Under the intrinsic value-based method, compensation cost is the excess, if any, of the quoted market price of the stock at grant date or other measurement date over the amount an employee must pay to acquire the stock.

.19 The determination of fair value, either for accounting under FASB Statement No. 123 or the pro forma disclosures under APB Opinion 25, can be achieved through use of an option-pricing model (for example, the Black-Scholes or a binomial model) that takes into account, as of the grant date, the exercise price and expected life of the option, the current price of the underlying stock and its expected volatility, expected dividends on the stock, and the risk-free interest rate for the expected term of the option. The discussion of stock option valuation techniques is beyond the scope of this Alert but further guidance is available in FASB Statement No. 123. Also, for some non-public entities with minimal trading information upon which to assess price volatility as required for traditional option valuation techniques, the entity may use a minimum value method. Under the minimum value method, the stock option value is generally considered to equal the current price of the stock reduced by the present value of the expected dividends on the stock, if any, during the option's term minus the present value of the exercise price. For this purpose the present value discount is based on the risk-free rate of return. However, the minimum value could also be computed using the standard option-pricing model and volatility of zero.

.20 It also is important to note that FASB Statement No. 123 requires a fair value method for all equity awards to non-employees, and use of the minimum value method, as described in the preceding paragraph, is not appropriate. This is demonstrated in the above sections of this Alert.

.21 Where options are granted near an IPO, the value at which stock is issued in the IPO should be carefully considered in assessing the market value of options. For such grants, the SEC staff expects the registrant to have objective evidence to support its determination of "fair value." Such objective evidence would include contemporaneous third-party transactions and independent appraisals. "Rule of thumb" discounts, management estimates, related-party transactions (even for cash), and general market data do not represent objective evidence for this purpose. The most objective evidence that

 Copyright © 2000, American Institute of Certified Public Accountants, Inc.

can be used to support the value assigned to stock, options, or warrants is information from a contemporaneous transaction where the value of the consideration received for the company's securities is objectively measurable, i.e., an equity transaction with a third party for cash that is entered into in the same time frame. Absent a contemporaneous transaction, an independent appraisal can form the basis for the valuation. The independent appraisal should have been performed at the time the stock, options, or warrants were issued. Appraisals performed "after the fact" are not acceptable. If the appraised value of the stock is substantially below the IPO price, the company must be able to reconcile the difference between the appraised value and the IPO price, i.e., explain the events or factors that support the difference in values.

.22 In 1999, the FASB issued an exposure draft addressing several issues regarding the accounting for employee stock options and awards under APB Opinion 25. Comments have been submitted and the FASB is re-deliberating many of the conclusions expressed in the exposure draft. A final interpretation of these issues is expected early in 2000. At this time it is expected that practice with respect to many aspects of APB Opinion 25 will be changed as a result of the interpretation.

Retroactive Earnings per Share Adjustment for Cheap Stock

.23 Cheap stock refers to stock issued for nominal consideration (i.e., a price below the price at which stock is subsequently sold in a public issuance of shares) to employees or others closely related to the company. SAB 98 Topic 4-D, *Earnings per Share Computations in an Initial Public Offering*, describes the SEC's position on this issue.

.24 In applying the requirements of FASB Statement No. 128, *Earnings per Share*, the SEC staff believes that nominal issuances are recapitalizations in substance. Accordingly, in computing basic earnings per share (EPS) for the periods covered by income statements included in the registration statement and in subsequent filings with the SEC, nominal issuances of common stock should be reflected in a manner similar to a stock split or stock dividend for which retroactive treatment is required by paragraph 54 of FASB Statement No. 128. Consequently, in computing basic EPS, nominal issuances of common stock would be included for all periods; whereas in computing diluted EPS for such periods, nominal issuances of common stock and potential common stock (e.g., options) would be included for all periods. In addition, use of the treasury stock method is not allowed and retroactive treatment is required even if anti-dilutive.

.25 This retroactive presentation of such nominal issuances as outstanding for all historical periods in the computation of EPS does not alter the requirement that entities determine whether the recognition of compensation expense for any issuance of equity instruments to employees is necessary.

.26 Guidance has not been provided on what constitutes "nominal consideration." SAB Topic 4-D states that it should be determined based upon facts and circumstances by a comparison of the "consideration an entity receives" to the security's fair value (at the date of the issuance).

Extinguishment of Related Party Debt

.27 The AICPA frequently receives questions about whether an entity should record an expense or a charge to equity when a company forgives a receivable from an individual that is a related party of the company. Typically in such situations, the company should record a charge to equity. As a reminder, it should be noted that in certain circumstances, such receivables from related parties often are recorded as a reduction in equity rather than as an asset. This is sometimes required, depending on the nature of the receivable, by the SEC (see SAB Topic 4-E, *Receivables from Sale of Stock*, and Topic 4-G, *Notes and Other Receivables from Affiliates*) and by EITF 85-1, *Classifying Notes Received for Capital Stock*.

.28 Similar to a company forgiving a loan from a related party, sometimes a company's outstanding loan is forgiven by a related party. Such a forgiveness usually should be recorded as a credit to equity. (APB Opinion 26, *Early Extinguishment of Debt*, paragraph 20 states "that extinguishment transactions between related parties may be in essence capital transactions".)

Other Accounting Literature Addressing Equity Transactions

.29 When auditing and accounting for equity transactions, members should review the FASB *Current Text* and the EITF index for a more complete list of accounting literature on such transactions. There are more than 50 accounting pronouncements addressing various equity transactions, including numerous EITFs on the subject. This is indicative of and exemplifies the careful research that is necessary when dealing with equity transactions.

.30 Furthermore, members should review the SEC's SAB Topics when auditing public companies. Several SAB Topics covering equity transactions have been referred to in this Alert.

Summary

.31 Accounting for equity transactions is complex and requires comprehensive research of accounting literature to ensure the appropriate accounting treatment. The above examples provide a summary of the appropriate accounting for certain equity transactions.

[The next page is 50,941.]

 Copyright © 2000, American Institute of Certified Public Accountants, Inc.

Section 16,160

Practice Alert 00-2 Guidance for Communication With Audit Committees Regarding Alternative Treatments of Financial Information Within Generally Accepted Accounting Principles

First Issued April, 2000; Updated March, 2004

NOTICE TO READERS

This Practice Alert is intended to provide practitioners with information that may help them improve the effectiveness and efficiency of their engagements and practices and is based on existing professional literature, the experience of the members of the Professional Issues Task Force (PITF) and information provided by certain AICPA member firms to their own professional staff. This information represents the views of the members of the PITF and has not been approved by any senior technical committee of the AICPA. The auditing portion of this publication is an *Other Auditing Publication* as defined in Statement on Auditing Standards (SAS) No. 95, *Generally Accepted Auditing Standards*. Other Auditing Publications have no authoritative status; however, they may help the auditor understand and apply SASs. If an auditor applies the auditing guidance included in an *Other Auditing Publication*, the auditor should be satisfied that, in his or her judgment, it is both appropriate and relevant to the circumstances of the subject audit. This publication was reviewed by the AICPA Audit and Attest Standards staff and published by the AICPA, and is presumed to be appropriate.

Introduction

.01 The role of the audit committee with respect to overseeing management's financial reporting responsibilities and the independent auditor's audit of the financial statements has become increasingly important. Likewise, the auditor's responsibility with respect to communicating with the Audit Committee has also increased. This Practice Alert is intended to provide auditors with information that will assist them in preparing for and participating in discussions with audit committees.

.02 In December 1999, the Auditing Standards Board (ASB) issued SAS No. 90, *Audit Committee Communications*. SAS No. 90 amended SAS No. 61, *Communication With Audit Committees*, to require the independent auditor of an SEC client to discuss with a client's audit committee certain information relating to the auditor's judgment about the quality, not just acceptability, of the entity's accounting principles. In addition, the amendment to SAS No. 61 encouraged a three-way discussion among the auditor, management and the audit committee. SAS No. 90 was issued in response to Recommendation No. 8 of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees (the "BRC"). The BRC was formed in response to recommendations by SEC Chairman Arthur Levitt and issued its final report in February 1999.

.03 Additionally, on July 30, 2002, President George W. Bush signed into law the Sarbanes-Oxley Act of 2002 (the "Act"). The Act created new requirements in the communication between auditors and their publicly held audit clients. Auditors must report to and be overseen by a company's audit committee, not management. Section 204, *Auditor Reports to Audit Committees*, of the Act states:

> Each registered public accounting firm that performs for any issuer any audit required by [Section 10A of the Securities Exchange Act of 1934] shall timely report to the audit committee of the issuer—
>
> 1. All critical accounting policies and practices to be used;
> 2. All alternative treatments of financial information within generally accepted accounting principles that have been discussed with management officials of the issuer, ramifications of the use of such alternative disclosures and treatments, and the treatment preferred by the registered public accounting firm; and
> 3. Other material written communications between the registered public accounting firm and the management of the issuer, such as any management letter or schedule of unadjusted differences.

.04 The information in this Practice Alert was developed to assist auditors in the identification of matters that may be relevant to a discussion with an entity's audit committee of all alternative treatments of financial information within generally accepted accounting principles that have been discussed with management officials of the issuer.

Recommendations to Meet the Objectives of SAS No. 61 and the Sarbanes-Oxley Act of 2002

.05 As previously stated, an auditor of any public company is required to timely report to that company's audit committee all alternative treatments of financial information within generally accepted accounting principles that have been discussed with management officials of the issuer, ramifications of the use of such alternative disclosures and treatments, and the treatment preferred by the registered public accounting firm. To meet this requirement, auditors of public companies should consider the following:

- **Manner of Communications.** Communications should be understandable to all members of the audit committee.
- **Timeliness of Communications.** Discussions with the audit committee should be sufficiently frequent to ensure that audit committee members are advised of issues on a timely basis.
- **Relevance of Issues Discussed.** Periodic communications with the audit committee need not encompass all accounting principles, estimates and judgments. Rather, the communications could build on prior communications and address those accounting principles and unusual transactions that are more significant in any particular period's financial statements. For example, an asset impairment policy might be discussed in greater detail in periods in which impairment charges are under consideration, including periods in which impairment charges were considered but determined not to be needed.

.06 The auditor may implement the three core communication considerations described above as follows:

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

1. **Manner of Communications**

   The auditor should tailor communications with the audit committee to the professional and educational backgrounds of the committee members. The auditor can enhance the accounting and financial literacy of the audit committee members by providing presentations on accounting issues, professional publications and financial press articles that will help the members understand critical and significant accounting and financial reporting issues.

2. **Timeliness of Communications**

   Timely communication is inherently dependent upon management, the audit committee and the independent auditor sharing a common understanding of the timetable and key milestones in the financial reporting continuum. The auditor should attempt to complete the quarterly reviews and annual audit procedures in sufficient time to provide for discussion of significant matters as required by SAS No. 61 with the audit committee on a timely basis and not later than the filing of the entity's Form 10-Q or Form 10-K.

3. **Relevance of Issues Discussed**

   Topics that the auditor should discuss with the audit committee would include but not be limited to the following:

   1. **The accounting principles applied by the entity for which acceptable alternative principles are available**. The manner in which each significant alternative accounting principle would affect the transparency, understandability and usefulness of the financial information could be discussed. The discussion could include identification of the financial statement amounts that are affected by the choice of principles as well as information concerning accounting principles used by peer group companies. **Pursuant to the requirements of the Sarbanes-Oxley Act of 2002, the auditor must report to the audit committee as to the treatment preferred by the auditor.**
   2. **Judgments and estimates that affect the financial statements**. The discussion with the audit committee may include major items for which judgments and estimates are significant, including how such judgments and estimates are determined and subsequently monitored. Generally a discussion of judgments and estimates would cover the appropriate disposition of previously established estimates when the events that caused their creation are no longer applicable. To the extent that judgments and estimates involve a range of possible outcomes, the discussion could indicate how the recorded estimate relates to the range and how various selections within the range would affect the financial reporting. In particular, if the entity has significant contingencies for which no recorded estimated liability has been provided, the discussion might consider the current and future financial statement impact of management's decisions. If the enterprise has recorded estimates that are "slow moving" in terms of resolution of the matters to which the estimate relates (e.g., litigation or environmental reserves), management and the auditor might address the continued need for the recorded estimate as well as the impact of changes in the estimate and the balance of the remaining estimated amount on

the perception of the enterprise's financial condition and performance. The adequacy of the disclosures of such contingencies, including the exposure to losses in excess of any recorded amounts, could also be discussed.

3. **Consideration of factors affecting asset and liability carrying values.** Management and the auditor could discuss factors including, but not limited to (*a*) the company's bases for determining useful lives assigned to tangible and intangible assets and salvage values, (*b*) discount rates used to value pension and post-retirement obligations, and (*c*) the carrying value of other assets and liabilities. The discussion should include the type and quality of evidence supportive of such factors. The discussion also might include an explanation of the manner in which factors affecting carrying values were selected and how alternative selections would have affected the financial condition and earnings of the enterprise. The audit committee generally should be made aware of the effect such judgments have on the financial statements.

4. **Use of special structures and timing of actions that affect financial statements.** Examples of special structures or timing decisions would include off balance sheet financing, research and development activities, and timing of transactions in order to recognize revenues or avoid recognition of expenses. Any special purpose financing structures or unusual transactions that affect ownership rights (such as leveraged recapitalizations, joint ventures, and preferred stock of subsidiaries) might be discussed with the audit committee. The discussion could include information about comparative structures used in practice and insight regarding the impact of these special structures on the risks and rewards of the entity and the timing and amounts of reported income and cash flow. The discussion also could address the impact of such structures on the transparency and understandability of the enterprise's economic position as compared to its financial statements.

5. **Evolving issues and choices that affect financial reporting.** Examples of issues and choices affecting financial reporting would include revenue recognition practices such as "gross versus net presentation" or "upfront recognition," outsourcing employee services, tax planning strategies, lease versus buy decisions, use of "restructuring plans," and classification of investments as held-to-maturity versus available-for-sale versus trading. The discussion should address not only the issues and choices but a comparison of how such choices affect financial reporting as compared to effects that would have resulted from other available choices.

6. **The frequency and significance of transactions with related parties particularly those that are not in the ordinary course of business.** Examples of these kinds of related party transactions include compensation arrangements, loans, related party leases, use of corporate assets, or employment of close relatives. The discussion could address such matters as whether the enterprise had similar transactions at similar prices with unrelated parties, whether transactions were undertaken on

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

a best available price basis, and whether the transactions or pricing of the transactions impacted financial reporting in any significant manner that would not be obvious to a user of the financial statements. Management and the auditor could consider informing the audit committee of the financial statement impact and disclosures of these items, as well as how such transactions reflect the underlying economics. The discussion might also address the adequacy and clarity of the disclosure of related party transactions.

Practitioners should be aware that the Nasdaq Stock Market, Inc. (the "Nasdaq") requires that a company's audit committee or another independent body of the board of directors review and approve all related party transactions.

7. **Unusual arrangements**. Examples of unusual arrangements would include bill-and-hold transactions, self-insurance, multi-element arrangements contemporaneously negotiated, and sales of assets or licensing arrangements with continuing involvement by the enterprise. Such arrangements could be brought to the attention of the audit committee members to ensure that they understand how the business and financial reporting is being affected. The discussion could address the manner in which financial reporting was affected by the transactions, the transparency of the financial reporting and disclosures, and the impact of the unusual transactions on the comparability of financial condition and performance among past and future periods.

8. **Clarity and transparency**. Management and the auditor could discuss the clarity and transparency of the financial statements and disclosures. Examples of items to discuss would include details about restructuring activities, activity in reserve accounts, market risk and other risk disclosures, details and comparative data discussed in management's discussion and analysis, disclosure of alternative measures of performance whether in financial statements or other materials filed with the SEC or otherwise publicly distributed, and segment disclosures.

9. **Audit adjustments arising from the audit**. The discussion should address adjustments recommended by the auditor that, in the opinion of the auditor, have a significant effect on the entity's financial reporting process. Further, because of the issuance of SAS No. 89, *Audit Adjustments*, the auditor also must inform the audit committee "about uncorrected misstatements aggregated by the auditor during the current engagement and pertaining to the latest period presented that were determined by management to be immaterial, both individually and in the aggregate, to the financial statements taken as a whole." The auditor should also discuss the effect of unrecorded adjustments on subsequent years' financial statements.

10. **Materiality thresholds and cost/benefit judgments**. The discussion could address the qualitative and quantitative criteria used by management in making its materiality assessments. The discussion could also address the performance measures or other specific factors considered in making materiality judgments, for example, whether materiality is measured in relation to

sales, gross margins, segment margin, specific financial statement line items, or before and after special non-recurring items. The discussion might address how the materiality criteria affect the period to period comparability of reported financial condition and results of operations.

Discussion of Quality, Not Acceptability or Preferability, of Accounting Principles and Judgments

.07 Objective criteria have not been developed to aid in the consistent evaluation of an entity's accounting principles as applied in its financial statements. SAS No. 61, as amended, directs the discussion with the audit committee to include items that have a significant impact on whether the financial statements are representationally faithful, verifiable, neutral and consistent. These characteristics can serve as a basis for a discussion of quality in the broadest sense of the word since these are among the desired qualitative characteristics of accounting information as set forth in Financial Accounting Standards Board's Concepts Statement No. 2, *Qualitative Characteristics of Accounting Information* (CON 2).

Discussion of Aggressiveness vs. Conservatism in Financial Reporting

.08 BRC Recommendation No. 8 suggests that the auditor's communication with the audit committee should address the degree of aggressiveness or conservatism of the accounting principles applied in the financial statements. The concept of aggressiveness or conservatism was viewed by many as too ambiguous to be dealt with effectively in response to the BRC recommendation. As a result, the amendment to SAS No. 61 that requires the auditor to discuss quality with the audit committee, as discussed above, addresses the BRC recommendation by requiring a discussion of items that have a significant impact on representational faithfulness, verifiability and neutrality of the accounting information included in the financial statements as those terms are defined in CON 2. Accordingly, a discussion of aggressiveness vs. conservatism is not required. If, however, either the auditor or the audit committee desire to discuss this concept, the following discussion may be helpful.

.09 Conservatism may be defined as prudent reaction to try to ensure that uncertainty and risks inherent in business situations are adequately considered. The term today is often misunderstood and has sometimes been used to defend accounting judgments that may not be fully supportable. As a result, the crossover between what is conservative and what is aggressive is sometimes difficult to distinguish. In the current financial reporting environment, actions that are conservative to one person may be viewed as aggressive by another. An entity that provides reserves for losses based on an overly pessimistic view (and thus may have excess reserves that can be released into earnings in future periods) may be viewed as aggressive in the current reporting environment notwithstanding past experience of companies being viewed as aggressive for having failed to provide adequate reserves. Providing for losses on a "too-much, too-soon" basis is as erroneous as providing for losses "too-little, too-late." Conservatism in financial reporting should not be used to justify understatement of income or assets.

.10 Financial statements are useful in making investment and lending decisions when an entity's accounting principles are applied in a manner that is

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

reasonable in light of all known circumstances. Discussions with the audit committee of the degree of aggressiveness or conservatism in financial reporting may take into account the financial reporting effects of accounting principles on all of the financial statements and all periods presented as well as expected future financial statement effects. For example, the use of inappropriately low salvage values for depreciable assets will result in the understatement of current period assets and income. This will, however, overstate income in future periods as the company benefits from the continued use of fully depreciated operating assets.

.11 Choices among accounting principles and their application involve judgment. Judgments frequently involve the determination of a range of reasonableness. In practice, the terms conservative and aggressive are meant to connote management judgments that are within the range of reasonableness but are either on the low or on the high end of the range of reasonableness, respectively. Any discussions with the audit committee about the aggressiveness or conservatism of accounting principles should address the manner in which a reasonable range is determined and how choices are made and applied within that range.

Summary

.12 Under SAS No. 61 the auditor is required to communicate a number of matters, including the quality of an entity's accounting principles, with the entity's audit committee. The purpose of communication with the audit committee is to provide the audit committee with information that may assist it in overseeing the entity's financial accounting, reporting and disclosure process. The auditor's attention to the accounting and financial knowledge of audit committee members, the timing of communications, and the delivery of appropriate content in the proper context will enable auditors to provide significant insight and assistance to the audit committee to fulfill its oversight role while observing a high standard of professional practice.

[The next page is 50,961.]

Section 16,170

Practice Alert 00-3
Auditing Construction Contracts

September, 2000

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits and is based on existing professional literature, the experience of the members of the Professional Issues Task Force (PITF) and information provided by SEC Practice Section member firms to their own professional staff. This information represents the views of the members of the PITF and is not an official position of the AICPA. Official positions are determined through certain specific committee procedures, due process and deliberation. The information provided herein should be used only with the understanding that it is to be read in conjunction with the professional literature and that it is only a means of assisting auditors in meeting their professional responsibilities.

Introduction

.01 One of the more challenging audits is that of construction companies and other companies using the percentage of completion method of accounting for long-term contracts. This Practice Alert is intended to serve as a reminder of the important concepts, and provide some best practices for auditing such entities.

.02 The primary authoritative accounting literature for construction companies, and entities using contract accounting is SOP 81-1, *Accounting for Performance of Construction-Type and Certain Production-Type Contracts* [section 10,330]. A thorough understanding of this literature is critical to auditing such entities. The AICPA's guide entitled "A CPA's Guide to Accounting, Auditing and Tax for Construction Contractors" and the related self-study course, are useful tools in preparing for such audits.

.03 Auditing construction contractors or entities using contract accounting is complex. Such businesses rely on accurate and reliable estimates to operate their business as well as to prepare financial statements in accordance with generally accepted accounting principles. Therefore, it is critical that the auditor gain an understanding of the contractor's significant estimates and assumptions in operating its business. Remember that the audit of a contractor is an audit of a contractor's ability to estimate. There are several things to consider when auditing estimates (also see SAS No. 57, *Auditing Accounting Estimates*): Understand the internal control structure surrounding the estimate, consider the contractor's history of accurate estimates, compare actual to budgeted figures, and review subsequent events.

Best Practices

.04 The PITF has identified certain procedures that should be considered in performing an audit of a construction contractor. They are as follows:

- Read significant contracts. This procedure may seem obvious, but it is necessary in identifying the terms of the contract, any guarantees, penalties and incentives, as well as any cancellation and postponement provisions. For instance, reading the contract might identify the party responsible for additional expenses incurred as a result of weather delays (e.g., a colder than normal winter). Make sure the contracts are approved by the appropriate company personnel.
- Identify unique contracts and increase the amount of testing and professional skepticism relating to such contracts. These contracts increase the risk of improper estimates and thus improperly stated financial statements. If a company cannot reasonably estimate the cost or progress of a contract, it should be accounted for under the completed-contract method. For example, if a home building company decides to build power plants, they should consider accounting for such contracts under the completed-contract method until they are reasonably confident that its estimates in the power plant portion of the business are reliable.
- Understand the company's cash flow and how it will manage paying out expenses. Often expenses are due prior to receiving all the appropriate cash for the contract revenue. Some companies win long term contracts, but cannot fund the project long enough to realize the revenue earned. It is not uncommon for a customer to withhold 20%–25% of the contract price until they are satisfied with the quality of the completed contract.
- Recognize that the longer the contract period, the greater the risk that an estimate will be incorrect. Also, the farther along a contract is toward completion, the less risk there is of an incorrect estimate. Finally, the more variables inherent in an estimate the greater the risk that an estimate will be incorrect.
- Confirm the terms and conditions of the contract as well as the normal billing procedures. When confirming a receivable the auditor should strongly consider confirming: the original contract price, total approved change orders, total billings and payments, retainage held and whether it accrues interest, detail of any claims, back charges or disputes, and estimated completion date or the estimate of percentage complete.
- Review the unapproved change orders of significant contracts. Change orders often arise during the life of a contract and estimated revenue and cost should be adjusted for changed orders that have been approved both as to scope and price. However, when a change order has been approved as to scope but not price careful evaluation of the specific facts and circumstances is required prior to inclusion in estimated contract revenues. To the extent that change orders are in dispute or are unapproved in regard to both scope and price they should be evaluated as claims. Generally speaking, if there is no verifiable evidence to support the recognition of revenue on an unapproved change order or claim, it should not be recognized.
- Visit construction contract sites. Visiting contract sites can be a very useful audit procedure. Such a visit can provide an opportunity to view

 Copyright © 2001, American Institute of Certified Public Accountants, Inc.

the progress of a contract. Consideration of a site visit might include significant contract sites, in which the work is in the very early stages of a contract. Such a visit may identify the complexities of performing the contract. For example, a contract being performed in remote regions of Alaska presents certain logistical risks that may not be appreciated or understood without visiting. The site visit also may provide auditors an opportunity to interview operational personnel and to gain a better understanding for the responsibility the Company is undertaking performing the contract. At the site visit an auditor should also speak with available subcontractors on site to get additional information about the progress of the engagement. Furthermore, the auditor should consider observing equipment and uninstalled inventory on site.

- Meet with project managers. Project managers play an important role in controlling and reporting job site costs. They are also close to the facts and are likely to get more prompt and accurate information than the accounting personnel. For example, a project manager may be aware of a large bill that will arrive relating to his or her project about which the accounting department has not yet been notified. Meeting with the project mangers will also assist the auditor in developing expectations for use in performing analytical review procedures. Also, consider having the project managers of significant contracts complete a questionnaire regarding the status of their contracts.
- Identify and understand the significant assumptions and uncertainties. This procedure is fundamental to performing an effective audit of an entity using contract accounting. Not performing this function results in an audit that does not comply with GAAS.
- Test contract costs to make sure that costs are matched with appropriate contracts. In some instances a company may shift costs from unprofitable contracts to profitable ones in an effort to defer losses.
- Audit estimated costs to complete. The focus should be on the key factors and assumptions, such as those that are (*a*) significant to the estimate, (*b*) sensitive to variation, (*c*) deviate from historical patterns, and are (*d*) subjective and susceptible to bias or misstatement. A review of revised or updated estimates of cost to complete and a comparison of the estimates with the actual costs incurred after the balance sheet date is also a useful procedure.
- See that losses are recorded as incurred, regardless of whether an entity is using the percentage-of-completion or the completed-contract method of recognizing revenue.
- Analytically review contacts completed and in progress. A detailed analytical review of completed contracts and contracts in progress will provide meaningful information in helping to focus the auditor's efforts on potential problem areas. The look back analysis also reveals significant information about the company's ability to estimate.
- See that there are appropriate disclosures relating to SOP 94-6, *Disclosure of Risks and Uncertainties* [section 10,640]. Entities using contract accounting probably should have more than generic disclosure about the use of significant estimates used in the preparation of financial statements. The AICPA SEC Practice Section has noticed that many companies include excellent disclosure about the risk of

contract losses and the possibility of inaccurate estimates in the forepart of their Form 10-K. It is the PITF's view that some of that enhanced disclosure would strengthen financial statement disclosure.

- Review the aging of receivables on contracts. This procedure will provide evidence that a Company is collecting funds on a timely basis.
- Consider the use of specialists in auditing construction contracts in accordance with SAS No.73, *Using the Work of a Specialist.*

.05 Auditing entities that use contract accounting is challenging in that the main element of the contractor's financial statements are based on estimates of cost, and, importantly, costs not shipments drive the revenue recognition process.

.06 Prior to auditing contractors an auditor should ensure that they have the appropriate expertise to understand the risks of the business. This additional knowledge will lead to an audit that meets or exceeds generally accepted auditing standards.

[The next page is 50,991.]

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Section 16,190

Practice Alert 01-1
Common Peer Review Recommendations

April, 2001

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits and is based on existing professional literature, the experience of the members of the Professional Issues Task Force (PITF) and information provided by SEC Practice Section member firms to their own professional staff. This information represents the views of the members of the PITF and is not an official position of the AICPA. Official positions are determined through certain specific committee procedures, due process and deliberation. The information provided herein should be used only with the understanding that it is to be read in conjunction with the professional literature and that it is only a means of assisting auditors in meeting their professional responsibilities.

Introduction

.01 The PITF believes that a summary of common peer review findings will be helpful to professionals as they consider critical and significant issues in planning and performing audits. The PITF hopes that by highlighting these items, the quality of audits will be enhanced and compliance with generally accepted auditing standards will be increased. Furthermore, the PITF hopes this alert will increase the sensitivity to these issues by professionals conducting peer reviews.

.02 Based on AICPA statistics of more than 21,000 peer reviews over the last four years, the PITF noted that approximately 94% of the peer review reports issued resulted in an unmodified report on the firm's quality control system. Approximately 5% resulted in modified reports and less than 1% resulted in adverse reports on the firm's quality control system. Overall, peer review results have improved since the inception of the peer review program.

.03 The most common peer review recommendations can be grouped into five categories: 1) implementation of new professional standards or pronouncements, 2) application of generally accepted accounting principles (GAAP) pertaining to equity transactions, 3) application of GAAP pertaining to revenue recognition considerations, 4) documenting audit procedures or audit findings, and 5) miscellaneous findings.

Implementation of New Professional Standards or Pronouncements

.04 Peer reviewers have noted that some firms have not implemented new professional standards and pronouncements on a timely basis. The most recent common examples of professional standards that these firms failed to implement

on a timely basis include the application of Independence Standards Board (ISB) No. 1, *Independence Discussion with Audit Committees* and SAS No. 85, *Management Representations*. ISB No. 1 requires a firm to disclose certain relationships and confirm its independence in writing with each of its SEC audit clients every year. Details about the ISB and ISB No. 1 can be found on the ISB Web site at www.cpaindependence.org. Also, Practice Alert 99-1, *Guidance for Independence Discussion with Audit Committees* [section 16,130], provides examples of ISB No. 1 letters. SAS No. 85 states that written representations from management should relate to all financial statement periods covered by the auditor's report. For example, if a firm is giving an opinion on the financial statements at and for the years ended December 31, 2000 and 1999, a representation letter should be obtained that includes representations for 1999 and 2000. These representations should be updated each year even if they were obtained in the previous year, such as 1999 in the previous example.

.05 There are frequently more than a dozen new pieces of authoritative professional literature issued each year. The most authoritative sources of new professional literature are issued by the Auditing Standard Board of the AICPA ("ASB"), the Financial Accounting Standards Board ("FASB"), and the SEC in the form of Staff Accounting Bulletins ("SAB's"). However, other authoritative literature is issued in the form of Statements of Position ("SOP") issued by the Accounting Standards Executive Committee of the AICPA ("AcSEC"), consensus positions of the Emerging Issues Task Force ("EITF") and standards and interpretations issued by the Independence Standards Board ("ISB") and the Governmental Accounting Standards Board ("GASB"). Other professional guidance that should be considered includes the AICPA Accounting General and Industry Audit Guides and related Risk Alerts.

.06 A firm's quality control system should be designed to provide reasonable assurance that its professionals are informed of changes to the professional literature. To assist a firm in achieving this objective, a professional may be designated to help ensure that the new pronouncements are understood and implemented in a timely fashion. Many firms rely on third-party practice aides to help them in this endeavor. This is most effective if the material is updated frequently and the firm's professionals are informed of the changes and how the changes might affect their specific client engagements. The PITF recommends that even when using third-party practice aids, each firm should assign an experienced professional who is responsible for helping to ensure new pronouncements are implemented in a timely manner.

Equity Transactions

.07 Accounting for equity transactions can be complicated and some professionals do not encounter many of these transactions very frequently. Consequently, in January 2000, the PITF issued Practice Alert 00-1, *Accounting for Certain Equity Transactions* [section 16,150]. This Alert provided some of the more common examples, which require careful consideration in determining the appropriate accounting treatment. Common examples where GAAP has been misapplied include (1) stock issued for goods and services, (2) the issuance of warrants, (3) conversion features, and (4) stock options plans. The PITF strongly encourages consultation with other qualified professionals when auditing these transactions. Accounting for many equity transactions may be complicated and therefore, this engagement area may need to be assessed as moderate to high-risk.

 Copyright © 2001, American Institute of Certified Public Accountants, Inc.

Revenue Recognition

.08 Accounting for revenue continues to be an area of focus at the SEC. Specifically, in December of 1999, the SEC issued SAB 101, *Revenue Recognition*, in an attempt to clarify guidance on when it is appropriate for companies to recognize revenue. In October 2000, the SEC also published answers to frequently asked questions ("FAQ's") on SAB 101 which is available at www.SEC.gov/info/accountants.shtml. In November 1998, the PITF issued Practice Alert 98-3, *Revenue Recognition Issues* [section 16,120]. That Alert is intended to remind auditors of certain factors or conditions that can be indicative of increased audit risk relative to improper, aggressive or unusual revenue recognition practices and suggests ways in which auditors may reduce the risk of failing to detect such practices. Additionally, the AICPA's revenue toolkit is available electronically at www.aicpa.org/members/div/auditstd/pubaud.htm. Loading the toolkit from this Web site requires the use of the software Acrobat Reader. The toolkit can also be purchased from the AICPA at 888/777-7077 by requesting product number 022506. Finally, SOP 97-2, *Software Revenue Recognition* [section 10,700], is an important resource for software companies, whether auditing or accounting for revenue.

Documentation

.09 SAS No. 41, *Working Papers*, is the authoritative literature that provides guidance for documentation requirements. Other SASs (e.g., SAS Nos. 55, 61, and 82) also contain specific documentation requirements. The PITF members and the SECPS Peer Review Committee have noted that documentation in the following areas could be improved:

- Fraud risk factors, the disposition of such identified factors, or the planned procedures to address these risk factors.
- The firm's understanding of the internal control system and the basis for reliance on that system.
- Materiality considerations including those relating to waived audit adjustments.
- The extent of auditing procedures performed, the person(s) performing specific procedures, and the conclusion reached.
- Analytical procedures used in planning the nature, timing and extent of the other auditing procedures to be performed; as substantive procedures to audit account balances, classes-of-transactions or assertions; and in the overall review of the financial information during the final stage of the audit.
- Compliance with loan covenants, or whether the company had obtained formal waiver letters from lenders that, when necessary, cover at least a year from the balance sheet date.
- The consideration of going concern and, if necessary, management's plan to keep the entity operating.
- Consultation on significant matters.
- The extent of competent evidential matter supporting significant estimates.

- The completion of an accounting disclosure checklist when required by the firm's quality control policies and procedures. This document, when prepared correctly leads to complete financial statement disclosures complying with GAAP. Some of the more common deficiencies are incomplete disclosures related to deferred income taxes, the use of estimates and advertising policies and costs.
- The performance of appropriate quarterly review procedures. The PITF issued Practice Alert 00-4, *Quarterly Review Procedures for Public Companies* [section 16,180], in October 2000. This Alert provides auditors with the required quarterly review procedures and suggested procedures that should be considered when performing a quarterly review for a public company.
- Documenting SAS No. 61, *Communication With Audit Committees*, and SAS No. 90, *Audit Committee Communications*. If this communication is not in writing, it must be documented in the working papers as to what, when and with whom the communications occurred.

Miscellaneous

.10 Peer reviewers have also noted deficiencies in the following areas:

- Performing ongoing monitoring procedures or a timely annual inspection. A firm's monitoring procedures or annual inspection needs to be completed timely so that the results and recommendations can be communicated and implemented prior to the firm's next busy season. A firm may elect to have the external peer review substitute for the internal inspection in the year an external peer review is performed.
- Performing an appropriate concurring partner review on an SEC attest engagement. Firms that are members of the SECPS are required to have a concurring review performed by a qualified partner of the firm or another firm. The concurring review partner should not be associated with the performance of the engagement. A partner, as defined by the SECPS, is an individual who is legally a partner, owner or shareholder in a CPA firm or a sole practitioner and should be party to any partnership, ownership or shareholder agreement of the firm.

.11 A concurring partner reviewer's responsibility as documented in the SECPS membership requirement (www.aicpa.org/members/div/secps/coparemere.htm) is fulfilled by performing the following procedures: 1) discussing significant accounting, auditing and financial reporting matters with the audit engagement partner; 2) discussing the audit engagement team's identification and audit of high-risk transactions and account balances; 3) reviewing documentation of the resolution of significant accounting, auditing and financial reporting matters, including documentation of consultation with firm personnel or resources external to the firm's organization (such as standard-setters, regulators, other accounting firms, the AICPA, and state societies); 4) reviewing a summary of unadjusted audit differences 5) reading the financial statements and auditors' report; and 6) confirming with the audit engagement partner that there are no significant unresolved matters. Engagement files should contain evidence that the concurring partner review was performed timely and that SECPS membership requirements were met. Typically, a concurring review takes longer than a couple of hours and may take many hours on larger engagements.

 Copyright © 2001, American Institute of Certified Public Accountants, Inc.

- Obtaining verification of independence when a firm uses per diem and contract employees, or outside concurring reviewers. Such independence is necessary to comply with professional standards.
- Compliance with the SEC rules on performing bookkeeping services for public companies. Instances were noted where firms were maintaining the client's fixed assets records and preparing and computing fixed asset depreciation schedules for audit clients. The SEC prohibits an auditor from performing such services because they believe it impairs auditor independence. The SECPS has also noted instances where the auditor was assisting their SEC client in closing out their books, including preparing routine accruals. This activity would appear to impair independence.
- Meeting the auditor's responsibilities with respect to performing and documenting subsequent event procedures in connection with the re-issuance of opinions or the issuance of consents. A firm is required to update discussions with management and attorneys, and obtain a formal written management representation letter up to the filing or effective date, or as close thereto as reasonable and practicable.

Annual Reviewers' Alert

.12 The AICPA publishes an Annual Reviewers' Alert each year that provides peer review team captains and firms with information highlighting significant matters in the profession, such as issues raised by the SEC and new accounting and auditing pronouncements. In the spring of 2001, the AICPA anticipates that this publication will be available online at www.aicpa.org. Team captains and the firm's quality control leaders should obtain and read this publication.

Summary

.13 This Alert summarizes some of the more significant common peer review recommendations. Every professional is advised to consider all of these issues when performing audits to help ensure that every audit is performed in compliance with generally accepted auditing standards.

[The next page is 51,011.]

Section 16,200

Practice Alert 01-2 Audit Considerations in Times of Economic Uncertainty

October, 2001

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits and is based on existing professional literature, the experience of the members of the Professional Issues Task Force (PITF) and information provided by SEC Practice Section member firms to their own professional staff. This information represents the views of the members of the PITF and is not an official position of the AICPA. Official positions are determined through certain specific committee procedures, due process and deliberation. The information provided herein should be used only with the understanding that it is to be read in conjunction with the professional literature and that it is only a means of assisting auditors in meeting their professional responsibility.

Introduction

.01 During the past several months, the U.S. economy has suffered some significant declines. The U.S. Commerce Department has reported declines that are consistent with a slowing economy: consumer confidence has dropped, plant closings and lay-offs have increased dramatically, profit margins for many companies have slipped and many dot-com companies have failed. Some economists predict a recession, which could result in further deterioration in internally generated cash flows and restrictions on the availability of capital.

.02 Periods of economic uncertainty lead to challenging conditions for companies due to potential deterioration of operating results, increased external scrutiny, and reduced access to capital. These conditions can result in increased incentives for companies to adopt practices that may be incorrect or inconsistently applied in an effort to address perceived expectations of the capital markets, creditors or potential investors. During such times, professional skepticism should be heightened and the status quo should be challenged. This Practice Alert is designed to remind auditors of issues to consider during these times.

Professional Skepticism

.03 The third general auditing standard stipulates that due professional care be exercised in planning and conducting an audit engagement. Due professional care requires that the auditor exercise professional skepticism in gathering and evaluating audit evidence. Although the auditor neither assumes that management is dishonest nor assumes unquestioned honesty, the auditor should consider the increased risk associated with the potential increases in external pressure faced by management in times of economic decline.

.04 As a result of perceived external pressures, companies may be tempted to manage earnings through conduct of non-recurring transactions or through changes in the method of calculating key estimates, such as reserves, fair values or impairments. Companies may also adopt inappropriate accounting practices resulting in improper recognition or omission of financial transactions. Material non-recurring transactions may require special disclosure to facilitate the reader's understanding of the reported financial results, and the guidance in APB No. 20, *Accounting Changes*, should be applied in reporting on the effect of changes in estimates. Inappropriate transactions or accounting practices that may result in errors requiring adjustments of financial statements might include premature recognition of revenue, failure to record returns, inflating inventories, failure to appropriately accrue for contingent liabilities that are probable and estimable, and failure to record "misplaced" or otherwise unpaid purchase invoices. Additionally, an auditor should be particularly skeptical of non-system adjustments or fourth-quarter events that result in significant revenue recognition, loss accrual or non-cash earnings.

.05 The SEC has recently focused significant renewed attention with respect to potential inappropriate over-accrual or misuse of restructuring reserves. In this regard, auditors also have to be skeptical that provisions for restructuring costs and asset write-downs are not unduly conservative. Relevant accounting guidance can be found in SAB 100, *Restructuring and Impairment Charges*, and EITF Issue 94-3, *Liability Recognition for Certain Employee Termination Benefits and Other Costs to Exit an Activity (Including Certain Costs Incurred in a Restructuring)*. Additionally, the increased focus of external analysts on revenue rather than traditional measures of operating performance has resulted in the SEC providing companies with expanded interpretive guidance in SAB 101, *Revenue Recognition in Financial Statements*, which addresses recognition and classification of revenue.

.06 The appropriate level of professional skepticism is needed when corroborating management's representations. Management's explanations should make business sense. Additionally, the auditor may need to consider corroborating management's explanations with other evidence when practicable, including discussions with members of the board of directors or audit committee.

.07 Other indicators of potential increased accounting and reporting risk calling for increased professional skepticism include:

1. **Liquidity matters**
   - The company is undercapitalized and is relying heavily on bank loans and other credit and is in danger of violating loan covenants.
   - The company appears to be dependent on an IPO for future funding.
   - The company is having difficulty obtaining or maintaining financing.
   - The company is showing liquidity problems.
2. **Quality of earnings**
   - The company is changing significant accounting policies and assumptions to less conservative ones.
   - The company is generating profits but not cash flow.

 Copyright © 2001, American Institute of Certified Public Accountants, Inc.

3. **Industry characteristics**

   - The company is a dot-com or Internet company or a supplier to those types of companies.
   - The company is not a market leader. Companies that are not market leaders sometimes must sell products below cost to match competitors' pricing.

4. **Management characteristics**

   - Management's compensation is largely tied to earnings or the appreciation of stock options.
   - The company appears vulnerable to the weakening economic conditions and management is not proactive in addressing changing conditions.
   - The company's management is selling their investment in company securities more than in the past.
   - There is a significant change in members of senior management or the board of directors.

.08 The following paragraphs serve as reminders for considerations when auditing the following specific accounts.

Inventory

.09 When auditing inventory, consider the following issues:

- The reason for an unusual increase in inventory balances. Reduction in turnover, increased backlog or deterioration in aging of inventories may be signs that the company has excessive inventory on hand.
- Whether the company's product is technologically attractive to consumers. If not, consider the company's plan to sell the inventory and at what cost.
- Whether declining prices and shrinking profit margins are causing inventory to be valued over market.
- Whether the reduced production at a manufacturing facility is leading to an over-capitalization of inventory overhead rather than expensing the costs of excess capacity.
- Whether there are material or unusual sales cancellations and returns after year-end.
- Whether there are indications of "channel stuffing."

.10 An auditor should also be aware of any:

- Unfavorable purchase commitments.
- Unfavorable sales commitments or arrangements.

Accounts Receivable

.11 When auditing accounts receivable, consider the following circumstances:

- An increase in the aging of receivable balances. This event may be indicative of weakening economic conditions. Many companies that sell to Internet-related companies may need to increase their bad debt provisions this year since some of these Internet-related companies are facing financial challenges that may include bankruptcy.
- Internal controls over credit functions are weak. Consider a company's policies for reviewing the amount of customer credit extended to each customer.
- Receivable amounts that are increasing at a faster rate than revenue.
- Concentration of receivables in one geographic area or economic sector.
- The existence of extended payment terms or return privileges.
- Significant decreases in accounts receivable confirmation response rates from the prior year.
- Compliance with revenue recognition pronouncements, such as SOP 97-2, *Software Revenue Recognition*, and SAB 101, *Revenue Recognition in Financial Statements*.

Investments

.12 An auditor should determine whether the classification of securities is appropriate. For example, an auditor should consider whether the company has the ability, as well as the intent, to hold securities to maturity that are classified as such.

Long-Lived Assets, Including Goodwill and Intangibles

.13 Industry downturns and cash flow erosion may indicate an impairment of fixed assets, goodwill or other intangibles. Financial Accounting Standards Board's (FASB) Statement No. 121, *Accounting for the Impairment of Long-Lived Assets to Be Disposed Of*, provides guidance in this area. In that regard, significant idle plant capacity or equipment no longer used in operations may need to be written off, unless alternative uses exist.

.14 Goodwill and intangibles should be analyzed to consider whether the amortization assumptions still appear reasonable. For example, if a company purchases a patent that is amortized over 10 years and the technology of the product has changed to where the patent is no longer used, it may be necessary to write-down or write-off the asset.

.15 In June 2001, the FASB issued Statement No. 142, *Goodwill and Other Intangibles*. This Statement addresses financial accounting and reporting for acquired goodwill and other intangible assets and supersedes APB Opinion No. 17, *Intangible Assets*. The Statement also addresses how intangible assets that are acquired individually or with a group of other assets should be accounted for in financial statements upon their acquisition. FASB Statement No. 142 is required to be applied starting with fiscal years beginning after December 15, 2001.

Deferred Taxes and Other Deferred Charges

.16 An auditor should consider whether the assumptions and expectations of future benefits of deferred tax assets and other deferred charges appear reasonable. In weighing positive and negative evidence for purposes of

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

assessing the need for or amount of a deferred tax asset valuation allowance, FASB Statement No. 109, Accounting for Income Taxes, requires that the weight given to evidence be commensurate with the ability to objectively verify that evidence. As a result, recent historical losses are given significant weight while expectations about future profits may not be given much weight.

Accounts Payable

.17 An auditor should consider whether the company has delayed making payments on its outstanding payables. This may result from the company properly managing cash, but it may also be a result of a company experiencing cash flow shortages. An increasing accounts payable balance with flat or decreasing sales may be evidence of cash flow concerns.

Debt

.18 An auditor should carefully review loan agreements and test for compliance with loan covenants. In this regard, an auditor should consider any "cross default" provisions; that is, a violation of one loan covenant affecting other loan covenants. An auditor should also keep in mind that any debt with covenant violations that are not waived by the lender for a period of more than a year from the balance sheet date may need to be classified in the balance sheet as a current liability.

.19 As always, an auditor should review the debt payment schedules and consider whether the company has the ability to pay current debt installments or to refinance the debt if necessary. When making such an evaluation, it is important to remember that it is quite possible that the company will not generate as much cash flow as it did in the previous year.

Going Concern

.20 During times of economic uncertainty, an auditor should have a heightened sense of awareness of a company's ability to continue as a going concern. SAS 59, *An Entity's Ability to Continue as a Going Concern*, addresses an auditor's responsibility to evaluate whether there is substantial doubt about the entity's ability to continue as a going concern. Negative trends, loan covenant violations and legal proceedings are examples of items that might indicate that there could be substantial doubt about the ability of an entity to continue as a going concern. When evaluating management's plans to continue as a going concern, an appropriate level of professional skepticism is important. For example, the company's assumptions to continue as a going concern should be scrutinized to assess whether they are based on overly optimistic or "once in a lifetime" occurrences.

Other Considerations

.21

- An auditor should consider the extent of procedures that may be necessary relating to unusual and significant transactions noted during the audit, including unusual or "non-routine" journal entries. Many times, these entries are made on the parent company's books, or as part of a consolidating entry, or in the last few days of the month.

- An auditor should be aware of new developments in his or her client's business. Analytical reviews, therefore, should emphasize the comparison of relationships with independent data. When expected fluctuations do not occur, or when unexpected fluctuations do occur, an auditor should investigate the reasons. It is also important to consider whether the relationships between financial and nonfinancial information make sense. For example, in a cable TV company, if the number of subscribers declined from the prior year, it would make sense, absent a rate increase, that revenue declined also.
- An auditor should consider whether significant declines in stock prices may result in option pricing changes or other compensation benefits being promised to employees.
- An auditor should be aware of inconsistent approaches to write-downs.
- An auditor should consider off-balance sheet risks; for example, the risks related to the failure to perform a contract efficiently. Large fixed fee contracts can subject companies to large risks.
- An auditor should consider a company's ability to forecast and anticipate changes in market conditions. The inability to forecast and foresee changes in market conditions should heighten an auditor's professional skepticism. Companies that are proactive and lead market changes often perform better in times of economic uncertainty than those that are reactive.
- Professional skepticism relating to the above should also be maintained when reviewing quarterly financial statements for public companies.
- An auditor should not allow client or self-imposed deadlines to pressure him or her into accounting and auditing decisions that are not well thought out. An auditor should also consult with other professionals whenever appropriate—for example, on a complex accounting or auditing issue.

Summary

.22 Auditing companies in times of economic uncertainty is challenging. As such, auditors need to maintain the appropriate levels of professional skepticism and due professional care.

[The next page is 51,051.]

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

Section 16,220

Practice Alert 02-2
Use of Specialists

First issued
May, 2002;
Updated October, 2002

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits and is based on existing professional literature, the experience of members of the Professional Issues Task Force (PITF) and information provided by the SEC Practice Section member firms to their own professional staff. This information represents the views of the members of the PITF and has not been approved by any senior technical committee of the AICPA. The auditing portion of this publication is an *Other Auditing Publication* as defined in Statement on Auditing Standards (SAS) No. 95, *Generally Accepted Auditing Standards*. Other Auditing Publications have no authoritative status; however, they may help the auditor understand and apply SASs. If an auditor applies the auditing guidance included in an Other Auditing Publication, he or she should be satisfied that, in his or her judgment, it is both appropriate and relevant to the circumstances of his or her audit. This publication was reviewed by the AICPA Audit and Attest Standards staff and published by the AICPA, and is presumed to be appropriate.

Introduction

.01 During the performance of an audit engagement, the auditor may decide to use the work of a specialist. A specialist is a person with a special skill or knowledge in a particular field other than accounting or auditing. The specialist may be either engaged by the client or by the auditor, or employed by the audit firm or the client. Although the auditor is expected to be knowledgeable about business matters in general, the auditor is not expected to have or obtain the same level of understanding of a subject field as an expert in that particular field. Examples of areas where specialists are utilized in audit engagements include:

- Valuations of certain types of assets, for example: land and buildings, plant and machinery, works of art, minerals and precious stones.
- Valuations of businesses and derivatives.
- Information technology.
- Determination of quantities or physical condition of assets, for example: minerals stored in stockpiles, and underground mineral and petroleum reserves.
- Actuarial valuations.

- Measurement of work completed and to be completed on construction contracts in progress for the purpose of revenue recognition. For example, providing corroborating evidence on the progress and possible obstacles to completing a hydroelectric plant.
- Legal interpretations of contacts and agreements, statutes, and government and other regulations.
- Evaluation of significant issues relating to federal, state or local income and other tax matters.

.02 Auditors may encounter difficulty in determining the appropriate situations in which to utilize a specialist and, in those cases when a specialist is appropriately utilized, understanding the findings of the specialist. The current guidance when specialists are used is broad and focuses on the use of all kinds of specialists. The purpose of this Practice Alert is to assist auditors in understanding their responsibilities both with respect to the use of specialists that have been engaged or employed by the audit client and the use of specialists engaged or employed by the audit firm.

Decision to Use a Specialist

.03 The decision to obtain the assistance of a specialist is generally made in the planning stage of the audit engagement. The auditor should ascertain whether or not specialized knowledge will be needed in order to corroborate management's assertions with respect to amounts in the financial statements. The auditor should not accept an engagement when it is not possible to obtain an appropriate level of understanding of the subject matter, either directly or through the use of a specialist.

Use of a Specialist Engaged or Employed by the Audit Client

.04 With respect to specialists engaged or employed by the audit client, the auditor should consider the specialist's qualifications and experience in the planning stage of the engagement. SAS No. 73, *Using the Work of a Specialist*, states that the auditor should consider the professional certification, license or other recognition of the competence of the specialist in his or her field, as appropriate. In addition, the reputation and standing of the specialist in the views of peers or others familiar with the specialist's capability or performance can assist the auditor in assessing the specialist's qualifications.

.05 After the auditor has become satisfied with the qualifications and experience of the specialist, the auditor should then obtain an understanding of the specialist's work. The auditor can obtain the understanding in many ways, including reading professional literature dealing with the subject specialty, discussing the subject with other auditors who have performed similar engagements in the same field, discussing the subject with the specialist or with other specialists and attending relevant seminars on the subject. The auditor should consider the following:

- The objectives and scope of the specialist's work;
- The specialist's relationship to the client;
- The specialist's methods and the assumptions used, including the comparability to those used in the preceding period and those used by similar specialists, if known;

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- The specialist's compliance with the auditor's requirements;
- The appropriateness of using the specialist's work for the intended purpose; and
- The form and content of the specialist's findings.

.06 In those situations where the audit client has engaged the specialist, during the planning process the auditor performs the necessary procedures to ascertain the nature of the specialist's relationship to the audit client. The auditor should assess the risk that the specialist's objectivity may be impaired. A specialist that is engaged by the client need not be independent, only objective. If the auditor determines that the specialist's objectivity might be impaired, the auditor should either engage another specialist or should perform additional procedures with respect to some or all of the specialist's assumptions, methods or findings to determine whether the findings are not unreasonable.

.07 If the auditor concludes that he or she will use the findings of a specialist, consideration should be given to the need to communicate with the specialist to confirm the terms of the specialist's engagement and to cover such matters as:

- The objectives and scope of the specialist's work.
- Clarification of the specialist's relationship with the client.
- Information as to the assumptions and methods intended to be used by the specialist and, if appropriate, as to their consistency with those used in the prior period and compared to those used by other industry specialists.
- The specialist's compliance with the auditor's requirements.
- The appropriateness of using the specialist's work for the intended purpose.
- The form and content of the specialist's findings as well as a general outline as to the specific items the auditor expects the specialist will cover in the report.
- The auditor's intended use of the specialist's work.
- The identification of the data to be supplied by the client to the specialist, so that the auditor is aware of what needs to be subjected to audit testing.
- Any non-client data that the specialist intends to use.
- The extent of the specialist's access to appropriate records and files.
- Confidentiality of the client's information.
- Documentation or further information required supporting the auditor's procedures and report.

.08 The auditor should consider obtaining a confirmation directly from the specialist regarding the nature and scope of his/her engagement.

.09 The use of a specialist does not allow the auditor to delegate his or her audit responsibilities. Therefore, the auditor must be able to understand the methods and assumptions used by the specialist in order to fulfill his or her audit responsibilities.

.10 The reliability of the source data used by the specialist is significant to the accuracy of the specialist's findings and ultimately, the audited financial statements. Therefore, the auditor performs procedures to corroborate the data, both accounting and non-accounting, that the client provided to the specialist, taking into account the auditor's assessment of control risk. The auditor's procedures may include making inquiries of the specialist to determine whether the specialist is satisfied as to the accuracy of the source data, identifying and conducting appropriate tests and considering the reliability and relevance of the data provided by the client to the specialist. For example, for an actuarial computation with respect to a pension plan, the auditor may, on a test basis, compare the demographic information to the client's personnel files and the payroll information to the payroll ledgers. In addition, the auditor may analytically review the rate of return on the plan portfolio for reasonableness and may test the forecasted earnings stream and the cap rate used in the valuation.

.11 The auditor should evaluate whether the specialist's findings support the related assertions in the financial statements. Ordinarily, the auditor would use the work of the specialist unless the auditor concluded that the specialist's findings are unreasonable. For example, an actuary with respect to an automobile insurance company client may conclude that the loss reserves should decrease over the percentage used in the previous year. The finding may be deemed unreasonable if the auditor is aware that the experience in the subject state during that year was that losses had increased statewide. If the findings appear to be unreasonable, additional audit procedures may be necessary or the opinion of another specialist may be obtained. If the matter was not resolved to the auditor's satisfaction, the auditor would consider whether to qualify his or her report or disclaim an opinion because of a scope limitation.

.12 The auditor would ordinarily not mention the work or findings of a specialist when expressing an unqualified opinion on audited financial statements, except in very limited circumstances described in SAS No. 73.

.13 The auditor should consider incorporating a specific representation in the client representation letter if the audit client has engaged a specialist. An example representation is as follows:

> We assume responsibility for the findings of specialists inevaluating the (describe assertion) and have adequately considered the qualifications of the specialists in determining the amounts and disclosures used in the financial statements and underlying accounting records. We did not give nor cause any instructions to be given to specialists with respect to the values or amounts derived in an attempt to bias their work, and we are not otherwise aware of any matters that have had an impact on the objectivity of the specialists.

Use of Specialists Engaged or Employed by the Audit Firm

.14 Except at the time of employment and as necessary to satisfy ongoing educational and licensing requirements, the auditor would not ordinarily need to check the qualifications of a specialist employed by the audit firm. In addition, the internal specialist is subject to the firm's requirements with respect to independence.

.15 The auditor will need to make a determination as to whether the specialist is part of the audit engagement team. If the specialist is effectively

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

functioning as a member of the audit team, SAS No. 73 does not apply. SAS No. 22, *Planning and Supervision*, will apply in that situation since the specialist requires the same supervision and review as any assistant. For example, if a specialist is used to perform procedures as part of the engagement team, such as performing computer assisted audit techniques, then SAS No. 22 applies. Specific guidance with respect to the use of information technology specialists is provided later in this Practice Alert. However, if the client engages the audit firm's actuarial department to perform procedures with respect to a pension plan, and the auditor subsequently utilized that work, the specialist is not a member of the engagement team and the auditor should follow the guidance as outlined in the previous section of this Practice Alert.

.16 Generally, using a specialist within the audit firm reduces audit risk, as the specialist should be familiar with the firm's professional policies. In addition, the other members of the audit team are generally familiar with the specialist's qualifications. Auditors employed by firms that make use of subsidiaries or affiliated organizations should take special care in assessing the internal specialist's familiarity with firm policies. Even though the specialist and the auditor may be part of the same "parent" firm, the specialist may not be familiar with the audit firm's policies.

.17 If the auditor has engaged an outside specialist, an understanding with the specialist about the engagement should be obtained. The auditor may want to document the understanding and the arrangements with the specialist in writing. All other procedures with respect to the methods and assumptions used by the specialist and the use of the specialist's findings are consistent with those utilized for specialists engaged or employed by the client.

Examples of Specific Types of Specialists to Be Utilized

Information Technology ("IT") Specialists

.18 The use of IT specialists is a significant aspect of many audit engagements. The Public Oversight Board's Panel on Audit Effectiveness issued a report in August 2000 which called for more effective participation in audits by IT specialists. The IT specialist is usually employed or engaged by the audit firm and the use of IT specialists is covered by SAS No. 22 and SAS No. 94, *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit.*

.19 SAS No. 94 provides guidance to assist auditors in determining whether to use the work of an IT specialist. To determine whether an IT specialist is needed, it is recommended that the auditor consider the following factors:

- The complexity of the entity's systems and IT controls, and the manner in which they are used
- The significance of changes made to existing systems or the implementation of new systems
- The extent to which data is shared
- The extent of the entity's participation in electronic commerce
- The entity's use of emerging technologies
- The significance of audit evidence that is available only in electronic form.

.20 The extent of involvement of an IT specialist will depend on the complexity of information technology used in critical transaction cycles, control risk assessments and the information technology skills available in the engagement team. The role of the IT specialist may be to assist the engagement team in the following areas:

- Performing a preliminary review of computer processing
- Designing and implementing tests of controls and substantive tests related to information technology systems, including the use of computer assisted audit techniques
- Interpreting the test results
- Drafting client communications, such as internal control and management letters.

.21 In addition, the IT specialist can assist the auditor in addressing many audit procedures. The IT specialist can examine the client's data files and information and detect and highlight transactions or patterns that show possible irregularities. Examples where an IT specialist may be used to assist the auditor are as follows:

- Ratio analysis
- Revenue and other cut-off testing
- Accounts receivable or payable aging
- Examination of purchase ledger transactions
- Summarizing payments by vendor or invoice numbers
- Testing for duplicate invoices
- Searching for payments to specific individuals
- Stratifying payments by size and extracting unusual ones
- Analyzing payroll data in the search for unusual payments
- Matching payments to payroll master files to test for correct rates and deductions.

.22 IT specialists can also perform digit analysis—the process of using mathematical formulas and probability equations to examine data sets for irregularities. Examples include number duplication, excessive round numbers and identification of identical or near-identical entries in data subsets.

.23 When an IT specialist is used, the auditor's responsibility for information technology aspects of an audit cannot be transferred to that specialist. The auditor is responsible for:

- Determining, in consultation with the IT specialist, the objectives of the review of computer processing and the procedures to be performed
- Participating appropriately in performing the work
- Reviewing the results of the specialist's work
- Evaluating the results of the review as it affects audit risk and strategy and modifying the audit procedures to be performed accordingly
- Ensuring that the workpapers adequately document all information technology aspects of the audit.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Business Valuation Specialists

.24 The Financial Accounting Standards Board's (FASB) Statement No. 141, *Business Combinations*, and FASB Statement No. 142, *Goodwill and Other Intangible Assets*, valuations that are performed in connection with purchase price allocations after a business combination and the impairment test required thereafter generally should be performed by a specialist. Although the auditor may have sufficient expertise to review the valuation, it is advisable for auditors to consider utilizing a valuation specialist. This is particularly so when the transaction and valuation has a material impact on the company's financial statements. That specialist may be internal or external, as considered necessary. The auditor should perform procedures to evaluate whether the specialist's findings support the related assertions in the financial statements

---

[The next page is 51,071.]

Section 16,230

Practice Alert 02-3
Reauditing Financial Statements

September, 2002

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits and is based on existing professional literature, the experience of members of the Professional Issues Task Force (PITF) and information provided by the SEC Practice Section member firms to their own professional staff. This information represents the views of the members of the PITF and has not been approved by any senior technical committee of the AICPA. The auditing portion of this publication is an *Other Auditing Publication* as defined in Statement on Auditing Standards (SAS) No. 95, *Generally Accepted Auditing Standards. Other Auditing Publications* have no authoritative status; however, they may help the auditor understand and apply SASs. If an auditor applies the auditing guidance included in an *Other Auditing Publication*, he or she should be satisfied that, in his or her judgment, it is both appropriate and relevant to the circumstances of his or her audit. This publication was reviewed by the AICPA Audit and Attest Standards staff and published by the AICPA, and is presumed to be appropriate.

Introduction

.01 An auditor may be engaged to reaudit and report on financial statements that have been previously audited and reported on by another auditor (the predecessor auditor). The auditor conducting a reaudit engagement (defined in SAS No. 84, *Communications Between Predecessor and Successor Auditors*, as the successor auditor but hereinafter referred to as the reauditor) should not place reliance on the work of the predecessor auditor. Even when a reputable firm has already audited the financial statements, the reaudit work performed and the conclusions reached are solely the responsibility of the reauditor.

.02 There are two common circumstances under which a firm may be requested to perform a reaudit:

- The predecessor auditor is unwilling or unable to reissue its report for the intended purpose. For example, a company may plan to file a registration statement with the Securities and Exchange Commission (SEC) for an initial public offering and the predecessor auditor is unwilling to be associated with the financial statements of an SEC registrant or the predecessor auditor may not be independent under the independence rules applicable to SEC registrants or may no longer be in business.
- A company may wish to have another firm audit and report on its financial statements. Sometimes, the company or the underwriter with respect to an initial public offering may desire to have the current period and all prior periods audited by the same auditor, necessitating reaudits of prior periods.

.03 The reauditor should be aware of the audit guidance provided in paragraphs 14 through 20 of SAS No. 84. The purpose of this Practice Alert is to provide practitioners with additional factors to consider when performing a reaudit engagement.

Client/Engagement Acceptance Procedures and Considerations

.04 In determining whether to accept an engagement involving a reaudit for a new client, the reauditor should request permission from the prospective client to make inquiries of the predecessor auditor. Specific consent from the prospective client is required to make sure that confidential information is not disclosed inappropriately. The reauditor, in determining whether to accept the engagement, should perform the communications with the predecessor auditor as required in paragraphs 7 through 10 of SAS No. 84, including inquiries as to (*a*) information that might bear on the integrity of management; (*b*) any disagreements with management as to accounting principles, auditing procedures or other similarly significant matters; (*c*) communications to audit committees or others with equivalent authority and responsibility regarding fraud, illegal acts by clients, and internal control related matters, and; (*d*) the predecessor auditor's understanding as to the reasons for the change of auditors. The reauditor should indicate to the predecessor auditor that the purpose of the inquiries is to obtain information about whether to accept an engagement to perform a reaudit. In the absence of unusual circumstances, the predecessor auditor should respond promptly and fully, on the basis of known facts, to the reauditor's reasonable inquiries. If due to unusual circumstances, the predecessor auditor does not fully respond to the inquiries, the predecessor auditor should clearly state that the response is limited.

.05 In some situations, the predecessor auditor (a firm) might not be able to respond fully to the reauditor's inquiries, for example, when the predecessor firm no longer employs the predecessor audit engagement team. In such situations, the reauditor should make reasonable efforts to locate the predecessor audit engagement partner or other senior members of the engagement team and make appropriate inquiries. In some cases, another firm may employ the partner who had responsibility for the predecessor firm's engagement or other senior members of the engagement team. The firm that currently employs a member or members of the predecessor audit engagement team is not a "predecessor auditor" as defined in SAS No. 84. That firm, however, would normally be expected to facilitate inquiries to such individuals provided that specific authorization to respond is obtained by the reauditor from the prospective client in a form satisfactory to the firm and the individuals, and the reauditor and prospective client acknowledge, in a form satisfactory to the firm, that the firm is not placing itself in the position of a predecessor auditor. When such specific authorization and acknowledgement has been provided, a member or members of the predecessor audit engagement team ordinarily should, absent certain other circumstances that would limit their response, respond to the inquiries of the reauditor based on the full extent of the individuals' knowledge.

.06 The reauditor also should consider information pertaining to the integrity of management and any disagreements between management and the predecessor that may be obtained by performing the following procedures:

- Inquiring of bankers, lawyers, underwriters and others with knowledge of management.

 Copyright © 2002, American Institute of Certified Public Accountants, Inc.

- Reading the Form 8-K reporting the resignation or dismissal of the predecessor auditor and the predecessor auditor's response, if available.
- Reading the audit committee communications issued by the predecessor auditor.
- Reading the management representation letters including the summary of uncorrected financial statement misstatements.
- Reading the company's copies of correspondence with the predecessor auditor and regulators, if applicable.

.07 In circumstances where the predecessor auditor is unwilling or unable to reissue its report, the reauditor should consider the reasons and their implications, especially when the predecessor disagreed with management over accounting or auditing matters or restricts access to his or her audit documentation.

.08 In making a decision to perform a reaudit, the firm's client acceptance procedures should consider the following:

- The ability of the reauditor to perform his or her firm's normal client acceptance procedures. The firm should consider performing background checks of key executives. In addition, the firm should consider implementing additional procedures in accepting reaudit engagements, such as required consultation with and approval by, designated senior firm personnel prior to acceptance of the reaudit engagement. National and large regional firms should consider designating members of senior management or the firm's national technical group, or personnel of equivalent authority, for this purpose.
- Reading the previously issued financial statements on which the reaudit is to be performed. The reauditor should consider conducting interviews of executive management, including the CEO, the CFO, and the Audit Committee. Based on those discussions and from discussions with the predecessor auditors, the reauditor may be in a position to make a preliminary assessment about, among other matters, significant accounting policies, balances and transactions.
- The need for advising the client that since the reaudit is a new audit, the risk exists that material misstatements may be identified that were not identified by the predecessor auditor or that the reauditor's judgment regarding the appropriate application of generally accepted accounting principles or the materiality of previously identified misstatements may differ from that of the predecessor auditor.
- Whether the reaudit is being undertaken in connection with his or her current audit of a subsequent period (hereinafter referred to as a "current period audit"), as a separate engagement to be reported on before completing a current period audit, or as a one-time engagement. If the engagement is a one-time engagement, the potential reauditor should strongly consider the reasons that he or she is not performing the current period audit and may wish to consider not accepting the engagement on that basis.
- The ability to obtain third party confirmation or other primary audit evidence as of the balance sheet date(s) or the need to obtain confirmations as of a subsequent date and test the intervening transactions.
- The ability to obtain the necessary audit evidence, especially in significant areas, such as inventories, receivables and revenue.

- The predecessor auditor's representation regarding whether there have been any disagreements regarding accounting or other matters with management.
- Whether there has been a significant change in the top management team of the client and whether current management is willing, and has sufficient knowledge of the financial statements subject to the reaudit, to make all required management representations. The possible difficulties in obtaining the representation letter in these circumstances are discussed later in this Alert.
- Whether there have been significant changes in internal control subsequent to the reaudit period and whether an adequate understanding of internal control in operation during the reaudit period can be obtained to plan the reaudit.
- Whether sufficient audit evidence can be obtained in support of material financial statement assertions in situations where significant amounts of information are initiated, recorded, processed, or reported electronically, and no other documentation of those transactions is produced or maintained, other than through the IT system (e.g., a telecommunications company that uses IT to create a log of the services provided to its customers, initiate and process its billings for the services and automatically record such amounts in electronic accounting records that are part of the system used to produce the entity's financial statements).

Planning the Reaudit

.09 In a reaudit, the nature, timing and extent of the audit procedures performed and the conclusions reached in the reaudit are solely the responsibility of the reauditor. Notwithstanding the procedures performed by the predecessor auditor, the reauditor must perform an audit in accordance with generally accepted auditing standards (GAAS). Accordingly, the reauditor should not assume responsibility for the predecessor auditor's work or plan to divide responsibility with the predecessor auditor under SAS No. 1, section 543, *Part of Audit Performed by Other Independent Auditors*. The predecessor auditor is not a specialist as defined in SAS No. 73, *Using the Work of a Specialist*, or an internal auditor as defined in SAS No. 65, *The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements*.

.10 The reauditor should request that the client specifically authorize the predecessor auditor to allow access to the predecessor auditor's audit documentation for the period or periods under reaudit and the period prior to the reaudit period. The reauditor should consider the information obtained from inquiries of the predecessor auditor and review of the predecessor auditor's report and audit documentation in planning the reaudit. Ordinarily, the reauditor documents his or her review of the predecessor auditor's audit documentation and any information identified with continuing audit significance in the reaudit audit documentation. The reauditor should consider specifically examining the predecessor auditor's audit documentation with respect to the following:

- Understanding of internal controls and control risk assessments,
- The identification of internal control related matters noted in the audit, reportable conditions and material weaknesses,

 Copyright © 2002, American Institute of Certified Public Accountants, Inc.

- The identification of fraud risk factors and the results of audit procedures in response to specifically identified fraud risk factors,
- Understanding the company's business,
- Uncorrected financial statement misstatements,
- Other identified risks of material misstatement,
- And other audit documentation with respect to critical or significant accounting and audit areas.

.11 The extent, if any, to which the predecessor auditor permits access to his or her audit documentation is a matter of the predecessor auditor's judgment. However, it is customary for the predecessor auditor, absent any unusual circumstances such as impending, threatened, or potential litigation, disciplinary proceedings or non-payment of outstanding fees, to permit the reauditor to review the audit documentation, including documentation of planning, internal control, audit results, and other matters of continuing accounting and auditing significance.

.12 If possible, in order to maximize effectiveness and efficiency, the reaudit should be planned in conjunction with the current audit, if applicable, and the audit procedures for both should be coordinated.

Understanding the Client's Business

.13 As a result of inquiries of the predecessor auditor and review of the predecessor auditor's audit documentation, the reauditor may obtain significant information, including copies of audit documentation, related to understanding the entity's business that the reauditor may use in planning the reaudit. If the reauditor decides to utilize that information, he or she should corroborate the information through inquiries of management, inspection of key documents, and such other audit procedures as he or she considers necessary in the circumstances.

Understanding of Internal Control, Assessment of Control Risk and Tests of Controls

.14 The reauditor, as required by GAAS, should obtain an understanding of internal control for those periods on which the reauditor is asked to report. Information obtained from his or her review of the predecessor auditor's audit documentation may assist the reauditor in obtaining the required understanding and evaluating the design of relevant controls. The reauditor should perform procedures to corroborate the understanding and evaluation and determine whether key controls have been placed in operation. If the reauditor plans to assess control risk below the maximum, he or she should design and perform appropriate tests of controls to determine that relevant controls were operating effectively during the reaudit period. The reauditor may either test relevant controls in operation during the reaudit period or test relevant controls in operation currently, and perform a "rollback" of changes in the design of the internal controls to the prior periods.

.15 In instances where a "rollback" is not possible and control risk will be assessed at maximum, audit evidence should be obtained via substantive testing. However, the reauditor should consider whether it is possible to design

effective substantive tests that by themselves will provide sufficient evidence that financial statement assertions are not materially misstated in circumstances when a significant portion of the information supporting one or more financial statement assertions is electronically initiated, recorded, processed, or reported. Refer to paragraph 68 of SAS No. 55, *Consideration of Internal Control in a Financial Statement Audit*, as amended by SAS No. 78, for guidance.

Substantive Audit Procedures

.16 Some substantive testing, which may include analytical procedures and tests of details, is required for all material account balances and classes of transactions. In performing analytical procedures, the reauditor should develop his or her own expectations and use those expectations to determine matters requiring further investigation.

.17 The reauditor may consider the knowledge obtained from his or her review of the predecessor auditor's audit documentation and inquiries of the predecessor auditor to determine the nature, timing and extent of procedures to be applied in the circumstances and to assist in determining his or her expectations when performing analytical procedures.

Inventory

.18 Since the reauditor did not observe physical inventories in the prior years, the reauditor must be able to perform satisfactory alternative procedures if inventories are material, including a current physical observation and performing a "rollback" of amounts to prior periods. The reauditor also should perform tests of intervening transactions and analytical procedures. Refer to paragraph 20 of SAS No. 84 for guidance.

Confirmations With Third Parties

.19 The reauditor may consider responses to confirmation requests received by the predecessor auditor, provided the reauditor is able to obtain copies from the predecessor auditor. The responses may relate to, for example, cash, accounts receivable, debt and transactions with related parties. The reauditor should evaluate the process used by the predecessor auditor in controlling the confirmation process and in selecting the accounts/items for confirmation and the persons or entities for inquiry. The reauditor is responsible for conclusions as to the adequacy of the confirmation responses received by the predecessor auditor, including the number and quality of those replies, and for alternative procedures with respect to nonreplies. The reauditor should consider directly obtaining confirmation responses relating to significant matters.

.20 In those instances where the reauditor is not able to obtain copies of confirmation requests from the predecessor auditor or when the reauditor concludes that additional evidence is required, the reauditor should: 1) reconfirm the amounts/terms of balances and transactions as of the balance sheet date, or 2) confirm at a date subsequent to the period of the reaudit, in connection with a current audit or otherwise, and apply appropriate tests of intervening transactions. The reauditor may consider these procedures to be more effective than obtaining copies of the confirmation requests from the predecessor auditor. In addition, the reauditor should perform appropriate

 Copyright © 2002, American Institute of Certified Public Accountants, Inc.

subsequent events procedures (e.g., inspection of subsequent payments on accounts receivable), which may provide additional evidence concerning certain assertions.

.21 If the substance of an inquiry to lawyers relates to a significant matter, the reauditor should obtain responses directly.

Opening Balances and Consistency of Application of Accounting Principles

.22 The reauditor obtains audit evidence concerning the impact of the opening balances on the financial statements being reaudited and the consistency of application of accounting principles from a variety of procedures. The reauditor may be able to obtain some evidence regarding opening balances and consistency of accounting principles by reading the audited financial statements for the prior period and the predecessor auditor's report thereon, and making inquiry and reviewing the audit documentation of the predecessor auditor.

.23 In performing these procedures, the reauditor should consider the independence and professional reputation of the predecessor auditor, and whether there are factors that preclude obtaining any evidence from reading the audited financial statements for the prior period and the predecessor auditor's report or reviewing the predecessor auditor's audit documentation. In addition, if, for any reason, the reauditor is not permitted to review the audit documentation of the predecessor auditor, the reauditor will not be able to obtain any evidence from reading the audited financial statements for the prior period and the predecessor auditor's report. Accordingly, the reauditor should perform appropriate alternative procedures with respect to the opening balances as of the beginning of the reaudit period and with respect to the consistency of accounting principles.

.24 The audit procedures performed on the reaudit period transactions may provide some audit evidence about the opening balances. For example, audit evidence gathered during the reaudit may provide some assurance about the existence and valuation of receivables and inventory recorded at the beginning of the year. Regardless of the procedures performed, the nature, timing and extent of such procedures are solely the responsibility of the reauditor.

Uncorrected Financial Statement Misstatements

.25 The reauditor should evaluate the treatment and effects of uncorrected financial statement misstatements on both opening and closing balances of the period under reaudit. With respect to uncorrected misstatements that were identified by the predecessor auditor, the predecessor auditor and the reauditor may have different methods of evaluating uncorrected misstatements and may come to different conclusions with respect to their effects on the financial statements taken as a whole; accordingly, the reauditor cannot be held to any decisions of the entity and the predecessor auditor regarding the materiality of uncorrected misstatements or their disposition. In evaluating the effects of any uncorrected misstatements, irrespective of whether identified by the predecessor auditor or by the reauditor during the reaudit, including those that exist at the beginning and end of the period under reaudit, the reauditor alone is responsible for obtaining sufficient evidential matter to support his or her conclusion that the financial statements are free of material misstatement.

Representation Letters

.26 Practical difficulties may arise in obtaining a representation letter with respect to a reaudit engagement. In some situations, a different management team is in place currently than during the original audit period. Current management may believe that it bears no responsibility for financial statements developed by prior management and may resist a request for their signatures on the representation letter. This situation does not alleviate the need for obtaining an appropriately signed representation letter from current management for all periods being reported on.

.27 The reauditor is advised to discuss the requirement for a signed representation letter early in the process to make sure that appropriate officials are aware of their responsibility for the audited financial statements and the efforts they must undertake to be able to provide the representations to the reauditor. If the reauditor is unable to obtain the written representations that he or she deems necessary from current management for all periods being reported on, a scope limitation exists.

Reporting Implications

.28 The reauditor should not issue a report that reflects divided responsibility as described in SAS No. 1, section 543 unless in connection with the reaudit, the reauditor has informed the predecessor auditor that he or she will rely on, and where applicable, refer to, the predecessor auditor's report on certain subsidiaries or divisions.

.29 In some circumstances, the reauditor may not be able to complete a reaudit. For example, during a current period audit, the reauditor may conclude that controls are insufficient to allow the reauditor to rely on the types of procedures available to evaluate accounts such as inventory. If the reauditor is unable to obtain sufficient competent evidential matter to express an opinion on the financial statements, the reauditor qualifies the opinion or disclaims an opinion because of the inability to perform procedures the reauditor considers necessary in the circumstances. The SEC does not generally accept such reports. In such situations, the reauditor may elect to resign from the engagement.

Other Audit Issues

.30 Because the reaudit report is dated as of the date that the reauditor completes fieldwork, subsequent events procedures are to be performed through that date. Subsequent events are disclosed in the reaudited financial statements if their disclosure is required to keep the financial statements from being misleading.

.31 The reauditor's consideration of the entity's ability to continue as a going concern for a reasonable period of time takes into consideration the reauditor's knowledge of relevant conditions and events that exist or have occurred prior to completion of the reaudit fieldwork. The reauditor should consider whether the financial statements adequately disclose such conditions and events, other conditions and events occurring subsequent to the balance sheet date, their possible effects, and any mitigating factors, including management's plans. If the reauditor concludes that substantial doubt remains about the entity's ability to continue as a going concern, the audit report should include an explanatory paragraph reflecting that conclusion.

 Copyright © 2002, American Institute of Certified Public Accountants, Inc.

Internal Inspection

.32 It is important that a firm monitor its reaudits to determine whether the engagements are being performed in accordance with generally accepted auditing standards and the firm's system of quality controls. Accordingly, a firm's internal inspection program should consider addressing the firm's reaudit engagements, including engagement acceptance procedures.

[The next page is 51,091.]

Section 16,240

Practice Alert 03-1
Audit Confirmations

January, 2003

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits and is based on existing professional literature, the experience of members of the Professional Issues Task Force (PITF) and information provided by the SEC Practice Section member firms to their own professional staff. This information represents the views of the members of the PITF and has not been approved by any senior technical committee of the AICPA. The auditing portion of this publication is an *Other Auditing Publication* as defined in Statement on Auditing Standards (SAS) No. 95, *Generally Accepted Auditing Standards*. Other Auditing Publications have no authoritative status; however, they may help the auditor understand and apply SASs. If an auditor applies the auditing guidance included in an Other Auditing Publication, he or she should be satisfied that, in his or her judgment, it is both appropriate and relevant to the circumstances of his or her audit. This publication was reviewed by the AICPA Audit and Attest Standards staff and published by the AICPA, and is presumed to be appropriate.

Introduction

.01 SAS No. 67, *The Confirmation Process*, provides guidance to auditors about obtaining evidence from third parties about financial statement assertions made by management. SAS No. 31, *Evidential Matter*, states that it is generally presumed that evidential matter obtained from independent sources outside an entity provides greater assurance of reliability than evidence secured solely within the entity.

.02 The purpose of this practice alert is to communicate additional guidance to practitioners with respect to the use of audit confirmations.

General Confirmation Guidance

.03 Audit confirmations can prove to be an effective audit procedure with respect to many different accounts, including accounts receivable, notes receivable, inventory, consigned merchandise, construction and production contracts, investment securities, market values, accounts payable, notes payable, lines of credit, account balances and other information from financial institutions, and other actual and contingent liabilities. In addition, confirmations can be used to obtain audit evidence with respect to related parties and unusual transactions.

Improving Confirmation Response Rates

.04 The effectiveness of the confirmation procedure is influenced by both the willingness and the ability of the respondents to respond accurately to the

information presented on the confirmation. To improve the confirmation response rates, the auditor should request information that the recipient is likely and able to confirm. The confirmation request should include relevant information required for a response by the recipient. For example, with respect to accounts receivable confirmations, recipients may be more likely to reply and identify discrepancies if the confirmation request is sent with their monthly statement. The auditor may also consider attaching a list of outstanding invoices and unapplied credits making up the account balance to the confirmation request. In addition, when the verification of an account balance is difficult or complex, the auditor may ask the recipient to confirm supporting information from which the auditor can later compute the ending account balance. For example, instead of asking an individual to confirm a mortgage balance that includes a complex interest calculation, the auditor could request confirmation of the original balance, interest rate, number of installments and the date the last installment was paid.

.05 In some cases, the effectiveness of the confirmation is improved by not providing relevant information with the request, but rather by asking the respondent to indicate his or her understanding of the information (an "open" confirmation). This may be particularly appropriate when seeking confirmation of terms of a transaction, rather than amounts.

.06 The following techniques may be used by the auditor to improve the confirmation response rate:

- Use clear wording.
- Send the confirmation to a specified individual.
- Identify the organization being audited.
- Consider requesting the client to hand-sign the confirmation requests. Hand signing a confirmation may increase the confirmation rate when the signature on the confirmation is familiar to the recipient.
- Set response deadlines.
- Send second and consider third requests.
- Call the respondent to obtain oral confirmation and request that the written confirmation be returned.

Negative vs. Positive Confirmation Requests

.07 In designing the confirmation request, the auditor should consider the assertions being addressed and the factors that affect the reliability of the evidence obtained through confirmation procedures. One factor to consider is the form of the request—that is, a positive or negative request. A positive confirmation request is one in which the recipient is asked to respond directly to the auditor as to whether he or she agrees with the information presented. The positive form provides evidential matter that is inherently more reliable than negative confirmations. However, the positive form only provides audit evidence if responses are received directly from the recipients.

.08 Recipients of negative confirmation requests are asked to respond only if they disagree with the information presented. The auditor places reliance on the absence of any reply to a specific request by implicitly making the assumption that the customer received the confirmation request and agreed with the information shown. SAS No. 67, paragraph 20, states that negative confirmation requests may be used to reduce audit risk to an acceptable level when all of the following conditions are met:

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- The combined assessed level of inherent and control risk is low,
- A large number of small balances is involved, and
- The auditor has no reason to believe that recipients of the requests are unlikely to give them consideration. (For example, the auditor may become satisfied that recipients are not unlikely to give adequate consideration by considering the results of positive confirmation procedures performed in prior years on the engagement or on similar engagements.)

.09 The auditor should consider performing other substantive procedures to supplement the use of negative confirmations. In addition, the auditor should investigate and determine the effects on the audit of relevant information provided in responses to negative confirmations. Additionally, the auditor can send some positive confirmation requests as well as the negative requests. When only negative confirmations are used, auditors generally should send more confirmation requests than that which would have been sent if positive confirmations had been used.

Nonresponses to Positive Confirmations

.10 The auditor should seek corroborative evidence that customers for which positive confirmation requests are returned undelivered do exist. The auditor ordinarily sends second, and sometimes third, requests in the event of a non-response. Those subsequent requests may be either oral or written, given consideration for such factors as timing. In any event, the auditor should take appropriate follow-up actions with respect to all non-responding requests (see "Alternative Procedures" below). Also, customers who do not reply and confirmation requests returned undelivered should normally be reported to a client official who is not directly involved in the area subject to confirmation.

Responses to Positive Confirmation Requests Indicating Exceptions

.11 An exception to a positive confirmation request occurs when the respondent disagrees with, questions, or otherwise provides information that is different from the information presented. All exceptions should be thoroughly investigated.

.12 If an exception cannot be resolved or follow-up procedures indicate that the exception represents a misstatement, the auditor should: (1) determine the cause of the misstatement, (2) extrapolate the misstatement (together with other misstatements included in the same sampling application, if applicable) over the population to determine whether additional audit evidence is required to reduce the risk of material misstatement to an appropriately low level, and (3) consider whether the potential exists that fraud may have occurred (see SAS No. 99, *Consideration of Fraud in a Financial Statement Audit*). If similar misstatements could exist, additional audit procedures would generally be necessary to determine the extent of possible misstatements and their effect on the achievement of confirmation audit objectives. In the case of fraud, an extensive investigation may be necessary before such determination could be made. All unreconciled misstatements should normally be reported to a client official not directly associated with the accounts or other information subject to the request for confirmation. The auditor also should consider whether responses indicate matters that should be reported to the audit committee.

Confirmations Received Via Fax or Electronically

.13 The auditor should communicate directly with the intended recipients. In order to validate confirmations received via fax or electronically, the auditor should consider (*a*) verifying by telephone with the purported sender the source and contents of a response received by fax or e-mail and (*b*) asking the sender to mail the original confirmation directly to the auditor. All procedures performed and conclusions reached should be documented in the audit workpapers.

Management Requests to Not Confirm

.14 When management requests that the auditor not confirm certain balances or other information, the auditor should consider the basis for the request. A common reason that a client provides for requesting that the auditor not confirm a balance or other information is some type of dispute between the client and the customer. The existence of a dispute, by itself, is not an appropriate reason for not confirming a balance or other information. The auditor should be alert to the risk that an assertion of a "dispute" may be intended to divert the auditor from an inappropriate transaction.

.15 The auditor should very carefully consider the reasons that management is making the request to not confirm and should challenge those reasons and seek corroborating evidence. The auditor should not just rely on a management representation as to the reason. If the auditor accepts the validity of management's request not to seek external confirmation regarding a particular matter, alternative procedures should be applied to obtain sufficient appropriate evidence regarding the matter that would have been the subject of the confirmation.

.16 If management requests the auditor to not confirm certain accounts or other information, the auditor should consider including a schedule of such accounts, including the reasons for the request not to confirm, in the client representation letter.

.17 If the auditor deems management's request to be reasonable and is able to satisfy him/herself by applying alternative procedures, there is no limitation on the scope of the work and the auditor's report need not include a reference to the omission of procedures or to the use of alternative procedures. If management's request is not deemed reasonable and the restrictions significantly limit the scope of the audit, ordinarily the auditor should disclaim an opinion, or withdraw from the engagement. In those situations, the auditor may wish to consult his or her legal counsel.

Alternative Procedures

.18 After the auditor has decided to obtain a confirmation about an account or transaction, or an event or other matter, the item should be either confirmed or subjected to alternative procedures. The auditor should perform appropriate alternative procedures for all non-responses to positive confirmations, positive or negative confirmations that were returned undelivered and accounts that were selected but not confirmed at the client's request.

.19 Paragraph 31 of SAS No. 67 provides for the omission of alternative procedures to non-responding positive confirmations, in limited circumstances, if both of the following conditions are present:

- The auditor has not identified any unusual qualitative factors or systematic characteristics related to the non-responses.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- When testing for overstatement of amounts, the non-responses in the aggregate, when projected as 100% misstatements to the population and added to the sum of all other unadjusted differences, would not affect the auditor's decision about whether the financial statements are materially misstated.

.20 However, the auditor should use caution in deciding not to perform alternative procedures, since unusual factors or systemic characteristics may not be evident and, even with projection of the items as misstatements, underlying causes that might indicate other misstatements would not be identified.

.21 Examples of alternative procedures include examining cash receipt records, remittance advices or other evidence of subsequent collection, shipping records, evidence of receipt of goods by the customer, invoices, customer correspondence, etc. The nature and extent of the procedures selected will depend on the assessed risk of material misstatement, the nature of the account balance or other information the auditor attempted to confirm, and the availability of audit evidence. Since evidence obtained through confirmation often is more persuasive than internal evidence, the auditor may need to perform a combination of alternative procedures in order to reduce audit risk to the intended level. The risk of misstatement should be considered in deciding the nature and extent of such procedures. The auditor should keep in mind the various possibilities as to why no response was received, including the possibility of fraud.

Use of Client Personnel

.22 The auditor should maintain control over the confirmation process—from the preparation of the confirmation request, through the mailing of the confirmation requests, to the receipt of the responses. However, in order to increase audit efficiency, client personnel can be utilized to facilitate the auditor's examination of differences and non-responses by:

- Listing and accumulating data.
- Reconciling book and reported amounts for the auditor's follow-up and examination.
- Accumulating documents for the auditor's inspection.

.23 Client personnel may investigate exceptions if the auditor supervises the activity and subsequently inspects, at least on a test basis, the evidence supporting the client's explanation of differences. The auditor should maintain control over the confirmations by maintaining the original confirmation reply and providing the client personnel with a copy or other record of the reply.

Confirmation Guidance With Respect to Specific Areas

.24 The following is intended to provide guidance and best practices with respect to the confirmation of specific financial statement accounts and other information:

Confirmation of Accounts Receivable

.25 Extensive guidance with respect to the confirmation of accounts receivable is provided in the AICPA Auditing Procedures Study, *Confirmation of Accounts Receivable*. Paragraph 34 of SAS No. 67 states the following:

Confirmation of accounts receivable is a generally accepted auditing procedure. . . Thus, there is a presumption that the auditor will request the confirmation of accounts receivable during an audit unless one of the following is true:

- Accounts receivable are immaterial to the financial statements.
- The use of confirmations would be ineffective.
- The auditor's combined assessed level of inherent and control risk is low, and the assessed level, in conjunction with the evidence expected to be provided by analytical procedures or other substantive tests of details, is sufficient to reduce audit risk to an acceptably low level for the applicable financial statement assertions. . .

.26 For the purposes of this requirement, "accounts receivable" is defined to include:

- Claims against customers that have arisen from the sale of goods or services in the normal course of business, and
- A financial institution's loans.

.27 Paragraph 34 of SAS No. 67 states that confirmation of accounts receivable is a generally accepted auditing procedure and establishes a presumption that must be overcome. As a presumption, it is not sufficient to merely assert that, for example, the use of confirmations would be ineffective. Rather it is necessary to provide evidence sufficient to overcome the presumption. A decision not to confirm accounts receivable must be documented. This documentation should include a thorough assessment of the reasons underlying that conclusion, and should make a compelling case that use of confirmations would truly be ineffective (if that is the reason) and not merely inconvenient.

.28 Paragraph 34 of SAS No. 67 states that the use of confirmations would be ineffective if, for example, "based on prior years' audit experience or on experience with similar engagements, the auditor concludes that response rates to properly designed confirmation requests will be inadequate, or if responses are known or expected to be unreliable." Additionally, the use of confirmations may not be effective because the federal government and certain companies may have a policy of not responding to confirmation requests. However, auditors should not opt out of confirming accounts receivable simply because it may be difficult to obtain the confirmation, without carefully considering ways to improve the effectiveness of the confirmation process.

.29 In addition, when confirmation procedures are not used because the auditor has concluded they would be ineffective, the auditor should consider whether to modify the nature or extent of alternative procedures by applying a combination of procedures or applying the procedures to a larger number of items than would have been confirmed. The auditor should consider that certain alternative procedures might be more difficult to perform if the entity utilizes electronic systems extensively and copies of shipping documents and other sources of audit evidence are not retrievable.

Confirmation of Terms of Unusual or Complex Agreements or Transactions

.30 The auditor should normally confirm the terms of unusual or complex agreements or transactions. This can be done in conjunction with the confirmation of account balances or separately. As the details of the matters may not be

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

known to the customer's lower-level accounting personnel, the confirmation may need to be addressed to customer personnel who would be familiar with the details. Such personnel may include executives in the company's sales department, the chief financial officer, the chief operating officer or the chief executive officer. Software companies, for example, present significant risks related to revenue recognition due to the complexity of revenue recognition methods and the risk of management override of controls over software sales contracts.

.31 SAS No. 99 states that the auditor should ordinarily presume that there is a risk of material misstatement due to fraud relating to revenue recognition. Therefore, the auditor should carefully evaluate the appropriateness of the client's accounting for revenue transactions and generally confirm the terms of transactions and the absence of any side agreements. The necessity of confirming terms of transactions and the absence of side agreements increases if the auditor encounters any of the following characteristics:

- Significant sales or volume of sales at or near the end of the reporting period.
- Use of non-standard contracts or contract clauses.
- Use of letters of authorization in lieu of signed contracts or agreements.
- Altered dates on contracts or shipping documents. The auditor should consider the possibility of fraud.
- Concurrent agreements or "linked" contracts and transactions.
- Lack of evidence of customer acceptance.
- Existence of bill-and-hold transactions.
- Existence of extended payment terms or non-standard installment receivables.
- Accounting/finance department's lack of involvement in sales transactions or in the monitoring of arrangements with distributors.
- Unusual volume of sales to distributors/retailers.
- Sales, other than sales of software, with commitments for future upgrades.
- Sales where significant uncertainties and/or obligations to the seller exist.
- Sales to value-added-resellers and distributors lacking financial strength.
- Increasing receivables from a customer, which may be an indicator of the customers' perceptions of the payment terms (e.g. payments not due until resale to end users).
- Aggressive accounting policies or practices (e.g. tone at the top regarding pressures for revenue and earnings).

Confirmation of Accounts Payable

.32 Confirmation with major suppliers, including those with small or zero balances, can substantially contribute to establishing the existence and completeness of accounts payable. In addition, confirmation of accounts payable

can prove to be an effective procedure in the detection of "round-trip" or "linked" transactions. "Roundtrip" or "linked" transactions occur when a company enters into a seemingly valid sales transaction with a customer but sends all or some of the sales proceeds back to the customer in another seemingly valid purchase transaction, often affecting a different accounting period. These types of transactions occur frequently in industries where analysts have focused on the revenue that companies display on financial statements instead of on income. For those companies in which round-tripping has been identified as a risk, the auditor should consider confirming balances for those major customers and/or suppliers in which the company both received revenue and made purchases during the year.

.33 Situations that may call for the confirmation of accounts payable include:

- Situations where client controls over payables and cash disbursements are poor or uncertain creating a greater risk of unprocessed and unrecorded vendor invoices.
- Situations where industry practices may create a higher risk of unrecorded liabilities and/or inappropriate accounting, e.g. internet entities, software companies, real estate, energy, telecommunications.
- Complex business transactions that create an environment where unrecorded accounts might exist, e.g. business combinations, royalty deals, etc.

.34 In confirming accounts payable, auditors generally use a blank request form in which the respondent is requested to fill in the missing information. This provides a more effective test for unrecorded liabilities. In addition, the auditor may find it effective to request that the respondent provide a detailed listing of the payable balance and ask for information about quid pro quo transactions (i.e. transactions resulting in an equal exchange), if any, and the related details. To obtain the intended degree of assurance from confirmation of suppliers, the following procedures should be considered:

- Review accounts payable subsidiary (purchase) ledger, suppliers' invoice files, disbursement records or purchase volume records by supplier, and inquire of client's personnel responsible for purchasing to identify and list major suppliers. It is usually efficient to maintain and annually update a carryforward list of major suppliers in the permanent file.
- Identify other suppliers from which confirmation of the accounts payable balance is desired. Consider advertising and other major suppliers of services, construction contractors, equipment suppliers, suppliers with known or suspected disputed balances, etc.

.35 When statements are not available from suppliers who did not reply to the confirmation requests and from suppliers with unusually large or, more importantly, unusually small balances who were not included with the suppliers subject to confirmation, the auditor should consider examining documentary evidence supporting payments made to those suppliers subsequent to the confirmation date to identify items that should have been accrued as payable at the confirmation date but were not.

Confirmations of Related Party Transactions

.36 The auditor should be cognizant of the fraud risks involved in transactions involving related parties and special purpose entities. In all financial

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

statement audits, the auditor should perform procedures to identify parties that are related to the entity being audited and to understand the relationship between the identified parties. Additionally, the auditor should gain an understanding of the business rationale for significant related party transactions. In order to fully understand a particular transaction, the auditor should consider confirming the transaction amount(s) and terms, including guarantees and other significant data, with the other parties to the transaction. In addition, the auditor should consider confirming significant information with intermediaries, such as banks, guarantors, agents or attorneys. Since it is possible for management to be on both sides of the transaction, more reliable audit evidence may come from the intermediaries. The auditor may be able to identify related parties through the confirmation of unusual transactions.

Evolving Alternatives to Confirmation

.37 An auditor is sometimes able to directly access information held by a third party concerning a client's account balance. For example, using the client's personal identification number, an auditor may be able to make an on-line inquiry about a client's bank balance information. While such procedures may provide competent evidence concerning that information, it does not meet the definition of confirmation. Paragraph 4 of SAS No. 67 states that confirmation is the process of obtaining and evaluating a direct communication from a third party in response to a request for a particular item affecting financial statement assertions. A direct confirmation from a third party in response to a request for information requires an active response from the third party. Accordingly, an on-line inquiry of the third party's database does not constitute a response and instead constitutes an alternative procedure. Such a procedure does not fulfill the auditor's confirmation responsibilities under generally accepted auditing standards.

[The next page is 51,111.]

Section 16,250

Practice Alert 03-2
Journal Entries and Other Adjustments

June, 2003

NOTICE TO READERS

This Practice Alert is intended to provide auditors with information that may help them improve the efficiency and effectiveness of their audits and is based on existing professional literature, the experience of members of the Professional Issues Task Force (PITF) and information provided by the SEC Practice Section member firms to their own professional staff. This information represents the views of the members of the PITF and has not been approved by any senior technical committee of the AICPA. The auditing portion of this publication is an Other Auditing Publication as defined in Statement on Auditing Standards (SAS) No. 95, *Generally Accepted Auditing Standards*. Other Auditing Publications have no authoritative status; however, they may help the auditor understand and apply Statements on Auditing Standards (SASs). If an auditor applies the auditing guidance included in an Other Auditing Publication, he or she should be satisfied that, in his or her judgment, it is both appropriate and relevant to the circumstances of his or her audit. This publication was reviewed by the AICPA Audit and Attest Standards staff and published by the AICPA, and is presumed to be appropriate.

Introduction

.01 The Auditing Standards Board has promulgated standards that address an auditor's understanding and evaluation of journal entries and other adjustments. For example, in SAS No. 94, *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit*, the Auditing Standards Board expanded the auditor's required understanding of the automated and manual procedures an entity uses to prepare its financial statements and related disclosures to include procedures an entity uses to (*a*) enter transaction totals into the general ledger, (*b*) initiate, record and process journal entries in the general ledger, and (*c*) record recurring and nonrecurring adjustments, such as consolidating adjustments, report combinations and reclassifications, that are not reflected in formal journal entries.

.02 In addition, SAS No. 99, *Consideration of Fraud in a Financial Statement Audit*, states, "Material misstatements of financial statements due to fraud often involve the manipulation of the financial reporting by (*a*) recording inappropriate or unauthorized journal entries throughout the year or at period end, or (*b*) making adjustments to amounts reported in the financial statements that are not reflected in formal journal entries, such as through consolidating adjustments, report combinations, and reclassifications. Accordingly, the auditor should design procedures to test the appropriateness of journal entries recorded in the general ledger and other adjustments (for example, entries posted directly to financial statement drafts) made in the preparation of the financial statements."

.03 SAS No. 99 further states, "Standard journal entries used on a recurring basis to record transactions such as monthly sales, purchases, and cash

disbursements, or to record recurring periodic accounting estimates generally are subject to the entity's internal controls. Nonstandard entries (for example, entries used to record nonrecurring transactions, such as a business combination, or entries used to record a nonrecurring estimate, such as an asset impairment) might not be subject to the same level of internal control. In addition, other adjustments, report combinations, and reclassifications generally are not reflected in formal journal entries and might not be subject to the entity's internal controls. Accordingly, the auditor should consider placing additional emphasis on identifying and testing items processed outside of the normal course of business."

.04 In response to the risk of management override, SAS No. 99, which will be effective for audits of calendar year 2003 financial statements, requires the auditor, in all audits, to (*a*) obtain an understanding of the entity's financial reporting process and controls over journal entries and other adjustments, (*b*) identify and select journal entries and other adjustments for testing, (*c*) determine the timing of the testing, and (*d*) inquire of individuals involved in the financial reporting process about inappropriate or unusual activity relating to the processing of journal entries or other adjustments.

.05 The purpose of this Practice Alert is to provide auditors with guidance regarding the design and performance of audit procedures to fulfill the responsibilities outlined in SAS No. 99 regarding journal entries and other adjustments.

Obtaining an Understanding of the Entity's Financial Reporting Process and Its Controls Over Journal Entries and Other Adjustments

.06 SAS No. 99 states, "An entity may have implemented specific controls over journal entries and other adjustments. For example, an entity may use journal entries that are preformatted with account numbers and specific user approval criteria, and may have automated controls to generate an exception report for any entries that were unsuccessfully proposed for recording or entries that were recorded and processed outside of established parameters. The auditor should obtain an understanding of the design of such controls over journal entries and other adjustments and determine whether they are suitably designed and have been placed in operation."

.07 An entity's financial reporting system also includes the use of nonstandard journal entries to record nonrecurring or unusual transactions or adjustments such as business combinations, or a nonrecurring estimate such as an asset impairment. Additionally, nonstandard entries include consolidation entries, reclassification entries, and spreadsheet or other worksheet adjustments. Because of the risk of misstatements (intentional or unintentional) oftentimes linked to nonstandard journal entries and other adjustments, the engagement team needs to obtain a thorough understanding of the entity's controls surrounding this aspect of the financial reporting process.

.08 Obtaining an understanding of the entity's financial reporting process helps the auditor to identify important information such as:

- The entity's written and unwritten policies and procedures regarding the initiation, recording and processing of standard and nonstandard journal entries and other adjustments;
- The sources of significant debits and credits to an account;
- Individuals responsible for initiating entries to the general ledger, transaction processing systems, or consolidation;

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- Approvals and reviews required for such entries and other adjustments;
- The mechanics for recording journal entries and other adjustments (for example, whether entries are initiated and recorded online with no physical evidence, or created in paper form and entered in batch mode);
- Controls, if any, designed to prevent and detect fictitious entries and unauthorized changes to journals and ledgers; and
- Controls over the integrity of the process used to generate reports used by the auditors.

Assessing the Risk of Material Misstatement Resulting From Journal Entries and Other Adjustments

.09 Although SAS No. 99 requires the auditor to test journal entries and other adjustments regardless of the risk assessment, the nature, timing, extent and focus of the testing will be influenced by the auditor's risk assessments. The auditor should assess the nature and risk of management's incentive to manipulate earnings or financial ratios through financial statement misstatement. That assessment should be made in conjunction with the interim reviews as well as the year-end audit. For example, if a client has loan covenant ratios that depend on earnings, and net income is close to causing covenant violations, then the auditor may assess the risk of material misstatement as higher. The auditor may also assess the risk of material misstatement as higher when executive compensation is tied to earnings thresholds and earnings are close to the threshold. Additionally, market expectations in many cases have led to earnings manipulations. In those cases where the auditor determines that the risk of fraudulent journal entries is high due to questions regarding the integrity of management, the auditor should reassess his or her client acceptance/continuance decision.

.10 SAS No. 99 states, "Members of the audit team should discuss the potential for material misstatement due to fraud. The discussion should include an exchange of ideas or "brainstorming" among the audit team members, including the auditor with final responsibility for the audit, about how and where they believe the entity's financial statements might be susceptible to material misstatement due to fraud, how management could perpetrate and conceal fraudulent financial reporting, and how assets of the entity could be misappropriated."

.11 Journal entries and other adjustments oftentimes exist only in electronic form, which requires extraction of the desired data by an auditor with information technology (IT) knowledge and skills or the use of an IT specialist. In audits of entities with complex IT systems, the IT auditors and/or IT specialists should be included in the brainstorming session. In the brainstorming session, the auditors normally will discuss the following:

- The various ways in which management could originate and post inappropriate journal entries or other adjustments.
- The kinds of unusual combinations of debits and credits that the engagement team should be looking for.
- The types of journal entries or other adjustments that could result in a material misstatement that would not likely be detected by standard audit procedures.

Inquiries of Individuals Involved in the Financial Reporting Process

.12 SAS No. 99, paragraph 24, states, "The auditor should inquire of others within the entity about the existence or suspicion of fraud. The auditor should use professional judgment to determine those others within the entity to whom inquiries should be directed and the extent of such inquiries. In making this determination, the auditor should consider whether others within the entity may be able to provide information that will be helpful to the auditor in identifying risks of material misstatement due to fraud—for example, others who may have additional knowledge about or be able to corroborate risks of fraud identified in the discussions with management . . . or the audit committee." Where practical, regardless of the fraud risk assessment, the auditor should inquire of the entity's accounting and data entry personnel about whether those individuals were requested to make unusual entries during the audit period. The auditor should also consider asking selected programmers and IT staff about the existence of unusual and/or unsupported entries and specifically inquire about these entries, including whether any were initiated directly by top management outside the normal accounting process. The auditor should not expect client personnel to volunteer information about known or suspected fraud. However, those same individuals may be more likely to provide information if asked directly.

Assessment of Completeness of Journal Entry and Other Adjustments Sources

.13 It is important in testing journal entries and other adjustments that the auditor be aware of and consider the entire population of journal entries and other adjustments. The auditor's ability to detect fraud is adversely affected if he or she is not assured of access to all of the journal entries posted and other adjustments made during the audit period. The auditor should be aware that journal entries and other adjustments may be made outside of the general ledger and should obtain a complete understanding as to how the various general ledgers are combined and the accounts are grouped to create the consolidated financial statements. For example, at large, multi-national companies, multiple general ledgers are utilized, adjustments are made to convert from local GAAP to U.S. GAAP, and translation and other adjustments are made before the numbers are combined (perhaps at more than one level of sub-consolidation) and become subject to further elimination and adjusting entries. Appropriate procedures should be applied to all of the various sources of information from which journal entries and other adjustments are selected for testing to assist the auditor in assessing completeness. The nature and extent of these procedures will depend on the engagement risk assessments and the client's systems for recording transactions.

Identification and Selection of Journal Entries and Other Adjustments for Testing

.14 After the auditor has made his or her assessment of the risk of fraudulent journal entries and other adjustments and has performed appropriate procedures to assess completeness, he or she should design procedures, based on that assessment, to test the appropriateness of the journal entries and other

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

adjustments from the various sources previously identified including (*a*) journal entries recorded in the general ledger, and (*b*) top side consolidation or report entries that are not actually posted to the general ledger. The auditor should test the appropriateness of selected journal entries and other adjustments in all engagements—including those in which the risk of fraudulent journal entries is assessed as low. Those tests are performed to confirm that entries are appropriately approved by management, are adequately supported and reflect the underlying events and transactions. Such tests should be designed to detect inappropriate entries.

.15 After considering the identified population of journal entries and other adjustments, the auditor should use professional judgment to determine the nature, timing and extent of the testing of journal entries and other adjustments. SAS No. 99 requires that the auditor consider:

- The auditor's assessment of the risk of material misstatement due to fraud.
- The effectiveness of controls that have been implemented over journal entries and other adjustments.
- The entity's financial reporting process and the nature of the evidence that can be examined.
- The characteristics of fraudulent entries or adjustments.
- The nature and complexity of the accounts.
- Journal entries or other adjustments processed outside the normal course of business.

.16 For many entities, routine processing of transactions involves a combination of manual and automated steps and procedures. Similarly, the processing of journal entries and other adjustments might involve both manual and automated procedures and controls. Regardless of the method, the auditor's procedures should include selecting, from the various sources of information from which journal entries and other adjustments are posted, specific entries and other adjustments to be tested and examining the support for those items. In addition, the auditor should be aware that journal entries and other adjustments might exist in either electronic or paper form. In an IT environment, it may be necessary for the auditor to employ computer-assisted audit techniques ("CAATs") (for example, report writers, software or data extraction tools, or other systems based techniques) to identify the journal entries and other adjustments to be tested. In addition, the CAATs ordinarily are designed to detect the following:

- Entries made at unusual times of day, that is, outside regular business hours.
- Entries made by unusual users, blank or nonsensical user names, senior management, or the IT staff.
- Electronic entries that, through management manipulation, are not documented in the general ledger.

.17 Additionally, it is normally beneficial if the CAATs filter out recurring transactions in order to identify nonrecurring transactions and foot the detail in accounting records. The CAATs should be designed specifically to assist in evaluating whether all journal entries and other adjustments are included in the population to be reviewed. Firms utilizing internal IT specialists to perform the CAATs should invest appropriate resources in training to ensure that the IT specialists are able to competently perform the procedures and understand the importance of detecting any inappropriate journal entries or other adjustments.

.18 Characteristics of fraudulent journal entries may include entries (*a*) made to unrelated, unusual, or seldom-used accounts, (*b*) made by individuals who typically do not make journal entries, (*c*) recorded at the end of the period or as post-closing entries that have little or no explanation or description, (*d*) made either before or during the preparation of the financial statements that do not have account numbers, or (*e*) containing round numbers or a consistent ending number. The auditor should look for unusual entries during both the year-end and quarter-end cut-off procedures. Additionally, any entries that were reversed at the beginning of the subsequent period should be scrutinized more carefully. Also, the auditor ordinarily should consider looking for unusual entries that affect revenue.

.19 Inappropriate journal entries may be applied to accounts that (*a*) contain transactions that are complex or unusual in nature, (*b*) contain significant estimates and period-end adjustments, (*c*) have been prone to errors in the past, (*d*) have not been reconciled on a timely basis or contained unreconciled differences, (*e*) contain intercompany transactions, or (*f*) are otherwise associated with an identified risk of material misstatement due to fraud. The auditor should recognize, however, that inappropriate journal entries also might be made to other accounts.

.20 Several high profile cases that resulted in restatements and allegedly involved management fraud, purportedly extensively utilized inappropriate journal entries and other adjustments. In many of those instances, management accomplished the fraud by posting numerous improper journal entries in relatively small amounts, which impacted large balance sheet and income statement accounts thereby not resulting in a significant fluctuation being identified through analytical procedures. The affected accounts included receivables, inventory, fixed assets, accumulated depreciation, goodwill, prepaid expenses and operating expenses, among others. If management is committed to creating fraudulent financial statements it can design journal entries to, among other things:

- Mask the diversion of funds.
- Record topside adjustments that improperly increase revenue.
- Improperly adjust segment reporting.
- Improperly reverse purchase accounting reserves.
- Improperly write-off uncollectible accounts receivable to purchase accounting reserve accounts and intercompany accounts thereby not reducing income.
- Understate payables through the recording of post-closing journal entries to increase various revenue accounts.
- Improperly decrease accounts payable and general and administrative expenses.
- Improperly capitalize costs as fixed assets or construction in progress instead of expensing those costs as incurred.
- Improperly record adjustments to allowances.

.21 In audits of entities that have several locations or components, the auditor should consider the need to select journal entries from locations based on factors set forth in SAS 47, *Audit Risk and Materiality in Conducting an Audit* (AICPA *Professional Standards*, vol. 1, AU sec. 312.18). Those factors

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

include (*a*) the nature and amount of assets and transactions executed at the location or component, (*b*) the degree of centralization of records or information processing, (*c*) the effectiveness of the control environment, particularly with respect to management's direct control over the exercise of authority delegated to others and its ability to effectively supervise activities at the location or component, (*d*) the frequency, timing, and scope of monitoring activities by the entity or others at the location or component, and (*e*) judgments about materiality of the location or component.

.22 After considering the factors outlined above, as well as the number and monetary amount of journal entries and other adjustments, the auditor should select journal entries and other adjustments from the population and examine documentary evidence indicating that the journal entries are properly supported and approved by management. The selections should include both journal entries recorded in the general ledger and top side or report adjustments that are not actually posted to the general ledger. Because fraudulent journal entries often are made at the end of a reporting period, the auditor's testing ordinarily should focus on the journal entries made at that time. However, because material misstatements in financial statements due to fraud can occur throughout the period and may involve extensive efforts to conceal how it is accomplished, the auditor should consider whether there is also a need to test journal entries throughout the period under audit. Additionally, if entries are used to correct errors in financial statements of a previous period, the auditor should evaluate whether those previously issued financial statements should be restated.

.23 The auditor should introduce an element of unpredictability regarding the dollar amount and types of journal entries and other adjustments tested. Often, companies are able to perpetrate fraud when, over a period covering several engagements, management is able to determine the auditor's scope and/or strategy and therefore design inappropriate journal entries and other adjustments that have a high probability of not being tested.

.24 SAS No. 100, *Interim Financial Information*, paragraph 23, states, "The accountant performing the review of interim financial information ordinarily will also be engaged to perform an audit of the annual financial statements of the entity. Certain auditing procedures may be performed concurrently with the review of interim financial information." SAS No. 100 is effective for interim periods with fiscal years beginning after December 15, 2002. As a matter of good practice, the auditor should consider auditing journal entries and other adjustments concurrently with the interim reviews. The auditor should especially focus on journal entries and other adjustments that were reversed at the beginning of the subsequent period.

Other Adjustments

.25 In many cases, entities utilize spreadsheets to group general ledger accounts and make consolidating adjustments, reclassifications and other adjustments to arrive at financial statement amounts. Those consolidating adjustments, report combinations and reclassifications that are not reflected in formal journal entries should also be tested based on the auditor's risk assessment. Tests of other adjustments would normally involve comparing the adjustments to underlying supporting information, and considering the rationale underlying the adjustment as well as the reason it was not reflected in a formal journal entry.

Documentation

.26 SAS No. 96, *Audit Documentation*, requires that audit documentation be sufficient to show that the accounting records agree or reconcile with the financial statements or other information being reported on. The results of procedures performed relative to the entity's journal entries and other adjustments should be documented in the appropriate section of the current audit file. This documentation should include:

- The procedures used by the engagement team to assess the completeness of the population of journal entries and other adjustments subject to review and testing.
- The journal entries and other adjustments that were selected for testing and the basis therefore.
- The procedures performed to audit the journal entries and other adjustments.
- The conclusions reached.
- Who performed and reviewed the work.

[The next page is 51,131.]

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Section 16,260

Practice Alert 03-3
Acceptance and Continuance of Clients and Engagements

December, 2003

NOTICE TO READERS

This Practice Alert is intended to provide practitioners with information that may help them improve the effectiveness and efficiency of their engagements and practices and is based on existing professional literature, the experience of members of the Professional Issues Task Force (PITF) and information provided by certain AICPA member firms to their own professional staff. This information represents the views of the members of the PITF and has not been approved by any senior technical committee of the AICPA. The auditing portion of this publication is an Other Auditing Publication as defined in Statement on Auditing Standards (SAS) No. 95, *Generally Accepted Auditing Standards*. Other Auditing Publications have no authoritative status; however, they may help the auditor understand and apply Statements on Auditing Standards (SASs). If an auditor applies the auditing guidance included in an Other Auditing Publication, the auditor should be satisfied that, in his or her judgment, it is both appropriate and relevant to the circumstances of the subject audit. This publication was reviewed by the AICPA Audit and Attest Standards staff and published by the AICPA, and is presumed to be appropriate.

Introduction

.01 AICPA Statement on Quality Control Standards (SQCS) No. 2, *System of Quality Control for a CPA Firm's Accounting and Auditing Practice*, which applies to all "audit, attest, accounting and review, and other services for which standards have been established by the AICPA Auditing Standards Board or the AICPA Accounting and Review Services Committee under rule 201 or 202 of the AICPA Code of Professional Conduct" states, in paragraphs 14 through 16:

> Policies and procedures should be established for deciding whether to accept or continue a client relationship and whether to perform a specific engagement for that client. Such policies and procedures should provide the firm with reasonable assurance that the likelihood of association with a client whose management lacks integrity is minimized. Establishing such policies and procedures does not imply that a firm vouches for the integrity or reliability of a client, nor does it imply that a firm has a duty to any person or entity but itself with respect to acceptance, rejection, or retention of clients. However, prudence suggests that a firm be selective in determining its client relationships and the professional services it provides.
>
> Such policies and procedures should also provide reasonable assurance that the firm:
>
> *a.* Undertakes only those engagements that the firm can reasonably expect to be completed with professional competence.

b. Appropriately considers the risks associated with providing professional services in the particular circumstances.

To minimize the risk of misunderstandings regarding the nature, scope, and limitations of the services to be performed, policies and procedures should provide for obtaining an understanding with the client regarding those services.

.02 The firm's client acceptance and continuance policies represent a key element in mitigating litigation and business risk. The firm must be aware that the integrity and reputation of a client's management could reflect on the reliability of the client's accounting records and financial representations, and therefore on the firm's reputation or involvement in litigation.

Acceptance of Clients and Engagements

.03 The firm should perform an evaluation of **all** potential new clients. The firm should strive to be associated with only those clients that have the following characteristics:

- Management possessing competence and integrity,
- A financial and accounting officer who is knowledgeable about the business and the decisions made by the top operating management,
- Management that is committed to the application of appropriate accounting principles,
- Appropriately comprehensive and sound internal controls that are consistent with the size and organizational structure of the business, and
- An appropriate corporate governance structure.

.04 The firm may also wish to consider the future business prospects of the prospective client including whether it has a viable business with good long-range prospects and is adequately financed.

.05 The firm should develop client acceptance procedures designed to identify and reject prospective clients of questionable reputation, and potential engagements that involve a high risk of litigation or regulatory investigations. The client acceptance procedures also should require the firm to consider its independence and ability to provide professional services, with reference to industry expertise, size of engagement, and personnel available to staff the engagement.

.06 As a best practice, for the higher risk audit clients, including all SEC audit clients, the appropriate level of firm management should review and approve all client acceptance decisions.

Continuance of Clients and Engagements

.07 Risks similar to those involved in new client acceptance pertain to the firm's continued association with certain existing clients.

.08 Each client for which the firm performs recurring attest engagements[1] should be evaluated annually to determine whether the firm should continue the relationship. The continuance assessments should be completed

[1] As defined in the AICPA *Code of Professional Conduct*, an attest engagement is one that requires independence under AICPA professional standards such as audits and reviews of financial statements or agreed-upon procedures performed under the attestation standards.

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

sufficiently in advance of engagement commencement so that identified risks and resulting actions can be included in engagement strategy and staffing plans or so that terminations can be initiated on a timely basis.

.09 If a significant change in management, directors, owners, or legal counsel; or a significant change in financial condition or the nature of the entity's business has occurred, the firm should determine whether to continue the client relationship.

.10 As a best practice, for the higher risk audit clients, including all SEC audit clients, the appropriate level of firm management should review and approve all client continuance decisions.

The Client Acceptance and Continuance Process

.11 In developing its client acceptance and continuance process, the firm should include procedures that include the following elements. Each of these elements is discussed in detail in this Practice Alert. Certain of these elements may not be applicable to the acceptance or continuance of a compilation or review engagement. Practitioners should exercise professional judgment in determining the applicability of each of the following to the acceptance or continuance of a specific engagement.

- Availability of competent personnel to perform the engagement
- Communication with predecessor accountants or auditors
- Assessment of management's commitment to the appropriate application of generally accepted accounting principles
- Assessment of management's commitment to implementing and maintaining effective internal control
- Assessment of the entity's financial viability
- Independence and objectivity
- Inquiry of third parties
- Background investigations
- Other considerations

Availability of Competent Personnel to Perform the Engagement

.12 In evaluating whether to accept or continue an accounting and auditing client relationship, the firm should determine whether competent personnel would be available to provide professional services to the client. In addition, the firm should consider how the addition of a prospective client would affect the firm's ability to staff its existing engagements requiring similar expertise. The firm should not undertake or continue a professional relationship unless the necessary technical and/or industry expertise are available to provide quality services, or the firm has a viable plan to develop the necessary expertise in time to provide quality services.

Communication With Predecessor Accountants or Auditors

.13 Before accepting an appointment as auditor, SAS No. 84, *Communications Between Predecessor and Successor Auditors*, requires that the firm

communicate with the predecessor auditors to ascertain whether there is any professional reason why the firm should not accept the engagement. As a best practice, the firm may extend this requirement to all potential accounting and auditing engagements. However, a successor accountant is not required to communicate with a predecessor accountant in connection with acceptance of a compilation or review engagement. In those cases where a firm is considering accepting an engagement to reaudit and report on financial statements that have been previously audited and reported on by another auditor, the firm should refer to the guidance in Practice Alert 02-3, *Reauditing Financial Statements* [section 16,230].

.14 A predecessor auditor is an auditor who (1) has reported on the most recent audited financial statements or was engaged to perform, but did not complete an audit of any subsequent financial statements, and (2) has resigned, declined to stand for reappointment, or been notified that his or her services have been, or may be, terminated. The SEC considers an auditor who is named as an "auditor of record" in a registrant's registration statement to be a predecessor auditor, regardless of whether the auditor rendered an auditor's report.

.15 Although efforts should be undertaken to hold discussions with the predecessor accountants before submitting a proposal, SAS No. 84 recognizes that practical, competitive factors may preclude this. For example:

- The present auditors are asked to repropose on the engagement, in a competitive situation.
- The firm is asked to submit a proposal without the present auditor's knowledge.

.16 Accordingly, the requirements of SAS No. 84 to make inquiry of the predecessor auditor do not become operative until the prior auditor-client relationship is terminated. If the firm is asked to submit a proposal in these circumstances, the firm should make it clear to the prospective client that, if the firm's proposal is accepted, the rules of the profession require the firm to communicate with the predecessor auditor before the firm can agree to accept the engagement. This requirement should be made clear during the proposal process.

.17 The firm's communication with the predecessor auditor should include all specific and reasonable inquiries that will assist the firm in determining whether to accept the client. Matters subject to inquiry of the predecessor auditors should include (1) information that might bear on the integrity of management; (2) disagreements with management as to accounting principles, auditing procedures, or other similarly significant matters; (3) communications with audit committees or others with equivalent authority and responsibility regarding fraud, illegal acts by clients, and internal-control related matters; and (4) the predecessor auditors' understanding as to the reasons for the change in auditors. The firm's inquiries should also cover other matters pertinent to its consideration of accepting the engagement such as adequacy of internal control; pending or threatened litigation or regulatory investigations; material contingencies or going concern considerations and; whether the predecessor auditor will be willing to reissue its report or otherwise provide a consent with respect to previously issued financial statements, if applicable. The successor auditor may receive limited responses from the predecessor auditor depending upon the circumstances surrounding the change in auditors.

.18 Usually only after the firm has accepted the engagement, should the firm make arrangements to review the predecessor's workpapers. That review should, however, occur prior to commencement of the engagement.

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

.19 If the prospective client is subject to SEC reporting requirements, as early as possible in the acceptance process, the firm should ascertain what the prospective client plans to report to the SEC on Form 8-K regarding the change in independent accountants and whether the replaced accountant agrees with the proposed content of the report. Furthermore, before formally accepting an engagement, the firm should obtain a copy of the company's Form 8-K as filed, together with the prior accountant's response, and determine whether the contents confirm the firm's previous understanding. The firm is deemed to have formally accepted an engagement when it either signs an initial engagement letter or other agreement to perform attest services or begins to perform an attest engagement for a client, whichever is earlier.

.20 In those situations where the prior period financial statements were audited by a predecessor auditor who has ceased operations, the firm's ability to perform the required communications with the predecessor auditor prior to accepting the engagement is challenged. However, the firm's obligations are not mitigated. If the audit firm is unable to communicate with the individual at the predecessor firm who had responsibility for the audit or receives a limited response, the firm should consider whether to accept the engagement. In some situations, the predecessor auditor might not be able to respond fully to the audit firm's inquiries, such as when the predecessor firm no longer employs the predecessor audit engagement partner or other senior members of the audit engagement team. The audit firm should make reasonable efforts to locate the predecessor audit engagement partner or other senior members of the predecessor engagement team and make appropriate inquiries. In some cases, another accounting firm may employ the engagement partner who had responsibility for the predecessor firm's engagement or other senior members of the engagement team. By employing that engagement partner, that accounting firm is not a "predecessor auditor" as defined in SAS No. 84. That firm, however, would normally be expected to facilitate inquiries to such individuals.

Assessment of Management's Commitment to the Appropriate Application of Generally Accepted Accounting Principles

.21 In connection with the firm's evaluation of a prospective or continuing attest client, the firm should assess management's commitment to the appropriate application of GAAP. The firm should inquire of the prospective client about its significant accounting policies. If the prospective or continuing client is following accounting policies or practices that the firm believes are inappropriate, the firm should advise the prospective or continuing client of this and ascertain whether it is prepared to adopt accounting policies or practices that the firm believes would be appropriate in the circumstances. An unwillingness to do so on the part of the prospective or continuing client should usually result in a decision not to accept or continue a professional relationship with the client.

Assessment of Management's Commitment to Implementing and Maintaining Effective Internal Control

.22 The firm should assess management's attitude toward, and the significance it places on, the entity's internal control over financial reporting in

evaluating whether to accept or continue a professional relationship with an attest client. The firm's assessment should include inquiring of management regarding its commitment to implementing and maintaining effective internal control including its anti-fraud programs and controls and inquiring about the entity's control environment, risk assessment process, information and communications systems relevant to financial reporting, and control and monitoring activities that are in place and any changes that management believes should be made to enhance the effectiveness of the entity's internal control. Information that will assist the firm in determining whether there are material weaknesses or other reportable conditions in a prospective client's internal control might also be obtained during discussions with prior accountants and by reviewing copies of the predecessor accountants' reports on internal control related matters.

Assessment of the Entity's Financial Viability

.23 The firm should consider the financial viability of the entity in evaluating whether to accept or continue a client relationship. The firm should ordinarily choose not to accept an entity as an attest client if the firm believes that business failure may be imminent or it is very unlikely the entity would ultimately become a viable business enterprise. In such situations, the firm's association with the entity, if accepted as a client, would be short-lived and could expose the firm to litigation if the business failed, regardless of the quality of the firm's professional services.

.24 Ordinarily, a prospective client's financial condition can be evaluated by a careful reading of prior audited or reviewed financial statements, reading of documents filed with regulatory agencies, discussions with predecessor accountants or auditors, and discussions with management. If recent audited or reviewed financial statements are not available, the firm should obtain unaudited financial statements and discuss the prospective client's financial condition with its management. The firm should also consider obtaining the prospective client's most recent income tax return. The firm may also use outside service providers, such as Dun & Bradstreet. In addition, Moody's KMV ratings are generally available for non-financial companies with publicly owned equity securities and are an indicator of a company's risk of default in paying its debt. Fitch Bank Rating ratings are a similar indicator for banking entities, and are generally available for all domestic banks.

Independence and Objectivity

.25 During the client acceptance process, independence implications should be carefully considered, including: any financial interests of the firm or of covered persons; employment relationships that bear on independence; business relationships with the prospective client; and other relationships that could impact independence. Before accepting any new client or engagement, the firm should take appropriate steps to determine that it meets all independence and objectivity requirements with respect to the client and that acceptance of the engagement will not create a conflict of interests with respect to existing engagements.

.26 The aforementioned steps should include the adoption of procedures to obtain information from its professional personnel regarding potential conflicts of interests that would have to be considered in the client acceptance decision. For example, conflicts can arise in situations where two clients are considering a business combination, joint venture or other major transaction

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

with each other. In addition, certain entities are considered competitors that could raise conflict issues in the eyes of existing clients. The firm's professional personnel responsible for the overall engagement performance should also identify and evaluate the following:

- Services that the firm may have already provided to the prospective client or are in the process of providing that cause the firm to lack independence.
- Any relationships between firm personnel and officers and directors of the prospective client that could cause the firm to lack independence.
- Business relationships between the firm and the prospective client which could cause the firm to lack independence.
- The potential significance of the prospective client to the firm in terms of fees, status, or other factors which could possibly diminish the firm's ability to be objective and maintain independence when performing attest services.

.27 Since the prospective client is not presently a client of the firm, at this time there is no need for firm personnel to take any action to cure a personal independence issue such as stock ownership or loans. However, before signing an engagement letter or performing any professional services, the firm should add that client to its Restricted Entity List, if one is maintained, and inform partners and employees as to the newly restricted entity. The Restricted Entity List is often a database that includes all audit clients of the firm, and to the extent practicable its foreign-associated firms, that are SEC registrants and other entities that the firm is required to be independent of under the applicable SEC requirements. For practicable purposes, firms may exclude entities whose securities are not available for public sale. The maintenance of a Restricted Entity List was required for all SEC Practice Section member firms. The Public Company Accounting Oversight Board (the "PCAOB"), in its Interim Professional Auditing Standards (PCAOB Release No. 2003-006 dated April 18, 2003), adopted the SEC Practice Section requirement that registered public accounting firms ensure that they have "policies and procedures in place to comply" with applicable independence requirements. This requirement further specifically requires firms to establish independence policies covering relationships between the firm, its benefit plans, and its professionals, and restricted entities.

.28 In addition, during its annual continuance process, the firm should also address whether it has maintained independence with respect to the audit engagement. Those procedures should include an evaluation of nonaudit services provided to the client and an inquiry of all professional personnel responsible for overall engagement performance.

.29 The firm should be aware that the AICPA, in June 2003, adopted new independence rules governing nonattest services. Included in those new rules are revisions that require AICPA members to:

- Comply with the regulations of certain regulatory bodies such as state boards of accountancy, Securities and Exchange Commission, General Accounting Office, and Department of Labor, when performing services for attest clients that are governed by such regulators' independence rules;
- Assess the client's willingness and ability to oversee permitted nonattest services; and

- Document various aspects of the permitted nonattest services engagement (objective and nature of the services, client's acceptance of its responsibilities, practitioner's responsibilities, and any limitations of the engagement) prior to performing nonattest services.

.30 In addition, the AICPA Professional Ethics Executive Committee adopted more restrictive rules for certain services:

- Performing appraisal, valuation, and actuarial services would impair independence if the results of the service will be material to the client's financial statements and the services involve a significant degree of subjectivity. Actuarial valuations of a client's pension or postretirement benefit liabilities and valuations performed for non-financial statement purposes (for example, estate and gift tax-related valuations) are permitted provided all of the interpretation's other requirements are met.
- Performing certain financial information systems design and implementation services would impair independence, for example, when a member creates or makes more than insignificant modifications to the source code underlying a client's financial reporting system. Practitioners also are precluded from operating a client's local area network (LAN) since that activity is considered to be a management function.

.31 The final nonattest services rules are available at www.aicpa.org/download/ethics/interp_revisions_jun03.pdf.

Inquiry of Third Parties

.32 Timely confidential inquiries of attorneys, bankers, underwriters, and other sources, where appropriate, should be made in order to obtain information concerning the reputation or integrity of key management and significant owners of the prospective client.

Background Investigations

.33 On October 22, 2002, the AICPA SEC Practice Section sent a letter to the Managing Partners of all SEC Practice Section member firms regarding a report prepared by the Quality Control Inquiry Committee (QCIC) containing recommendations for the profession based on lessons learned from litigation (the "QCIC report"). That report is available at http://www.aicpa.org/download/secps/QCIC10-02Report.pdf.

.34 The QCIC report recommends that firms obtain background investigations on certain management personnel for **all** potential new SEC audit clients, and update background investigations whenever there is a significant change in management or the Board of Directors.

.35 The firm also may consider obtaining personnel background investigations for other prospective attest clients, and other current attest clients experiencing changes in key decision makers such as chairs of the company's board and audit committee (if applicable), chief executive officer, chief financial officer and principal accounting officer. Among other matters, a personnel background investigation may provide information regarding management integrity. Therefore, the extent of the personnel background investigations to be performed is subject to professional judgment.

.36 In addition, background investigations may be useful information in other situations, such as the following:

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

- Current or prospective clients considering an IPO.
- Existing clients where concerns arise about the integrity of management.
- Companies being acquired by an existing client.
- Nonclient entities seeking to acquire an existing client.
- Nonclient entities seeking to acquire a former client where the firm plans to reissue its report and/or consent to the inclusion of the firm's auditors' report in a filing of the acquirer (such as a registration statement).
- General due diligence regarding client related parties, major customers or suppliers, business partners, etc.

.37 Subjects of a background investigation may include the following:

- Corporate officers—CEO, President (COO), CFO, and Principal Accounting Officer.
- Directors—Chair of the Board and Chair of the Audit Committee.
- Principal owners or shareholders.
- Non-employee financial advisors.
- Anticipated underwriters for an IPO.
- Related entities or affiliated parties.

.38 The decision as to the specific individuals to be investigated should be based on the extent of their influence on the entity, its operations, its method of obtaining financing, and its financial reporting.

.39 If the firm maintains offices at more than one location or is a member of an association of firms, the firm should consider consulting with its other offices or with the other members of the association. The potential client and its principals may be known to other offices or affiliates of the firm when the company's operations are conducted at several locations or if the principals at one time were in business or employed in another city. The firm should consider coordinating its assessments with local offices and/or affiliates in locations with significant subsidiaries and branches.

.40 The firm should consider focusing background investigations on issues involving management reputation, management performance at prior companies, securities violations, regulatory investigations including SEC sanctions, frequent auditor changes, history of lawsuits against auditors and other professional advisors, financial difficulties, ties to organized crime, fraud allegations, accounting issues, lawsuits, bankruptcies, judgments and liens. The firm should consider performing a search of local and national media for information regarding the entity and identified personnel. Practitioners may also consider performing a search of media and/or litigation databases to identify background information on prospective clients.

.41 If the firm is unable to conduct a background investigation in-house, then it may want to contact attorneys or other outside specialists to conduct such an investigation. In addition, firms that perform credit investigations for financial institutions usually also perform background investigation services.

.42 If a background investigation is utilized, that investigation should be conducted as soon as practicable in the client acceptance or continuance process.

Other Considerations

.43 The following listing of other considerations is not intended to be all-inclusive and the firm should consider whether other conditions are present that may create significantly increased risk, and carefully assess those conditions that are identified.

Restrictions on Scope of Services

.44 The firm should avoid establishing a professional relationship with an entity whose management intends to impose restrictions on the scope of the firm's work, unless there are valid business reasons for the restrictions and those reasons are not the result of a desire to limit the firm's access to information that it may need to conduct unrestricted attest services. The entity may attempt to restrict scope indirectly by unreasonable fee constraints or by imposing unreasonable deadlines.

Entities Under Common Control

.45 When the firm serves all entities under common control, it has added assurance that all material transactions among entities in the controlled group will come to the firm's attention during the course of the engagement. There may be valid business reasons such as investee-investor relationships, affiliates that do not require attest services, or long-standing relationships with other accountants or auditors that preclude the firm from providing professional services to all entities in the group.

.46 In the firm's evaluation of a prospective client in a situation where the firm would perform attest services for only some of the entities under common control, the firm should make a careful investigation of the nature of the operations of the controlled group, the types of transactions executed among the entities, and the transactions between members of the group and controlling persons. The firm's investigation should include discussions with management and the Audit Committee where applicable, reading documents filed with regulatory agencies, and inquiries of predecessor or continuing accountants or auditors.

One-Time Engagements

.47 In a one-time engagement, the firm's risk may be increased, for example, by a lack of previous experience with management and the accounting records or by the fact that the firm will not be in as effective a position to review subsequent events or reevaluate positions taken and decisions made in prior engagements.

Business and Industry Environment

.48 The prospective or existing attest client may be operating in a business environment that creates increased risk to the firm. In evaluating whether to accept or continue a client relationship, the firm should be alert to such environmental conditions and carefully assess their significance and relevance to the firm's decision.

Timing Considerations

.49 There will be cases when, because of timing considerations, the firm is requested to submit its proposal before completion of its client acceptance procedures. In such cases, acceptance should be made contingent on satisfactory completion of the acceptance procedures. The prospective client should be

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

advised that the firm has not completed its acceptance procedures and changes could occur that may cause the firm to decline the engagement. The firm also should indicate that the prospective client should not announce the firm's appointment as auditors until the firm has completed its acceptance procedures. The engagement letter should not be issued and fieldwork should not begin until the firm's client acceptance procedures have been completed.

Documentation

.50 Whether or not an engagement is accepted or a professional relationship continued, the firm should appropriately document its consideration of the elements of the acceptance and continuance process discussed in this Practice Alert. If the prospective client becomes or is continued as an attest client of the firm, the firm should comply with its document retention policies regarding the client acceptance and/or continuance consideration. The documentation with respect to prospective clients not accepted need only be retained for purposes of review by the appropriate level of firm management.

[The next page is 51,151.]

Section 16,270

Practice Alert 04-1
Illegal Acts

November, 2004

NOTICE TO READERS

This Practice Alert is intended to provide practitioners with information that may help them improve the effectiveness and efficiency of their engagements and practices and is based on existing professional literature, the experience of members of the Professional Issues Task Force (PITF) and information provided by certain AICPA member firms to their own professional staff. This information represents the views of the members of the PITF and has not been approved by any senior technical committee of the AICPA. The auditing portion of this publication is an Other Auditing Publication as defined in Statement on Auditing Standards (SAS) No. 95, *Generally Accepted Auditing Standards,* and is intended to provide guidance to auditors of nonissuers.[1] Other Auditing Publications have no authoritative status; however, they may help the auditor understand and apply Statements on Auditing Standards (SASs). If an auditor applies the auditing guidance included in an Other Auditing Publication, the auditor should be satisfied that, in his or her judgment, it is both appropriate and relevant to the circumstances of the subject audit. This publication was reviewed by the AICPA Audit and Attest Standards staff and published by the AICPA, and is presumed to be appropriate.

Introduction

.01 In April 1988, the Auditing Standards Board issued SAS No. 54, *Illegal Acts by Client.* SAS No. 54 prescribes the nature and extent of the consideration an independent auditor should give to the possibility of illegal acts by a client in an audit of financial statements in accordance with generally accepted auditing standards. SAS No. 54 also provides guidance on the auditor's responsibility when a possible illegal act is detected.

.02 SAS No. 54 is the primary source of guidance with respect to the auditor's consideration of the possibility of illegal acts by a client in an audit of financial statements in accordance with generally accepted auditing standards. However, auditors performing audits in accordance with *Government Auditing Standards* (also referred to as the "Yellow Book") should also be aware that those standards include additional requirements related to illegal acts. Auditors should refer to SAS No. 74, *Compliance Auditing Considerations in Audits of Governmental Entities and Recipients of Governmental Financial Assistance*, and the AICPA's Audit Guide Government Auditing Standards *and*

[1] Nonissuer refers to any entity other than an "issuer." The term "issuer" is defined in Section 2 of the Sarbanes-Oxley Act as :

An issuer as defined in Section 3 of the Securities Exchange Act of 1934, the securities of which are registered under Section 12 of that Act, or that is required to file reports under Section 15(d) [of the Exchange Act] or that files or has filed a registration statement that has not yet become effective under the Securities Act of 1933, and that it has not withdrawn. [Parenthetical references to the United States Code omitted].

Circular A-133 Audits, for additional information on illegal acts and the auditor's reporting responsibilities when performing an audit under *Government Auditing Standards*.

.03 SAS No. 54 defines illegal acts as violations of laws or government regulations. Additionally, the AICPA's Audit Guide Government Auditing Standards *and Circular A-133 Audits*, states that it generally has been interpreted under GAAS that the term laws and regulations in SAS No. 54 implicitly includes provisions of contracts or grant agreements. Illegal acts by clients are acts attributable to the entity whose financial statements are under audit or acts by management or employees acting on behalf of the entity. Illegal acts by clients do not include personal misconduct by the entity's personnel unrelated to their business activities.

.04 Illegal acts are divided into two categories: (1) those having a **direct and material** effect on financial statement amounts and (2) those having only an **indirect** effect on the financial statements. Some laws and regulations have a direct and material effect on financial statement amounts. For example, tax laws affect accruals and the amount recognized as expense in the accounting period; applicable laws and regulations may affect the amount of revenue accrued under government contracts. Other laws and regulations, such as occupational safety and health, food and drug administration, environmental protection, equal employment opportunity, and antitrust violations, may have only an indirect effect on the financial statements.

The Auditor's Responsibility for Detection of Illegal Acts Having a Direct and Material Effect on the Financial Statements

.05 The auditor must consider laws and regulations that are generally recognized to have a direct and material effect on the financial statements. However, the auditor should consider such laws and regulations from the perspective of their known relation to audit objectives derived from financial statement assertions rather than from the perspective of legality, per se.

.06 The auditor's responsibility to detect and report misstatements resulting from illegal acts having a direct and material effect on the financial statements is the same as that for misstatements caused by error or fraud and includes assessing the risk that an illegal act may cause the financial statements to contain a material misstatement. The auditor should design the audit to provide reasonable assurance that such illegal acts will be detected. Care should be exercised in planning, performing, and evaluating the results of these procedures. The auditor's planning and risk assessment process should include consideration of the different characteristics of illegal acts and of factors indicating increased risk of illegal acts that have a direct and material effect on the financial statements.

The Auditor's Responsibility for Detection of Illegal Acts Having an Indirect Effect on the Financial Statements

.07 The auditor has no direct responsibility to detect and report misstatements resulting from illegal acts having an indirect effect on the financial statements (hereafter referred to as "indirect effect illegal acts") as the auditor

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

does not ordinarily have a sufficient basis for recognizing possible violations of laws and regulations that have only an indirect effect on the financial statements. The auditor's responsibility is limited to applying auditing procedures to such acts that come to the auditor's attention and being aware that such acts may exist. However, if specific information comes to the auditor's attention regarding the existence of possible indirect effect illegal acts, the auditor should apply audit procedures to determine the potential effects of the possible indirect effect illegal act on the financial statements.

Audit Procedures in the Absence of Specific Information Indicating the Existence of Possible Illegal Acts

.08 The auditor should perform the audit with an attitude of professional skepticism, remaining alert to conditions or events that indicate illegal acts may have occurred. Procedures applied for the purpose of forming an opinion on the financial statements may bring possible illegal acts to the auditor's attention. Considerations as to whether an act is illegal, or of doubtful legality, are frequently outside the auditor's expertise, therefore, the auditor should consider consulting with legal counsel. Additionally, laws and regulations can also vary considerably in terms of their significance to the financial statements.

.09 Possible illegal acts may come to the auditor's attention as a result of inquiries of management and others. The auditor is required to make inquiries of management concerning the client's compliance with laws and regulations. The auditor should also consider the need to obtain representations from the audit committee or others with equivalent authority and responsibility such as the board of directors or the owner in an owner-managed business, (hereinafter referred to as the "audit committee") and the chief legal officer that possible illegal acts brought to their attention have been communicated to the auditor.

.10 Other inquiries may include, but are not limited to:

- Discussions with principal officers as part of the planning process.
- Discussions with legal counsel and others as part of the evaluation of the adequacy of the accounting for, and the need for disclosure of, loss contingencies.
- Discussions with senior management as part of obtaining various written client representations.
- Inquiries of appropriate client personnel about whether the IRS has requested any information concerning possible illegal or improper payments as part of an IRS examination of tax returns, and about the content and significance of the client's replies to the IRS.
- Other inquiries of, and discussions with, client personnel regarding various matters during the course of performing auditing procedures. Examples of specific information, which might be obtained through the application of the audit procedures and the evaluation of the results of those procedures, that may raise a question concerning possible illegal acts are:
  (*a*) Unauthorized transactions, improperly recorded transactions, or transactions not recorded in a complete or timely manner in order to maintain accountability for assets.

(*b*) Investigation by a governmental agency, an enforcement proceeding, or payment of fines or penalties.

(*c*) Violations of laws or regulations cited in reports of examinations by regulatory agencies.

(*d*) Large payments for unspecified services to consultants, affiliates or employees.

(*e*) Sales commissions or agents' fees that appear excessive in relation to those normally paid by the client or to the services actually received.

(*f*) Large payments in cash, purchases of bank cashier's checks in large amounts payable to bearer, transfers to numbered bank accounts, or similar transactions.

(*g*) Unexplained payments made to government officials or employees.

(*h*) Failure to file tax returns or pay government duties or similar fees that are common to the entity's industry or the nature of its business.

.11 In addition, the auditor should obtain representations in the management representation letter regarding:

(1) The absence of any "violations or possible violations of laws or regulations whose effects should be considered for disclosure in the financial statements or as a basis for recording a loss contingency" and

(2) That the auditor has been informed of all possible illegal acts brought to the attention of management.

.12 The auditor should perform the audit with an attitude of professional skepticism, remaining alert to conditions or events that indicate illegal acts may have occurred. Procedures applied for the purpose of forming an opinion on the financial statements may bring possible illegal acts to the auditor's attention. Considerations as to whether an act is illegal, or of doubtful legality, are frequently outside the auditor's expertise, therefore, the auditor should consider consulting with legal counsel. Additionally, laws and regulations can also vary considerably in terms of their significance to the financial statements.

.13 Prior to commencement of the audit, the auditor should consider reaching an understanding with the audit committee as to the communication expectations. Included in the understanding should be the expected nature and extent of communications about violations deemed immaterial either individually or in the aggregate and those perpetrated by lower-level employees.

Action on Discovery of Possible Illegal Acts

.14 If, in the course of conducting an audit, the auditor detects or becomes aware of information indicating that an illegal act has or may have occurred, the auditor should perform the following:

(1) Obtain an understanding of the nature of the matter and the circumstances in which it has occurred, and sufficient other information to make a preliminary assessment of the matter and its possible effect on the financial statements.

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

(2) Obtain assurance that the audit committee or others with equivalent authority and responsibility such as the board of directors or the owner in an owner-managed business (the "audit committee") is adequately informed about possible illegal acts that come to the auditor's attention.

(3) Discuss the client investigation, if applicable, of the illegal act with the appropriate level of senior management and/or the audit committee.

(4) Evaluate the conclusions reached by the client as a result of the investigation, if applicable.

.15 If the audit is of the financial statements of a smaller or less complex, privately owned company that does not have an audit committee or the levels of management that would exist in a larger organization, the auditor should exercise the appropriate level of professional judgment in determining the extent of the audit procedures to be performed specifically, with respect to the communication that is required to the owner or owners and possibly to the company's legal counsel. In addition, if the owner is involved, and the matter is significant, the auditor should also consider withdrawing from the engagement.

.16 If the audit is of the financial statements of a local government that is overseen by a council or similar body, the auditor should report the information to the chief executive officer or the legislative body/board. If the chief executive officer is believed to be a party to the potential illegal act, the auditor should report the act directly to the legislative body/board.

Obtain an Understanding Regarding the Illegal Act

.17 In obtaining an understanding of the nature of the matter and the circumstances in which it has occurred, and sufficient other information to make a preliminary assessment of the matter and its possible effect on the financial statements, the auditor should inquire of the client's management at a level above those involved, if possible, and consult with the client's legal counsel or other specialists, as necessary. Based on the information that the auditor obtains about the possible illegal act, the auditor is required to:

- Determine whether it is likely that an illegal act has occurred,
- If so, determine and consider the possible effect of the illegal act on the client's financial statements, and
- If the matter is other than clearly inconsequential, determine whether the audit committee has been informed of the situation and is taking appropriate action to investigate the matter.

Determine Whether the Audit Committee Has Been Informed About the Illegal Act

.18 The communications with the audit committee should describe the act and the circumstances of its occurrence, as understood by the auditor. In addition, the auditor should communicate the potential effect on the financial statements and related disclosures. The communication may be either oral or written. If the communication is oral, the auditor should document the discussion.

Client Investigation of the Possible Illegal Act

.19 When the audit committee is informed of possible illegal acts that come to the auditor's attention, an investigation into the matter may be made by the audit committee. In certain circumstances, the auditor may insist on an investigation in order to conclude on the effect of the possible illegal act on the financial statements.

.20 Oftentimes in conducting these investigations, the audit committee may seek assistance from outside counsel and other experts such as forensic accountants, if necessary. The auditor may consider requesting that the audit committee keep the auditor apprised of the progress of the investigation and to facilitate discussions concerning the investigation between outside counsel and the auditor.

.21 At the conclusion of the investigation, the auditor should consider requesting that he or she attend the investigative team's presentation to the audit committee and documenting the discussion.

.22 After the audit committee has investigated the possible illegal act and presented the scope of their procedures, their conclusions and any remedial actions to the auditor, the auditor should evaluate the conclusions and determine how they affect the audit of the financial statements. The auditor should coordinate with the appropriate level of senior management and/or the audit committee, based upon the facts and circumstances, to facilitate the auditor's consultation with the client's outside legal counsel about the legal ramifications of the possible illegal act, including, for example, whether there is a penalty which might attach to the illegal act and, if so, the amount, or whether the transaction(s) in question has significance with respect to deductibility of stated amounts for tax purposes and under "cost plus" contracts or other similar situations that apply.

.23 Based on these discussions and the results of the investigation, the auditor should assess the need for additional audit procedures, disclosures in the financial statements, communication of internal control deficiencies, and/or modifications to the audit report. Depending on the results of the investigation, the auditor may also need to consider whether to withdraw from the engagement.

.24 If the client fails to give the occurrence of an illegal act the appropriate level of consideration or fails to take the steps deemed warranted, the auditor should consider the implications of the illegal act in relation to his or her initial evaluations and reevaluate:

- Engagement risk.
- Reliance on management's role in the functioning of internal control.
- Reliance on management's representations.
- Validity and propriety of other similar transactions.

.25 Additionally, the auditor should consider whether any concerns might be mitigated by the performance of additional substantive audit procedures.

.26 The auditor should be sure that the company's board of directors or audit committee is fully aware of the possible consequences of the act and has formally approved the course of action to be followed, when the circumstances so warrant.

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

Material Illegal Acts

.27 The materiality of an illegal act cannot be appropriately assessed by considering only the quantitative effects; the auditor must also consider the qualitative effects of the illegal act. These effects may often be found to overshadow the act's immediate effect. Accounting and disclosure ramifications of loss contingencies associated with illegal acts should be considered in accordance with FASB Statement No. 5, *Accounting for Contingencies*. The determination of the significance of potential illegal acts will generally entail consultation with the client's legal counsel.

Immaterial Illegal Acts

.28 The aggregate of all immaterial illegal acts should be evaluated in relation to the materiality level for the financial statements as a whole. The auditor should consider the effect of each individual misstatement and consider recording an individual misstatement that has a material effect on an individual account or group of accounts, even though that individual misstatement may be offset by other unadjusted misstatements. The auditor needs to also consider the qualitative aspects of the illegal act such as how the illegal act affects the auditor's ability to rely on management representations.

Disclosure of Illegal Acts to Third Parties

.29 Disclosure of an illegal act to parties other than the client's audit committee is not ordinarily part of the auditor's responsibility, and such disclosure would normally be precluded by the auditor's ethical or legal obligation of confidentiality, unless the matter affects his or her opinion on the financial statements. The auditor should recognize, however, that a duty to notify parties outside the client may exist. A duty to notify parties outside of the client may include the following:

- To a successor auditor when the successor makes inquiries in accordance with SAS No. 84, *Communications Between Predecessor and Successor Auditors*, as amended. In accordance with SAS No. 84, as amended, communications between predecessor and successor auditors require the specific permission of the client.
- In response to a subpoena.
- To a funding agency or other specified agency in accordance with requirements for the audits of entities that receive financial assistance from a government agency. *Government Auditing Standards* state that the client may be required by law or regulation to report illegal acts to specified external parties (for example, to a federal inspector general or a state attorney general) and that if the client fails to report such acts, then the auditor should report the illegal acts directly to the external party specified in the law or regulation. Additionally, when an illegal act involves assistance received directly or indirectly from a government agency, auditors may have a duty to report it directly if management fails to take appropriate steps to remedy the illegal acts that the auditor reported to it. See Chapter 5 of *Government Auditing Standards* and the AICPA Audit Guide Government Auditing Standards *and Circular A-133 Audits*, for additional guidance.

.30 Because potential conflicts with the auditor's ethical and legal obligations for confidentiality may be complex, the auditor may wish to consult with his or her legal counsel before discussing illegal acts with parties outside the client.

Reporting Considerations

.31 The auditor may be faced with various reporting issues as a result of becoming aware of acts that he or she suspects may be illegal. Depending upon the particular circumstances, the auditor may consider modifying the auditor's report. Such modification may result from one or more of the following considerations.

Scope Limitation

.32 Generally, the auditor should disclaim an opinion on the financial statements when precluded by the client from applying all the procedures considered necessary in the circumstances. In situations not involving a client-imposed scope restriction (e.g. appointment of the auditor after the client's physical inventory has been taken) and depending upon the auditor's assessment of the importance of the omitted procedures, the auditor may consider qualifying the opinion or disclaiming an opinion. In the latter case, the decision should reflect the auditor's assessment of the significance of the matter to the particular entity and the pervasiveness and magnitude of the potential direct and indirect effects of the acts in question on the client's financial statements taken as a whole.

Departure From Generally Accepted Accounting Principles

.33 When the auditor has been able to conduct the audit in accordance with generally accepted auditing standards and concludes an event or transaction has not been properly accounted for or disclosed in the financial statements, the auditor may qualify the opinion or issue an adverse opinion depending upon the magnitude of the potential effects of the event or transaction. If the departure from generally accepted accounting principles results from inadequate disclosure, the auditor's modified report should provide the information omitted by the client.

Inability to Determine Materiality of an Illegal Act

.34 In the event that the auditor is unable to conclude as to the materiality of an illegal act, the auditor should modify his or her report or disclaim an opinion to adequately reflect the uncertainty.

Client Refusal to Accept Report

.35 If the client refuses to accept a report that has been modified for a client-imposed scope restriction or a departure from generally accepted accounting principles, including inadequate disclosure, the auditor should withdraw from the engagement. If a client refuses to accept a report that has been modified for other reasons, the auditor may have no alternative but to withdraw from the engagement. In any case of withdrawal, the reasons for the withdrawal should be indicated in writing to the audit committee. Deciding whether there is a need to notify parties outside the client's organization of an illegal act is the responsibility of the company's management. However, as previously indicated, the auditor may have a duty to notify parties outside the client.

 Copyright © 2005, American Institute of Certified Public Accountants, Inc.

Audits Performed Under Government Auditing Standards

.36 Auditors performing audits under *Government Auditing Standards* also must issue a report on internal control over financial reporting and on compliance and other matters that reports on the scope and results of testing of the auditee's internal control over financial reporting and compliance with laws, regulations, and provisions of contracts or grant agreements. The AICPA Audit Guide Government Auditing Standards *and Circular A-133 Audits*, provides additional guidance on the auditor's responsibilities with regard to this report.

Documentation

.37 The audit documentation should include appropriate documentation with respect to:

- The required inquiries related to possible illegal acts and compliance with laws and regulations.
- Company policies relative to the prevention of illegal acts, and the use of directives and periodic representations concerning compliance with laws and regulations.
- Circumstances identified that indicate the possible existence of illegal acts and conclusions reached thereon, if applicable.
- The auditor's assessment of the procedures performed by the company to determine that the illegal act was properly accounted for and disclosed, if applicable.
- Whether any uncorrected misstatements appear to represent illegal acts, if applicable.
- Written representation from management concerning the absence of violations or possible violations of laws and regulations.
- Discussions with management, the audit committee, and, if applicable, the board of directors.
- Representations from the audit committee regarding satisfactory completion of any investigations into possible illegal acts undertaken at their direction and satisfactory resolution of the matters identified in the investigation, if applicable.

[The next page is 52,001.]

SUITABLE TRUST SERVICES CRITERIA AND ILLUSTRATIONS

Copyright © 2003 by American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants.

Permission is granted to make copies of this work provided that such copies are for personal, intraorganizational, or educational use only and are not sold or disseminated and provided further that each copy bears the following credit line: " Copyright © 2003 by American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. Used with permission."

This document is available on AICPA Online at www.aicpa.org.

[The next page is 52,011.]

STS Section 17,000

SUITABLE TRUST SERVICES CRITERIA AND ILLUSTRATIONS

TABLE OF CONTENTS

Section		Paragraph
17,100	Suitable Trust Services Criteria and Illustrations for Security, Availability, Processing Integrity, Online Privacy, and Confidentiality (Including WebTrust® and SysTrust®)	.01-.45
	Introduction	.01-.13
	Trust Services	.03-.05
	Assurance Services	.04
	Advisory Services	.05
	Principles, Criteria, and Illustrative Controls	.06-.07
	Consistency With Applicable Laws and Regulations, Defined Commitments, Service-Level Agreements, and Other Contracts	.08
	Foundation for Trust Services—Trust Services Principles and Criteria	.09-.11
	Trust Services—Offerings of SysTrust and WebTrust	.12-.13
	Principles and Criteria	.14-.40
	Security Principle and Criteria	.16-.17
	Security Principle and Criteria Table	.17
	Availability Principle and Criteria	.18-.20
	Availability Principle and Criteria Table	.20
	Processing Integrity Principle and Criteria	.21-.24
	Processing Integrity Principle and Criteria Table	.24
	Online Privacy Principle and Criteria	.25-.35
	AICPA/CICA Trust Services Privacy Components and Criteria	.29
	Global Impact of Privacy Criteria	.30-.31
	Consumer Recourse	.32-.34
	Online Privacy Principle and Criteria Table	.35
	Confidentiality Principle and Criteria	.36-.40
	Confidentiality Principle and Criteria Table	.40
	Appendix A—Consumer Arbitration	.41
	Appendix B—Illustrative Disclosures for E-Commerce Systems	.42
	Appendix C—Example System Description for Non–E-Commerce Systems	.43
	Appendix D—Practitioner Guidance on Scoping and Reporting Issues	.44
	Appendix E—Trust Services Privacy Principle, Criteria, and Illustrations	.45

Section		Paragraph
17,200	Suitable Trust Services Criteria and Illustrations for WebTrust® for Certification Authorities	.01-.72
	Introduction	.01-.05
	Overview	.06-.35
	Electronic Commerce	.06
	Public Key Infrastructure	.07-.12
	Digital Signature	.13-.17
	Differences Between Encryption Key Pairs and Signing Key Pairs	.18-.20
	Certification Authority	.21-.22
	Registration Authority	.23-.26
	Certification Practice Statements and Certificate Policies	.27
	The Difference Between Licensed and Nonlicensed CAs	.28
	The Hierarchal and Cross-Certified CA Models	.29-.33
	Business Issues Associated With CAs	.34-.35
	The WebTrust Seal of Assurance for Certification Authorities	.36-.50
	Practitioners as Assurance Professionals	.38-.39
	Obtaining and Keeping the WebTrust Seal of Assurance for Certification Authorities	.40-.50
	The Assurance Process	.40-.43
	Comparison of a WebTrust for Certification Authorities Examination With Service Auditor Reports	.44-.46
	Obtaining the WebTrust Seal	.47
	Keeping the WebTrust Seal	.48
	The Seal Management Process	.49
	WebTrust Seal Authentication	.50
	WebTrust Principles and Criteria for Certification Authorities	.51-.66
	WebTrust for Certification Authorities Principles	.51-.59
	Principle 1: CA Business Practices Disclosure	.52-.53
	Principle 2: Service Integrity	.54-.57
	Principle 3: CA Environmental Controls	.58-.59
	WebTrust for Certification Authorities Criteria	.60-.63
	WebTrust Principles and Criteria for Certification Authorities	.64-.66
	Principle 1: CA Business Practices Disclosure	.64
	Principle 2: Service Integrity	.65
	Principle 3: CA Environmental Controls	.66

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Section		Paragraph
17,200	Suitable Trust Services Criteria and Illustrations for WebTrust® for Certification Authorities—continued	
	Appendix A—Illustrative Examples of Practitioner Reports	.67
	Appendix B—Illustrative Examples of Management's Assertion	.68
	Appendix C—Illustrative Examples of Management's Representation	.69
	Appendix D—Comparison of WebTrust for Certification Authorities Criteria and ANSI X9.79	.70
	Appendix E—Comparison of CICA Section 5900, AICPA SAS No. 70, and AICPA/CICA WebTrust for Certification Authorities Reviews and Reports Covering the Business Activities of Certification Authority Organizations	.71
	Appendix F—Practitioner Policies and Guidance for WebTrust for Certification Authority Engagements	.72

[The next page is 52,051.]

Section 17,100

Suitable Trust Services Criteria and Illustrations for Security, Availability, Processing Integrity, Online Privacy, and Confidentiality (Including WebTrust® and SysTrust®)

Supersedes version 2.0 of the SysTrust Principles and Criteria and version 3.0 of the WebTrust Principles and Criteria. Effective for engagements beginning on or after April 1, 2003. Earlier implementation is encouraged.

March 2003

NOTICE TO READERS

The Suitable Trust Services Criteria and Illustrations present criteria established by the Assurance Services Executive Committee of the AICPA for use by practitioners when providing attestation services on systems in the subject matters of security, availability, processing integrity, online privacy, confidentiality, and certification authorities. The Assurance Services Executive Committee, in establishing and developing these criteria, followed due process procedures, including exposure of the proposed criteria for public comment. The Assurance Services Executive Committee has been designated as a senior committee and has been given authority to make public statements and publish measurement criteria without clearance from Council or the Board of Directors under Bylaw section 3.6 (AICPA, *Professional Standards*, vol. 2, BL sec. 360).

Introduction

.01 This section provides guidance when providing assurance services, advisory services, or both on information technology (IT)-enabled systems including electronic commerce (e-commerce) systems. It is particularly relevant when providing services with respect to security, availability, processing integrity, online privacy, and confidentiality.

.02 The guidance provided in this section includes:

- Trust Services principles and criteria
- Examples of system descriptions required for these engagements
- Sample practitioner reports for Trust Services engagements

Trust Services

.03 Trust Services (including WebTrust® and SysTrust®) are defined as a set of professional assurance and advisory services based on a common framework (that is, a core set of principles and criteria) to address the risks and opportunities of IT. Trust Services principles and criteria are issued by the Assurance Services Executive Committee.

Assurance Services

.04 Assurance services are those that result in the expression of an opinion by the reporting practitioner; for example, the opinion as to whether a defined system meets the principles and criteria for systems reliability. Assurance services are developed within the framework of Chapter 1, "Attest Engagements," of Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101), as amended. Only certified public accountants (CPAs) may provide the assurance services of Trust Services that result in the expression of a Trust Services, WebTrust, or SysTrust opinion.

Advisory Services

.05 In the context of Trust Services, advisory services include strategic, diagnostic, implementation and sustaining/managing services using Trust Services principles and criteria. Practitioners providing such services follow Statement on Standards for Consulting Services (AICPA, *Professional Standards*, vol. 2, CS sec. 100). There is no expression of an opinion by the practitioner under these engagements.

Principles, Criteria, and Illustrative Controls

.06 The following material sets out broad statements of principles and identifies specific criteria that should be achieved to meet each principle. Trust Services principles are broad statements of objectives. Criteria are benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter. Suitable criteria are objective, measurable, complete, and relevant—they will yield information useful to intended users. It is the view of the Assurance Services Executive Committee that the Trust Services principles and supporting criteria meet the characteristics for suitable criteria. Trust Services principles are used to describe the overall objective; however, the practitioner's opinion makes reference only to criteria.

.07 In the Trust Services Principles and Criteria, the criteria are supported by a list of illustrative controls. These illustrations are not intended to be all-inclusive and are presented as examples only. Actual controls in place at an entity may not be included in the list, and some of the listed controls may not be applicable to all systems and client circumstances. The practitioner should identify and assess the relevant controls the client has in place to satisfy the criteria. The choice and number of those controls would be based on the entity's management style, philosophy, size, and industry. In order to receive an unqualified opinion on a Trust Services engagement, all criteria must be met unless the criterion is clearly not applicable. In the context of the Trust Services Principles and Criteria, the term *policies* is used to refer to written statements that communicate management's intent, objectives, requirements, responsibilities, and/or standards for a particular subject. Such communications may be explicitly designated as policies, whereas others (such as communications with users not otherwise documented as policies, or written procedures) may be implicit. Policies may take many forms but should be in writing.

Consistency With Applicable Laws and Regulations, Defined Commitments, Service-Level Agreements, and Other Contracts

.08 Several of the principles and criteria refer to "consistency with applicable laws and regulations, defined commitments, service-level agreements,

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

and other contracts." Under normal circumstances, it would be beyond the scope of the engagement for the practitioner to undertake identification of *all* relevant "applicable laws and regulations, defined commitments, service-level agreements, and other contracts." Furthermore, Trust Services engagements do not require the practitioner to provide assurance of an entity's compliance with applicable laws and regulations, defined commitments, service-level agreements, and other contracts, but rather of the effectiveness of the entity's controls over monitoring compliance with them. Reference should be made to other professional standards related to providing assurance over compliance with laws, regulations, and agreements.

Foundation for Trust Services—Trust Services Principles and Criteria

.09 The Trust Services Principles and Criteria are organized into four broad areas:

a. *Policies.* The entity has defined and documented its policies[1] relevant to the particular principle.

b. *Communications.* The entity has communicated its defined policies to authorized users.

c. *Procedures.* The entity uses procedures to achieve its objectives in accordance with its defined policies.

d. *Monitoring.* The entity monitors the system and takes action to maintain compliance with its defined policies.

.10 A two-column format has been used to present and discuss the criteria. The first column presents the criteria—the attributes that the entity must meet to be able to demonstrate that it has achieved the principle. The second column provides illustrative controls. These are examples of controls that the entity might have in place to conform to the criteria. Alternative and additional controls may also be appropriate. In addition, examples of system descriptions for both e-commerce and non-e-commerce systems are included in Appendix B [paragraph .42] and Appendix C [paragraph .43], respectively, and Appendix B [paragraph .42] also includes sample disclosures for e-commerce systems.

.11 The following principles and related criteria have been developed by the AICPA/CICA for use by practitioners in the performance of Trust Services engagements such as SysTrust and WebTrust.

a. *Security.* The system[2] is protected against unauthorized access (both physical and logical).

b. *Availability.* The system is available for operation and use as committed or agreed.

---

[1] As noted in paragraph .07, the term *policies* refers to written statements which communicate management's intent, objectives, requirements, responsibilities, and/or standards for a particular subject. Some policies may be explicitly described as such, being contained in policy manuals or similarly labeled documents. However, some policies may be contained in documents without such explicit labeling, including for example, notices or reports to employees or outside parties.

[2] A *system* consists of five key components organized to achieve a specified objective. The five components are categorized as follows: (*a*) infrastructure (facilities, equipment, and networks), (*b*) software (systems, applications, and utilities), (*c*) people (developers, operators, users, and managers), (*d*) procedures (automated and manual), and (*e*) data (transaction streams, files, databases, and tables).

c. *Processing integrity.* System processing is complete, accurate, timely, and authorized.

d. *Online privacy.*[3] Personal information[4] obtained as a result of e-commerce is collected, used, disclosed, and retained as committed or agreed.

e. *Confidentiality.* Information designated as confidential is protected as committed or agreed.

Trust Services—Offerings of SysTrust and WebTrust

.12 SysTrust and WebTrust are two specific services developed by the AICPA that are based on the Trust Services Principles and Criteria. The Trust Services Principles and Criteria may, however, be used to offer services other than SysTrust and WebTrust.

.13 When a practitioner intends to provide assurance from SysTrust or WebTrust engagements, he or she needs to also follow the performance and reporting standards set forth in Chapter 1, "Attest Engagements," of SSAE No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101), as amended. In order to issue SysTrust or WebTrust reports, CPA firms must be licensed by the AICPA.

Principles and Criteria

.14 The Trust Services Principles and Criteria are presented in a two-column format. The first column identifies the criteria for each principle—the attributes that the entity must meet to be able to demonstrate that it has achieved the principle. The second column provides illustrative controls. These are examples of controls that the entity might have in place to meet the criteria. Alternative and/or additional controls can also be used. Illustrative controls are presented as examples only. It is the practitioner's responsibility to identify and document the policies, procedures, and controls actually in place at the entity under examination.

.15 As discussed earlier, in certain e-commerce environments, the terms and conditions, including the rights, responsibilities, and commitments of both parties, are implicit in the user's completion of a transaction on the Web site. To meet the underlying intent of the "Communications" category of the criteria in such circumstances, the policies and processes required by each of the "Communications" criteria should be disclosed on the entity's Web site. Examples of such disclosures for each of the Trust Services principles are contained in Appendix B [paragraph .42].

Security Principle and Criteria

.16 The *security principle* refers to the protection of the system components from unauthorized access, both logical and physical. In e-commerce and other systems, the respective parties wish to ensure that information provided is available only to those individuals who need access to complete the transaction or services, or follow up on questions or issues that may arise. Information

---

[3] The Enterprise Wide Privacy Task Force is in the process of developing criteria and other guidance on enterprise wide privacy. It is expected that that criteria will replace the online privacy criteria in this document upon issuance.

[4] The term *personal information* includes personally identifiable information and other sensitive information for which the entity has legal or other privacy obligations and commitments.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

provided through these systems is susceptible to unauthorized access during transmission and while it is stored on the other party's systems. Limiting access to the system components helps prevent potential abuse of system components, theft of resources, misuse of software, and improper access to, use, alteration, destruction, or disclosure of information. Key elements for the protection of system components include permitting authorized access and preventing unauthorized access to those components.

Security Principle and Criteria Table

.17 The system is protected against unauthorized access (both physical and logical).

Criteria	*Illustrative Controls*[5]
1.0 Policies: The entity defines and documents its policies for the security of its system.	
1.1 The entity's security policies are established and periodically reviewed and approved by a designated individual or group.	The entity's documented systems development and acquisition process includes procedures to identify and document authorized users of the system and their security requirements. User requirements are documented in service-level agreements or other documents. The security officer reviews security policies annually and submits proposed changes for approval by the information technology (IT) standards committee.
1.2 The entity's security policies include, but may not be limited to, the following matters: *a.* Identification and documentation of the security requirements of authorized users. *b.* Allowing access, the nature of that access, and who authorizes such access. *c.* Preventing unauthorized access. *d.* The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access. *e.* Assignment of responsibility and accountability for system security. *f.* Assignment of responsibility and accountability for system changes and maintenance.	The entity's documented security policies contain the elements set out in criterion 1.2.

(continued)

[5] Illustrative controls are presented as examples only. It is the practitioner's responsibility to identify and document the policies, procedures, and controls actually in place at the entity under examination.

Criteria	*Illustrative Controls*
g. Testing, evaluating, and authorizing system components before implementation.	
h. Addressing how complaints and requests relating to security issues are resolved.	
i. The procedures to handle security breaches and other incidents.	
j. Provision for allocation for training and other resources to support its system security policies.	
k. Provision for the handling of exceptions and situations not specifically addressed in its system security policies.	
l. Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts.	
1.3 Responsibility and accountability for the entity's system security policies, and changes and updates to those policies, are assigned.	Management has assigned responsibilities for the maintenance and enforcement of the entity security policy to the chief information officer (CIO). Others on the executive committee assist in the review, update, and approval of the policy as outlined in the executive committee handbook. Ownership and custody of significant information resources (for example, data, programs, and transactions) and responsibility for establishing and maintaining security over such resources is defined.
2.0 Communications: The entity communicates its defined system security policies to authorized users.	
2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	For its e-commerce system, the entity has posted a system description on its Web site. [*For an example of a system description for an e-commerce system, refer to Appendix B (paragraph .42).*] For its non–e-commerce system, the entity has provided a system description to authorized users. [*For an example of a system description for a non–e-commerce based system, refer to Appendix C (paragraph .43).*]
2.2 The security obligations of users and the entity's security commitments to users are communicated to authorized users.	The entity's security commitments and required security obligations of its customers and other external users are posted on the entity's Web site and/or as part of the entity's standard services agreement.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	For its internal users (employees and contractors), the entity's policies relating to security are reviewed with new employees and contractors as part of their orientation, and the key elements of the policies and their impact on the employee are discussed. New employees must sign a statement signifying that they have read, understand, and will follow these policies. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the entity's security policies. Security obligations of contractors are detailed in their contracts.
	A security awareness program has been implemented to communicate the entity's IT security policies to employees.
	The entity publishes its IT security policies on its corporate intranet.
2.3 Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	The security administration team is responsible for implementing the entity's security policies under the direction of the CIO.
	The security administration team has custody of and is responsible for the day-to-day maintenance of the entity's security policies, and recommends changes to the CIO and the IT steering committee.
2.4 The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users.	The process for customers and external users to inform the entity of possible security breaches and other incidents is posted on the entity's Web site and/or is provided as part of the new user welcome kit.
	The entity's security awareness program includes information concerning the identification of possible security breaches and the process for informing the security administration team.
	Documented procedures exist for the identification and escalation of security breaches, and other incidents.
2.5 Changes that may affect system security are communicated to management and users who will be affected.	Changes that may affect customers and users and their security obligations or the entity's security commitments are highlighted on the entity's Web site.
	Changes that may affect system security are reviewed and approved by affected customers under the provisions of the standard services agreement before implementation of the proposed change.
	Planned changes to system components and the scheduling of those changes are reviewed as part of the monthly IT steering committee meetings.

(continued)

Criteria	*Illustrative Controls*
	Changes to system components, including those that may affect system security, require the approval of the security administrator before implementation. There is periodic communication of changes, including changes that affect system security. Changes that affect system security are incorporated into the entity's ongoing security awareness program.
3.0 Procedures: The entity uses procedures to achieve its documented system security objectives in accordance with its defined policies.	
3.1 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: *a.* Registration and authorization of new users. *b.* Identification and authentication of users. *c.* The process to make changes and updates to user profiles. *d.* The process to grant system access privileges and permissions. *e.* Distribution of output restricted to authorized users. *f.* Restriction of logical access to offline storage, backup data, systems, and media. *g.* Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	*a.* Registration and authorization of new users: • Customers can self-register on the entity's Web site, under a secure session in which they provide new user information and select an appropriate user identification (ID) and password. Privileges and authorizations associated with self-registered customer accounts provide specific limited system functionality. • The ability to create or modify users and user access privileges (other than the limited functionality "customer accounts") is limited to the security administration team. • The line-of-business supervisor authorizes access privilege change requests for employees and contractors. Customer access privileges beyond the default privileges granted during self-registration are approved by the customer account manager. Proper segregation of duties is considered in granting privileges. b. Identification and authentication of users: • Users are required to log on to the entity's network and application systems with their user ID and password before access is granted. Unique user IDs are assigned to individual users. Passwords must contain at least six characters, one of which is nonalphanumeric. Passwords are case sensitive and must be updated every 90 days. *c.* Changes and updates to user profiles: • Changes and updates to self-registered customer accounts can be done by the individual user at any time on the entity's Web site after the user has successfully logged onto the system. Changes are reflected immediately. • Unused customer accounts (no activity for six months) are purged by the system.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	• Changes to other accounts and profiles are restricted to the security administration team and require the approval of the appropriate line-of-business supervisor or customer account manager. • Accounts for terminated employees are deactivated upon notice of termination being received from the human resources team. *d.* The process to grant system access privileges and permissions: • All paths that allow access to significant information resources are controlled by the access control system and operating system facilities. Access requires users to provide their user ID and password. Privileges are granted to authenticated users based on their user profiles. • The login session is terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up. *e.* Distribution of output: • Access to computer processing output is provided to authorized individuals based on the classification of the information. • Processing outputs are stored in an area that reflects the classification of the information. *f.* Restriction of logical access to offline storage, backup data, systems, and media: • Logical access to offline storage, backup data, systems, and media is limited to computer operations staff. *g.* Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices: • Hardware and operating system configuration tables are restricted to appropriate personnel. • Application software configuration tables are restricted to authorized users and under the control of application change management software. • Utility programs that can read, add, change, or delete data or programs are restricted to authorized technical services staff. Usage is logged and monitored by the manager of computer operations.

(continued)

Criteria	*Illustrative Controls*
	• The information security team, under the direction of the CIO, maintains access to firewall and other logs, as well as access to any storage media. Any access is logged and reviewed quarterly. • A listing of all master passwords is stored in an encrypted database and an additional copy is maintained in a sealed envelope in the entity safe.
3.2 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware such as firewalls and routers, is restricted to authorized individuals by card key systems and monitored by video surveillance. Physical access cards are managed by building security staff. Access card usage is logged. Logs are maintained and reviewed by building security staff. Requests for physical access privileges to the entity's computer facilities require the approval of the manager of computer operations. Documented procedures exist for the identification and escalation of potential security breaches. Offsite backup data and media are stored at service provider facilities. Access to offsite data and media requires the approval of the manager of computer operations.
3.3 Procedures exist to protect against unauthorized logical access to the defined system.	Login sessions are terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up by the security administrator. Virtual private networking (VPN) software is used to permit remote access by authorized users. Users are authenticated by the VPN server through specific "client" software and user ID and passwords. Firewalls are used and configured to prevent unauthorized access. Firewall events are logged and reviewed daily by the security administrator. Unneeded network services (for example, telnet, ftp, and http) are deactivated on the entity's servers. A listing of the required and authorized services is maintained by the IT department. This list is reviewed by entity management on a routine basis for its appropriateness for the current operating conditions.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	Intrusion detection systems are used to provide continuous monitoring of the entity's network and early identification of potential security breaches. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
3.4 Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.	In connection with other security monitoring, the security administration team participates in user groups and subscribes to services relating to computer viruses. Antivirus software is in place, including virus scans of incoming e-mail messages. Virus signatures are updated at least weekly. Any viruses discovered are reported to the security team and an alert is created for all users notifying them of a potential virus threat.
3.5 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.	The entity uses 128-bit secure sockets layer (SSL) encryption for transmission of private or confidential information over public networks, including user ID and password. Users are required to upgrade their browser to the most current version tested and approved for use by the security administration team to avoid possible security problems. Account activity, subsequent to successful login, is encrypted through a 128-bit SSL session. Users are logged out on request (by selecting the "Sign-out" button on the Web site) or after 10 minutes of inactivity.
3.6 Procedures exist to identify, report, and act upon system security breaches and other incidents.	Users are provided instructions for communicating potential security breaches to the information security team. The information security team logs incidents reported through customer hotlines and e-mail. Intrusion detection and other tools are used to identify, log, and report potential security breaches and other incidents. The system notifies the security administration team and/or the network administrator via e-mail and pager of potential incidents in progress. Incident logs are monitored and evaluated by the information security team daily. Documented incident identification and escalation procedures are approved by management.

(continued)

Criteria	*Illustrative Controls*
3.7 Procedures exist to provide that issues of noncompliance with system security policies are promptly addressed and that corrective measures are taken on a timely basis.	Security issues are recorded and accumulated in a problem report. Corrective action is noted and monitored by management. On a routine basis, security policies, controls, and procedures are audited by the internal audit department. Results of such examinations are reviewed by management, a response is prepared, and a remediation plan is put in place.
Criteria related to the system components used to achieve the objectives	
3.8 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software related to system security are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	The entity has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology. The SDLC methodology includes a framework for classifying data and creating standard user profiles that are established based on an assessment of the business impact of the loss of security. Users are assigned standard profiles based on needs and functional responsibilities. Owners of the information and data classify its sensitivity and determine the level of protection required to maintain an appropriate level of security. The security administration team reviews and approves the architecture and design specifications for new systems development and/or acquisition to ensure consistency with the entity's security objectives, policies, and standards. Changes to system components that may affect security require the approval of the security administration team. The access control and operating system facilities have been installed, including the implementation of options and parameters, to restrict access in accordance with the entity's security objectives, policies, and standards. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
3.9 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security are qualified to fulfill their responsibilities.	The entity has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the verified credentials are commensurate with the proposed position. New personnel are offered employment subject to background checks and reference validation.
	Candidates, including internal transfers, are approved by the line-of-business manager before the employment position is offered.
	Periodic performance appraisals are performed by employee supervisors and include the assessment and review of professional development activities.
	Personnel receive training and development in system security concepts and issues.
	Procedures are in place to provide alternate personnel for key system security functions in case of absence or departure.
Maintainability-related criteria applicable to the system's security	
3.10 Procedures exist to maintain system components, including configurations consistent with the defined system security policies.	Entity management receives a third-party opinion on the adequacy of security controls, and routinely evaluates the level of performance it receives (in accordance with its contractual service-level agreement) from the service provider that hosts the entity's systems and Web site.
	The IT department maintains a listing of all software and the respective level, version, and patches that have been applied.
	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests.
	Staffing, infrastructure, and software requirements are periodically evaluated and resources are allocated consistent with the entity's security policies.
	System configurations are tested annually, and evaluated against the entity's security policies and current service-level agreements. An exception report is prepared and remediation plans are developed and tracked.
	The IT steering committee, which includes representatives from the lines of business and customer support, meets monthly and reviews anticipated, planned, or recommended changes to the entity's security policies, including the potential impact of legislative changes.

(continued)

Criteria	*Illustrative Controls*
3.11 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	Senior management has implemented a division of roles and responsibilities that segregates incompatible functions. The entity's documented systems development methodology describes the change initiation, software development and maintenance, and approval processes, as well as the standards and controls that are embedded in the processes. These include programming, documentation, and testing standards. Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation into production. As part of the change control policies and procedures, there is a "promotion" process (for example, from "test" to "staging" to "production"). Promotion to production requires the approval of the business owner who sponsored the change and the manager of computer operations. When changes are made to key systems components, there is a "backout" plan developed for use in the event of major interruption(s).
3.12 Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Emergency changes that require deviations from standard procedures are logged and reviewed by IT management daily and reported to the affected line-of-business manager. Permanent corrective measures follow the entity's change management process, including line-of-business approvals.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system security policies.	
4.1 The entity's system security is periodically reviewed and compared with the defined system security policies.	The information security team monitors the system and assesses the system vulnerabilities using proprietary and other tools. Potential risk is evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed and implementation is monitored. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. The internal audit function conducts system security reviews as part of its annual audit plan. Results and recommendations for improvement are reported to management.
4.2 There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.	Logs are analyzed to identify trends that may have a potential impact on the entity's ability to achieve its system security objectives. Monthly IT staff meetings are held to address system security concerns and trends; findings are discussed at quarterly management meetings.
4.3 Environmental and technological changes are monitored and their effect on system security is assessed on a timely basis.	Senior management, as part of its annual IT planning process, considers developments in technology and the impact of applicable laws or regulations on the entity's security policies. The entity's IT security group monitors the security impact of emerging technologies. Users are proactively invited to contribute to initiatives to improve system security through the use of new technologies.

Availability Principle and Criteria

.18 The *availability principle* refers to the accessibility to the system, products, or services as advertised or committed by contract, service-level, or other agreements. It should be noted that this principle does not, in itself, set a minimum acceptable performance level for system availability. The minimum performance level is established through commitments made or by mutual agreement (contract) between the parties.

.19 Although there is a connection between system availability, system functionality, and system usability, the availability principle does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to specific tasks or problems). It does address system availability, which relates to whether the system is accessible for processing, monitoring, and maintenance.

Availability Principle and Criteria Table

.20 The system is available for operation and use as committed or agreed.

Criteria	*Illustrative Controls*
1.0 Policies: The entity defines and documents its policies for the availability of its system.	
1.1 The entity's system availability and related security policies are established and periodically reviewed and approved by a designated individual or group.	The entity's documented systems development and acquisition process includes procedures to identify and document authorized users of the system and their availability and related security requirements. User requirements are documented in service-level agreements or other documents. Management reviews the entity's availability and related security policies annually. Proposed changes are submitted as needed for approval by the information technology (IT) standards committee, which includes representation from the customer service department.
1.2 The entity's system availability and related security policies include, but may not be limited to, the following matters: *a.* Identification and documentation of the system availability and related security requirements of authorized users. *b.* Allowing access, the nature of that access, and who authorizes such access. *c.* Preventing unauthorized access. *d.* The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access. *e.* Assignment of responsibility and accountability for system availability and related security. *f.* Assignment of responsibility and accountability for system changes and maintenance. *g.* Testing, evaluating, and authorizing system components before implementation. *h.* Addressing how complaints and requests relating to system availability and related security issues are resolved.	The entity's documented availability and related security policies contain the elements set out in criterion 1.2.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
i. The procedures to handle system availability and related security breaches and other incidents.	
j. Provision for allocation for training and other resources to support its system availability and related security policies.	
k. Provision for the handling of exceptions and situations not specifically addressed in its system availability and related security policies.	
l. Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts.	
m. Recovery and continuity of service in accordance with documented customer commitments or other agreements.	
n. Monitoring system capacity to achieve customer commitments or other agreements regarding availability.	
1.3 Responsibility and accountability for the entity's system availability and related security policies, and changes and updates to those policies, are assigned.	Management has assigned responsibilities for the maintenance and enforcement of the entity's availability policies to the chief information officer (CIO). Others on the executive committee assist in the review, update, and approval of these policies as outlined in the executive committee handbook. Ownership and custody of significant information resources (for example, data, programs, and transactions) and responsibility for establishing and maintaining the system availability of and related security over such resources is defined.
2.0 Communications: The entity communicates the defined system availability policies to authorized users.	
2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	For its e-commerce system, the entity has posted a system description on its Web site. [*For an example of a system description for an e-commerce system, refer to Appendix B (paragraph .42).*]

(continued)

Criteria	*Illustrative Controls*
	For its non–e-commerce system, the entity has provided a system description to authorized users. [*For an example of a system description for a non–e-commerce based system, refer to Appendix C (paragraph .43).*]
2.2 The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.	The entity's system availability and related security commitments and required system availability and related security obligations of its customers and other external users are posted on the entity's Web site and/or as part of the entity's standard services agreement. Service-level agreements are reviewed with the customer annually. For its internal users (employees and contractors), the entity's policies relating to system availability and security are reviewed with new employees and contractors as part of their orientation, and the key elements of the policies and their impact on the employee are discussed. New employees must sign a statement signifying that they have read, understand, and will follow these policies. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the entity's policies. Obligations of contractors are detailed in their contract. A security awareness program has been implemented to communicate the entity's IT security policies to employees. The entity publishes its IT security policies on its corporate intranet.
2.3 Responsibility and accountability for the entity's system availability and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	The network operations team is responsible for implementing the entity's availability policies under the direction of the chief information officer (CIO). The security administration team is responsible for implementing the related security policies. The network operations team has custody of and is responsible for the day-to-day maintenance of the entity's availability policies, and recommends changes to the CIO and the IT steering committee. The security administration team is responsible for the related security policies. Availability and related security commitments are reviewed with the customer account managers as part of the annual IT planning process.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
2.4 The process for informing the entity about system availability issues and breaches of system security and for submitting complaints is communicated to authorized users.	The process for customers and external users to inform the entity of system availability issues, possible security breaches, and other incidents is posted on the entity's Web site and/or is provided as part of the new user welcome kit. The entity's user training program includes modules dealing with the identification and reporting of system availability issues, security breaches, and other incidents. The entity's security awareness program includes information concerning the identification of possible security breaches and the process for informing the security administration team. Documented procedures exist for the identification and escalation of system availability issues, security breaches, and other incidents.
2.5 Changes that may affect system availability and system security are communicated to management and users who will be affected.	Changes that may affect system availability, customers and users and their security obligations, or the entity's security commitments are highlighted on the entity's Web site. Changes that may affect system availability and related system security are reviewed and approved by affected customers under the provisions of the standard services agreement before implementation of the proposed change. Planned changes to system components and the scheduling of those changes are reviewed as part of the monthly IT steering committee meetings. Changes to system components, including those that may affect system security, require the approval of the manager of network operations and/or the security administration team, before implementation. There is periodic communication of system changes, including changes that affect availability and system security. Changes that affect system security are incorporated into the entity's ongoing security awareness program.

(continued)

Criteria	*Illustrative Controls*
3.0 Procedures: The entity uses procedures to achieve its documented system availability objectives in accordance with its defined policies.	
3.1 Procedures exist to protect the system against potential risks (for example, environmental risks, natural disasters, labor disputes, and routine operational errors and omissions) that might disrupt system operations and impair system availability.	A risk assessment is prepared and reviewed on a regular basis or when a significant change occurs in either the internal or external physical environment. Threats such as fire, flood, dust, power failure, excessive heat and humidity, and labor problems have been considered. Management maintains measures to protect against environmental factors (for example, fire, flood, dust, power failure, and excessive heat and humidity) based on its risk assessment. The entity's controlled areas are protected against fire using both smoke detectors and a fire suppression system. Water detectors are installed within the raised floor areas. The entity site is protected against a disruption in power supply to the processing environment by both uninterruptible power supplies (UPS) and emergency power supplies (EPS). This equipment is tested semiannually. Preventive maintenance agreements and scheduled maintenance procedures are in place for key system hardware components. Vendor warranty specifications are complied with and tested to determine if the system is properly configured. Procedures to address minor processing errors, outages, and destruction of records are documented. Procedures exist for the identification, documentation, escalation, resolution, and review of problems. Physical and logical security controls are implemented to reduce the opportunity for unauthorized actions that could impair system availability.
3.2 Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies.	Management has implemented a comprehensive strategy for backup and restoration based on a review of business requirements. Backup procedures for the entity are documented and include redundant servers, daily incremental backups of each server, and a complete backup of the entire week's changes on a weekly basis. Daily and weekly backups are stored offsite in accordance with the entity's system availability policies. Disaster recovery and contingency plans are documented.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	The disaster recovery plan defines the roles and responsibilities and identifies the critical information technology application programs, operating systems, personnel, data files, and time frames needed to ensure high availability and system reliability based on the business impact analysis. The business continuity planning (BCP) coordinator reviews and updates the business impact analysis with the lines of business annually. Disaster recovery and contingency plans are tested annually in accordance with the entity's system availability policies. Testing results and change recommendations are reported to the entity's management committee. The entity's management committee reviews and approves changes to the disaster recovery plan. All critical personnel identified in the business continuity plan hold current versions of the plan, both onsite and offsite. An electronic version is stored offsite.
3.3 Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies.	Automated backup processes include procedures for testing the integrity of the backup data. Backups are performed in accordance with the entity's defined backup strategy, and usability of backups is verified at least annually. Backup systems and data are stored offsite at the facilities of a third-party service provider. Under the terms of its service provider agreement, the entity performs an annual verification of media stored at the offsite storage facility. As part of the verification, media at the offsite location are matched to the appropriate media management system. The storage site is reviewed biannually for physical access security and security of data files and other items. Backup systems and data are tested as part of the annual disaster recovery test.
Security-related criteria relevant to the system's availability	
3.4 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: *a.* Registration and authorization of new users. *b.* Identification and authentication of users.	*a.* Registration and authorization of new users: • Customers can self-register on the entity's Web site, under a secure session in which they provide new user information and select an appropriate user identification (ID) and password. Privileges and authorizations associated with self-registered customer accounts provide specific limited system functionality.

(continued)

Criteria	*Illustrative Controls*
c. The process to make changes and updates to user profiles. d. The process to grant system access privileges and permissions. e. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	• The ability to create or modify users access privileges (other than the limited functionality "customer accounts") is limited to the security administration team. • The line-of-business supervisor authorizes access privilege change requests for employees and contractors. Customer access privileges beyond the default privileges granted during self-registration are approved by the customer account manager. Proper segregation of duties is considered in granting privileges. b. Identification and authentication of users: • Users are required to log on to the entity's network and application systems with their user ID and password before access is granted. Unique user IDs are assigned to individual users. Passwords must contain at least six characters, one of which is nonalphanumeric. Passwords are case sensitive and must be updated every 90 days. c. Changes and updates to user profiles: • Changes and updates to self-registered customer accounts can be done by the individual user at any time on the entity's Web site after the user has successfully logged onto the system. Changes are reflected immediately. • Unused customer accounts (no activity for six months) are purged by the system. • Changes to other accounts and profiles are restricted to the security administration team and require the approval of the appropriate line-of-business supervisor or customer account manager. • Accounts for terminated employees are deactivated upon notice of termination being received from the human resources team. d. The process to grant system access privileges and permissions: • All paths that allow access to significant information resources are controlled by the access control system and operating system facilities. Access requires users to provide their user ID and password. Privileges are granted to authenticated users based on their user profiles.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	• The login session is terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up.
	e. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices:
	• Hardware and operating system configuration tables are restricted to appropriate personnel.
	• Application software configuration tables are restricted to authorized users and under the control of application change management software.
	• Utility programs that can read, add, change, or delete data or programs are restricted to authorized technical services staff. Usage is logged and monitored by the manager of computer operations.
	• The information security team, under the direction of the CIO, maintains access to firewall and other logs, as well as access to any storage media. Any access is logged and reviewed quarterly.
	• A listing of all master passwords is stored in an encrypted database and an additional copy is maintained in a sealed envelope in the entity safe.
3.5 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware such as firewalls and routers, is restricted to authorized individuals by card key systems and monitored by video surveillance. Physical access cards are managed by building security staff. Access card usage is logged. Logs are maintained and reviewed by building security staff. Requests for physical access privileges to the entity's computer facilities require the approval of the manager of computer operations. Documented procedures exist for the identification and escalation of potential security breaches. Offsite backup data and media are stored at service provider facilities. Access to offsite data and media requires the approval of the manager of computer operations.

(continued)

Criteria	*Illustrative Controls*
3.6 Procedures exist to protect against unauthorized logical access to the defined system.	Login sessions are terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up by the security administrator. Virtual private networking (VPN) software is used to permit remote access by authorized users. Users are authenticated by the VPN server through specific "client" software and user ID and passwords. Firewalls are used and configured to prevent unauthorized access. Firewall events are logged and reviewed daily by the security administrator. Unneeded network services (for example, telnet, ftp, and http) are deactivated on the entity's servers. A listing of the required and authorized services is maintained by the IT department. This list is reviewed by entity management on a routine basis for its appropriateness for the current operating conditions. Intrusion detection systems are used to provide continuous monitoring of the entity's network and early identification of potential security breaches. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
3.7 Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.	In connection with other security monitoring, the security administration team participates in user groups and subscribes to services relating to computer viruses. Antivirus software is in place, including virus scans of incoming e-mail messages. Virus signatures are updated at least weekly. Any viruses discovered are reported to the security team and an alert is created for all users notifying them of a potential virus threat.
3.8 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.	The entity uses 128-bit secure sockets layer (SSL) encryption for transmission of private or confidential information over public networks, including user ID and password. Users are required to upgrade their browser to the most current version tested and approved for use by the security administration team to avoid possible security problems. Account activity, subsequent to successful login, is encrypted through a 128-bit SSL session. Users are logged out on request (by selecting the "Sign-out" button on the Web site) or after 10 minutes of inactivity.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
3.9 Procedures exist to identify, report, and act upon system availability issues and related security breaches and other incidents.	Users are provided instructions for communicating system availability issues, potential security breaches, and other issues to the help desk or customer service center. Documented procedures exist for the escalation of system availability issues and potential security breaches that cannot be resolved by the help desk. Network performance and system processing are monitored using system monitoring tools by onsite operations staff 24 hours a day, 7 days a week. Documented procedures exist for the escalation and resolution of performance and processing availability issues. Intrusion detection and other tools are used to identify, log, and report potential security breaches and other incidents. The system notifies the security administration team and/or the network administrator via e-mail and pager of potential incidents in progress. Incident logs are monitored and evaluated by the information security team daily. Documented incident identification and escalation procedures are approved by management. Network performance, system availability, and security incident statistics and comparisons to approved targets are accumulated and reported to the IT steering committee monthly. System performance and capacity analysis and projections are completed annually as part of the IT planning and budgeting process.
3.10 Procedures exist to provide that issues of noncompliance with system availability and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	System processing and security-related issues are recorded and accumulated in a problem report. Corrective action is noted and monitored by management. As a part of the monthly monitoring of the site, availability and site usage reports are compared to the disclosed availability levels. This analysis is used to forecast future capacity, reveal any performance issues, and provide a means of fine-tuning the system. Standard procedures exist for the documentation, escalation, resolution, and review of problems. On a routine basis, security policies, controls, and procedures are audited by the internal audit department. Results of such examinations are reviewed by management, a response is prepared, and a remediation plan is put in place.

(continued)

Criteria	*Illustrative Controls*
	Entity management evaluates the level of performance it receives from the Internet service provider (ISP) which hosts the entity Web site. This evaluation is done by evaluating the provider's actual performance as compared to agreed service-level commitments including measures for system processing performance levels, availability, and security controls the ISP has in place. Management receives an annual independent third-party report on the adequacy of internal controls from its Web-hosting service provider. Management reviews these reports and follows up with the service provider management on any open items or causes for concern.
Criteria related to the system components used to achieve the objectives	
3.11 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software related to system availability and security are consistent with defined system availability and related security policies.	The entity has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology. The SDLC methodology includes a framework for: • Establishing performance level and system availability requirements based on user needs. • Maintaining the entity's backup and disaster recovery planning processes in accordance with user requirements. • Classifying data and creating standard user profiles that are established based on an assessment of the business impact of the loss of security; assigning standard profiles to users based on needs and functional responsibilities. • Testing changes to system components to minimize the risk of an adverse impact to system performance and availability. • Development of "backout" plans before implementation of changes. Owners of the information and data establish processing performance and availability benchmarks, classify its sensitivity, and determine the level of protection required to maintain an appropriate level of security. The security administration team reviews and approves the architecture and design specifications for new systems development and/or acquisition to ensure consistency with the entity's availability and related security policies.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	Changes to system components that may affect systems processing performance, availability, and security require the approval of the security administration team.
	The access control and operating system facilities have been installed, including the implementation of options and parameters, to restrict access in accordance with the entity's security objectives, policies, and standards.
	The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
3.12 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting availability and security are qualified to fulfill their responsibilities.	The entity has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions.
	Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the verified credentials are commensurate with the proposed position. New personnel are offered employment subject to background checks and reference validation.
	Candidates, including internal transfers, are approved by the line-of-business manager before the employment position is offered.
	Periodic performance appraisals are performed by employee supervisors and include the assessment and review of professional development activities.
	Personnel receive training and development in system availability concepts and issues.
	Procedures are in place to provide alternate personnel for key system availability functions in case of absence or departure.
Maintainability-related criteria applicable to the system's availability	
3.13 Procedures exist to maintain system components, including configurations consistent with the defined system availability and related security policies.	Entity management receives a third-party opinion on the adequacy of security controls, and routinely evaluates the level of performance it receives (in accordance with its contractual service-level agreement) from the service provider that hosts the entity's systems and Web site.
	The IT department maintains a listing of all software and the respective level, version, and patches that have been applied.
	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests.

(continued)

Criteria	*Illustrative Controls*
	Staffing, infrastructure, and software requirements are periodically evaluated and resources are allocated consistent with the entity's availability and related security policies.
	System configurations are tested annually and evaluated against the entity's processing performance, availability, and security policies, and current service-level agreements. An exception report is prepared and remediation plans are developed and tracked.
	The IT steering committee, which includes representatives from the lines of business and customer support, meets monthly and reviews anticipated, planned, or recommended changes to the entity's availability and related security policies, including the potential impact of legislative changes.
3.14 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	Senior management has implemented a division of roles and responsibilities that segregates incompatible functions.
	The entity's documented systems development methodology describes the change initiation, software development and maintenance, and approval processes, as well as the standards and controls that are embedded in the processes. These include programming, documentation, and testing standards.
	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests.
	Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation into production.
	As part of the change control policies and procedures, there is a "promotion" process (for example, from "test" to "staging" to "production"). Promotion to production requires the approval of the business owner who sponsored the change and the manager of computer operations.
	When changes are made to key systems components, there is a "backout" plan developed for use in the event of major interruption(s).

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
3.15 Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Emergency changes that require deviations from standard procedures are logged and reviewed by IT management daily and reported to the affected line-of-business manager. Permanent corrective measures follow the entity's change management process, including line-of-business approvals.
4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system availability policies.	
4.1 The entity's system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.	Network performance and system processing are monitored using system monitoring tools by onsite operations staff 24 hours a day, 7 days a week. Network performance, system availability, and security incident statistics and comparisons to approved targets are accumulated and reported to the IT steering committee monthly. The customer service group monitors system availability and related customer complaints. It provides a monthly report of such matters together with recommendations for improvement, which are considered and acted on at the monthly IT steering committee meetings. The information security team monitors the system and assesses the system vulnerabilities using proprietary and other tools. Potential risk is evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed and implementation is monitored. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. The internal audit function conducts system availability and system security reviews as part of its annual audit plan. Results and recommendations for improvement are reported to management.
4.2 There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system availability and related security policies.	Network performance and system processing are monitored using system monitoring tools by onsite operations staff 24 hours a day, 7 days a week. Network performance, system availability, and security incident statistics and comparisons to approved targets are accumulated and reported to the IT steering committee monthly.

(continued)

Criteria	*Illustrative Controls*
	Future system performance, availability, and capacity requirements are projected and analyzed as part of the annual IT planning and budgeting process.
	Logs are analyzed to identify trends that may have a potential impact on the entity's ability to achieve its system availability and related security objectives.
	Monthly IT staff meetings are held to address system performance, availability, capacity, and security concerns and trends; findings are discussed at quarterly management meetings.
4.3 Environmental and technological changes are monitored and their effect on system availability and security is assessed on a timely basis.	The entity's data center facilities include climate and environmental monitoring devices. Deviations from optimal performance ranges are escalated and resolved.
	Senior management, as part of its annual IT planning process, considers developments in technology and the impact of applicable laws or regulations on the entity's availability and related security policies.
	The entity's customer service group monitors the impact of emerging technologies, customer requirements, and competitive activities.

Processing Integrity Principle and Criteria

.21 The *processing integrity principle* refers to the completeness, accuracy, timeliness, and authorization of system processing. Processing integrity exists if a system performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation. Completeness generally indicates that all transactions and services are processed or performed without exception, and that transactions and services are not processed more than once. Accuracy includes assurances that key information associated with the submitted transaction will remain accurate throughout the processing of the transaction and the transaction or services are processed or performed as intended. The timeliness of the provision of services or the delivery of goods is addressed in the context of commitments made for such delivery. Authorization includes assurances that processing is performed in accordance with the required approvals and privileges defined by policies governing system processing.

.22 The risks associated with processing integrity are that the party initiating the transaction will not have the transaction completed or the service provided correctly, and in accordance with the desired or specified request. Without appropriate processing integrity controls, the buyer may not receive the goods or services ordered, receive more than requested, or receive the wrong goods or services altogether. However, if appropriate processing integrity controls exist and are operational within the system, the buyer can be reasonably assured that the correct goods and services in the correct quantity at the correct price are received when promised. Processing integrity addresses all of the system components including procedures to initiate, record, process, and report

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

the information, product, or service that is the subject of the engagement. The nature of data input in e-commerce systems typically involves the user entering data directly over Web-enabled input screens or forms, whereas in other systems, the nature of data input can vary significantly. Because of this difference in data input processes, the nature of controls over the completeness and accuracy of data input in e-commerce systems may be somewhat different than for other systems. The illustrative controls outlined in the following table identify some of these differences.

.23 Processing integrity differs from data integrity. Processing integrity does not automatically imply that the information stored by the system is complete, accurate, current, and authorized. If a system processes information inputs from sources outside of the system's boundaries, an entity can establish only limited controls over the completeness, accuracy, authorization, and timeliness of the information submitted for processing. Errors that may have been introduced into the information and the control procedures at external sites are typically beyond the entity's control. When the information source is explicitly excluded from the description of the system that defines the engagement, it is important to describe that exclusion in the system description. In other situations, the data source may be an inherent part of the system being examined, and controls over the completeness, accuracy, authorization, and timeliness of information submitted for processing would be included in the scope of the system as described.

Processing Integrity Principle and Criteria Table

.24 System processing is complete, accurate, timely, and authorized.

Criteria	*Illustrative Controls*
1.0 Policies: The entity defines and documents its policies for the processing integrity of its system.	
1.1 The entity's processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group.	The entity's documented systems development and acquisition process includes procedures to identify and document authorized users of the system and their processing integrity and related security requirements. User requirements are documented in service-level agreements or other documents. The security officer reviews security policies annually and submits proposed changes as needed for approval by the information technology (IT) standards committee.
1.2 The entity's system processing integrity and related security policies include, but may not be limited to, the following matters: *a.* Identification and documentation of the system processing integrity and related security requirements of authorized users.	The entity's documented processing integrity and related security policies contain the elements set out in criterion 1.2.

(continued)

Criteria	*Illustrative Controls*
b. Allowing access, the nature of that access, and who authorizes such access.	
c. Preventing unauthorized access.	
d. The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access.	
e. Assignment of responsibility and accountability for system processing integrity and related security.	
f. Assignment of responsibility and accountability for system changes and maintenance.	
g. Testing, evaluating, and authorizing system components before implementation.	
h. Addressing how complaints and requests relating to system processing integrity and related security issues are resolved.	
i. The procedures to handle errors and omissions and other system processing integrity and related security breaches and other incidents.	
j. Provision for allocation for training and other resources to support its system processing integrity and related system security policies.	
k. Provision for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies.	
l. Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts.	

	Criteria	*Illustrative Controls*
1.3	Responsibility and accountability for the entity's system processing integrity and related system security policies, and changes, updates, and exceptions to those policies, are assigned.	Management has assigned responsibilities for the implementation of the entity's processing integrity and related security policies to the chief information officer (CIO). Others on the executive committee assist in the review, update, and approval of the policies as outlined in the executive committee handbook. Ownership and custody of significant information resources (for example, data, programs, and transactions) and responsibility for establishing and maintaining system processing integrity and related security over such resources is defined.
2.0	**Communications: The entity communicates its documented system processing integrity policies to authorized users.**	
2.1	The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users. If the system is an e-commerce system, additional information provided on its Web-site includes, but may not be limited to, the following matters: *a.* Descriptive information about the nature of the goods or services that will be provided, including, where appropriate: • Condition of goods (meaning, whether they are new, used, or reconditioned). • Description of services (or service contract). • Sources of information (meaning, where it was obtained and how it was compiled). *b.* The terms and conditions by which it conducts its e-commerce transactions including, but not limited to, the following matters: • Time frame for completion of transactions (*transaction* means fulfillment of orders where goods are being sold and delivery of service where a service is being provided).	For its e-commerce system, the entity has posted a system description including the elements set out in criterion 2.1 on its Web site. [*For an example of a system description and additional disclosures for an e-commerce system, refer to Appendix B (paragraph .42).*] For its non–e-commerce system, the entity has provided a system description to authorized users. [*For an example of a system description for a non–e-commerce based system, refer to Appendix C (paragraph .43).*]

(continued)

Criteria	*Illustrative Controls*
• Time frame and process for informing customers of exceptions to normal processing of orders or service requests. • Normal method of delivery of goods or services, including customer options, where applicable. • Payment terms, including customer options, if any. • Electronic settlement practices and related charges to customers. • How customers may cancel recurring charges, if any. • Product return policies and limited liability, where applicable. *c.* Where customers can obtain warranty, repair service, and support related to the goods and services purchased on its Web site. *d.* Procedures for resolution of issues regarding processing integrity. These may relate to any part of a customer's e-commerce transaction, including complaints related to the quality of services and products, accuracy, completeness, and the consequences for failure to resolve such complaints.	
2.2 The processing integrity and related security obligations of users and the entity's processing integrity and related security commitments to users are communicated to authorized users.	The entity's processing integrity and related security commitments and required processing integrity and related security obligations of its customers and other external users are posted on the entity's Web site and/or as part of the entity's standard services agreement. For its internal users (employees and contractors), the entity's policies relating to processing integrity and security are reviewed with new employees and contractors as part of their orientation, and the key elements of the policies and their impact on the employee are discussed. New employees must sign a statement signifying that they have read, understand, and will follow these policies. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the entity's processing integrity and security policies. Obligations of contractors are detailed in their contract.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	A security awareness program has been implemented to communicate the entity's processing integrity and related security policies to employees. The entity publishes its IT security policies on its corporate intranet.
2.3 Responsibility and accountability for the entity's system processing integrity and related security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.	Management has assigned responsibilities for the enforcement of the entity's processing integrity policies to the chief financial officer (CFO). The security administration team is responsible for implementing the entity's security policies under the direction of the CIO. Others on the executive committee assist in the review and update of the policy as outlined in the executive committee handbook. The security administration team has custody of and is responsible for the day-to-day maintenance of the entity's security policies, and recommends changes to the CIO and the IT steering committee. Processing integrity and related security commitments are reviewed with the customer account managers as part of the annual IT planning process.
2.4 The process for obtaining support and informing the entity about system processing integrity issues, errors and omissions, and breaches of systems security and for submitting complaints is communicated to authorized users.	The process for customers and external users to inform the entity of possible processing integrity issues, security breaches, and other incidents is posted on the entity's Web site and/or is provided as part of the new user welcome kit. The entity's user training and security awareness programs include information concerning the identification of processing integrity issues and possible security breaches, and the process for informing the security administration team. Documented procedures exist for the identification and escalation of system processing integrity issues, security breaches, and other incidents.
2.5 Changes that may affect system processing integrity and system security are communicated to management and users who will be affected.	Changes that may affect customers and users and their processing integrity and related security obligations or the entity's processing integrity and related security commitments are highlighted on the entity's Web site. Changes that may affect processing integrity and related system security are reviewed and approved by affected customers under the provisions of the standard services agreement before implementation of the proposed change. Planned changes to system components and the scheduling of those changes are reviewed as part of the monthly IT steering committee meetings.

(continued)

Criteria	*Illustrative Controls*
	Changes to system components, including those that may affect system security, require the approval of the security administrator and the sponsor of the change before implementation. There is periodic communication of changes, including changes that affect system security. Changes are incorporated into the entity's ongoing user training and security awareness programs.
3.0 Procedures: The entity uses procedures to achieve its documented system processing integrity objectives in accordance with its defined policies.	
3.1 The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integrity policies. If the system is an e-commerce system, the entity's procedures include, but may not be limited to, the following matters: • The entity checks each request or transaction for accuracy and completeness. • Positive acknowledgment is received from the customer before the transaction is processed.	The entity has established data preparation procedures to be followed by user departments. Data entry screens contain field edits and range checks, and input forms are designed to reduce errors and omissions. Source documents are reviewed for appropriate authorizations before input. Error handling procedures are followed during data origination to ensure that errors and irregularities are detected, reported, and corrected. Original source documents are retained on image management systems for a minimum of seven years, to facilitate the retrieval or reconstruction of data as well as to satisfy legal requirements. Logical access controls restrict data entry capability to authorized personnel. (See 3.5 in this table.) The customer account manager performs a regular review of customer complaints, back-order logs, and other transactional analysis. This information is compared to customer service agreements. The entity protects information from unauthorized access, modification, and misaddressing during transmission and transport using a variety of methods including: • Encryption of transmission information. • Batch header and control total reconciliations. • Message authentication codes and hash totals. • Private leased lines or virtual private networking connections with authorized users. • Bonded couriers and tamper-resistant packaging.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	Because of the Web-based nature of the input process, the nature of the controls to achieve the criterion set out in 3.1 may take somewhat different forms, such as: • Account activity, subsequent to successful login, is encrypted through a 128-bit secure sockets layer (SSL) session. • Web scripts contain error checking for invalid inputs. • The entity's order processing system contains edits, validity, and range checks, which are applied to each order to check for accuracy and completeness of information before processing. • Before a transaction is processed by the entity, the customer is presented with a request to confirm the intended transaction and the customer is required to click on the "Yes, please process this order" button before the transaction is processed. The entity e-mails an order confirmation to the customer-supplied e-mail address. The order confirmation contains order details, shipping and delivery information, and a link to an online customer order tracking service. Returned e-mails are investigated by customer service.
3.2 The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies. If the system is an e-commerce system, the entity's procedures include, but are not necessarily limited to, the following matters: • The correct goods are shipped in the correct quantities in the time frame agreed upon, or services and information are provided to the customer as requested. • Transaction exceptions are promptly communicated to the customer. • Incoming messages are processed and delivered accurately and completely to the correct IP address.	Responsibility for order processing, application of credits and cash receipts, custody of inventory, user account management, and database management have been segregated. The entity's documented systems development life cycle (SDLC) methodology is used in the development of new applications and the maintenance of existing applications. The methodology contains required procedures for user involvement, testing, conversion, and management approvals of system processing integrity features. Computer operations and job scheduling procedures exist, are documented, and contain procedures and instructions for operations personnel regarding system processing integrity objectives, policies, and standards. Exceptions require the approval of the manager of computer operations. The entity's application systems contain edit and validation routines to check for incomplete or inaccurate data. Errors are logged, investigated, corrected, and resubmitted for input. Management reviews error logs daily to ensure that errors are corrected on a timely basis.

(continued)

Criteria	*Illustrative Controls*
• Outgoing messages are processed and delivered accurately and completely to the service provider's (SP's) Internet access point. • Messages remain intact while in transit within the confines of the SP's network.	End-of-day reconciliation procedures include the reconciliation of the number of records accepted to the number of records processed to the number of records output. The following additional controls are included in the entity's e-commerce system: • Packing slips are created from the customer sales order and checked by warehouse staff as the order is packed. • Commercial delivery methods are used that reliably meet expected delivery schedules. Vendor performance is monitored and assessed periodically. • Service delivery targets are maintained and actual services provided are monitored against such targets. • The entity uses a feedback questionnaire to confirm customer satisfaction with completion of service or delivery of information to the customer. • Computerized back-order records are maintained and are designed to notify customers of back orders within 24 hours. Customers are given the option to cancel a back order or have an alternate item delivered. • Monitoring tools are used to continuously monitor latency, packet loss, hops, and network performance. • The organization maintains network integrity software and has documented network management policies. • Appropriately documented escalation procedures are in place to initiate corrective actions to unfavorable network performance.
3.3 The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing integrity policies. If the system is an e-commerce system, the entity's procedures include, but are not necessarily limited to, the following matters: • The entity displays sales prices and all other costs and fees to the customer before processing the transaction.	Written procedures exist for the distribution of output reports that conform to the system processing integrity objectives, policies, and standards. Control clerks reconcile control totals of transaction input to output reports daily, on both a system-wide and an individual customer basis. Exceptions are logged, investigated, and resolved. The customer service department logs calls and customer complaints. An analysis of customer calls, complaints, back-order logs, and other transactional analysis and comparison to the entity's processing integrity policies are reviewed at monthly management meetings, and action plans are developed and implemented as necessary.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
• Transactions are billed and electronically settled as agreed. • Billing or settlement errors are promptly corrected.	The following additional controls are included in the entity's e-commerce system: • All costs, including taxes, shipping, and duty costs, and the currency used, are displayed to the customer. Customer accepts the order, by clicking on the "yes" button, before the order is processed. • Customers have the option of printing, before an online order is processed, an "order confirmation" for future verification with payment records (such as credit card statement) detailing information about the order (such as item(s) ordered, sales prices, costs, sales taxes, and shipping charges). • All foreign exchange rates are displayed to the customer before performing a transaction involving foreign currency. • Billing or settlement errors are followed up and corrected within 24 hours of reporting by the customer.
3.4 There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.	Input transactions are date and time stamped by the system and identified with the submitting source (user, terminal, IP address). Each order has a unique identifier that can be used to access order and related shipment and payment settlement information. This information can also be accessed by customer name and dates of order, shipping, or billing. The entity maintains transaction histories for a minimum of 10 years. Order history information is maintained online for three years and is available for immediate access by customer service representatives. After three years, this information is maintained in offline storage. Original source documents are retained on image management systems for a minimum of seven years, to facilitate the retrieval or reconstruction of data as well as to satisfy legal requirements. The entity performs an annual audit of tapes stored at the offsite storage facility. As part of the audit, tapes at the offsite location are matched to the appropriate tape management system.

(continued)

Criteria	*Illustrative Controls*
Security-related criteria relevant to the system's processing integrity	
3.5 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: *a.* Registration and authorization of new users. *b.* Identification and authentication of authorized users. *c.* The process to make changes and updates to user profiles. *d.* The process to grant system access privileges and permissions. *e.* Distribution of output restricted to authorized users. *f.* Restriction of logical access to offline storage, backup data, systems, and media. *g.* Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	*a.* Registration and authorization of new users: • Customers can self-register on the entity's Web site, under a secure session in which they provide new user information and select an appropriate user identification (ID) and password. Privileges and authorizations associated with self-registered customer accounts provide specific limited system functionality. • The ability to create or modify users and user access privileges (other than the limited functionality "customer accounts") is limited to the security administration team. • The line-of-business supervisor authorizes access privilege change requests for employees and contractors. Customer access privileges beyond the default privileges granted during self-registration are approved by the customer account manager. Proper segregation of duties is considered in granting privileges. *b.* Identification and authentication of users: • Users are required to log on to the entity's network and application systems with their user ID and password before access is granted. Unique user IDs are assigned to individual users. Passwords must contain at least six characters, one of which is nonalphanumeric. Passwords are case sensitive and must be updated every 90 days. *c.* Changes and updates to user profiles: • Changes and updates to self-registered customer accounts can be done by the individual user at any time on the entity's Web site after the user has successfully logged onto the system. Changes are reflected immediately. • Unused customer accounts (no activity for six months) are purged by the system. • Changes to other accounts and profiles are restricted to the security administration team and require the approval of the appropriate line-of-business supervisor or customer account manager. • Accounts for terminated employees are deactivated upon notice of termination being received from the human resources team.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	d. The process to grant system access privileges and permissions: • All paths that allow access to significant information resources are controlled by the access control system and operating system facilities. Access requires users to provide their user ID and password. Privileges are granted to authenticated users based on their user profiles. • The login session is terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up.
	e. Distribution of output: • Access to computer processing output is provided to authorized individuals based on the classification of the information. • Processing outputs are stored in an area that reflects the classification of the information.
	f. Restriction of logical access to offline storage, backup data, systems, and media: • Logical access to offline storage, backup data, systems, and media is limited to computer operations staff.
	g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices: • Hardware and operating system configuration tables are restricted to appropriate personnel. • Application software configuration tables are restricted to authorized users and under the control of application change management software. • Utility programs that can read, add, change, or delete data or programs are restricted to authorized technical services staff. Usage is logged and monitored by the manager of computer operations. • The information security team, under the direction of the CIO, maintains access to firewall and other logs, as well as access to any storage media. Any access is logged and reviewed quarterly. • A listing of all master passwords is stored in an encrypted database and an additional copy is maintained in a sealed envelope in the entity safe.

(continued)

Criteria	*Illustrative Controls*
3.6 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, offline storage media, backup media and systems, and other system components such as firewalls, routers, and servers.	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware such as firewalls and routers, is restricted to authorized individuals by card key systems and monitored by video surveillance. Physical access cards are managed by building security staff. Access card usage is logged. Logs are maintained and reviewed by building security staff. Requests for physical access privileges to the entity's computer facilities require the approval of the manager of computer operations. Documented procedures exist for the identification and escalation of potential security breaches. Offsite backup data and media are stored at service provider facilities. Access to offsite data and media requires the approval of the manager of computer operations.
3.7 Procedures exist to protect against unauthorized logical access to the defined system.	Login sessions are terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up by the security administrator. Virtual private networking (VPN) software is used to permit remote access by authorized users. Users are authenticated by the VPN server through specific "client" software and user ID and passwords. Firewalls are used and configured to prevent unauthorized access. Firewall events are logged and reviewed daily by the security administrator. Unneeded network services (for example, telnet, ftp, and http) are deactivated on the entity's servers. A listing of the required and authorized services is maintained by the IT department. This list is reviewed by entity management on a routine basis for its appropriateness for the current operating conditions. Intrusion detection systems are used to provide continuous monitoring of the entity's network and early identification of potential security breaches. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
3.8 Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.	In connection with other security monitoring, the security administration team participates in user groups and subscribes to services relating to computer viruses. Antivirus software is in place, including virus scans of incoming e-mail messages. Virus signatures are updated at least weekly. Any viruses discovered are reported to the security team and an alert is created for all users notifying them of a potential virus threat.
3.9 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.	The entity uses 128-bit secure sockets layer (SSL) encryption for transmission of private or confidential information over public networks, including user ID and password. Users are required to upgrade their browser to the most current version tested and approved for use by the security administration team to avoid possible security problems. Account activity, subsequent to successful login, is encrypted through a 128-bit SSL session. Users are logged out on request (by selecting the "Sign-out" button on the Web site) or after 10 minutes of inactivity.
3.10 Procedures exist to identify, report, and act upon system processing integrity issues and related security breaches and other incidents.	Users are provided instructions for communicating system processing integrity issues and potential security breaches to the IT hotline. Processing integrity issues are escalated to the manager of computer operations. The information security team investigates security-related incidents reported through customer hotlines and e-mail. Production run and automated batch job scheduler logs are reviewed each morning and processing issues are identified, escalated, and resolved. Intrusion detection and other tools are used to identify, log, and report potential security breaches and other incidents. The system notifies the security administration team and/or the network administrator via e-mail and pager of potential incidents in progress. Incident logs are monitored and evaluated by the information security team daily. Documented incident identification and escalation procedures are approved by management.
3.11 Procedures exist to provide that issues of noncompliance with system processing integrity and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	Computer operations team meetings are held each morning to review the previous day's processing. Processing issues are discussed, remedial action is taken, and additional action plans are developed, where necessary, and implemented.

(continued)

Criteria	*Illustrative Controls*
	Standard procedures exist for the review, documentation, escalation, and resolution of system processing problems.
	Entity management routinely evaluates the level of performance it receives from the Internet service provider (ISP) which hosts the entity's Web site. This includes evaluating the security controls the ISP has in place by an independent third party as well as following up with the ISP management on any open items or causes for concern.
	Processing integrity and related security issues are recorded and accumulated in a problem report. Corrective action is noted and monitored by management.
	On a routine basis, processing integrity and related security policies, controls, and procedures are audited by the internal audit department. Results of such examinations are reviewed by management, a response is prepared, and a remediation plan is put in place.
Criteria related to the system components used to achieve the objectives	
3.12 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software related to processing integrity and security are consistent with defined processing integrity and related security policies.	The entity has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology.
	The SDLC methodology includes a framework for assigning ownership of systems and classifying data. Process owners are involved in development of user specifications, solution selection, testing, conversion, and implementation.
	Owners of the information and data classify its sensitivity and determine the level of protection required to maintain an appropriate level of security.
	The security administration team reviews and approves the architecture and design specifications for new systems development and/or acquisition to ensure consistency with the entity's processing integrity and related security objectives, policies, and standards.
	Process owner review, approval of test results, and authorization are required for implementation of changes.
3.13 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting processing integrity and security are qualified to fulfill their responsibilities.	A separate systems quality assurance group reporting to the CIO has been established.
	The entity has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the verified credentials are commensurate with the proposed position. New personnel are offered employment subject to background checks and reference validation. Candidates, including internal transfers, are approved by the line-of-business manager before the employment position is offered. Periodic performance appraisals are performed by employee supervisors and include the assessment and review of professional development activities. Personnel receive training and development in computer operations, system design and development, testing, and security concepts and issues. Procedures are in place to provide alternate personnel for key system processing functions in case of absence or departure.
Maintainability-related criteria applicable to the system's processing integrity	
3.14 Procedures exist to maintain system components, including configurations consistent with the defined system processing integrity and related security policies.	Entity management receives a third-party opinion on the adequacy of security controls, and routinely evaluates the level of performance it receives (in accordance with its contractual service-level agreement) from the service provider that hosts the entity's systems and Web site. The IT department maintains a listing of all software and the respective level, version, and patches that have been applied. Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Staffing, infrastructure, and software requirements are periodically evaluated and resources are allocated consistent with the entity's processing integrity and related security policies. System configurations are tested annually, and evaluated against the entity's processing integrity and security policies and current service-level agreements. An exception report is prepared and remediation plans are developed and tracked. The IT steering committee, which includes representatives from the lines of business and customer support, meets monthly and reviews anticipated, planned, or recommended changes to the entity's processing integrity and related security policies, including the potential impact of legislative changes.

(continued)

Criteria	*Illustrative Controls*
3.15 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	Senior management has implemented a division of roles and responsibilities that segregates incompatible functions. The entity's documented systems development methodology describes the change initiation, software development and maintenance, and testing and approval processes, as well as the standards and controls that are embedded in the processes. These include programming, documentation, and testing standards. Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Changes to system infrastructure and software are developed and tested in a separate development and test environment before implementation into production. As part of the change control policies and procedures, there is a "promotion" process (for example, from "test" to "staging" to "production"). Promotion to production requires the approval of the business owner who sponsored the change and the manager of computer operations. When changes are made to key systems components, there is a "backout" plan developed for use in the event of major interruption(s).
3.16 Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Emergency changes that require deviations from standard procedures are logged and reviewed by IT management daily and reported to the affected line-of-business manager. Permanent corrective measures follow the entity's change management process, including line-of-business approvals.
Availability-related criteria applicable to the system's processing integrity	
3.17 Procedures exist to protect the system against potential risks (for example, environmental risks, natural disasters, and routine operational errors and omissions) that might impair system processing integrity.	A risk assessment is prepared and reviewed on a regular basis or when a significant change occurs in either the internal or external physical environment. Threats such as fire, flood, dust, power failure, excessive heat and humidity, and labor problems have been considered.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	Management maintains measures to protect against environmental factors (for example, fire, dust, power failure, and excessive heat and humidity) based on its risk assessment. The entity's controlled areas are protected against fire using both smoke detectors and a fire suppression system. Water detectors are installed within the raised floor areas.
	The entity site is protected against a disruption in power supply to the processing environment by both uninterruptible power supplies (UPS) and emergency power supplies (EPS). This equipment is tested semiannually.
	Preventive maintenance agreements and scheduled maintenance procedures are in place for key system hardware components.
	Vendor warranty specifications are complied with and tested to determine if the system is properly configured.
	Procedures to address minor processing errors, outages, and destruction of records are documented.
	Procedures exist for the identification, documentation, escalation, resolution, and review of problems.
	Physical and logical security controls are implemented to reduce the opportunity for unauthorized actions that could impair system processing integrity.
3.18 **Procedures exist to provide for restoration and disaster recovery consistent with the entity's defined processing integrity policies.**	Management has implemented a comprehensive strategy for backup and restoration based on a review of business requirements. Backup procedures for the entity are documented and include redundant servers, daily incremental backups of each server, and a complete backup of the entire week's changes on a weekly basis. Daily and weekly backups are stored offsite in accordance with the entity's system policies.
	Disaster recovery and contingency plans are documented.
	The disaster recovery plan defines the roles and responsibilities and identifies the critical information technology application programs, operating systems, personnel, data files, and time frames needed to ensure high availability and system reliability based on the business impact analysis.
	The business continuity planning (BCP) coordinator reviews and updates the business impact analysis with the lines of business annually.

(continued)

Criteria	*Illustrative Controls*
	Disaster recovery and contingency plans are tested annually in accordance with the entity's system policies. Testing results and change recommendations are reported to the entity's management committee. The entity's management committee reviews and approves changes to the disaster recovery plan. All critical personnel identified in the business continuity plan hold current versions of the plan, both onsite and offsite. An electronic version is stored offsite.
3.19 Procedures exist to provide for the completeness, accuracy, and timeliness of backup data and systems.	Automated backup processes include procedures for testing the integrity of the backup data. Backups are performed in accordance with the entity's defined backup strategy, and usability of backups is verified at least annually. Backup systems and data are stored offsite at the facilities of a third-party service provider. Under the terms of its service provider agreement, the entity performs an annual verification of media stored at the offsite storage facility. As part of the verification, media at the offsite location are matched to the appropriate media management system. The storage site is reviewed biannually for physical access security and security of data files and other items. Backup systems and data are tested as part of the annual disaster recovery test.
4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with the defined system processing integrity policies.	
4.1 System processing integrity and security performance is periodically reviewed and compared with the defined system processing integrity and related security policies.	System processing is monitored using system monitoring tools by onsite operations staff 24 hours a day, 7 days a week. Processing logs, performance and security incident statistics, and comparisons to approved targets are reviewed by the operations team daily and are accumulated and reported to the IT steering committee monthly. The customer service group monitors system processing and related customer complaints. It provides a monthly report of such matters together with recommendations for improvement, which are considered and acted on at the monthly IT steering committee meetings.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	The information security team monitors the system and assesses the system vulnerabilities using proprietary and other tools. Potential risk is evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed and implementation is monitored. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. The internal audit function conducts processing integrity and system security reviews as part of its annual audit plan. Results and recommendations for improvement are reported to management.
4.2 There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system processing integrity and related security policies.	System processing is monitored using system monitoring tools by onsite operations staff 24 hours a day, 7 days a week. Processing logs and performance and security incident statistics and comparisons to approved targets are reviewed by the operations team daily and are accumulated and reported to the IT steering committee monthly. Future system processing performance and capacity requirements are projected and analyzed as part of the annual IT planning and budgeting process. Logs are analyzed to identify trends that may have a potential impact on the entity's ability to achieve its system processing integrity and related security objectives. Monthly IT staff meetings are held to address system processing, capacity, and security concerns and trends; findings are discussed at quarterly management meetings.
4.3 Environmental and technological changes are monitored and their impact on system processing integrity and security is assessed on a timely basis.	The entity's data center facilities include climate and environmental monitoring devices. Deviations from optimal performance ranges are escalated and resolved. Senior management, as part of its annual IT planning process, considers developments in technology and the impact of applicable laws or regulations on the entity's processing integrity and related security policies. The entity's customer service group monitors the impact of emerging technologies, customer requirements, and competitive activities.

Online Privacy Principle and Criteria[6]

.25 The *online privacy principle* focuses on protecting the personal information an organization may collect from its customers through its e-commerce systems. Even though the controls an organization may have in place to protect such information may extend beyond its Web-based systems and may even include its service providers, it is not the intent of this principle to address protection of the privacy of all personal information an entity may collect, from all sources. The AICPA and CICA have established a separate task force to consider principles and criteria relevant to enterprise-wide privacy.

.26 E-commerce facilitates the gathering of information from and about individuals and its subsequent exchange with other entities. Some consumers like this because it allows them to receive targeted marketing materials that focus on their needs. On the other hand, many consumers consider such uses of information about them to be an invasion of their privacy. For this reason, it is important that entities inform their customers about the kinds of information that are collected about them, the uses of such information, customer options, and related matters. In addition, many countries have implemented laws and regulations covering the privacy of information obtained through e-commerce.

.27 Privacy can have many aspects, but for purposes of this principle and the corresponding criteria, *privacy* is defined as the rights and obligations of individuals and entities with respect to the collection, use, disclosure, and retention of personal information. *Personal information* is defined as any information relating to an identified or identifiable individual. Such information includes but is not limited to the customer's name; address; telephone number; Social Security, insurance, or other government identification numbers; employer; credit card numbers; personal or family financial information; personal or family medical information; employment history; history of purchases or other transactions; credit records; and similar information. *Sensitive information* is defined as personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offenses or criminal convictions.[7]

.28 It is important for consumers to have confidence that an entity takes appropriate steps to protect personal information. Although it can be relatively easy to establish an e-commerce system, the underlying technology can be complex and can entail a multitude of information protection and related security issues. The privacy of information transmitted over the Internet or other public networks can be compromised relatively easily. Without the use of basic encryption techniques, for example, consumer credit card numbers can be intercepted and stolen during transmission. Without appropriate firewalls and other security practices, personal information residing on an entity's e-commerce computer system can be

---

[6] The *AICPA/CICA Privacy Framework* for protecting personal information can be used by CPAs, both in industry and public practice, to assist the organizations they serve in addressing privacy issues. The *Framework* is broader in scope than AICPA/CICA Trust Services Online Privacy Principle and Criteria, which focused primarily on Web-based electronic commerce online privacy. The *Framework* encompasses any form of collection, use, disclosure, and retention of personal information, including online and offline applications. For Trust Services engagements (including SysTrust and WebTrust) with reporting periods beginning on or after April 1, 2004, the AICPA/CICA Privacy Framework Principle and Criteria are to be used in place of the AICPA/CICA Trust Services Online Privacy Principle and Criteria and will become known as the AICPA/CICA Trust Services Privacy Principle and Criteria. The AICPA/CICA Trust Services Privacy Principle and Criteria are included in Appendix E [paragraph .45] along with parts of the *Framework*. To view the entire *Framework*, go to www.aicpa.org/privacy. Earlier application is encouraged.

[7] This is the meaning of the term as defined by the European Union (EU) directives, and the United States Safe Harbor Privacy Principles, July 21, 2000.

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

intentionally or unintentionally provided to third parties not related to the entity's business.

AICPA/CICA Trust Services Privacy Components and Criteria

.29 The AICPA/CICA Privacy Framework consists of 10 privacy components[8] and related criteria that are essential to the proper protection and management of personal information. These privacy components and criteria are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices. The following are the 10 privacy components:

1. *Management.* The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. *Notice.* The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. *Choice and Consent.* The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. *Collection.* The entity collects personal information only for the purposes identified in the notice.
5. *Use and Retention.* The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes.
6. *Access.* The entity provides individuals with access to their personal information for review and update.
7. *Disclosure to Third Parties.* The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. *Security.* The entity protects personal information against unauthorized access (both physical and logical).
9. *Quality.* The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. *Monitoring and Enforcement.* The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Global Impact of Privacy Criteria

.30 E-commerce by its nature is global. As companies cross international boundaries, they are faced with the challenges of meeting standards and complying with laws regarding privacy. Organizations that wish to tap into the global marketplace without adequate privacy standards and disclosures may face prohibitions or restrictions on how they do business.

.31 Consumers from around the world are concerned about how their information will be used, how it is protected, what process is in place that will allow them to correct erroneous information, and who will have access to this information. Without proper controls and without proper related disclosure, these consumers may choose to do business elsewhere, where there are adequate controls.

---

[8] Although some privacy regulations use the term *principle,* the term *component* is used in the *Framework* to represent that concept since the term principle has been previously defined in the Trust Services literature.

Consumer Recourse

.32 Because of the unique nature of e-commerce, customers are concerned about how their complaints are addressed. If a Web site is unwilling or unable to address a consumer's concerns, what recourse does the consumer have? If the consumer is in one country and the business is in another, how will the consumer's rights be protected? Some governments already require consumer recourse procedures to ensure consumer protection. Traditional dispute resolution through the court system can be time-consuming and expensive.

.33 A third-party dispute mechanism (such as those offered by the National Arbitration Forum) can provide an effective means for consumer recourse. All such mechanisms should conform to the principles of arbitration in Appendix A [paragraph .41], "Consumer Arbitration." For entities in countries that have programs mandated by regulatory bodies, each program would be followed and disclosed on the site's e-commerce systems.

.34 The online privacy criteria require the entity to:

a. Commit to the use of a third-party dispute resolution mechanism that conforms to the principles of arbitration in Appendix A [paragraph .41]. Such third-party dispute resolution may be provided by any organization or governmental function offering such service.

b. Disclose its procedures for consumer recourse for issues not resolved by the entity.[9]

Online Privacy Principle and Criteria Table

.35 Personal information obtained as a result of e-commerce is collected, used, disclosed, and retained as committed or agreed.

Criteria	*Illustrative Controls*
1.0 Policies: The entity defines and documents its policies regarding the protection of personal information obtained as a result of e-commerce.	
1.1 The entity's privacy and related security policies are established and periodically reviewed and approved by a designated individual or group.	The entity's documented systems development and acquisition process includes procedures to identify and document authorized users of the system and their online privacy requirements. User requirements are documented in service-level agreements or other documents. The chief privacy officer (CPO) reviews the entity's privacy and related security policies annually and submits proposed changes as needed for approval by the executive committee.
1.2 The entity's online privacy and related security policies include, but may not be limited to, the following matters: *a.* Identification and documentation of the online privacy and related security requirements of authorized users.	The entity's documented online privacy and related security policies contain the elements set out in criterion 1.2.

[9] In some countries around the world, third-party arbitration is not an accepted means for the handling of consumer complaints. In those countries, the entity should follow customary laws and regulations. Such practices should be disclosed on its e-commerce systems.

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
b. Allowing access, the nature of that access, and who authorizes such access.	
c. Preventing unauthorized access.	
d. The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access.	
e. Assignment of responsibility and accountability for online privacy and related security.	
f. Assignment of responsibility and accountability for system changes and maintenance.	
g. Testing, evaluating, and authorizing system components before implementation.	
h. Addressing how complaints and requests relating to online privacy and related security issues are resolved, and use of a third-party dispute resolution process that conforms to the principles of arbitration. [*See Appendix A (paragraph .41).*]	
i. The procedures to handle online privacy and related security breaches and other incidents.	
j. Provision for allocation for training and other resources to support its online privacy and related system security policies.	
k. Provision for the handling of exceptions and situations not specifically addressed in its online privacy and related system security policies.	
l. Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts.	
m. Providing notice to the customer regarding the information collected.	

(continued)

Criteria	*Illustrative Controls*
n. Providing choice to the customer regarding the type(s) of information gathered and any options the customer has regarding the collection of this information.	
o. Permitting access by the customer to his or her personal information for update and corrective purposes.	
p. Record retention and destruction practices.	
1.3 Responsibility and accountability for the entity's online privacy and related system security policies, and changes and updates to those policies, are assigned.	Management has assigned responsibilities for the maintenance and enforcement of the entity's online privacy and related system security policies to the CPO. Others on the executive committee assist in the review, update, and approval of the policies as outlined in the executive committee handbook. Ownership and custody of significant information resources (for example, data, programs, and transactions) and responsibility for establishing and maintaining the online privacy of and related security over such resources is defined.
2.0 Communications: The entity communicates its defined policies regarding the protection of personal information to internal and external users.	
2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	The entity has posted a system description on its Web site. [*For an example of a system description for an e-commerce system, refer to Appendix B (paragraph .42).*]
2.2 The online privacy and related security obligations of users and the entity's online privacy and related security commitments to users are communicated to authorized users and disclosed on the entity's Web site. These disclosures include, but are not limited to, the following matters: *a.* The specific kinds and sources of information being collected and maintained, the use of that information, and possible third-party distribution of that information.	The entity's disclosed user obligations and privacy and related security commitments contain the elements set out in criterion 2.2. For its internal users (employees and contractors), the entity's policies relating to online privacy and security are reviewed with new employees and contractors as part of their orientation, and the key elements of the policies and their impact on the employee are discussed. New employees must sign a statement signifying that they have read, understand, and will follow these policies. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the entity's policies. Security and privacy obligations of contractors are detailed in their contract.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
If information is provided to third parties, disclosure includes any limitation on the reliance on the third party's privacy practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's privacy practices and controls that meet or exceed those of the entity. Such third parties might include: • Parties who participate in completing the transaction (for example, credit card processors, delivery services, and fulfillment organizations). • Parties not related to the transaction (for example, marketing organizations to whom information is provided).	A privacy awareness program has been implemented to communicate the entity's online privacy and related security policies to employees. The entity publishes its online privacy and related security policies on its corporate intranet.
b. Choices regarding how personal information collected from an individual online may be used and/or distributed. Individuals are given the opportunity to opt out of such use, by either not providing such information or denying its ditribution to parties not involved with the transaction.	
c. Sensitive information needed for the e-commerce transaction. Individuals must opt in before this information is gathered and transmitted.	
d. The consequences, if any, of an individual's refusal to provide information or of an individual's decision to opt out of (or not opt in to) a particular use of such information.	
e. How personal information collected can be reviewed and, if necessary, corrected or removed.	

(continued)

Criteria	*Illustrative Controls*
2.3 If the entity's Web site uses cookies or other tracking methods (for example, Web bugs and middleware), the entity discloses how they are used. If the customer refuses cookies, the consequences, if any, of such refusal are disclosed.	The entity discloses its use of cookies on its Web site.
2.4 The process for obtaining support and informing the entity about breaches of online privacy and systems security is communicated to authorized users.	The process for customers and external users to inform the entity of possible privacy and related security breaches and other incidents is posted on the entity's Web site. The entity's privacy awareness program includes information concerning the identification of possible security breaches and the process for informing the security administration team. Documented procedures exist for the identification and escalation of privacy and security breaches and other incidents.
2.5 The entity discloses its procedures for consumer recourse for issues regarding privacy that are not resolved by the entity. These complaints may relate to collection, use, and distribution of personal information, and the consequences for failure to resolve such complaints. This resolution process has the following attributes: *a.* Management's commitment to use a specified third-party dispute resolution service or other process mandated by regulatory bodies in the event the customer is not satisfied with the entity's proposed resolution of such a complaint together with a commitment from such third party to handle such unresolved complaints. *b.* Procedures to be followed in resolving such complaints, first with the entity and, if necessary, with the designated third party. *c.* What use or other action will be taken with respect to the personal information which is the subject of the complaint until the complaint is satisfactorily resolved.	The entity discloses its consumer recourse procedures on its Web site.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
2.6 The entity discloses any additional privacy practices needed to comply with applicable laws or regulations or any self-regulatory programs in which the entity participates.	The entity discloses additional privacy practices on its Web site.
2.7 In the event that a disclosed online privacy policy is discontinued or changed to be less restrictive, the entity provides clear and conspicuous customer notification of the revised policy.	Changes to the entity's online privacy policies are disclosed on its Web site for a minimum period of three months from the effective date of the change.
2.8 The entity notifies users when they have left the site covered by the entity's online privacy policies.	The entity uses pop-up windows to notify users that they are leaving the site covered by the entity's online privacy policies. Use of pop-up windows for this purpose is disclosed on the entity's Web site.
2.9 Responsibility and accountability for the entity's online privacy and related system security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.	Management has assigned responsibility and accountability for the entity's privacy policies to the CPO. Responsibility and accountability for the entity's security policies is assigned to the chief information officer (CIO). The CPO has custody of and is responsible for the day-to-day maintenance of the entity's online privacy policies, and recommends changes to the management committee.
2.10 Changes that may affect online privacy and system security are communicated to management and users who will be affected.	Changes that may affect customers and users and their online privacy or related security obligations or the entity's online privacy or related security commitments are highlighted on the entity's Web site. Planned changes to system components and the scheduling of those changes are reviewed as part of the monthly information technology (IT) steering committee meetings. Changes to system components that may affect online privacy require the approval of the CPO before implementation. There is periodic communication of changes, including changes that may affect online privacy and system security. Changes that affect online privacy or system security are incorporated into the entity's ongoing privacy and security awareness programs.

(continued)

Criteria	*Illustrative Controls*
3.0 Procedures: The entity uses procedures to achieve its documented privacy objectives in accordance with its defined policies.	
3.1 The entity's procedures provide that personal information is disclosed only to parties essential to the transaction, unless customers are clearly notified before providing such information. If the customer was not clearly notified when he or she submitted the information, customer permission is obtained before such information is released to third parties.	Entity procedures require that customers are given the clear and conspicuous option about sharing their information with other parties not associated with the transaction and that there are controls in place to track those options within the entity's database.
3.2 The entity's procedures provide that personal information obtained as a result of e-commerce is used by employees only in ways associated with the entity's business.	Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits disclosures of information and other data to which the employee has access to other individuals or entities. Appropriate access controls are in place that limit access to sensitive, confidential, or personal information based on job function and need.
3.3 The entity has procedures to edit and validate personal information as it is collected, created, or maintained.	The entity accepts data only from the customer or other reliable sources and uses reliable collection methods. Before completing the transaction, customers are prompted by the system to check the personal data they have entered. Customers have the opportunity to correct any personal data entered before completing the transaction.
3.4 The entity has procedures to obtain assurance or representation that the information protection and privacy policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity's disclosed privacy policies.	The entity outsources technology support or service and transfers data to the outsource provider. The entity obtains representation about the controls that are followed by the outsource provider and obtains a report on the effectiveness of such controls from the outsource provider's independent auditor.
3.5 Customer permission is obtained before downloading files and information to be stored, altered, or copied on a customer's computer. *a.* If the customer has indicated to the entity that it does not want cookies, the entity has controls to ensure that cookies are not stored on the customer's computer.	The entity requests the customer's permission before it intentionally stores, alters, or copies information in the customer's computer. The entity requests the customer's permission before it performs any diagnostic or inventory on the customer's computer. The consumer registration page notifies and requests permission from consumers to use cookies to expedite site registration and logon. Customers are prompted when files are to be downloaded as part of the service.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
b. The entity requests customer permission to store, alter, or copy information (other than cookies) in the customer's computer.	
3.6 In the event that a disclosed privacy practice is discontinued or changed to be less restrictive, the entity has procedures to protect personal information in accordance with the privacy practices in place when such information was collected, or obtains customer consent to follow the new privacy practice with respect to the customer's personal information.	Data collected before and after each privacy policy change are tracked in the entity's database. When changes to a less restrictive policy are made, the entity sends notification of such changes and deletions to affected customers and requests that the customers opt in to the new policy. Customers who do not opt in to the new policy will continue to be protected under the old policy.
Security-related criteria relevant to online privacy	
3.7 Procedures exist to restrict logical access to personal information obtained through e-commerce including, but not limited to, the following matters:	*a.* Registration and authorization of new users: • Customers can self-register on the entity's Web site, under a secure session in which they provide new user information and select an appropriate user identification (ID) and password. Privileges and authorizations associated with self-registered customer accounts provide specific limited system functionality. • The ability to create or modify users and user access privileges (other than the limited functionality "customer accounts") is limited to the security administration team. • The line-of-business supervisor authorizes access privilege change requests for employees and contractors. Customer access privileges beyond the default privileges granted during self-registration are approved by the customer account manager. Proper segregation of duties is considered in granting privileges.
a. Registration and authorization of new users.	
b. Identification and authentication of users.	*b.* Identification and authentication of users: • Users are required to log on to the entity's network and application systems with their user ID and password before access is granted. Unique user IDs are assigned to individual users. Passwords must contain at least six characters, one of which is nonalphanumeric. Passwords are case sensitive and must be updated every 90 days.
c. The process to make changes and updates to user profiles.	
d. The process to grant system access privileges and permissions.	
e. Procedures to prevent customers, groups of individuals, or other entities from accessing other than their own private or sensitive information.	
f. Procedures to limit access to personal information to only authorized employees based upon their assigned roles and responsibilities.	
g. Distribution of output restricted to authorized users.	
h. Restriction of logical access to offline storage, backup data, systems, and media.	

(continued)

Criteria	*Illustrative Controls*
i. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	*c.* Changes and updates to user profiles: • Changes and updates to self-registered customer accounts can be done by the individual user at any time on the entity's Web site after the user has successfully logged onto the system. Changes are reflected immediately. • Unused customer accounts (no activity for six months) are purged by the system. • Changes to other accounts and profiles are restricted to the security administration team and require the approval of the appropriate line-of-business supervisor or customer account manager. • Accounts for terminated employees are deactivated upon notice of termination being received from the human resources team. *d.* The process to grant system access privileges and permissions: • All paths that allow access to significant information resources are controlled by the access control system and operating system facilities. Access requires users to provide their user ID and password. Privileges are granted to authenticated users based on their user profiles. • The login session is terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up. *e.* Restriction of access to information of other customers: • Corporate customers are assigned a unique company identifier that is required as part of the login process. Logical access software is used to restrict user access based on the company identifier used at login. • Individual customers are restricted to their own information based on their unique user ID. *f.* Restriction of access to personal information: • Requests for privileges to access information designated as private require the approval of the assigned data owner.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	g. Distribution of output: • Access to computer processing output is provided to authorized individuals based on the classification of the information. • Processing outputs are stored in an area that reflects the classification of the information.
	h. Restriction of logical access to offline storage, backup data, systems, and media: • Logical access to offline storage, backup data, systems, and media is limited to computer operations staff.
	i. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices: • Hardware and operating system configuration tables are restricted to appropriate personnel. • Application software configuration tables are restricted to authorized users and under the control of application change management software. • Utility programs that can read, add, change, or delete data or programs are restricted to authorized technical services staff. Usage is logged and monitored by the manager of computer operations. • The information security team, under the direction of the CIO, maintains access to firewall and other logs, as well as access to any storage media. Any access is logged and reviewed quarterly. • A listing of all master passwords is stored in an encrypted database and an additional copy is maintained in a sealed envelope in the entity safe.
3.8 Procedures exist to restrict physical access to the components of the entity's system(s) that contain or protect personal information obtained through e-commerce including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware such as firewalls and routers, is restricted to authorized individuals by card key systems and monitored by video surveillance. Physical access cards are managed by building security staff. Access card usage is logged. Logs are maintained and reviewed by building security staff.

(continued)

Criteria	*Illustrative Controls*
	Requests for physical access privileges to the entity's computer facilities require the approval of the manager of computer operations.
	Documented procedures exist for the identification and escalation of potential security breaches.
	Offsite backup data and media are stored at service provider facilities. Access to offsite data and media requires the approval of the manager of computer operations.
3.9 Procedures exist to protect against unauthorized logical access to e-commerce system(s).	Virtual private networking (VPN) software is used to permit remote access by authorized users. Users are authenticated by the VPN server through specific "client" software and user ID and passwords.
	Firewalls are used and configured to prevent unauthorized access. Firewall events are logged and reviewed daily by the security administrator.
	Unneeded network services (for example, telnet, ftp, and http) are deactivated on the entity's servers. A listing of the required and authorized services is maintained by the IT department. This list is reviewed by entity management on a routine basis for its appropriateness for the current operating conditions.
	Intrusion detection systems are used to provide continuous monitoring of the entity's network and early identification of potential security breaches.
	The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
3.10 Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.	In connection with other security monitoring, the security administration team participates in user groups and subscribes to services relating to computer viruses.
	Antivirus software is in place, including virus scans of incoming e-mail messages. Virus signatures are updated at least weekly.
	Any viruses discovered are reported to the security team and an alert is created for all users notifying them of a potential virus threat.
3.11 A minimum of 128-bit encryption or other equivalent security techniques are used to protect transmissions of user authentication and other personal information passed over the Internet or other public networks.	The entity uses 128-bit secure sockets layer (SSL) encryption for transmission of private or confidential information over public networks, including user ID and password. Users are required to upgrade their browser to the most current version tested and approved for use by the security administration team to avoid possible security problems.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	Account activity, subsequent to successful login, is encrypted through a 128-bit SSL session. Users are logged out on request (by selecting the "Sign-out" button on the Web site) or after 10 minutes of inactivity.
	Transmission of private customer information to third-party service providers for processing is done over leased lines.
3.12 Procedures exist to identify, report, and act upon privacy and related security breaches and other incidents.	Customers are directed to an area of the Web site with instructions to enable the customer to contact the incident response hotline by telephoning or to post a message about security breaches or possible online privacy breaches as soon as they become concerned. These customer comments are followed up within 24 hours for evaluation, and a report is issued to the customer and CPO.
	Users are provided instructions for communicating potential security breaches to the information security team. The information security team logs incidents reported through customer hotlines and e-mail.
	Intrusion detection and other tools are used to identify, log, and report potential security breaches and other incidents. The system notifies the security administration team and/or the network administrator via e-mail and pager of potential incidents in progress.
	Incident logs are monitored and evaluated by the information security team daily.
	Documented incident identification and escalation procedures are approved by management.
3.13 Procedures exist to provide that issues of noncompliance with online privacy and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	Privacy and related security breaches or other incidents are reported immediately to the IT security team and the CPO. Corrective action, decided upon in conjunction with the CPO, is noted and monitored by management.
	Security policies, controls, and procedures are audited by the internal audit department as part of its ongoing internal audit plan. Results of such examinations are reviewed by management, a response is prepared, and a remediation plan is put in place.
Criteria related to the system components used to achieve the objectives	
3.14 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software related to online privacy and security are consistent with defined online privacy and related security policies.	The entity has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology.

(continued)

Criteria	*Illustrative Controls*
	The SDLC methodology includes a framework for classifying data, including customer and regulatory privacy requirements. Standard user profiles are established based on privacy requirements and an assessment of the business impact of the loss of security. Users are assigned standard profiles based on needs and functional responsibilities.
	Owners and custodians of personal information collected through the entity's e-commerce systems classify its sensitivity and determine the level of protection required to maintain an appropriate level of privacy.
	The CPO and/or the security administration team reviews and approves the architecture and design specifications for new systems development and/or acquisition to ensure consistency with the entity's online privacy and related security policies.
	Changes to system components that may affect security require the approval of the CPO and/or the security administration team.
	The access control and operating system facilities have been installed, including the implementation of options and parameters, to restrict access in accordance with the entity's online privacy and related security policies.
	The entity contracts with third parties to conduct periodic privacy and security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
	Periodic assessments are conducted by the internal audit team to compare existing online privacy and system security features to documented online privacy and system security policies and to regulatory requirements.
3.15 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting online privacy and security are qualified to fulfill their responsibilities.	The entity has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions.
	Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the verified credentials are commensurate with the proposed position. New personnel are offered employment subject to background checks and reference validation.
	Candidates, including internal transfers, are approved by the line-of-business manager before the employment position is offered.
	Periodic performance appraisals are performed by employee supervisors and include the assessment and review of professional development activities.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	Personnel receive training and development in privacy and system security concepts and issues. Attendance and execution of these programs is monitored by the CPO. Procedures are in place to provide alternate personnel for key privacy and system security functions in case of absence or departure.
Maintainability-related criteria relevant to online privacy	
3.16 Procedures exist to maintain system components, including configurations consistent with the defined online privacy and related security policies.	Entity management receives a third-party opinion on the adequacy of privacy procedures and related security controls, and routinely evaluates the level of performance it receives (in accordance with its contractual service-level agreement) from the service provider that hosts the entity's systems and Web site. The IT department maintains a listing of all software and the respective level, version, and patches that have been applied. Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Staffing, infrastructure, and software requirements are periodically evaluated and resources are allocated consistent with the entity's online privacy and related security policies. System configurations are tested annually, and evaluated against the entity's online privacy and related security policies and current service-level agreements. An exception report is prepared and remediation plans are developed and tracked. The IT steering committee, which includes the CPO, representatives from the lines of business, and customer support, meets monthly and reviews anticipated, planned, or recommended changes to the entity's online privacy and related security policies, including the potential impact of legislative changes.
3.17 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	Senior management has implemented a division of roles and responsibilities that segregates incompatible functions. The entity's documented systems development methodology describes the change initiation, software development and maintenance, and approval processes, as well as the standards and controls that are embedded in the processes. These include programming, documentation, and testing standards. Simulated data is used for software development and testing. Personal information is not used for this purpose.

(continued)

Criteria	*Illustrative Controls*
	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Changes to system infrastructure and software are developed and tested in a separate development and test environment before implementation into production. As part of the change control policies and procedures, there is a "promotion" process (for example, from "test" to "staging" to "production"). Promotion to production requires the approval of the business owner who sponsored the change and the manager of computer operations.
3.18 Procedures exist to require that emergency changes are documented and authorized (including after-the-fact approval).	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Emergency changes that require deviations from standard procedures are logged and reviewed by IT management daily and reported to the affected line-of-business manager. Permanent corrective measures follow the entity's change management process, including line-of-business approvals.
4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with its defined policies regarding the protection of personal information.	
4.1 The entity's privacy and security performance is periodically reviewed and compared with the entity's defined online privacy and related security policies.	The information security team monitors the system and assesses the system vulnerabilities using proprietary and other tools. Potential risk is evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed and implementation is monitored. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. The internal audit function conducts privacy assessment and related security reviews as part of its annual audit plan. Results and recommendations for improvement are reported to management.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
4.2 There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its online privacy and related security policies.	Logs are analyzed to identify trends that may have a potential impact on the entity's ability to achieve its privacy and related system security objectives. Monthly IT staff meetings are held to address privacy and related system security concerns and trends; findings are discussed at quarterly management meetings.
4.3 Environmental and technological changes are monitored and their impact on the entity's online privacy and security is assessed on a timely basis.	The CPO, in conjunction with outside legal counsel, monitors legislative privacy requirements and evolving industry privacy practices in the key markets which the entity serves. Senior management, as part of its annual IT planning process, considers developments in technology and the impact of applicable laws or regulations on the entity's online privacy and related security policies. The entity's customer service group monitors the impact of emerging technologies, customer requirements, and competitive activities.

Confidentiality Principle and Criteria

.36 The *confidentiality principle* focuses on information designated as confidential. Unlike personally identifiable information, which is being defined by regulation in a number of countries worldwide, there is no widely recognized definition of confidential information. In the course of communicating and transacting business, partners often exchange information they require to be maintained on a confidential basis. In most instances, the respective parties wish to ensure that the information they provide is available only to those individuals who need access to complete the transaction or resolution on any questions that arise. To enhance business partner confidence, it is important that the business partner is informed about the entity's confidentiality practices. The entity needs to disclose its practices relating to the manner in which it provides for authorized access to and uses and shares information designated as confidential.

.37 Examples of the kinds of information that may be subject to confidentiality include:

- Transaction details
- Engineering drawings
- Business plans
- Banking information about businesses
- Inventory availability
- Bid or ask prices
- Price lists
- Legal documents

- Client and customer lists
- Revenue by client and industry

.38 Also, unlike personal information, there are no defined rights of access to confidential information to ensure its accuracy and completeness. As a result, interpretations of what is considered to be confidential information can vary significantly from business to business and in most cases are driven by contractual arrangements. As a result, it is important for those engaged or expecting to be engaged in business relationships to understand and to accept what information is to be maintained on a confidential basis and what, if any, rights of access or other expectations an entity might have to update that information to ensure its accuracy and completeness.

.39 Information that is provided to another party is susceptible to unauthorized access during transmission and while it is stored on the other party's computer systems. For example, an unauthorized party may intercept business partner profile information and transaction and settlement instructions while they are being transmitted. Controls such as encryption can be used to protect the confidentiality of this information during transmission, whereas firewalls and rigorous access controls can help protect the information while it is stored on computer systems.

Confidentiality Principle and Criteria Table

.40 Information designated as confidential is protected as committed or agreed.

Criteria	*Illustrative Controls*
1.0 Policies: The entity defines and documents its policies related to the protection of confidential information.	
1.1 The entity's system confidentiality and related security policies are established and periodically reviewed and approved by a designated individual or group.	The entity's documented systems development and acquisition process includes procedures to identify and document authorized users of the system and their confidentiality and related security requirements. User requirements are documented in service-level agreements, nondisclosure agreements, or other documents. The security officer reviews the entity's confidentiality and related security policies annually and proposed changes as needed for the approval by the information technology (IT) standards committee, which includes representation from the customer service department.
1.2 The entity's policies related to the protection of confidential information and security include, but are not limited to, the following matters:	The entity's documented confidentiality and related security policies contain the elements set out in criterion 1.2.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
a. Identification and documentation of the confidentiality and related security requirements of authorized users.	
b. Allowing access, the nature of that access, and who authorizes such access.	
c. Preventing unauthorized access.	
d. The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access.	
e. Assignment of responsibility and accountability for confidentiality and related security.	
f. Assignment of responsibility and accountability for system changes and maintenance.	
g. Testing, evaluating, and authorizing system components before implementation.	
h. Addressing how complaints and requests relating to confidentiality and related security issues are resolved.	
i. The procedures to handle confidentiality and related security breaches and other incidents.	
j. Provision for allocation for training and other resources to support its system confidentiality and related security policies.	
k. Provision for the handling of exceptions and situations not specifically addressed in its system confidentiality and related security policies.	
l. Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts.	

(continued)

Criteria	*Illustrative Controls*
1.3 Responsibility and accountability for the entity's confidentiality and related security policies, and changes and updates to those polices, are assigned.	Management has assigned responsibilities for implementation of the entity's confidentiality policies to the vice president, human resources team. Responsibility for implementation of the entity's security policies has been assigned to the chief information officer (CIO). Others on the executive committee assist in the review, update, and approval of the policies as outlined in the executive committee handbook. Ownership and custody of significant information resources (for example, data, programs, and transactions) and responsibility for establishing and maintaining confidentiality of and related security over such resources is defined.
2.0 Communications: The entity communicates its defined policies related to the protection of confidential information to internal and external users.	
2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	For its e-commerce system, the entity has posted a system description on its Web site. [*For an example of a system description for an e-commerce system, refer to Appendix B (paragraph .42).*] For its non–e-commerce system, the entity has provided a system description to authorized users. [*For an example of a system description for a non–e-commerce based system, refer to Appendix C (paragraph .43).*]
2.2 The confidentiality and related security obligations of users and the entity's confidentiality and related security commitments to users are communicated to authorized users before the confidential information is provided. This communication includes, but is not limited to, the following matters: *a.* How information is designated as confidential and ceases to be confidential. *b.* How access to confidential information is authorized. *c.* How confidential information is used.	The entity's confidentiality and related security commitments and required confidentiality and security obligations of its customers and other external users are posted on the entity's Web site; or the entity's confidentiality policies and practices are outlined in its customer contracts, service-level agreements, vendor contract terms and conditions, and its standard nondisclosure agreement. Signed nondisclosure agreements are required before sharing information designated as confidential with third parties. Customer contracts, service-level agreements, and vendor contracts are negotiated before performance or receipt of service. Changes to the standard confidentiality provisions in these contracts require the approval of executive management.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
d. How confidential information is shared.	For its internal users (employees and contractors), the entity's policies relating to confidentiality and security are reviewed with new employees and contractors as part of their orientation, and the key elements of the policies and their impact on the employee are discussed. New employees must sign a statement signifying that they have read, understand, and will follow these policies. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the entity's security policies. Confidentiality and security obligations of contractors are detailed in their contract.
e. If information is provided to third parties, disclosures include any limitations on reliance on the third party's confidentiality practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's confidentiality practices and controls that meet or exceed those of the entity.	
f. Confidentiality practices needed to comply with applicable laws and regulations.	A security awareness program has been implemented to communicate the entity's confidentiality and security policies to employees. The entity publishes its confidentiality and related security policies on its corporate intranet.
2.3 Responsibility and accountability for the entity's confidentiality and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	The security administration team is responsible for implementing the entity's confidentiality and related security policies under the direction of the CIO. The security administration team has custody of and is responsible for the day-to-day maintenance of the entity's confidentiality and related security policies, and recommends changes to the CIO and the IT steering committee. Confidentiality and related security commitments are reviewed with the customer account managers as part of the annual IT planning process.
2.4 The process for informing the entity about breaches of confidentiality and system security and for submitting complaints is communicated to authorized users.	The process for customers and external users to inform the entity of possible confidentiality or security breaches and other incidents is posted on the entity's Web site and/or is provided as part of the new user welcome kit. The entity's security awareness program includes information concerning the identification of possible confidentiality and security breaches and the process for informing the security administration team. Documented procedures exist for the identification and escalation of possible confidentiality or security breaches and other incidents.

(continued)

Criteria	*Illustrative Controls*
2.5 Changes that may affect confidentiality and system security are communicated to management and users who will be affected.	Changes that may affect customers and users and their confidentiality and related security obligations or the entity's confidentiality and security commitments are highlighted on the entity's Web site. Changes that may affect confidentiality and system security are reviewed and approved by affected customers under the provisions of the standard services agreement before implementation of the proposed change. Planned changes to system components and the scheduling of those changes are reviewed as part of the monthly IT steering committee meetings. Changes to system components, including those that may affect system security, require the approval of the security administrator before implementation. There is periodic communication of changes, including changes that may affect confidentiality and system security. Changes that affect confidentiality or system security are incorporated into the entity's ongoing security awareness program.
3.0 Procedures: The entity uses procedures to achieve its documented confidentiality objectives in accordance with its defined policies.	
3.1 The entity's procedures provide that confidential information is disclosed to parties only in accordance with its defined confidentiality and related security policies.	Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has access. Logical access controls are in place that limit access to confidential information based on job function and need. Requests for access privileges to confidential data require the approval of the data owner. Business partners are subject to nondisclosure agreements (NDAs) or other contractual confidentiality provisions.
3.2 The entity has procedures to obtain assurance or representation that the confidentiality policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity's defined confidentiality and related security policies, and that the third party is in compliance with its policies.	The entity outsources technology support or service and transfers data to an outsource provider. The requirements of the service provider with respect to confidentiality of information provided by the entity are included in the service contract. Legal counsel reviews third-party service contracts to assess conformity of the service provider's confidentiality provisions with the entity's confidentiality policies. The entity obtains representation about the controls that are followed by the outsource provider and obtains a report on the effectiveness of such controls from the outsource provider's independent auditor.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
3.3 In the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive, the entity has procedures to protect confidential information in accordance with the confidentiality practices in place when such information was received, or obtains customer consent to follow the new confidentiality practice with respect to the customer's confidential information.	Changes to confidentiality provisions in business partner contracts are renegotiated with the business partner. When changes to a less restrictive policy are made, the entity attempts to obtain the agreement of its customers to the new policy. Confidential information for those customers who do not agree to the new policy is either removed from the system and destroyed or isolated and receives continued protection under the old policy.

Security-related criteria relevant to confidentiality

3.4 Procedures exist to restrict logical access to confidential information including, but not limited to, the following matters: *a.* Registration and authorization of new users. *b.* Identification and authentication of all users. *c.* The process to make changes and updates to user profiles. *d.* The process to grant system access privileges and permissions. *e.* Procedures to prevent customers, groups of individuals, or other entities from accessing other than their own confidential information. *f.* Procedures to limit access to confidential information to only authorized employees based upon their assigned roles and responsibilities. *g.* Distribution of output containing confidential information restricted to authorized users. *h.* Restriction of logical access to offline storage, backup data, systems, and media.	*a.* Registration and authorization of new users: • Customers can self-register on the entity's Web site, under a secure session in which they provide new user information and select an appropriate user identification (ID) and password. Privileges and authorizations associated with self-registered customer accounts provide specific limited system functionality. • The ability to create or modify users and user access privileges (other than the limited functionality "customer accounts") is limited to the security administration team. • The line-of-business supervisor authorizes access privilege change requests for employees and contractors. Customer access privileges beyond the default privileges granted during self-registration are approved by the customer account manager. Confidentiality and proper segregation of duties are considered in granting privileges. *b.* Identification and authentication of users: • Users are required to log on to the entity's network and application systems with their user ID and password before access is granted. Unique user IDs are assigned to individual users. Passwords must contain at least six characters, one of which is nonalphanumeric. Passwords are case sensitive and must be updated every 90 days.

(continued)

Criteria	*Illustrative Controls*
i. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	*c.* Changes and updates to user profiles: • Changes and updates to self-registered customer accounts can be done by the individual user at any time on the entity's Web site after the user has successfully logged onto the system. Changes are reflected immediately. • Unused customer accounts (no activity for six months) are purged by the system. • Changes to other accounts and profiles are restricted to the security administration team and require the approval of the appropriate line-of-business supervisor or customer account manager. • Accounts for terminated employees are deactivated upon notice of termination being received from the human resources team. *d.* The process to grant system access privileges and permissions: • All paths that allow access to significant information resources are controlled by the access control system and operating system facilities. Access requires users to provide their user ID and password. Privileges are granted to authenticated users based on their user profiles. • The login session is terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up. *e.* Restriction of access to information of other customers: • Corporate customers are assigned a unique company identifier that is required as part of the login process. Logical access software is used to restrict user access based on the company identifier used at login. • Individual customers are restricted to their own information based on their unique user ID. *f.* Restriction of access to confidential information: • Requests for privileges to access confidential customer information require the approval of the customer account manager.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	• Simulated customer data is used for system development and testing purposes. Confidential customer information is not used for this purpose. *g.* Distribution of output: • Access to computer processing output is provided to authorized individuals based on the classification of the information. • Processing outputs are stored in an area that reflects the classification of the information. *h.* Restriction of logical access to offline storage, backup data, systems, and media: • Logical access to offline storage, backup data, systems, and media is limited to computer operations staff. *i.* Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices: • Hardware and operating system configuration tables are restricted to appropriate personnel. • Application software configuration tables are restricted to authorized users and under the control of application change management software. • Utility programs that can read, add, change, or delete data or programs are restricted to authorized technical services staff. Usage is logged and monitored by the manager of computer operations. • The information security team, under the direction of the CIO, maintains access to firewall and other logs, as well as access to any storage media. Any access is logged and reviewed quarterly. • A listing of all master passwords is stored in an encrypted database and an additional copy is maintained in a sealed envelope in the entity safe.
3.5 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware such as firewalls and routers, is restricted to authorized individuals by card key systems and monitored by video surveillance.

(continued)

Criteria	*Illustrative Controls*
	Physical access cards are managed by building security staff. Access card usage is logged. Logs are maintained and reviewed by building security staff.
	Requests for physical access privileges to the entity's computer facilities require the approval of the manager of computer operations.
	Documented procedures exist for the identification and escalation of potential security breaches.
	Offsite backup data and media are stored at service provider facilities. Access to offsite data and media requires the approval of the manager of computer operations.
3.6 Procedures exist to protect against unauthorized logical access to the defined system.	Login sessions are terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up by the security administrator.
	Virtual private networking (VPN) software is used to permit remote access by authorized users. Users are authenticated by the VPN server through specific "client" software and user ID and passwords.
	Firewalls are used and configured to prevent unauthorized access. Firewall events are logged and reviewed daily by the security administrator.
	Unneeded network services (for example, telnet, ftp, and http) are deactivated on the entity's servers. A listing of the required and authorized services is maintained by the IT department. This list is reviewed by entity management on a routine basis for its appropriateness for the current operating conditions.
	Intrusion detection systems are used to provide continuous monitoring of the entity's network and early identification of potential security breaches.
	The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
3.7 Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.	In connection with other security monitoring, the security administration team participates in user groups and subscribes to services relating to computer viruses.
	Antivirus software is in place, including virus scans of incoming e-mail messages. Virus signatures are updated at least weekly.
	Any viruses discovered are reported to the security team and an alert is created for all users notifying them of a potential virus threat.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
3.8 A minimum of 128-bit encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks.	The entity uses 128-bit secure sockets layer (SSL) encryption for transmission of private or confidential information over public networks, including user ID and password. Users are required to upgrade their browser to the most current version tested and approved for use by the security administration team to avoid possible security problems. Account activity, subsequent to successful login, is encrypted through a 128-bit SSL session. Users are logged out on request (by selecting the "Sign-out" button on the Web site) or after 10 minutes of inactivity. Confidential information submitted to the entity over its trading partner extranet is encrypted using 128-bit SSL. Transmission of confidential customer information to third-party service providers is done over leased lines.
3.9 Procedures exist to identify, report, and act upon confidentiality and security breaches and other incidents.	Users are provided instructions for communicating potential confidentiality and security breaches to the information security team. The information security team logs incidents reported through customer hotlines and e-mail. Intrusion detection and other tools are used to identify, log, and report potential security breaches and other incidents. The system notifies the security administration team and/or the network administrator via e-mail and pager of potential incidents in progress. Incident logs are monitored and evaluated by the information security team daily. Documented incident identification and escalation procedures are approved by management.
3.10 Procedures exist to provide that issues of noncompliance with defined confidentiality and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	Security and confidentiality problems are reported immediately to the customer account manager, recorded, and accumulated in a problem report. Corrective action, decided upon in conjunction with the customer account manager, is noted and monitored by management. The vice president, customer services is responsible for assessing the customer service impact of potential confidentiality breaches and coordinating response activities. On a routine basis, security policies, controls, and procedures are audited by the internal audit department. Results of such examinations are reviewed by management, a response is prepared, and a remediation plan is put in place.

(continued)

Criteria	*Illustrative Controls*
Criteria related to the system components used to achieve the objectives	
3.11 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software related to confidentiality and security are consistent with defined confidentiality and related security policies.	The entity has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology. The SDLC methodology includes a framework for classifying data, including customer confidentiality requirements. Standard user profiles are established based on customer confidentiality requirements and an assessment of the business impact of the loss of security. Users are assigned standard profiles based on needs and functional responsibilities. Internal information is assigned to an owner based on its classification and use. Customer account managers are assigned as custodians of customer data. Owners of internal information and custodians of customer information and data classify its sensitivity and determine the level of protection required to maintain an appropriate level of confidentiality and security. The security administration team reviews and approves the architecture and design specifications for new systems development and/or acquisition to ensure consistency with the entity's confidentiality and related security policies. Changes to system components that may affect security require the approval of the security administration team. The access control and operating system facilities have been installed, including the implementation of options and parameters, to restrict access in accordance with the entity's confidentiality and related security policies. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
3.12 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting confidentiality and security are qualified to fulfill their responsibilities.	The entity has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions. Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the verified credentials are commensurate with the proposed position. New personnel are offered employment subject to background checks and reference validation.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
	Candidates, including internal transfers, are approved by the line-of-business manager before the employment position is offered.
	Periodic performance appraisals are performed by employee supervisors and include the assessment and review of professional development activities.
	Personnel receive training and development in systems confidentiality and security concepts and issues.
	Procedures are in place to provide alternate personnel for key system confidentiality and security functions in case of absence or departure.
Maintainability-related criteria relevant to confidentiality	
3.13 Procedures exist to maintain system components, including configurations consistent with the defined system confidentiality and related security policies.	Entity management receives a third-party opinion on the adequacy of security controls, and routinely evaluates the level of performance it receives (in accordance with its contractual service-level agreement) from the service provider that hosts the entity's systems and Web site.
	The IT department maintains a listing of all software and the respective level, version, and patches that have been applied.
	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests.
	Staffing, infrastructure, and software requirements are periodically evaluated and resources are allocated consistent with the entity's confidentiality and related security policies.
	System configurations are tested annually, and evaluated against the entity's security policies and current service-level agreements. An exception report is prepared and remediation plans are developed and tracked.
	The IT steering committee, which includes representatives from the lines of business and customer support, meets monthly and reviews anticipated, planned, or recommended changes to the entity's confidentiality and related security policies, including the potential impact of legislative changes.

(continued)

Criteria	*Illustrative Controls*
3.14 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	Senior management has implemented a division of roles and responsibilities that segregates incompatible functions. The entity's documented systems development methodology describes the change initiation, software development and maintenance, and approval processes, as well as the standards and controls that are embedded in the processes. These include programming, documentation, and testing standards. Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation into production. As part of the change control policies and procedures, there is a "promotion" process (for example, from "test" to "staging" to "production"). Promotion to production requires the approval of the business owner who sponsored the change and the manager of computer operations. When changes are made to key systems components, there is a "backout" plan developed for use in the event of major interruption(s).
3.15 Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Emergency changes that require deviations from standard procedures are logged and reviewed by IT management daily and reported to the affected line-of-business manager. Permanent corrective measures follow the entity's change management process, including line-of-business approvals.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls*
4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with its defined confidentiality policies.	
4.1 The entity's confidentiality and security performance is periodically reviewed and compared with the defined confidentiality and related security policies.	The information security team monitors the system and assesses the system's vulnerabilities using proprietary and other tools. Potential risk is evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed and implementation is monitored. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. The internal audit function conducts system security reviews as part of its annual audit plan. Results and recommendations for improvement are reported to management.
4.2 There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its confidentiality and related security policies.	Logs are analyzed to identify trends that may have a potential impact on the entity's ability to achieve its system confidentiality and related security objectives. Monthly IT staff meetings are held to address system security concerns and trends; findings are discussed at quarterly management meetings.
4.3 Environmental and technological changes are monitored and their impact on confidentiality and security is assessed on a timely basis.	Trends and emerging technologies and their potential impact on customer confidentiality requirements are reviewed with corporate customers as part of the annual performance review meeting. Senior management, as part of its annual IT planning process, considers developments in technology and the impact of applicable laws or regulations on the entity's confidentiality and related security policies. The entity's customer service group monitors the impact of emerging technologies, customer requirements, and competitive activities.

.41

Appendix A

Consumer Arbitration

This appendix applies to engagements that use an arbitration program. Should a program mandated by a regulatory body be in effect, that program would be followed and disclosed. This appendix provides additional information about the arbitration process.

Before arbitration can take place, two parties must agree to it. An agreement may take many forms other than a written contract. Both parties show their agreement by some reasonable, affirmative act. An organization's Web site may invite acceptance by conduct, such as a check box or other means, and may propose limitations on the kind of conduct that constitutes acceptance. For example, consumers may find the following language at a Web site, which would constitute acceptance of an agreement:

> By accessing this Web site or ordering products described on this site, you agree to be bound by certain terms and conditions. Please read these terms and conditions carefully.

The terms and conditions would elaborate on arbitration, consumer recourse, and other issues for both the consumer and the Web site.

Principles of Arbitration

Under the model adopted for Trust Services, arbitration must be based on the rules of law, applied consistently. Outlined below, as an example, are the 12 principles identified by the National Arbitration Forum (NAF).

1. *Fundamentally fair process.* All parties in an arbitration process are entitled to fundamental fairness.
2. *Access to information.* Information about arbitration should be reasonably accessible before the parties commit to an arbitration contract.
3. *Competent and impartial arbitrators.* The arbitrators should be both skilled and neutral.
4. *Independent administration.* An arbitration should be administered by someone other than the arbitrator or the parties themselves.
5. *Contracts for dispute resolution.* An agreement to resolve disputes through arbitration is a contract and should conform to the legal principles of contract and statutory law. Arbitration contracts drafted by a fiduciary party should be accompanied by an accurate explanation of the advantages and disadvantages of arbitration.
6. *Reasonable costs.* The cost of an arbitration should be proportionate to the claim and reasonably within the means of the parties, as required by applicable law.
7. *Reasonable time limits.* A dispute should be resolved with reasonable promptness.
8. *Right to representation.* All parties have the right to be represented in an arbitration, if they wish, for example, by an attorney or other representative.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

9. *Settlement and mediation.* The preferable process is for the parties themselves to resolve the dispute.
10. *Hearings.* Hearings should be convenient, efficient, and fair for all.
11. *Reasonable discovery.* The parties should have access to the information they need to make a reasonable presentation of their case to the arbitrator.
12. *Award and remedies.* The remedies resulting from arbitration must conform to the law.

Appendix B

Illustrative Disclosures for E-Commerce Systems

This appendix sets out illustrative disclosures for electronic commerce (e-commerce) systems that are required to meet the Trust Services principles. The disclosures are set out separately by Trust Services principles; they are illustrative only and should be tailored according to the particular organization's system.

System Description

Rather than addressing the components of a system (used for describing non–e-commerce systems), an organization may describe the functionality of the system covered by the WebTrust examination, as follows:

> Example System Description
>
> Our site (abc-xyz.org) enables users to create and manage their own online store (myABC-xyz.org). It also covers the back-end fulfillment and settlement systems that integrate with abc-xyx.org to facilitate ordering from customer sites created on our site and the use of third-party service providers with which we have contracted to provide various services related to our site.
>
> Entrepreneurs and small business owners can use the abc-xyz.org suite of business services to take advantage of the online world. abc-xyz.org's Web browser interface can be used to create your own online store (complete with product ordering). You design the site and control the customer experience.
>
> The WebTrust seal covers the functionality set out in our abc-xyz.org site that allows users to create and manage their own online store. It also covers the back-end fulfillment and settlement systems that integrate with abc-xyz.org to facilitate ordering from customer sites created on abc-xyz.org, myABC-xyz.org—e-commerce and Web publishing made easy. Entrepreneurs and small business owners can use the abc-xyz.org suite of business services to take advantage of the convenience, reach, and speed of the online world. myABC-xyz.org's simple Web browser interface can be used to create your own online store (complete with secure ordering) within minutes. You design the site, control the customer experience, list the products, and fulfill orders in a secure environment.

Disclosures Related to Specific Principles and Criteria

The following tables set out illustrative disclosures for e-commerce systems.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Security

Criteria Reference	*Illustrative Disclosures*
2.2 The security obligations of users and the entity's security commitments to users are communicated to authorized users.	Even though we strive to protect the information you provide through ABC.com, no data transmission over the Internet can be guaranteed to be 100 percent secure. As a result, even though we strive to protect your information, we cannot ensure or warrant the security of any information you transmit to or receive from us through our Web site and online services. We review our security policies on a regular basis, and changes are made as necessary. They undergo an intense review on an annual basis by the information technology (IT) department. These defined security policies detail access privileges, information collection needs, accountability, and other such matters. Documented system security objectives, policies, and standards are consistent with system security requirements defined in contractual, legal, and other service-level agreements. For example, only a select group of authorized individuals within ABC have access to user information. A complete policy with details regarding access, scripting, updates, and remote access is available for review by qualified personnel within the organization. This document is not available to the general public for study. ABC.com operates secure data networks that are password-protected and are not available to the public. When transmitting information between you and ABC.com, data security is handled through a security protocol called secured sockets layer (SSL). SSL is an Internet security standard using data encryption and Web server authentication. Encryption strength is measured by the length of the key used to encrypt the data; that is, the longer the key, the more effective the encryption. Using the SSL protocol, data transmission between you and the ABC.com server is performed at a 128-bit level of encryption strength.
2.4 The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users.	Should you feel that there has been a breach to the security of this site, please contact us *immediately* at (800) 123-1234.
2.5 Changes that may affect system security are communicated to management and users who will be affected.	Any changes that affect the security of our Web site as it affects you as a site user will be communicated to you by posting the highlight of the change to the Web page that summarizes our security policies and significant controls.

Availability

Criteria Reference	*Illustrative Disclosures*
2.2 The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.	To allow sufficient time for file maintenance and backup, the maximum number of hours per day that our network will be made available is 22 hours per day, 7 days a week. In the event of a disaster or other prolonged service interruption, the entity has arranged for the use of alternative service sites to allow for full business resumption within 24 hours. Our company's defined security policies detail access privileges, information collection needs, accountability, and other such matters. They are reviewed and updated at quarterly management meetings and undergo an intense review on an annual basis by the information technology (IT) department. Documented system security objectives, policies, and standards are consistent with system security requirements defined in contractual, legal, and other service-level agreements. For example, current policy prohibits shared identifications (IDs); each support person has his or her own unique ID to log on and maintain network equipment. A complete policy with details regarding access, scripting, updates, and remote access is available for review by qualified personnel. This document will not be released to the general public for study.
2.4 The process for informing the entity about system availability issues and breaches of system security and for submitting complaints is communicated to authorized users.	Management has in place a consumer hotline to allow customers to telephone in any comments, complaints, or concerns regarding the security of the site and availability of the system. If you are unable to obtain access to this site, please contact our customer support personnel at (800) 123-2345. Should you believe that there has been a breach to the security of this site please contact us *immediately* at (800) 123-1234.
2.5 Changes that may affect system availability and system security are communicated to management and users who will be affected.	Highlights of any changes that affect the security of our Web site and availability of the system as it affects you as a site user will be communicated to you by e-mail seven days in advance of the anticipated change. The highlights of the change will be posted to the Web page that summarizes our availability and security policies.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Processing Integrity

Criteria Reference	*Illustrative Disclosures*
2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users. If the system is an e-commerce system, additional information provided on its Web-site includes, but may not be limited to, the following matters: *a.* Descriptive information about the nature of the goods or services that will be provided, including, where appropriate: • Condition of goods (meaning, whether they are new, used, or reconditioned). • Description of services (or service contract). • Sources of information (meaning, where it was obtained and how it was compiled). *b.* The terms and conditions by which it conducts its e-commerce transactions including, but not limited to, the following matters: • Time frame for completion of transactions (*transaction* means fulfillment of orders where goods are being sold and delivery of service where a service is being provided). • Time frame and process for informing customers of exceptions to normal processing of orders or service requests. • Normal method of delivery of goods or services, including customer options, where applicable.	You can purchase new and used books on our site; used books are clearly labeled as such. The mortgage rate information we obtain for your brokerage transaction is gathered from 12 different lending institutions on a daily basis. A complete listing of these lending institutions can be obtained by clicking here [*insert hot link / URL*]. ABC's Online RFQ Brokerage is the online clearing house for requests for quotes (RFQ) on custom-made parts. Through our unique service, OEM manufacturers looking for parts will be connected to contract manufacturers looking for work. RFQs published on our online brokerage undergo an intensive review process to ensure that contract manufacturers get all the information needed to compose a quote. ABC's trained personnel will work closely with OEM manufacturers new to the outsourcing market to ease their fears. Contract manufacturers participating in the RFQ bidding process are members of ABC's BizTrust program. New members are subjected to an assortment of checks such as credit checks and reference checks to ensure that they are qualified to bid on RFQs. The results from these checks are organized into an easy-to-read BizTrust Report accessible by all members of ABC. The nationwide survey, conducted by the compensation-research firm of Dowden & Co., presents data on 20X2 compensation gathered from among more than 900 employers of information systems professionals, including corporations of all sizes, in every industry group, and from every U.S. region. The survey was completed July 20X1. Our policy is to ship orders within one week of receipt of a customer-approved order. Our experience is that over 90 percent of our orders are shipped within 48 hours; the remainder is shipped within one week. We will notify you by e-mail within 24 hours if we cannot fulfill your order as specified at the time you placed it and will provide you the option of canceling the order without further obligation. You will not be billed until the order is shipped. You have the option of downloading the requested information now or we will send it to you on CD-ROM by UPS two-day or Federal Express overnight delivery.

(continued)

Criteria Reference	*Illustrative Disclosures*
• Payment terms, including customer options, if any.	Credit approval is required before shipment. All goods will be invoiced on shipment according to either our normal terms of settlement (net 30 days), or where alternative contractual arrangements are in place, those arrangements shall prevail.
• Electronic settlement practices and related charges to customers.	We require an electronic funds transfer of fees and costs at the end of the transaction. For new customers, a deposit may be required.
• How customers may cancel recurring charges, if any.	To cancel your monthly service fee, send us an e-mail at Subscriber@ABC.com or call us at (800) 555-1212. Be sure to include your account number.
• Product return policies and limited liability, where applicable.	Purchases can be returned for a full refund within 30 days of receipt of shipment. Call our toll-free number or e-mail us for a return authorization number, which should be written clearly on the outside of the return package.
c. Where customers can obtain warranty, repair service, and support related to the goods and services purchased on its Web site.	Warranty and other service can be obtained at any one of our 249 locations worldwide that are listed on this Web site. A list of these locations is also provided with delivery of all of our products.
d. Procedures for resolution of issues regarding processing integrity. These may relate to any part of a customer's e-commerce transaction, including complaints related to the quality of services and products, accuracy, completeness, and the consequences for failure to resolve such complaints.	Transactions at this site are covered by binding arbitration conducted through our designated arbitrator [*name of arbitrator*]. They can be reached at www.name.org or by calling toll-free (800) 111-2222. For the details of the terms and conditions of arbitration, click here [*insert hot link / URL*].
	Our process for consumer dispute resolution requires that you contact our customer toll-free hotline at (800) 555-1234 or contact us via e-mail at custhelp@ourcompany.com. If your problem has not been resolved to your satisfaction you may contact the Cyber Complaint Dispute Resolution Association, which can be reached at (877) 123-4321 during normal business hours (8:00 a.m. – 5:00 p.m. central time) or via their Web site at www.ccomplaint.com.
	For the details of the terms and conditions of arbitration, click here [*insert hot link / URL*].
	For transactions at this site, should you, our customer, require follow-up or response to your questions or complaints, you may contact us at www.xxxquestions.org. If your follow-up or your complaint is not handled to your satisfaction, you should contact the e-commerce ombudsman who handles consumer complaints for e-commerce in this country. He or she can be reached at www.ecommercombud.org or by calling toll-free at (800) XXX-XXXX.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria Reference	*Illustrative Disclosures*
2.2 The processing integrity and related security obligations of users and the entity's processing integrity and related security commitments to users are communicated to authorized users.	Our company's defined processing integrity policies and related security policies are communicated to all authorized users of the company. The security policies detail access privileges, information collection needs, accountability, and other such matters. They are reviewed and updated at quarterly management meetings and undergo an intense review on an annual basis by the information technology (IT) department. Documented system security objectives, policies, and standards are consistent with system security requirements defined in contractual, legal, and other service-level agreements. For example, current policy prohibits shared identifications (IDs); each support person has his or her own unique ID to log on and maintain network equipment. A complete policy with details regarding access, scripting, updates, and remote access is available for review by qualified personnel. This document will not be released to the general public for study.
2.4 The process for obtaining support and informing the entity about system processing integrity issues, errors and omissions, and breaches of systems security and for submitting complaints is communicated to authorized users.	For service and other information, contact one of our customer service representatives at (800) 555-1212 between 7:00 a.m. and 8:00 p.m. (central standard time) or you can write to us as follows: Customer Service Department ABC Company 1234 Anystreet Anytown, Illinois 60000 or CustServ@ABC.com Should you believe that there has been a breach to the integrity or security of this site, please contact us *immediately* at (800) 123-1234.
2.5 Changes that may affect system processing integrity and system security are communicated to management and users who will be affected.	Highlights of any changes that affect the security of our Web site and processing integrity of the system as it affects you as a site user will be communicated to you by e-mail seven days in advance of the anticipated change. The highlights of the change will be posted to the Web page that summarizes our processing integrity and security policies.

Online Privacy

Criteria Reference	*Illustrative Disclosures*
2.2 The online privacy and related security obligations of users and the entity's online privacy and related security commitments to users are communicated to authorized users and disclosed on the entity's Web site. These disclosures include, but are not limited to, the following matters: *a.* The specific kinds and sources of information being collected and maintained, the use of that information, and possible third-party distribution of that information. If information is provided to third parties, disclosure includes any limitation on the reliance on the third party's privacy practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's privacy practices and controls that meet or exceed those of the entity. Such third parties might include: • Parties who participate in completing the transaction (for example, credit card processors, delivery services, and fulfillment organizations). • Parties not related to the transaction (for example, marketing organizations to whom information is provided).	We will need certain information—such as name, Internet address or screen name, billing address, type of computer, and credit card number—to provide our service to you. Your e-mail address is used to send information about our company. Your credit card number is used for billing purposes for the products you order. We may also use this information, along with information such as your age, income level, and postal code, to keep you informed about additional products and services from our company, and to send promotional material that may be of interest to you from some of our partners. Your age, income level, and postal code are also used to tailor the content displayed to correspond to your preferences. We do not provide information gathered from you to any other third parties except as required by law.
b. Choices regarding how personal information collected from an individual online may be used and/or distributed. Individuals are given the opportunity to opt out of such use, by either not providing such information or denying its distribution to parties not involved with the transaction.	You can choose not to receive information and promotional material from us and/or our partners by letting us know on the registration screen when you sign up for the product or service. If you subsequently wish to change your preference to opt in or opt out, go to the xxx screen, or send an e-mail to xxx@domain.com with the message opt in or opt out in the subscribe field.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria Reference	*Illustrative Disclosures*
c. Sensitive information needed for the e-commerce transaction. Individuals must opt in before this information is gathered and transmitted.	Before we can process your insurance application, we require that you click here [*insert hot link / URL*] to give us your permission to submit your medical history to the various insurance companies we use. This is your explicit permission for us to process your request. If you do not wish to have this information transmitted, we will be unable to process your application. You may call our customer service department for additional information or assistance.
d. The consequences, if any, of an individual's refusal to provide information or of an individual's decision to opt out of (or not opt in to) a particular use of such information.	The minimum information you need to provide to complete the transaction is highlighted on the Web page. You will be unable to place an order without providing this minimum information.
e. How personal information collected can be reviewed and, if necessary, corrected or removed.	This site provides you with the ability to correct, update, or remove your information by e-mailing CustServ@ABC.com.
2.3 If the entity's Web site uses cookies or other tracking methods (for example, Web bugs and middleware), the entity discloses how they are used. If the customer refuses cookies, the consequences, if any, of such refusal are disclosed.	Cookies are used to personalize Web content and suggest items of potential interest based on your previous buying habits. This cookie can be read only by us. If you do not accept this cookie, you may be asked to re-enter your name and account number several times during a visit to our Web site or if you return to the site later. By accepting a cookie, certain information [*disclose information*] will be tracked and used for marketing purposes. Our cookies expire in 30 days. Certain advertisers on our site use tracking methods, including cookies, to analyze patterns and paths through this site. To opt out of this practice, refer to their privacy policy at www.domain.com/privacy/opt-out.html.
2.4 The process for obtaining support and informing the entity about breaches of online privacy and systems security is communicated to authorized users.	Should you feel that there has been a breach to the security of this site, please contact us *immediately* at (800) 123-1234. If you have any questions about our organization or our policies on privacy as stated at this site, please contact CustServ@ABC.com. Access to your customer data file is made available to our customer support representatives to fully service your inquiries. After hours, our customer support inquiries are managed by our service provider xxx, who is contractually required to comply with our privacy policy.

(continued)

Criteria Reference	*Illustrative Disclosures*
2.5 The entity discloses its procedures for consumer recourse for issues regarding privacy that are not resolved by the entity. These complaints may relate to collection, use, and distribution of personal information, and the consequences for failure to resolve such complaints. This resolution process has the following attributes: *a.* Management's commitment to use a specified third-party dispute resolution service or other process mandated by regulatory bodies in the event the customer is not satisfied with the entity's proposed resolution of such a complaint together with a commitment from such third party to handle such unresolved complaints. *b.* Procedures to be followed in resolving such complaints, first with the entity and, if necessary, with the designated third party. *c.* What use or other action will be taken with respect to the personal information which is the subject of the complaint until the complaint is satisfactorily resolved.	Transactions at this site, with respect to privacy, are covered by binding arbitration conducted through our designated arbitrator [*name of arbitrator*]. They can be reached at www.name.org or by calling toll-free (800) 111-2222. For the details of the terms and conditions of arbitration, click here [*insert hot link / URL*]. For transactions at this site with respect to privacy, should you, our customer, require follow-up or response to your questions or complaints, you may contact us at www.xxxquestions.org. If your follow-up or your complaint is not handled to your satisfaction, then you should contact the e-commerce ombudsman who handles consumer complaints for e-commerce in this country. He or she can be reached at www.ecommercombud.org or by calling toll-free at (800) XXX-XXXX.
2.6 The entity discloses any additional privacy practices needed to comply with applicable laws or regulations or any self-regulatory programs in which the entity participates.	Federal law requires that all personal information be removed from the system after three years of inactivity.
2.7 In the event that a disclosed online privacy policy is discontinued or changed to be less restrictive, the entity provides clear and conspicuous customer notification of the revised policy.	During the period from May 31 to August 31, 20XX, we collected customer telephone numbers. Starting September 1, we no longer require this information for the processing of your transaction. On September 30, 20XX, we were acquired by XYZ Co. Accordingly, we adopted the privacy policies of XYZ Co., which allow the distribution of collected personal information to third parties. Because our previous policy did not allow for the distribution of such personal information, we will obtain your permission before the distribution of such information collected before September 30, 20XX.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria Reference	*Illustrative Disclosures*
2.8 The entity notifies users when they have left the site covered by the entity's online privacy policies.	Many of our partners have pages that look and navigate like our site. We will notify you via a one-time pop-up window to let you know that you are leaving our site and are no longer covered by our privacy practices. We strive to protect your information and suggest that you read the privacy policies of the site to which you are redirected *before* supplying any personal information. In accordance with our privacy policy we will not pass any information to these sites without your express consent.
2.10 Changes that may affect online privacy and system security are communicated to management and users who will be affected.	Highlights of any changes that affect the security of our Web site and online privacy as it affects you as a site user will be communicated to you by e-mail seven days in advance of the anticipated change. The highlights of the change will be posted to the Web page that summarizes our online privacy and security policies.

Confidentiality

Criteria Reference	Illustrative Disclosures
2.2 The confidentiality and related security obligations of users and the entity's confidentiality and related security commitments to users are communicated to authorized users before the confidential information is provided. This communication includes, but is not limited to, the following matters: *a.* How information is designated as confidential and ceases to be confidential. *b.* How access to confidential information is authorized. *c.* How confidential information is used. *d.* How confidential information is shared. *e.* If information is provided to third parties, disclosures include any limitations on reliance on the third party's confidentiality practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's confidentiality practices and controls that meet or exceed those of the entity. *f.* Confidentiality practices needed to comply with applicable laws and regulations.	XYZ manufacturing.com is a high-quality custom manufacturer of electronic components. Customers and potential customers can submit engineering drawings, specifications, and requests for manufacturing price quotes through our Web site or e-mail. Access to your information is limited to our employees and any third-party subcontractors we may elect to use in preparing our quote. We will not use any information you provide for any purpose other than a price quote and subsequent manufacturing and order fulfillment on your behalf. However, access may need to be provided in response to subpoenas, court orders, legal process, or other needs to comply with applicable laws and regulations. Using our encryption software, you may designate information as confidential by checking the "Confidential Treatment" box. This software can be downloaded from our site and will accept information in most formats. Such information will automatically be encrypted using our public key before transmission over the Internet. You may transmit such information to us through our Web site or by e-mail. Access to information designated as confidential will be restricted only to our employees with a need to know. We will not provide such information to third parties without your prior permission. When we provide information to third parties, we do not provide your company name. However, we make no representation regarding third-party confidential treatment of such information. Our confidentiality protection is for a period of two years, after which we will cease to provide such protection. In addition, should such information become public through your actions or other means, our confidentiality protection ceases. If you are not a customer at the time of submitting such information, you will be provided with an account number and password. You may use this account number and password to access the information you have submitted, plus any related price quote information provided by us. You may also set up an additional 10 sub-accounts and passwords so others in your organization can also access this information. Our services and the protection of confidential information are subject to third-party dispute resolution. This process is described under "Arbitration Process" elsewhere on our Web site.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria Reference	*Illustrative Disclosures*
2.4 The process for informing the entity about breaches of confidentiality and system security and for submitting complaints is communicated to authorized users.	If you have any questions about our organization or our policies on confidentiality as stated at this site, please contact CustServ@XYZ-manufacturing.com. Should you feel that there has been a breach to the security of this site, please contact us *immediately* at (800) 123-1234.
2.5 Changes that may affect confidentiality and system security are communicated to management and users who will be affected.	Effective January 200X, we eliminated our "secret" category of information. Information submitted under such secret category will continue to be protected in accordance with our commitments at that time.

Appendix C

Example System Description for Non-E-Commerce Systems

The purpose of a system description is to delineate the boundaries of the system covered by management's assertion or the subject matter of the practitioner's report (in this example, a pension processing service). The system description should be an integrated part of the entity's communication of policies related to the specific principles subject to the practitioner's attestation. In all cases, the system description should accompany the practitioner's report.

Background

XYZ Co. Pension Services (XPS), based in New York, New York, with offices across North America, manages and operates the Pension Administration System (PAS) on behalf of pension plan sponsors who are XPS Co.'s customers. The plan members are the employees of XPS Co.'s customers who are enrolled in the pension plan. XPS uses PAS for recordkeeping of pension-related activities.

Infrastructure

PAS uses a three-tier architecture, including proprietary client software, application servers, and database servers.

Various peripheral devices, such as tape cartridge silos, disk drives, and laser and impact printers, are also used.

Software

The PAS application was developed by programming staff in XITD's (XYZ Co.'s Information Technology Department) Systems Development and Application Support area. PAS enables the processing of contributions to members' pension plans and withdrawals at retirement, based on plan rules. PAS generates all the required reports for members, plan sponsors, and tax authorities. PAS also provides a facility to record investments and related transactions (purchases, sales, dividends, interest, and other miscellaneous transactions). Batch processing of transactions is performed nightly.

PAS provides a facility for online data input and report requests. In addition, PAS accepts input from plan sponsors in the form of digital or magnetic media or files transmitted via the telecommunications infrastructure.

People

XPS has a staff of approximately 200 employees organized in the following functional areas:

- Pension administration includes a team of specialists for set-up of pension rules, maintenance of master files, processing of contributions to PAS, reporting to plan sponsors and members, and assistance with inquiries from plan members;

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- Financial operations is responsible for processing of withdrawals, deposit of contributions and investment accounting;
- Trust accounting is responsible for bank reconciliation; and
- Investment services is responsible for processing purchases of stocks, bonds, certificates of deposits, and other financial instruments.

XITD has a staff of approximately 50 employees who are dedicated to PAS and related infrastructure and are organized in the following functional areas:

- The help desk provides technical assistance to users of PAS and other infrastructure, as well as plan sponsors.
- Systems development and application support provides application software development and testing for enhancements and modifications to PAS.
- Product support specialists prepare documentation manuals and training material.
- Quality assurance monitors compliance with standards, and manages and controls the change migration process.
- Information security and risk is responsible for security administration, intrusion detection, security monitoring, and business-recovery planning.
- Operational services performs day-to-day operation of servers and related peripherals.
- System software services installs and tests system software releases, monitors daily system performance, and resolves system software problems.
- Technical delivery services maintains job scheduling and report distribution software, manages security administration, and maintains policies and procedures manuals for the PAS processing environment.

Voice and data communications maintains the communication environment, monitors the network and provides assistance to users and plan sponsors in resolving communication problems and network planning.

Procedures

The pension administration services covered by this system description include:

- Pension master file maintenance.
- Contributions.
- Withdrawals.
- Investment accounting.
- Reporting to members.

These services are supported by XYZ Co.'s Information Technology Department (XITD), which supports PAS 24 hours a day, 7 days a week. The key support services provided by XITD include:

- Systems development and maintenance.
- Security administration and auditing.

- Intrusion detection and incident response.
- Data center operations and performance monitoring.
- Change controls.
- Business recovery planning.

Data

Data, as defined for the PAS, constitutes the following:

- Master file data.
- Transaction data.
- Error and suspense logs.
- Output reports.
- Transmission records.
- System and security files.

Transaction processing is initiated by the receipt of paper documents, electronic media, or calls to XYZ's call center. Transaction data are processed by PAS in either online or batch modes of processing, and are used to update master files. Output reports are available either in hard copy or through a report-viewing facility to authorized users based on their job functions. Pension statement and transaction notices are mailed to plan sponsors and members.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.44

Appendix D

Practitioner Guidance on Scoping and Reporting Issues

This appendix deals with issues related to engagement planning, performance, and reporting using the Trust Services principles and criteria. It does not deal with reporting issues under the WebTrust® Program for Certification Authorities. This has been separately considered and issued.[1]

Specifically, this section deals with:

- Engagement elements.
- The practitioner's report.
- Reporting on multiple principles.
- Additional reporting guidance.
- Agreed-upon procedure engagements.
- Other matters.

As Trust Services attestation or audit reports are issued under Chapter 1, "Attest Engagements," of Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101), as amended, the practitioner should be familiar with the relevant standards.

Engagement Elements

Trust Services Principles

Trust Services provides for a modular approach using five different principles—security, availability, processing integrity, online privacy, and confidentiality. It is possible for the client to request a separate Trust Services examination that covers one or any combination of the principles. Principles provide the basis for describing various aspects of the system under examination with logical groupings of suitable criteria.

Trust Services Criteria

Criteria are the benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter.

Under the U.S. attestation standards,[2] suitable criteria must have each of the following attributes:

- *Objectivity*—Criteria should be free from bias.
- *Measurability*—Criteria should permit reasonably consistent measurements, qualitative or quantitative, of subject matter.

---

[1] Audit reporting for certification authorities is dealt with in section 17,200, *Suitable Trust Services Criteria and Illustrations for WebTrust® for Certification Authorities.*

[2] See Chapter 1, "Attest Engagements," of Statement on Standards for Attestation Engagements (SSAE) No. 10: *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101.24).

- *Completeness*—Criteria should be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted.
- *Relevance*—Criteria should be relevant to the subject matter.

The Trust Services criteria meet the requirement for being suitable criteria and are the result of a public exposure and comment process.

Management's Assertion

Under AICPA attestation standards, management must provide the practitioner with a written assertion or the practitioner will be required to modify his or her report.[3] Specifically, management asserts that, during the period covered by the report and based on the AICPA/CICA Trust Services criteria, it maintained effective controls over the system under examination to satisfy the stated Trust Services principle(s). For engagements covering only certain principles, management's assertion should only address the principles covered by the engagement.

In a WebTrust engagement, the practitioner is engaged to examine both that an entity complied with the Trust Services criteria and that it maintained effective controls over the system based on the Trust Services criteria. In order to receive a WebTrust seal, both compliance and operating effectiveness must be addressed. This differs from a SysTrust® engagement in which the practitioner is engaged to examine only that an entity maintained effective controls over the system under examination based on the Trust Services criteria.

Under the AICPA standards, the practitioner may report on either management's assertion or the subject matter of the engagement. When the practitioner reports on the assertion, the assertion should accompany the practitioner's report or the first paragraph of the report should contain a statement of the assertion.[4] When the practitioner reports on the subject matter, the practitioner may want to request that management make its assertion available to the users of the practitioner's report.

If one or more criteria have not been achieved, the practitioner issues a qualified or adverse report. Under AICPA attestation standards, when issuing a qualified or adverse report the practitioner should report directly on the subject matter rather than on the assertion.

Period of Coverage

The practitioner's report and management's assertion (when required) always should specify the time period covered by the report and assertion, respectively. A practitioner may issue a report for a period of time or at a point in time. The determination of an appropriate period should be at the discretion of the practitioner and the entity.

Factors to be considered in establishing the reporting period may include the following:

- The anticipated users of the report and their needs.
- The need to support a "continuous" audit model.
- The degree and frequency of change in each of the system components.

---

[3] See chapter 1 of SSAE No. 10 (AT sec. 101.58) for a description of a practitioner's options, if a written assertion is not obtained.

[4] See chapter 1 of SSAE No. 10 (AT sec. 101.64).

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- The cyclical nature of processing within the system.
- Historical information about the system.

For WebTrust or SysTrust seals on Web sites, the report must be refreshed at least every 12 months. A three-month grace period is permitted from the end of the reporting period to allow for the practitioner to complete the fieldwork and prepare the report. For example, if the current report is for the period ending December 31, 20X2, the next report must be for a period ending no later than December 31, 20X3, and must be posted no later than March 31, 20X4. In this example, the first report may continue to be posted to the client's Web site until March 31, 20X4.

The Practitioner's Report

There are a variety of reporting alternatives that are discussed below.

Reporting on the Entity's Controls to Achieve the Criteria

This reporting alternative provides an opinion on the operating effectiveness of controls based on one or more Trust Services principle(s) and criteria. The practitioner can issue either a SysTrust report (and corresponding seal), if applicable, or a Trust Services report. A WebTrust report (and corresponding seal) cannot be issued for this type of engagement since the practitioner is not also reporting on whether the entity has complied with the criteria.

Reporting on the Entity's Having Complied With the Criteria

This reporting alternative provides an opinion on the operating effectiveness of controls based on one or more Trust Services principle(s) and criteria and whether the entity complied with the criteria. In this type of engagement, the practitioner can issue either a WebTrust or a SysTrust report (and corresponding seal) as appropriate.

Reporting on the Suitability of the Design of Control Procedures

A practitioner may be asked to conduct a Trust Services engagement addressing the suitability of design of controls for a system, prior to the system's implementation. In such an engagement, the practitioner can issue a Trust Services report, but cannot issue a WebTrust or SysTrust report or corresponding seal.

Reporting on Multiple Principles

In most cases, a practitioner will be asked to report on one or more Trust Services principles and related criteria, rather than on the entire set of five principles. The practitioner, in the introductory paragraph, makes reference to the principles included in the scope of examination but makes no further statement that the entire set of principles was not included in the scope of the examination.

When the client asks the practitioner to examine and report on its conformity with two or more Trust Services principles and related criteria, there are a number of issues that the practitioner should consider, which are discussed in this section.

Individual or Combined Report

When engaged to perform a Trust Services examination for multiple principles, the practitioner can, depending on the needs of the client, issue either a combined report or individual reports for each of the principles. For the purpose

of this discussion, it is assumed that the practitioner has been asked to report on the client's conformity with three sets of principles and criteria: security, online privacy, and confidentiality.

The first issue is to decide whether this represents (1) one engagement to examine three principles or (2) three engagements that examine one principle each. This can affect, among other matters, the engagement letter, the content and number of representation letters, and whether one audit report or multiple audit reports will be issued.

A Trust Services examination for multiple principles can be performed either as a single engagement involving those three principles or as three separate engagements involving one principle each. In either case, the practitioner's report(s) should clearly communicate the nature of the engagement(s).

There can be reporting complications when a qualified report is appropriate for one or more, but not all three, of the principles. In certain instances, the practitioner may decide not to issue such a report. In order to ensure a clear understanding with the client on this matter, the engagement letter might include language indicating that "a report may or may not be issued."

Failure to Meet Criteria

There may be instances, with a multiple principle engagement, in which the entity fails to meet the relevant criteria for one or more of the multiple principles. If one or more relevant criteria have not been met, the practitioner cannot issue an unqualified report. Under AICPA attestation standards, when issuing a qualified or adverse report, the practitioner should report directly on the subject matter rather than on the assertion.

In the situation where, for example, the entity did not meet the confidentiality criteria but met all of the security and online privacy criteria, the practitioner, depending upon how the engagement was structured, has the following options available:

1. Issue one report that deals with all three principles. Because the report would be qualified, no seal would be issued. Since this option would most likely not accomplish the client's objective of obtaining a seal, the practitioner should consider the next option.
2. Issue multiple reports (for example, two reports), with segregation of the confidentiality principle into a separate report. The other two principles would have an unqualified report, thereby enabling the entity to obtain the seal.[5] The practitioner may then either issue a separate qualified report for confidentiality or withdraw from the confidentiality engagement. In either case, the practitioner may wish to issue recommendations to management on how the deficiencies can be corrected. The impact of the deficiency for confidentiality would need to be assessed to ascertain its effect, if any, on the other principles.[6]

In the situation where the practitioner treats each principle as a separate engagement with separate engagement letters, option (2) would be the most appropriate.

---

[5] In determining whether a WebTrust seal would be issued in such circumstances, the practitioner should consider the guidance under the section "Responsibility for Communicating Lack of Compliance in Other Principle(s)."

[6] Chapter 1 of SSAE No. 10 (AT sec. 501.34 and 601.53).

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Different Examination Periods

There may be situations where the entity requests that more than one principle be examined, but due to various reasons the principles will have different reporting periods (either the length of the reporting period, the date that the various reporting periods begin, or both). Ideally, it would be more efficient for the practitioner to have such periods coincide. When different reporting periods exist, the practitioner should consider whether to issue separate or combined reports. Separate reports covering the separate principles are less complex to prepare than a combined report. If a combined report is issued, the different reporting periods would need to be detailed in the introductory and opinion paragraphs of the report to ensure that the different examination periods are highlighted.

Additional Reporting Guidance

Special Issues for Initial Reports

Typically, an initial report would need to cover a period of two months or more. However, an initial report covering a period of less than two months (including a point-in-time report) can be issued in any of the following circumstances:

- When the conditions dictate (see Table 1).
- When an entity wishes to restore a Trust Services seal following a significant event that caused the entity to no longer comply with the criteria (that necessitated removal of the practitioner's report and the Trust Services seal from the entity's site).
- When an entity requests a Trust Services engagement for a system that is in the pre-implementation stage. The report would be a point in time rather than a period in time. Such a report would indicate that the system has not been placed in operation.

Similar to any attest engagement, before a practitioner can render an opinion, sufficient and competent evidential matter needs to be obtained.[7] For all criteria, there needs to be sufficient client transaction volumes and other procedure and control evidence to provide the practitioner with the necessary evidential matter. Therefore, in accepting an engagement that will result in the issuance of a report on a period of less than two months (including a point-in-time report) the practitioner should consider, as it relates to management's assertion about compliance with the criteria and the operating effectiveness of its controls, whether there will be an appropriate testing period ("look-back period") to provide sufficient evidence to enable the practitioner to issue such a report. The period over which a practitioner should perform tests is a matter of judgment.

The period of time over which the practitioner would need to perform tests of controls to determine that such controls were operating effectively will vary with the nature of the controls being tested and the frequency with which the specific controls operate and specific policies are applied. Some controls operate continuously while others operate only at certain times.

If it is concluded that there will be an appropriate "look-back period" to provide sufficient evidential matter, the practitioner may undertake the engagement to issue a report covering a period of less than two months, or a point-in-time

[7] Chapter 1 of SSAE No. 10 (AT sec. 101.51).

report. If the practitioner decides to issue a point-in-time report, the report should indicate that the firm has examined management's assertion as of [*Month, day, year*], rather than during a period.

The Trust Services practitioner should, in addition to considering the guidance herein, consider the relevant attest standards[8] with respect to the wording of such a report, to assure that he or she is complying with such attest standards.

The length of the relevant initial period should be determined by the practitioner's professional judgment based on factors such as those set out in Table 1.

Table 1

Considerations for Use of a Shorter Initial Period	*Considerations for Use of a Longer Initial Period*
• Clients for whom other control examinations have already been performed	• Start-up operation that has not generated, during pre-implementation stages, sufficient transaction volume and conditions typical of expected normal operations
• Established site, with little transaction volatility	• Operations that experience volatile transaction volumes
• Operations that experience infrequent changes to disclosures, policies, and related controls	• Complex operations
• Start-up operation with significant transaction volumes and operating conditions (typical of expected normal operations) during the practitioner's pre-implementation testing period and a transition to a live operational site that expects infrequent changes in policies and controls once it is operational	• Operations that experience frequent changes to disclosures, policies, and related controls or significant instances that lack compliance with disclosures, policies, and related controls

Use of Third-Party Service Providers

The practitioner may encounter situations where the entity under examination uses a third-party service provider to accomplish some of the Trust Services criteria. The AICPA/CICA *Effects of a Third-Party Service Provider in a WebTrust or Similar Engagement* provides applicable guidance for these situations and is available for download at www.aicpa.org.

Considerations When Restoring a Removed Seal

The following guidance applies when an entity wishes to restore the seal following a significant event that caused the entity to no longer comply with the criteria (that necessitated removal of the practitioner's report and the Seal from the entity's site). It is important that the entity consider disclosing to its users the nature of the significant event that created the "out of compliance" situation and the steps taken to remedy the situation. The entity should consider disclosing the event on its Web site or as part of its management assertion. Likewise, before issuing a new report, the practitioner should consider the significance of the event, the related corrective actions, and whether appropriate disclosure has been made. The practitioner also should consider whether

[8] See chapter 1 of SSAE No. 10 (AT sec. 101.84–.87) and Appendix A (AT sec. 101.110) for additional reporting guidance.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

this matter should be (1) disclosed as part of management's assertion, (2) emphasized in a separate explanatory paragraph in the practitioner's report, or (3) both.

Responsibility for Communicating Lack of Compliance in Other Principle(s)

During an examination of a client's conformity with a Trust Services principle, information about compliance or control deficiencies related to principles and criteria that are not within the defined scope of the engagement may come to the practitioner's attention. For example, while engaged only to report on controls related to the security principle, a practitioner may become aware that the entity is not complying with its privacy policy as stated on its Web site (for example, it is disclosing personal information to selected third parties). Although the practitioner is not responsible for detecting information outside the scope of his or her examination, the practitioner should consider such information when it comes to his or her attention and evaluate whether the identified deficiencies are significant (that is, whether such deficiencies could materially mislead users of the system).

If the practitioner determines that such deficiencies are significant, they should be communicated in writing to management. Management should be asked either to correct the deficiency (in this case, cease providing the information to third parties) or to properly disclose their actual practices publicly so that users are aware of actual policies (in this case, the privacy statement would be amended to reflect the fact that they do provide information to third parties).

If the practitioner concludes that omission of this information would be significant and if management is unwilling to either correct the deficiency or to disclose the information, the practitioner should consider withdrawing from the engagement.

Cumulative Reporting

Under Trust Services reporting guidelines, the period reported upon by a practitioner is limited to the current period under examination and shall not exceed 12 months. A cumulative report that covers the current examination period and prior periods that were subject to similar examinations by the practitioner is not recommended. The relevance of a cumulative reporting period has been questioned given the significant pace of growth and change in technological systems, especially those for electronic commerce.

Qualified or Adverse Opinions

Under the AICPA attestation standards, reservations about the subject matter or the assertion refers to any unresolved reservation about the assertion or about the conformity of the subject matter with the criteria, including the adequacy of the disclosure of material matters. They can result in either a qualified or an adverse opinion, depending on the materiality of the departure from the criteria against which the subject matter was evaluated.

Subsequent Events

Events or transactions sometimes occur subsequent to the point in time or period of time of the subject matter being tested but prior to the date of the practitioner's report that have a material effect on the subject matter and therefore require adjustment or disclosure in the presentation of the subject

matter or assertion. These occurrences are referred to as *subsequent events*. In performing an attest engagement, a practitioner should consider information about subsequent events that comes to his or her attention. Two types of subsequent events require consideration by the practitioner.

The first type consists of events that provide additional information with respect to conditions that existed at the point in time or during the period of time of the subject matter being tested. This information should be used by the practitioner in considering whether the subject matter is presented in conformity with the criteria and may affect the presentation of the subject matter, the assertion, or the practitioner's report.

The second type consists of those events that provide information with respect to conditions that arose subsequent to the point in time or period of time of the subject matter being tested that are of such a nature and significance that their disclosure is necessary to keep the subject matter from being misleading. This type of information will not normally affect the practitioner's report if the information is appropriately disclosed.

While the practitioner has no responsibility to detect subsequent events, the practitioner should inquire of the responsible party (and his or her client if the client is not the responsible party) as to whether they are aware of any subsequent events, through the date of the practitioner's report, that would have a material effect on the subject matter or assertion.[9] The representation letter ordinarily would include a representation concerning subsequent events.

The practitioner has no responsibility to keep informed of events subsequent to the date of his or her report; however, the practitioner may later become aware of conditions that existed at that date that might have affected the practitioner's report had he or she been aware of them. In such circumstances, the practitioner may wish to consider the guidance in Statement on Auditing Standards (SAS) No. 1, section 561, *Subsequent Discovery of Facts Existing at the Date of the Auditor's Report* (AICPA, *Professional Standards*, vol. 1, AU sec. 561).[10]

Agreed-Upon Procedures Engagements

A client may request that a practitioner perform an agreed-upon procedures engagement related to the Trust Services principles and criteria. In such an engagement, the practitioner performs specified procedures agreed to by the specified parties,[11] and reports his or her findings. Because the needs of the parties may vary widely, the nature, timing, and extent of the agreed-upon procedures may vary as well; consequently, the specified parties assume responsibility for the sufficiency of the procedures since they best understand their own needs. In an agreed-upon procedures engagement, the practitioner does not perform an examination or review of an assertion or subject matter or express an opinion or negative assurance about the assertion or subject matter.

---

[9] For certain subject matter, specific subsequent event standards have been developed to provide additional requirements for engagement performance and reporting. Additionally, a practitioner engaged to examine the design or effectiveness of internal control over items not covered by Chapter 5, "Reporting on an Entity's Internal Control Over Financial Reporting," or Chapter 6, "Compliance Attestation," of SSAE No. 10, as amended, should consider the subsequent events guidance set forth in Chapter 5 (AT sec. 501.65–.68), and Chapter 6 (AT sec. 601.50–.52).

[10] Chapter 1 of SSAE No. 10 (AT sec. 101.95–.99).

[11] The specified users and the practitioner agree upon the procedures to be performed by the practitioner.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

The practitioner's report on agreed-upon procedures is a presentation of procedures and findings.[12] The use of an agreed-upon procedures report is restricted to the specified parties who agreed upon the procedures. In such engagements, issuance of a seal is not appropriate.

Other Matters

All Trust Services engagements should be performed in accordance with the applicable professional standards and the Trust Services license agreement. Because users are seeking a high level of assurance, WebTrust and SysTrust are examination level engagements. Accordingly, it is not appropriate to provide these services with the intent of providing a moderate level or a review report. Although permissible, a moderate assurance or review level Trust Services engagement may not provide the desired degree of usefulness for the intended users.

Illustrative Reports

The following illustrative reports are for both SysTrust and WebTrust engagements. Illustrations 1 through 3 are period-of-time report examples. Illustration 4 is a point-in-time report example.

Under the SSAEs, the first paragraph of the practitioner's report will state that the practitioner has performed an examination of management's assertion about compliance with the Trust Services criteria or, alternatively, that the practitioner has examined the subject matter. The practitioner may opine (1) on management's assertion or (2) directly on the subject matter. Both alternatives are covered in the illustrative reports.

These reports are for illustrative purposes and should be modified in accordance with the applicable professional standards as the specific engagement facts and circumstances warrant.

[12] Agreed-upon procedures engagements are performed under Chapter 2, "Agreed-Upon Procedures Engagements," of SSAE No. 10 (AT sec. 201).

Illustration 1—SysTrust Report for Systems Reliability—Reporting Directly on the Subject Matter (Period-of-Time Report)

Independent Practitioner's SysTrust Report on System Reliability

To the Management of ABC Company, Inc.:

We have examined the effectiveness of ABC Company, Inc.'s (ABC Company) controls over the reliability of its _____ [*system under examination*] System during the period [*Month, day, year*] through [*Month, day, year*], based on the AICPA/CICA Trust Services Criteria for systems reliability. Maintaining the effectiveness of these controls is the responsibility of ABC Company's management. Our responsibility is to express an opinion based on our examination.

A reliable system is one that is capable of operating without material error, fault, or failure during a specified period in a specified environment. The AICPA/CICA Trust Services Availability, Security, and Processing Integrity Criteria [*hot link to applicable principles and criteria*] are used to evaluate whether ABC Company's controls over the reliability of its _____ [*system under examination*] System are effective.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of ABC Company's relevant system availability, security, and processing integrity controls; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, ABC Company maintained, in all material respects, effective controls over the reliability of the _____ [*system under examination*] System to provide reasonable assurance that:

- The System was available for operation and use, as committed or agreed;
- The System was protected against unauthorized access (both physical and logical); and
- The System processing was complete, accurate, timely, and authorized during the period [*Month, day, year*] through [*Month, day, year*], based on the AICPA/CICA Trust Services Criteria for systems reliability.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

The SysTrust seal on ABC Company's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

[*See Notes to Illustrative Reports prepared under AICPA standards.*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Illustration 2—WebTrust Report for Consumer Protection—Reporting Directly on the Subject Matter (Period-of-Time Report)

Independent Practitioner's WebTrust Report on Consumer Protection

To the Management of ABC Company, Inc.:

We have examined ABC Company, Inc.'s (ABC Company) compliance with the AICPA/CICA Trust Services Criteria for consumer protection, and based on these Criteria, the effectiveness of controls over the Online Privacy and Processing Integrity of the _____ (*system under examination*) System during the period [*Month, day, year*] through [*Month, day, year*]. The compliance with these criteria and maintaining the effectiveness of these controls is the responsibility of ABC Company's management. Our responsibility is to express an opinion based on our examination.

Within the context of AICPA/CICA Trust Services, consumer protection addresses the controls over personally identifiable information and the processing of electronic commerce transactions. The AICPA/CICA Trust Services Online Privacy and Processing Integrity Criteria are used to evaluate whether ABC Company's controls over consumer protection of its [*system under examination*] System are effective. Consumer protection does not address the quality of ABC Company's goods [*information or services*] nor their suitability for any customer's intended purpose.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of ABC Company's relevant online privacy and processing integrity controls; (2) testing and evaluating the operating effectiveness of the controls; (3) testing compliance with the Online Privacy and Processing Integrity Criteria; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, ABC Company complied, in all material respects, with the criteria for consumer protection and maintained, in all material respects, effective controls over the _____ [*system under examination*] System to provide reasonable assurance that:

- Personal information obtained as a result of electronic commerce was collected, used, disclosed, and retained as committed or agreed, and
- System processing was complete, accurate, timely, and authorized during the period [*Month, day, year*] through [*Month, day, year*], based on the AICPA/CICA Trust Services Criteria for consumer protection.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

The WebTrust seal on ABC Company's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

This report does not include any representation as to the quality of the ABC Company's goods [*information or services*] nor their suitability for any customer's intended purpose.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

[*See Notes to Illustrative Reports prepared under AICPA standards.*]

Illustration 3—Report for One Principle—Reporting Directly on the Subject Matter (Period-of-Time Report Including Schedule Describing Controls)

Independent Practitioner's SysTrust Report

To the Management of ABC Company, Inc.:

We have examined the effectiveness of ABC Company, Inc.'s (ABC Company) controls, described in Schedule X, over the security of its _____ [*system under examination*] System during the period [*Month, day, year*] through [*Month, day, year*], based on the AICPA/CICA Trust Services Security Criteria. Maintaining the effectiveness of these controls is the responsibility of ABC Company's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of ABC Company's relevant security controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, ABC Company maintained, in all material respects, effective controls, described in Schedule X, over the security of the _____ [*system under examination*] System to provide reasonable assurance that the _____ [*system under examination*] System was protected against unauthorized access (both physical and logical) during the period [*Month, day, year*] through [*Month, day, year*], based on the AICPA/CICA Trust Services Security Criteria.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

The SysTrust seal on ABC Company's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

[*See Notes to Illustrative Reports prepared under AICPA standards.*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Schedule X—Controls Examined Supporting AICPA/CICA Trust Services Security Criteria

The system is protected against unauthorized access (both physical and logical).

1.0 Policies: The entity defines and documents its policies for the security of its system.	**Controls**
1.1 The entity's security policies are established and periodically reviewed and approved by a designated individual or group.	The company's documented systems development and acquisition process includes procedures to identify and document authorized users of the system and their security requirements. User requirements are documented in service-level agreements or other documents. The security officer reviews security policies annually and submits proposed changes for the approval by the information technology standards committee.
1.2 The entity's security policies include, but may not be limited to, the following matters: *a.* Identification and documentation of the security requirements of authorized users. *b.* Allowing access, the nature of that access, and who authorizes such access. *c.* Preventing unauthorized access. *d.* The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access. *e.* Assignment of responsibility and accountability for system security. *f.* Assignment of responsibility and accountability for system changes and maintenance. *g.* Testing, evaluating, and authorizing system components before implementation. *h.* Addressing how complaints and requests relating to security issues are resolved. *i.* The procedures to handle security breaches and other incidents. *j.* Provision for allocation for training and other resources to support its system security policies.	The company's documented security policies contain the elements set out in criterion 1.2.

(continued)

	Policies: The entity defines and documents its policies for the security of its system.	Controls
	k. Provision for the handling of exceptions and situations not specifically addressed in its system security policies.	
	l. Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts.	
1.3	Responsibility and accountability for the entity's system security policies, and changes and updates to those policies, are assigned.	Management has assigned responsibilities for the maintenance and enforcement of the company security policy to the chief information officer (CIO). Others on the executive committee assist in the review, update, and approval of the policy as outlined in the executive committee handbook. Ownership and custody of significant information resources (for example, data, programs, and transactions) and responsibility for establishing and maintaining security over such resources is defined.

This schedule is for illustrative purposes only and does not contain all the criteria for the security principle. When the practitioner is reporting on more than one principle, a similar format would be used to detail the appropriate criteria and controls. The practitioner is not bound by this presentation format and may utilize other alternative presentation styles.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Illustration 4—Report for One Principle—Reporting on Management's Assertion (Point-in-Time Report)

Independent Practitioner's WebTrust Report

To the Management of ABC Company, Inc.:

We have examined management's assertion [*hot link to management's assertion*] that ABC Company, Inc. (ABC Company) as of [*Month, day, year*] complied with the AICPA/CICA Trust Services Security Criteria and, based on these Criteria, maintained effective controls to provide reasonable assurance the _____ [*system under examination*] System was protected against unauthorized access (both physical and logical). This assertion is the responsibility of ABC Company's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of ABC Company's relevant security controls, (2) testing and evaluating the operating effectiveness of the controls, (3) testing compliance with the Security Criteria, and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, management's assertion that ABC Company complied with AICPA/CICA Trust Services Security Criteria and, based on these Criteria, maintained effective controls to provide reasonable assurance that the _____ [*system under examination*] System was protected against unauthorized access (both physical and logical) as of [*Month, day, year*] is fairly stated, in all material respects.

OR

In our opinion, ABC Company's management's assertion referred to above is fairly stated, in all material respects, based on the AICPA/CICA Trust Services Security Criteria.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

The WebTrust seal of assurance on ABC Company's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

[*See Notes to Illustrative Reports prepared under AICPA standards.*]

.45

Appendix E

Trust Services Privacy Principle, Criteria, and Illustrations

Privacy is defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information.

Personal Information

Personal information is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual. Some examples of personal information are:

- Name
- Home or e-mail address
- Identification number (e.g., Social Security or Social Insurance Numbers)
- Physical characteristics
- Consumer purchase history

Some personal information is considered *sensitive*. Some laws and regulations define the following to be sensitive personal information:

- Information on medical or health conditions
- Financial information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions

Sensitive personal information generally requires an extra level of protection and a higher duty of care. For example, sensitive information may require explicit consent rather than implicit consent.

Some information about or related to people cannot be associated with specific individuals. Such information is referred to as nonpersonal information. This includes statistical or summarized personal information for which the identity of the individual is unknown or linkage to the individual has been removed. In such cases, the individual's identity cannot be determined from the information that remains, because the information is "de-identified" or "anonymized." Nonpersonal information ordinarily is not subject to privacy protection because it can not be linked to an individual.

Privacy, Confidentiality, and Security

Privacy is about individuals having control over the collection, use, and disclosure of their personal information. Unlike privacy, there is not a widely accepted

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

definition of confidentiality[1] but, in most cases, it is about keeping business information from being disclosed to unauthorized parties. Confidentiality is usually driven by agreements or contractual arrangements. Security is one of the 10 components of the Framework. The criteria for the security component of privacy are substantially equivalent to the criteria for the Trust Services Security Principle.

AICPA/CICA Trust Services Privacy Principle

Personal information is collected, used, retained, and disclosed in conformity with the commitments in the entity's privacy notice and with the AICPA/CICA Trust Services Privacy Criteria.

AICPA/CICA Trust Services Privacy Components and Criteria

The Framework contains 10 privacy components[2] and related criteria that are essential to the proper protection and management of personal information. These privacy components and criteria are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices. The following are the 10 privacy components:

1. *Management.* The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. *Notice.* The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. *Choice and Consent.* The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. *Collection.* The entity collects personal information only for the purposes identified in the notice.
5. *Use and Retention.* The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes.
6. *Access.* The entity provides individuals with access to their personal information for review and update.
7. *Disclosure to Third Parties.* The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. *Security.* The entity protects personal information against unauthorized access (both physical and logical).
9. *Quality.* The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. *Monitoring and Enforcement.* The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

---

[1] AICPA/CICA Trust Services provides a Confidentiality Principle and Criteria which may be helpful for addressing confidentiality.

[2] Although some privacy regulations use the term *principle,* the term *component* is used in the Framework to represent that concept since the term principle has been previously defined in the Trust Services literature.

For each of the 10 privacy components, there are relevant, objective, complete, and measurable criteria for evaluating an entity's privacy policies, communications, and procedures and controls. *Privacy policies* are written statements that convey management's intent, objectives, requirements, responsibilities, and/or standards. *Communications* refers to the organization's communication to individuals, internal personnel, and third parties about its privacy notice and its commitments therein and other relevant information. *Procedures and controls* are the other actions the organization takes to achieve the criteria.

Framework Presentation

The Framework is presented in a three-column format. The first column contains the Trust Services Privacy criteria.[3] The second column, which contains illustrations and explanations, is designed to enhance the understanding of the criteria. The illustrations are not intended to be comprehensive, nor are any of the illustrations required for an entity to have met the Trust Services Privacy criteria. The third column contains additional considerations, including supplemental information such as good privacy practices and selected requirements of specific laws and regulations that pertain to a certain industry or country.

The criteria identified in the 10 privacy components provide a basis for designing, implementing, maintaining, and evaluating a privacy program in order to meet an entity's needs by CPAs/CAs in public practice, industry, government, and education.

Practitioner Use of the Framework for Providing Advisory Services

Practitioners can provide a variety of advisory services to their clients, which include strategic, diagnostic, implementation, and sustaining/managing services using the Framework principle, components, and criteria. It could include, for example, advising clients on system weaknesses, assessing risk, and recommending a course of action using the Framework criteria as a benchmark.

Practitioners in the United States providing such advisory services follow Statement on Standards for Consulting Services, *Consulting Services: Definition and Standards* (AICPA, *Professional Standards*, vol. 2, CS sec. 100). Canadian practitioners are not required to comply with any specific set of standards with respect to advisory service engagements but, as noted above, are expected to meet the standards set out in Sections 5000–5900 of the CICA Handbook.

Practitioner Use of the Framework for Providing Attestation or Assurance Services

- Practitioners also can use the criteria to perform an examination of an organization's privacy under Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Engagements: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101), as amended, or the *CICA Handbook—Assurance,* Section 5025, "Standards for Assurance Engagements." In addition, the practitioner guidance included in the AICPA/CICA Trust Services Criteria is applicable to these types of engagements.[4]

---

[3] These criteria meet the definition of "criteria established by a recognized body" described in the third general standard for attestation engagements in the United States in Chapter 1 of Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Engagements: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101.24), as amended, and in the standards for assurance engagements in Canada (*CICA Handbook*, paragraph 5025.41).

[4] Chapter 10, of the *AICPA / CICA Privacy Resource Guide* also includes guidance on performing privacy assurance engagements.

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Trust Services Privacy Components and Criteria

Management

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
1.0	**The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.**		
1.1	**Policies and Communications**		
1.1.0	**Privacy Policies** The entity defines and documents its privacy policies with respect to: • Notice (See 2.1.0) • Choice and Consent (See 3.1.0) • Collection (See 4.1.0) • Use and Retention (See 5.1.0) • Access (See 6.1.0) • Onward Transfer and Disclosure (See 7.1.0) • Security (See 8.1.0) • Quality (See 9.1.0) • Monitoring and Enforcement (See 10.1.0)	Privacy policies are documented (in writing) and made readily available to internal personnel and third parties who need them.	

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
1.1.1	**Communication to Internal Personnel** Privacy policies and the consequences of noncompliance with such policies are communicated at least annually to the entity's internal personnel responsible for collecting, using, retaining, and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.	The entity: • Periodically communicates to internal personnel (for example, on a network or a Web site) relevant information about the entity's privacy policies and changes to its privacy policies. • Requires internal personnel to confirm (initially and periodically) their understanding of an agreement to comply with the entity's privacy policies. • Educates and trains internal personnel (initially and periodically) who have access to personal information or are charged with the security of personal information about privacy awareness, concepts, and issues.	Privacy policies encompass security policies relevant to the protection of personal information.

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
1.1.2	**Responsibility and Accountability for Policies** Responsibility and accountability are assigned to a person or group for documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.	The entity assigns responsibility for privacy policies to a designated person, such as a corporate privacy officer. (Those assigned responsibility for privacy policies may be different from those assigned for other policies, such as security.) The authority and accountability of the designated person or group are clearly documented. Responsibilities include: • Establishing standards to classify the sensitivity of personal information and to determine the level of protection required • Formulating and maintaining the entity's privacy policies • Monitoring and updating the entity's privacy policies • Delegating authority for enforcing the entity's privacy policies • Monitoring the degree of compliance and initiating action to improve the training or clarification of policies and practices	

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		The Board periodically includes privacy in its regular review of corporate governance. The entity requires users, management, and third parties to confirm (initially and annually) their understanding of and agreement to comply with the entity's privacy policies and procedures related to the security of personal information.	
1.2	**Procedures and Controls**		
1.2.1	**Review and Approval** Privacy policies and procedures and changes thereto are reviewed and approved by management.	Privacy policies and procedures are: • Reviewed and approved by senior management or a management committee. • Reviewed at least annually and updated as needed.	
1.2.2	**Consistency of Privacy Policies and Procedures With Laws and Regulations** Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever there are changes to such laws and regulations. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.	Corporate counsel or the legal department: • Determines which privacy laws and regulations are applicable in the jurisdictions in which the entity operates. • Reviews the entity's privacy policies and procedures to ensure they are consistent with the applicable laws and regulations.	

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
1.2.3	**Consistency of Commitments With Privacy Policies and Procedures** Entity personnel or advisors review contracts for consistency with privacy policies and procedures and address any inconsistencies.	Management and the corporate counsel or the legal department review all contracts and service-level agreements for consistency with the entity's privacy policies and procedures.	
1.2.4	**Infrastructure and Systems Management** Entity personnel or advisors review the design, acquisition, implementation, configuration, and management of the infrastructure, systems, and procedures and changes thereto for consistency with the entity's privacy policies and procedures and address any inconsistencies.	Procedures are in place to: • Govern the development, acquisition, implementation, and maintenance of information systems and the related technology used to collect, use, retain, and disclose personal information. • Ensure that the entity's backup and disaster-recovery planning processes are consistent with its privacy policies and procedures. • Classify the sensitivity of classes of data, and determine the classes of users who should have access to each class of data. Users are assigned user-access profiles based on their need for access and their functional responsibilities as they relate to personal information.	

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		• Assess planned changes to systems and procedures for their potential effect on privacy. • Test changes to system components to minimize the risk of an adverse effect on the systems that process personal information. All test data are anonymized. • Require the documentation and approval by the privacy officer and business unit manager before implementing the changes to systems and procedures that handle personal information, including those that may affect security. Emergency changes may be documented and approved on an after-the-fact basis. The Information Technology (IT) department maintains a listing of all software and the respective level, version, and patches that have been applied. Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	
1.2.5	**Supporting Resources** Resources are provided by the entity to implement and support its privacy policies.	Management reviews annually the assignment of personnel, budgets, and allocation of other resources to its privacy program.	

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
1.2.6	**Qualifications of Personnel** The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received needed training.	The qualifications of internal personnel responsible for protecting the privacy and security of personal information are ensured by procedures such as: • Formal job descriptions (including responsibilities, educational and professional requirements and organizational reporting for key privacy management positions) • Hiring procedures (including the comprehensive screening of credentials, background checks, and reference checking) • Training programs related to privacy and security matters • Performance appraisals (performed by supervisors, including assessments of professional development activities)	

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
1.2.7	**Changes in Business and Regulatory Environments** For each jurisdiction in which the entity operates, the effect on privacy of changes in the following factors is identified and addressed: • Business operations and processes • People • Technology • Legal • Contracts, including service-level agreements Privacy policies and procedures are updated for such changes.	The entity has an ongoing process in place to monitor, assess, and address the effect on privacy of changes in: • Business operations and processes • People assigned responsibility for privacy and security matters • Technology (prior to implementation) • Legal and regulatory environments • Contracts, including service-level agreements with third parties (Changes that alter the privacy and security related clauses in contracts are reviewed and approved by the privacy officer or corporate counsel before they are executed.)	

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Notice

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
2.0	**The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.**		
2.1	**Policies and Communications**		
2.1.0	**Privacy Policies** The entity's privacy policies address providing notice to individuals.		
2.1.1	**Communication to Individuals** Notice is provided to individuals regarding the following privacy policies: • Purpose for collecting personal information • Choice and Consent (See 3.1.1) • Collection (See 4.1.1) • Use and Retention (See 5.1.1) • Access (See 6.1.1) • Onward Transfer and Disclosure (See 7.1.1) • Security (See 8.1.1) • Quality (See 9.1.1) • Monitoring and Enforcement (See 10.1.1) If personal information is collected from sources other than the individual, such sources are described in the notice.	The entity's privacy notice: • Describes the purposes for which personal information is collected. • Indicates that the purpose for collecting sensitive personal information is part of a legal requirement. • May be provided in various ways (for example, in a face-to-face interview, a telephone interview, an application form or questionnaire, or electronically). Written notice is the preferred method.	Notice also may describe situations in which personal information will be disclosed, such as: • Certain processing for purposes of public security or defense • Certain processing for purposes of public health or safety • When allowed or required by law The purpose described in the notice should be stated in such a manner that the individual can reasonably understand the purpose and how the personal information is to be used. Such purpose should be consistent with the business purpose of the entity and not overly broad. Consideration should be given to providing a summary level notice with links to more detailed sections of the policy.

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
2.2	**Procedures and Controls**		
2.2.1	**Provision of Notice** Notice is provided to the individual about the entity's privacy policies and procedures: • At or before the time personal information is collected, or as soon as practical thereafter. • At or before the entity changes its privacy policies and procedures, or as soon as practical thereafter. • Before personal information is used for new purposes not previously identified (See 3.2.2, "Consent for New Purposes and Uses.")	Privacy notice is: • Readily accessible and available when personal information is first collected from the individual. • Provided in a timely manner (that is, at or before the time personal information is collected, or as soon as practical thereafter) to enable individuals to decide whether or not to submit personal information to the entity. • Clearly dated to allow individuals to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. In addition, the entity: • Tracks previous iterations of the entity's privacy policies and procedures. • Informs individuals of a change to a previously communicated privacy notice, for example, by posting the notification on the entity's Web site, by sending written notice via the mail, or by sending an e-mail. • Documents that changes to privacy policies and procedures were communicated to individuals.	Some regulatory requirements indicate that a privacy notice is to be provided on a periodic basis, for example, annually in the Gramm-Leach-Bliley Act (GLBA).

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
2.2.2	**Entities and Activities Covered** An objective description of the entities and activities covered by the privacy policies and procedures is included in the entity's privacy notice.	The privacy notice describes the particular entities, business segments, locations, and types of information covered, for example: • Operating jurisdictions (legal and political) • Business segments and affiliates. • Lines of business • Types of third parties (for example, delivery companies and other types of service providers) • Types of information (for example, information about customers and potential customers) • Sources of information (for example, mail order or online) The entity informs individuals when they leave the Web site and are no longer covered by the entity's privacy policies and procedures.	
2.2.3	**Clear and Conspicuous** Clear and conspicuous language is used in the entity's privacy notice.	The privacy notice is: • In plain and simple language. • Appropriately labeled, easy to see, and not in fine print. • Linked to or displayed on the Web site at points of data collection.	If multiple notices are used for different subsidiaries or segments of an entity, similar formats should be encouraged to avoid consumer confusion and clarify their understanding of any differences.

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
			Some regulations, such as GLBA, may contain specific information that a disclosure must contain. Illustrative notices are often available for certain industries and types of collection, use, retention, and disclosure.

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Choice and Consent

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
3.0	**The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.**		
3.1	**Policies and Communications**		
3.1.0	**Privacy Policies** The entity's privacy policies address the choices available to individuals and the consent to be obtained.		
3.1.1	**Communication to Individuals** Individuals are informed: • About the choices available to them with respect to the collection, use, and disclosure of personal information. • That implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires otherwise.	The entity's privacy notice describes, in a clear and concise manner: • The choices available to the individual regarding the collection, use, and disclosure of personal information • The process an individual should follow to exercise these choices (for example, checking an "opt-out" box to decline receiving marketing materials) • The consequences of failing to provide personal information Individuals are advised that: • Personal information not essential to the purposes identified in the privacy notice need not be provided.	Some laws and regulations (such as Principle 11, Limits on the Disclosure of Personal Information, section 1 of the Australian Privacy Act of 1988) provide specific exemptions for the entity not to obtain the individual's consent. Examples of such situations include: • The recordkeeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person. • Use of the information for that other purpose is required or authorized by or under law.

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		• Preferences may be changed and consent may be withdrawn at a later time, subject to legal or contractual restrictions and reasonable notice. The type of consent required depends on the nature of the personal information and the method of collection (for example, an individual subscribing to a newsletter gives implied consent to receive communications from the entity).	
3.1.2	**Consequences of Denying or Withdrawing Consent** When personal information is collected, individuals are informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information for purposes identified in the notice.	The entity informs individuals at the time of collection: • About the consequences of refusing to provide personal information (For example, transactions may not be processed.) • About the consequences of denying or withdrawing consent (For example, opting out of receiving information about products and services may result in not being made aware of sales promotions.) • About how they will or will not be affected by failing to provide more than the minimum required personal information (For example, services or products will still be provided.)	

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
3.2	**Procedures and Controls**		
3.2.1	**Implicit or Explicit Consent** Implicit or explicit consent is obtained from the individual at or before the time personal information is collected or as soon as practical thereafter. The individual's preferences expressed in his or her consent are confirmed and implemented.	The entity: • Obtains and documents an individual's consent in a timely manner (that is, at or before the time personal information is collected, or as soon as practical thereafter). • Confirms an individual's preferences (in writing or electronically). • Documents and manages changes to an individual's preferences. • Ensures that an individual's preferences are implemented. • Addresses conflicts in the records about an individual's preferences. • Ensures that the use of personal information, throughout the entity and by third parties, is in accordance with an individual's preferences.	
3.2.2	**Consent for New Purposes and Uses** If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the individual is notified, and implicit or explicit consent is obtained prior to such new use or purpose.	When personal information is to be used for a purpose not previously specified, the entity: • Notifies the individual and documents the new purpose. • Obtains and documents consent or withdrawal of consent to use the personal information for the new purpose.	If policies are changed but do not constitute new purposes or uses, the organization may wish to consult with legal counsel.

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		• Ensures that personal information is being used in accordance with the new purpose or, if consent was withdrawn, not so used.	
3.2.3	**Explicit Consent for Sensitive Information** Explicit consent is obtained directly from the individual when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.	The entity collects sensitive information only if the individual provides explicit consent. *Explicit consent* requires that the individual affirmatively agree, through some action, to the use or disclosure of the sensitive information. Explicit consent is obtained directly from the individual and documented, for example, by requiring the individual to check a box or sign a form. This is sometimes referred to as opt in.	The Personal Information Protection and Electronic Documents Act (PIPEDA), Schedule 1, clause 4.3.6, states that an organization should generally seek explicit consent when the information is likely to be considered sensitive. Most jurisdictions referenced to in Attachment D, "Comparison of International Privacy Concepts," prohibit the collection of sensitive data, unless specifically allowed. For example, in the European Union (EU) member state of Greece, Article 7 of Greece's "Law on the protection of individuals with regard to the processing of personal data" states that "The collection and processing of sensitive data is forbidden." However, a permit to collect and process sensitive data may be obtained.

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
3.2.4	**Consent for Online Data Transfers to/from an Individual's Computer** Consent is obtained before personal information is transferred to/from an individual's computer.	If the customer has indicated to the entity that it does not want cookies, the entity has controls to ensure that cookies are not stored on the customer's computer. The entity requests customer permission to store, alter, or copy personal information (other than cookies) in the customer's computer. Organizations will not download software that will transfer personal information without obtaining permission.	Consideration should be given to software that is designed to mine or extract information from a computer and therefore may be used to extract personal information, e.g., spyware.

Collection

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
4.0	**The entity collects personal information only for the purposes identified in the notice.**		
4.1	**Policies and Communications**		
4.1.0	**Privacy Policies** The entity's privacy policies address the collection of personal information.		Some jurisdictions, such as some countries in Europe, require entities that collect personal information to register with their regulatory body.
4.1.1	**Communication to Individuals** Individuals are informed that personal information is collected only for the purposes identified in the notice.	The entity's privacy notice discloses the types of personal information collected and the methods used to collect personal information.	
4.1.2	**Types of Personal Information Collected and Methods of Collection** The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are documented and described in the privacy notice.	Examples of the types of personal information collected are: • Financial (for example, financial account information) • Health (for example, information about physical or mental status or history) • Demographic (for example, age, income range, social geo-codes). Examples of methods of collecting and third-party sources of personal information are: • Credit reporting agencies • Over the telephone • Via the Internet using forms, cookies, or Web beacons	Some jurisdictions, such as those in the EU, require that individuals have the opportunity to decline the use of cookies.

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		The entity's privacy notice discloses that it uses cookies and Web beacons and how they are used. The notice also describes the consequences if the cookie is refused.	
4.2	**Procedures and Controls**		
4.2.1	**Collection Limited to Identified Purpose** The collection of personal information is limited to that necessary for the purposes identified in the notice.	Systems and procedures are in place to: • Specify the personal information essential for the purposes identified in the notice and differentiate it from optional personal information. • Periodically review the entity's program or service needs for personal information (for example, once every five years or when there are changes to the program or service). • Obtain explicit consent when sensitive personal information is collected (see 3.2.3, "Explicit Consent for Sensitive Information.") • Monitor that the collection of personal information is limited to that necessary for the purposes identified in the privacy notice and that all optional data is identified as such.	

(continued)

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
4.2.2	**Collection by Fair and Lawful Means** Methods of collecting personal information are reviewed by management, legal counsel, or both before they are implemented to confirm that personal information is obtained: • Fairly, without intimidation or deception, and • Lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information	The entity's legal counsel reviews the methods of collection and any changes thereto.	It may be considered a deceptive practice: • To use tools, such as cookies and Web beacons, on the entity's Web site to collect personal information without providing notice to the individual. • To link information collected during an individual's visit to a Web site with personal information from other sources without providing notice to the individual. • To use a third party to collect information in order to avoid providing notice to individuals. Entities should consider legal and regulatory requirements in jurisdictions other than the one in which they operate. (For example, an entity in Canada collecting personal information about Europeans may be subject to certain European legal requirements.) A review of complaints may help to identify whether there are unfair or unlawful practices.

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
4.2.3	**Collection From Third Parties** Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.	The entity: • Performs due diligence before establishing a relationship with a third-party data provider. • Reviews the privacy policies and collection methods of third parties before accepting personal information from third-party data sources.	Contracts include provisions requiring personal information to be collected fairly and lawfully and from reliable sources. If information collected from third parties is to be combined with information collected from the individual, consideration should be given to providing notice to such individuals.

Use and Retention

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
5.0	**The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes.**		
5.1	**Policies and Communications**		
5.1.0	**Privacy Policies** The entity's privacy policies address the use and retention of personal information.		
5.1.1	**Communication to Individuals** Individuals are informed that personal information is: • Used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise. • Retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation.	The entity's privacy notice describes the uses of personal information, for example: • Processing business transactions such as claims and warranties, payroll, taxes, benefits, stock options, bonuses, or other compensation schemes • Addressing inquiries or complaints about products or services, or interacting during the promotion of products or services • Product design and development, or purchasing of products or services • Participation in scientific or medical research activities, marketing, surveys, or market analysis	

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		• Participation in scientific or medical research activities, marketing, surveys, or market analysis • Personalization of Web sites or downloading software • Legal requirements • Direct marketing The entity's privacy notice explains that personal information will be retained only as long as necessary to fulfill the stated purposes, or for a period specifically required by law or regulation.	
5.2	**Procedures and Controls**		
5.2.1	**Use of Personal Information** Personal information is used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.	Systems and procedures are in place to monitor the use of personal information to ensure: • Use in conformity with the purposes identified in the entity's privacy notice. • Use in agreement with the consent received from the individual • Compliance with applicable laws and regulations	Some regulations have specific provisions concerning the use of personal information. Examples are the GLBA, the Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA).

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
5.2.2	**Retention of Personal Information** Personal information is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise. Personal information no longer retained is disposed and destroyed of in a manner that prevents loss, misuse, or unauthorized access.	The entity: • Documents its retention policies and disposal procedures. • Erases or destroy records in accordance with the retention policies, regardless of the method of storage (for example, electronic or paper-based). • Retains, stores, and disposes of archived and backup copies of records in accordance with its retention policies. • Ensures that personal information is not kept beyond the standard retention time unless there is a justified business reason for doing so. • Locates and removes specified personal information about an individual as required, for example, removing credit card numbers after the transaction is complete. • Regularly and systematically destroys, erases, or makes anonymous personal information no longer required to fulfill the identified purposes or required by laws and regulations. Contractual requirements should be considered when establishing retention practices.	Some laws specify the retention period for personal information; for example, HIPAA has a six-year retention period from the date of creation or last in effect for personal information. There may be other statutory record retention requirements; for example, certain data may need to be retained for tax purposes or in accordance with employment laws.

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Access

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
6.0	**The entity provides individuals with access to their personal information for review and update.**		
6.1	**Policies and Communications**		
6.1.0	**Privacy Policies** The entity's privacy policies address providing individuals with access to their personal information.		
6.1.1	**Communication to Individuals** Individuals are informed about how they may obtain access to their personal information to review, update, and correct that information.	The entity's privacy notice: • Explains how individuals may gain access to their personal information and any costs associated with obtaining such access. • Outlines the means by which individuals may update and correct their personal information (for example, in writing, by phone, by e-mail, or by using the entity's Web site).	
6.2	**Procedures and Controls**		
6.2.1	**Access by Individuals to Their Personal Information** Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.	Procedures are in place to: • Determine whether the entity holds or controls personal information about an individual. • Communicate the steps to be taken to gain access to the personal information.	Some laws and regulations specify: • Provisions and requirements for providing access to personal information (for example, HIPAA). • Requirements that requests for access to personal information be submitted in writing.

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		• Respond to an individual's request on a timely basis. • Provide a copy of personal information, upon request, in printed or electronic form that is convenient to both the individual and the entity. • Record requests for access, actions taken, including denial of access, and unresolved complaints and disputes.	
6.2.2	**Confirmation of an Individual's Identity** The identity of individuals who request access to their personal information is authenticated before they are given access to that information.	Employees are adequately trained to authenticate the identity of individuals before granting: • Access to their personal information • Requests to change sensitive or other personal information (for example, to update information such as address or bank details). The entity: • Does not use government-issued identifiers (for example, Social Security numbers or Social Insurance numbers) for authentication. • Mails information about a change request only to the address of record or, in the case of a change of address, to both the old and new addresses.	The extent of authentication considers the type and sensitivity of personal information that is made available. Different techniques may be considered for the different channels: • Web • Interactive voice response system • Call center • In person

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		• Requires that a user identification (ID) and password (or equivalent) be used to access user account information online.	
6.2.3	**Understandable Personal Information, Time Frame, and Cost** Personal information is provided to the individual in an understandable form, in a reasonable time frame, and at a reasonable cost, if any.	The entity: • Provides personal information to the individual in a format that is understandable (for example, not in code, not in a series of numbers, not in overly technical language or other jargon) and in a form convenient to both the individual and the entity. • Makes a reasonable effort to locate the personal information requested and, if personal information cannot be found, keeps sufficient records to demonstrate that a reasonable search was made. • Takes reasonable precautions to ensure that personal information released does not identify another person, directly or indirectly. • Provides access to personal information in a time frame that is similar to the entity's normal response times for other business transactions, or as permitted or required by law.	

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		• Provides access to personal information in archived or backup systems and media. • Informs individuals of the cost of access at the time the access request is made or as soon as practicable thereafter. • Charges the individual for access to personal information at an amount, if any, that is not excessive in relation to the entity's cost of providing access. • Provides an appropriate physical space to inspect personal information.	
6.2.4	**Denial of Access** Individuals are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.	The entity: • Outlines the reasons why access to personal information may be denied. • Records all denials of access and unresolved complaints and disputes. • Provides the individual with partial access in situations in which access to some of his or her personal information is justifiably denied. • Provides the individual with a written explanation as to why access to personal information is denied.	Some laws and regulations (for example, Principle 5, "Information Relating to Records Kept by Record-Keeper," point 2 of the Australian Privacy Act of 1988) cover situations in which the individual cannot review the reasons for denial of access.

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		• Provides a formal escalation and review process if access to personal information is denied. (See 6.2.7, "Escalation of Complaints and Disputes.") • Conveys the entity's legal rights and the individual's right to challenge, if applicable.	
6.2.5	**Updating or Correcting Personal Information** Individuals are able to update or correct personal information held by the entity. If practical and economically feasible to do so, the entity provides such updated or corrected information to third parties that previously were provided with the individual's personal information.	The entity: • Describes the process an individual must follow to update or correct personal information records (for example, in writing, by phone, by e-mail, or by using the entity's Web site). • Verifies the accuracy and completeness of personal information that an individual updates or changes (for example, by edit and validation controls, and forced completion of mandatory fields). • Records the date, time, and identification of the person making the change if the entity's employee is making a change on behalf of an individual.	In some jurisdictions (for example, PIPEDA, Schedule 1, clauses 4.5.2 and 4.5.3), personal information cannot be erased, but an entity is bound to cease further processing.

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		• Notifies third parties to whom personal information has been disclosed of amendments, erasures, or blocking of personal information, if it is possible and reasonable to do so.	
6.2.6	**Statement of Disagreement** Individuals are informed, in writing, about the reason a request for correction of personal information was denied, and how they may appeal.	If an individual and an entity disagree about whether personal information is complete and accurate, the individual may ask the entity to accept a statement claiming that the personal information is not complete and accurate. The entity: • Documents instances where an individual and the entity disagree about whether personal information is complete and accurate. • Informs the individual, in writing, of the reason a request for correction of personal information is denied, citing the individual's right to appeal. • Informs the individual, when access to personal information is requested or when access is actually provided, that the statement of disagreement may include information about the nature of the change sought by the individual and the reason for its refusal by the entity.	Some regulations (for example, HIPAA) have specific requirements for denial of requests and handling of disagreements from individuals. If a challenge is not resolved to the satisfaction of the individual, when appropriate, the existence of such challenge is communicated to third parties having access to the information in question.

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		• If appropriate, notifies third parties who have previously been provided with personal information that there is a disagreement.	
6.2.7	**Escalation of Complaints and Disputes** Complaints and other disputes are escalated until they are resolved.	The entity has established a formal escalation process to address complaints and disputes that are not resolved. The entity: • Trains employees responsible for handling individuals' complaints and disputes about the escalation process. • Documents unresolved complaints and disputes. • Escalates complaints and disputes for review by management. • Resolves complaints and disputes on a timely basis. • Engages an external, third-party dispute resolution service (for example, an arbitrator), when appropriate, to assist in the resolution of complaints and disputes.	Some laws (for example, PIPEDA) permit escalation through the court system up to the most senior court.

Disclosure to Third Parties

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
7.0	**The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.**		
7.1	**Policies and Communications**		
7.1.0	**Privacy Policies** The entity's privacy policies address the disclosure of personal information to third parties.		
7.1.1	**Communication to Individuals** Individuals are informed that personal information is disclosed to third parties only for the purposes identified in the notice and for which the individual has provided implicit or explicit consent unless a law or regulation specifically allows or requires otherwise. Disclosure includes any limitation on the third party's privacy practices and controls. Lack of such disclosure indicates that the third party's privacy practices and controls meet or exceed those of the entity.	The entity's privacy notice: • Describes the practices related to the sharing of personal information (if any) with third parties and the reasons for information sharing. • Identifies third parties or classes of third parties to whom personal information is disclosed. • Informs individuals that personal information is disclosed to third parties only for the purposes (1) identified in the notice and (2) for which the individual has provided implicit or explicit consent, or as specifically allowed or required by law or regulation. Individuals are informed if third parties provide lower levels of protection.	The entity's privacy notice may disclose: • The process used to assure the privacy and security of personal information that has been disclosed to a third party. • How personal information shared with a third party will be kept up-to-date, so that outdated or incorrect information shared with a third party will be changed if the individual has changed his or her information.

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
7.1.2	**Communication to Third Parties** Privacy policies are communicated to third parties to whom personal information is disclosed.	Prior to sharing personal information with a third party, the entity communicates its privacy policies to and obtains a written agreement from the third party that its practices are substantially equivalent to the entity's.	
7.2	**Procedures and Controls**		
7.2.1	**Disclosure of Personal Information** Personal information is disclosed to third parties only for the purposes described in the notice and for which the individual has provided implicit or explicit consent, unless a law or regulation specifically allows or requires otherwise.	Systems and procedures are in place to: • Prevent the disclosure of personal information to third parties unless an individual has given implicit or explicit consent for the disclosure. • Document the nature and extent of personal information disclosed to third parties. • Test whether disclosure to third-parties is in compliance with the entity's privacy policies and procedures, or as specifically allowed or required by law or regulation. • Document any third-party disclosures for legal reasons.	Personal information may be disclosed through various legal processes to law enforcement or regulatory agencies. Some laws and regulations have specific provisions for the disclosure of personal information. Some permit disclosure of personal information without consent while others require verifiable consent.

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
7.2.2	**Protection of Personal Information** Personal information is disclosed only to third parties who have agreements with the entity to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction.	Systems and procedures are in place to: • Provide a level of protection of personal information equivalent to that of the entity when information is provided to a third party (that is, by contract or agreement). • Affirm that the level of protection of personal information by third parties is equivalent to that of the entity, for example, by obtaining assurance (for example, an auditor's report), contractual obligation, or other representation (for example, written annual confirmation). • Limit the third party's use of personal information to purposes necessary to fulfill the contract. • Communicate the individual's preferences to the third party. • Refer any requests for access or complaints about the personal information transferred by the entity to the privacy officer. • Specify how and when third parties are to dispose of or return any personal information provided by the entity.	The entity is responsible for personal information in its possession or custody, including information that has been transferred to a third party. Some regulations (for example, from the U.S. federal financial regulatory agencies) require that an entity take reasonable steps to oversee appropriate service providers by exercising appropriate due diligence in the selection of service providers. The EU requires substantially equivalent privacy protection before transferring personal information to a third party. Some jurisdictions, including some countries in Europe, require entities that transfer personal information to register with their regulatory body prior to transfer. PIPEDA requires a comparable level of protection while the personal information is being processed by a third party. Article 25 of the U.S./EU's Safe Harbor requires that such transfers take place only where the third party ensures an adequate level of protection.

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
7.2.3	**New Purposes and Uses** Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of the individual.	Systems and procedures are in place to: • Notify individuals and obtain their consent prior to disclosing personal information to a third party for purposes not identified in the privacy notice. • Document whether the entity has notified the individual and received the individual's consent. • Monitor that personal information is being provided to third parties only for uses specified in the privacy notice.	Other types of onward transfers include transfers to third parties who are: • Subsidiaries or affiliates. • Providing a service requested by the individual. • Law enforcement or regulatory agencies. • In another country and may be subject to other requirements.
7.2.4	**Misuse of Personal Information by a Third Party** The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.	The entity: • Monitors complaints to identify indications of any misuse of personal information by third parties. • Responds to any knowledge of a third party using or disclosing personal information in variance with the entity's privacy policies and procedures or contractual arrangements. • Mitigates, to the extent practicable, any harm caused by the use or disclosure of personal information by the third party in violation of the entity's privacy policies and procedures.	

(continued)

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		• Takes remedial action in the event that a third party misuses personal information. (For example, contractual clauses address the ramification of misuse of personal information.)	

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Security

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
8.0	**The entity protects personal information against unauthorized access (both physical and logical).**		
8.1	**Policies and Communications**		
8.1.0	**Privacy Policies** The entity's privacy policies address the security of personal information.	Privacy policies adequately address security measures to safeguard the privacy of personal information whether in electronic, paper, or other forms. Security measures are consistent with the sensitivity of the personal information.	Personal information in any location under control of the entity or deemed to be under control of the entity must be protected.
8.1.1	**Communication to Individuals** Individuals are informed that precautions are taken to protect personal information.	The entity's privacy notice describes the general types of security measures used to protect the individual's personal information, for example: • Employees are authorized to access personal information based on job responsibilities. • Authentication is used to prevent unauthorized access to personal information stored electronically. • Physical security is maintained over personal information stored in hard copy form, and encryption is used to prevent unauthorized access to personal information sent over the Internet.	Users, management, providers, and other parties should strive to develop and adopt good privacy practices and to promote conduct that recognizes security needs and respects the legitimate interests of others. Consideration should be given to disclosing in the privacy notice the security obligations of individuals, such as keeping user IDs and passwords confidential and reporting security compromises.

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		• Special security safeguards are applied to sensitive information.	Consideration should be given to disclosing in the privacy notice the security obligations of individuals, such as keeping user IDs and passwords confidential and reporting security compromises.
8.2	**Procedures and Controls**		
8.2.1	**Information Security Program** A security program has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction.	The entity's security program addresses the following matters related to protection of personal information: *a.* Periodic risk assessments *b.* Identification and documentation of the security requirements of authorized users *c.* Allowing access, the nature of that access, and who authorizes such access *d.* Preventing unauthorized access by using effective physical and logical access controls *e.* The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access *f.* Assignment of responsibility and accountability for security	Safeguards employed may consider the nature and sensitivity of the data, as well as the size and complexity of the entity's operations. For example, the entity may protect personal information and other sensitive information to a level greater than it applies for other information. Consideration should be given to limiting the disclosure of detailed security procedures so as not to compromise internal security. Some regulations (for example, HIPAA) provide a greater level of detail and guidance on specific security measures to be considered and implemented. Some security rules (for example, GLBA-related rules for safeguarding information) require: *(continued)*

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		g. Assignment of responsibility and accountability for system changes and maintenance *h* Implementing system software upgrades and patches *i.* Testing, evaluating, and authorizing system components before implementation *j.* Addressing how complaints and requests relating to security issues are resolved *k.* Handling errors and omissions, security breaches, and other incidents *l.* Procedures to detect actual and attempted attacks or intrusions into systems and to proactively test security procedures (for example, penetration testing) *m.* Allocating training and other resources to support its security policies *n.* Provision for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies *o.* Disaster recovery plans and related testing	• Board (or committee or individual appointed by the board) approval and oversight of the entity's information security program. • That an entity take reasonable steps to oversee appropriate service providers by: —Exercising appropriate due diligence in the selection of service providers. —Requiring service providers by contract to implement and maintain appropriate safeguards for the personal information at issue. Some security laws (for example, California SB1386) require entities to notify individuals if the protection of their personal information is compromised.

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		p. Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts *q.* A requirement that users, management, and third parties confirm (initially and annually) their understanding of and agreement to comply with the entity's privacy policies and procedures related to the security of personal information The entity's security program prevents access to personal information in computers, media and paper-based information that are no longer in active use by the organization (e.g. computers, media and paper-based information in storage, sold or otherwise disposed of).	
8.2.2	**Logical Access Controls** Logical access to personal information is restricted by procedures that address the following matters: *a.* Authorizing and registering internal personnel and individuals	Systems and procedures are in place to: • Establish the level and nature of access that will be provided to users based on the sensitivity of the data and the user's legitimate business need to access the personal information.	User authorization processes consider: • How the data is accessed (internal or external network), as well as the media and technology platform of storage.

(continued)

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	b. Identifying and authenticating internal personnel and individuals *c.* Making changes and updating access profiles *d.* Granting system access privileges and permissions *e.* Preventing individuals from accessing other than their own personal or sensitive information *f.* Limiting access to personal information to only authorized internal personnel based upon their assigned roles and responsibilities *g.* Distributing output only to authorized internal personnel *h.* Restricting logical access to offline storage, backup data, systems, and media *i.* Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls) *j.* Preventing the introduction of viruses, malicious code, and unauthorized software	• Authenticate users, for example, by user name and password, certificate, external token, or biometrics. • Require the user to provide a valid ID and password to be authenticated by the system before access is granted to systems handling personal information. • Require enhanced security measures for remote access, such as additional or dynamic passwords, dial-back controls, digital certificates, or secure ID cards, virtual private network (VPN), properly configured firewalls. • Implement intrusion detection and monitoring systems.	• Access to paper and backup media containing personal information. • Denial of access to joint accounts without other methods to authenticate the actual individuals.

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
8.2.3	**Physical Access Controls** Physical access is restricted to personal information in any form (including the components of the entity's system(s) that contain or protect personal information).	Systems and procedures are in place to: • Manage logical and physical access to personal information, including hard copy, archival, and backup copies. • Log and monitor access to personal information. • Prevent the unauthorized or accidental destruction or loss of personal information. • Investigate breaches and attempts to gain unauthorized access. • Maintain physical control over the distribution of reports containing personal information. • Securely dispose of waste containing confidential information (for example, shredding).	Physical safeguards may include the use of locked file cabinets, card access systems, physical keys, sign-in logs, and other techniques to control access to offices, data centers, and other locations in which personal information is processed or stored.
8.2.4	**Environmental Safeguards** Personal information, in all forms, is protected against unlawful destruction, accidental loss, natural disasters, and environmental hazards.	Management maintains measures to protect against environmental factors (for example, fire, flood, dust, power failure, and excessive heat and humidity) based on its risk assessment. The entity's controlled areas are protected against fire using both smoke detectors and a fire suppression system. Water detectors are installed within the raised floor areas.	

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		The entity site is protected against a disruption in power supply to the processing environment by both uninterruptible power supplies and emergency power supplies. This equipment is tested semiannually.	
8.2.5	**Transmitted Personal Information** Personal information is protected when transmitted by mail and over the Internet and public networks by deploying industry standard encryption technology for transferring and receiving personal information.	Systems and procedures are in place to: • Address the confidentiality of information and communication, and the appropriate protection of personal information transmitted over the Internet or other public networks. • Define minimum levels of encryption and controls. • Employ industry standard encryption technology, for example, 128 bit secure socket layer (SSL), for transferring and receiving personal information. • Approve external network connections. • Protect personal information sent by mail, courier, or other physical means.	Some regulations (for example, HIPAA) have specific provisions for the electronic transmission and authentication of signatures with respect to health information records (that is, associated with the standard transactions). Some credit card vendors have issued minimum requirements for protecting cardholder data, including the requirement to use encryption techniques for credit card and transaction-related data in transmission and in storage. As technology, market, and regulatory conditions evolve, new measures may become necessary to meet acceptable levels of protection (for example, 128-bit SSL encryption, including user IDs and passwords).

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
8.2.6	**Testing Security Safeguards** Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually.	Systems and procedures are in place to: • Regularly test the effectiveness of the key administrative, technical, and physical safeguards protecting personal information. • Periodically undertake independent audits of security controls using either internal or external auditors. • Test card access systems and other physical security devices at least annually. • Document and test disaster recovery and contingency plans at least annually to ensure their viability. • Periodically undertake threat and vulnerability testing, including security penetration reviews and Web vulnerability and resilience. • Make appropriate modifications to security policies and procedures on a periodic basis, taking into consideration the results of tests performed and new and changing threats and vulnerabilities.	The frequency and nature of the testing of security safeguards will vary with the entity's size and complexity, the nature and scope of its activities, and the sensitivity of personal information. Some security regulations (for example, GLBA-related rules for safeguarding information) require an entity to: • Conduct regular tests of key controls, systems, and procedures by independent third parties or by staff independent of those that develop or maintain security (or at least have these independent parties review results of testing). • Assess and possibly adjust its information security at least annually.

Quality

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
9.0	**The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.**		
9.1	**Policies and Communications**		
9.1.0	**Privacy Policies** The entity's privacy policies address the quality of personal information.		
9.1.1	**Communication to Individuals** Individuals are informed that they are responsible for providing the entity with accurate and complete personal information, and for contacting the entity if correction of such information is required.	The entity's privacy notice explains that the extent to which personal information is kept accurate and complete depends on the use of the information.	
9.2	**Procedures and Controls**		
9.2.1	**Accuracy and Completeness of Personal Information** Personal information is accurate and complete for the purposes for which it is to be used.	Systems and procedures are in place to: • Edit and validate personal information as it is collected, created, maintained, and updated. • Record the date when the personal information is obtained or updated.	

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		• Specify when and how the personal information is to be updated and the source for the update (for example, annual reconfirmation of information held and methods for individuals to proactively update personal information). • Indicate how to verify the accuracy and completeness of personal information obtained directly from an individual, received from a third party (see 4.2.3, "Collection From Third Parties"), or disclosed to a third party (see 7.2.2, "Protection of Personal Information"). • Ensure personal information used on an ongoing basis is sufficiently accurate and complete to make decisions, unless there are clear limits to the need for accuracy. • Ensure personal information is not routinely updated, unless such a process is necessary to fulfill the purposes for which it is to be used.	
		The entity undertakes periodic assessments to check the accuracy of personal information records and to correct them, as necessary.	

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
9.2.2	**Relevance of Personal Information** Personal information is relevant to the purposes for which it is to be used.	Systems and procedures are in place to: • Ensure personal information is sufficiently relevant for the purposes for which it is to be used and to minimize the possibility that inappropriate information is used to make business decisions about the individual. • Periodically assess the relevance of personal information records and to correct them, as necessary, to minimize the use of inappropriate data for decision making.	

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Monitoring and Enforcement

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
10.0	**The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.**		
10.1	**Policies and Communications**		
10.1.0	**Privacy Policies** The entity's privacy policies address the monitoring and enforcement of privacy policies and procedures.		
10.1.1	**Communication to Individuals** Individuals are informed about how to contact the entity with complaints.	The entity's privacy notice: • Describes how individuals can contact the entity with complaints (for example, via an e-mail link to the entity's Web site or a telephone number). • Provides relevant contact information to which the individual can direct complaints (for example, name, telephone number, mailing address, and e-mail address of the individual or office responsible for handling complaints).	
10.2	**Procedures and Controls**		
10.2.1	**Complaint Process** A process is in place to address complaints.	The corporate privacy officer or other designated individual is authorized to address privacy-related complaints, disputes, and other problems.	

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		Systems and procedures are in place that set out: • Procedures to be followed in communicating and resolving complaints about the entity • Action that will be taken with respect to the disputed information until the complaint is satisfactorily resolved • Remedies available in case of a breach of personal information and how to communicate this information to an individual • Recourse available and formal escalation process to review and approve any recourse offered to individuals • Contact information and procedures to be followed with any designated third-party dispute resolution or similar service (if offered)	
10.2.2	**Dispute Resolution and Recourse** Every complaint is addressed and the resolution is documented and communicated to the individual.	The entity has a formally documented process in place to: • Record and respond to all complaints in a timely manner. • Periodically review unresolved disputes and complaints to ensure they are resolved in a timely manner.	Some regulations (for example HIPAA and COPPA) have specific procedures and requirements.

(continued)

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		• Identify trends and the potential need to change the entity's privacy policies and procedures. • Address complaints that cannot be resolved. • Use specified independent third-party dispute resolution services or other process mandated by regulatory bodies in the event the individual is not satisfied with the entity's proposed resolution, together with a commitment from such third parties to handle such recourses. If the entity offers a third-party dispute resolution process for complaints that cannot be resolved directly with the entity, an explanation is provided about how an individual can use that process.	
10.2.3	**Compliance Review** Compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts is reviewed and documented and the results of such reviews are reported to management. If problems are identified, the entity's privacy policies and procedures are enforced.	Systems and procedures are in place to: • Annually review compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts. • Document periodic reviews, for example, internal audit plans, audit reports, compliance checklists, and management sign-off, are maintained.	

(continued)

Reference	*Criteria*	*Illustrations and Explanations of Criteria*	*Additional Considerations*
		• Report the results of the compliance review and recommendations for improvement to management, and implement a remediation plan. • Monitor the resolution of issues and vulnerabilities noted in the compliance review to ensure that appropriate corrective action is taken on a timely basis (that is, privacy policies and procedures are revised, as necessary).	
10.2.4	**Instances of Noncompliance** Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective measures are taken on a timely basis.	Systems and procedures are in place to: • Notify employees of the need to report privacy breaches and security vulnerabilities in a timely manner. • Inform employees of the appropriate channels to report security vulnerabilities and privacy breaches. • Document instances of noncompliance with privacy policies and procedures. • Monitor the resolution of security vulnerabilities and privacy breaches to ensure appropriate corrective measures are taken on a timely basis. • Identify trends that may require revisions to privacy policies and procedures.	

ATTACHMENT A

Transition From AICPA/CICA Trust Services Online Privacy Principle and Criteria to the AICPA/CICA Trust Services Privacy Principle and Criteria

Transition Guidance

For Trust Services assurance privacy engagements with reporting periods beginning on or after April 1, 2004, the AICPA/CICA Privacy Framework Principle and Criteria are to be used in place of the AICPA/CICA Trust Services Online Privacy Principle and Criteria and will become known as the AICPA/CICA Trust Services Privacy Principle and Criteria. Earlier application is encouraged.

WebTrust Online Privacy Seal or WebTrust Consumer Protection Seal[5]

Existing WebTrust Online Privacy Engagements

For those entities wishing to continue to display a WebTrust Online Privacy seal or a WebTrust Consumer Protection seal (both seals require an attestation or assurance report based on the AICPA/CICA Trust Services Online Privacy Principle and Criteria), a new unqualified report must be issued using the new AICPA/CICA Trust Services Privacy Principle and Criteria when the examination to renew the seal covers a period beginning on or after April 1, 2004.

New Online Privacy Engagements

When the privacy engagement relates to an online segment, an entity may choose to display a WebTrust Online Privacy seal or a WebTrust Consumer Protection seal. For these engagements:

- The scope of the engagement needs to include, but is not limited to, an online business segment of the entity. Use of the WebTrust Seal is only permitted in circumstances where the online business segment is included in the scope of the practitioner's examination.
- WebTrust seals are trademarked and service-marked graphic images and their use is subject to the Trust Services License agreement. The Trust Services license agreement and the guidance established for the Trust Services program permit the images to be displayed on a client's Web site or electronically, subject to certain requirements:
  - The practitioner must be licensed under the Trust Services license agreement.
  - The entity must have received a report from the practitioner that does not include a qualification or scope limitation.
  - The seal must be issued using the AICPA/CICA processes and be listed on the Institutes' server.
  - Fees as established by the Trust Services license agreement for the use of the seal must be paid to the Institutes.

---

[5] Currently, the use of a seal for other types of privacy assurance/attestation reports is under consideration. Please contact Karyn Waller at the AICPA (kwaller@aicpa.org) or Bryan Walker at the CICA (bryan.walker@cica.ca) for additional information.

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

When the WebTrust Seal is used, the Task Force recommends that the practitioner's report includes language such as the following: "The WebTrust Online Privacy Seal constitutes a symbolic representation of the contents of the independent auditor's report and it is not intended, nor should it be construed, to update that report or provide any additional assurance."

AICPA
Assurance Services Executive Committee

SUSAN RUCKER, *Chair*
GARI FAILS
EVERETT C. JOHNSON, JR.
JOHN LAINHART
THOMAS SIDERS
MIKE STARR
KEITH VANCE
THOMAS WALLACE
NEAL WEST

AICPA Staff

ANTHONY J. PUGLIESE
Vice President, Member Innovation

J. LOUIS MATHERNE
Direction, Business Assurance and Advisory Services

CICA
Assurance Services Development Board

DOUG MCPHIE, *Chair*
MARILYN KUNTZ
DOUG TIMMINS

CICA Staff

CAIRINE M. WILSON
Vice President, Innovation

GREGORY P. SHIELDS
Director, Assurance Services Development

AICPA/CICA
Trust Services Task Force

THOMAS E. WALLACE, *Chair*
GARY BAKER
BRUCE R. BARRICK
EFRIM BORITZ
JOSEPH G. GRIFFIN
ARTURO LOPEZ
EMIL RAGONES
DONALD E. SHEEHY
CHRISTIAN R. STORMER
ALFRED F. VAN RANST, JR.
MIKLOS VASARHELYI
JEFF WARD

Staff Contacts

BRYAN WALKER, CICA
Principal, Assurance Services Development

KARYN WALLER, AICPA
Senior Technical Manager, Trust Services

For issues related to this release, please e-mail assure@aicpa.org.

The AICPA and CICA are extremely grateful to Chris Leach for co-chairing this task force at its inception and to Robert Parker, Robert Reimer, David Ross and Kerry Shackelford for their technical assistance with this document.

[The next page is 52,201.]

 Copyright © 2004, American Institute of Certified Public Accountants, Inc.

Section 17,200

Suitable Trust Services Criteria and Illustrations for WebTrust® for Certification Authorities

March 2003

NOTICE TO READERS

The Suitable Trust Services Criteria and Illustrations present criteria established by the Assurance Services Executive Committee of the AICPA for use by practitioners when providing attestation services on systems in the subject matters of security, availability, processing integrity, online privacy, confidentiality, and certification authorities. The Assurance Services Executive Committee, in establishing and developing these criteria, followed due process procedures, including exposure of the proposed criteria for public comment. The Assurance Services Executive Committee has been designated as a senior committee and has been given authority to make public statements and publish measurement criteria without clearance from Council or the Board of Directors under Bylaw section 3.6 (AICPA, *Professional Standards*, vol. 2, BL sec. 360).

Introduction

.01 This document provides a framework for licensed WebTrust® practitioners to assess the adequacy and effectiveness of the controls employed by certification authorities (CAs).[1] The importance of this function will continue to increase as the need for third-party authentication to provide assurance with respect to electronic commerce (e-commerce) business activities increases. As a result of the technical nature of the activities involved in securing e-commerce transactions, this document also provides a brief overview of public key infrastructure (PKI) using cryptography, trusted third-party concepts, and their increasing use in e-commerce.

.02 Confidentiality, authentication, integrity, and nonrepudiation are the four most important ingredients required for trust in e-commerce transactions. The emerging response to these requirements is the implementation of PKI technology. PKI uses digital certificates and asymmetric cryptography to address these requirements. PKI provides a means for relying parties (that is, recipients

[1] Within the electronic commerce (e-commerce) industry, companies whose main business is to act as certification authorities, or companies who have established a certification authority function to support an e-commerce business activity, are routinely referred to as *CAs* or as performing a *CA function*.

In Canada and certain other jurisdictions, public accounting professionals, including the practitioners who are licensed to perform WebTrust® assurance services, carry the title of *chartered accountants*, also routinely referred to as CAs or as being a CA.

To avoid confusion in this document, the term *practitioner*, which is used widely in accounting literature, is used to identify a certified public accountant (CPA) or the equivalent, who is licensed to perform WebTrust assurance services.

In summary:

- The term CA is *never* used in this standard to refer to a chartered accountant.
- The term CA is used *only* to denote a certification authority (CA) or to refer to the certification authority function (CA function).
- The term *practitioner* is used to denote a properly qualified and licensed certified public accountant.

of certificates who act in reliance on those certificates, digital signatures verified using those certificates, or both) to know that another individual's or entity's public key actually belongs to that individual or entity. CA organizations and CA functions have been established to address this need.

.03 Public key cryptography is critical to establishing secure e-commerce. However, it has to be coupled with other secure protocols to provide a comprehensive security solution. Several cryptographic protocols require digital certificates (in effect, electronic credentials) issued by an independent, trusted third party (the CA) to authenticate the transaction. CAs have assumed an increasingly important role in secure e-commerce. Although there is a large body of existing national, international, and proprietary standards and guidelines for the use of cryptography, the management of digital certificates, and the policies and practices of CAs, these standards have not been applied or implemented uniformly.

.04 To increase consumer confidence in the Internet as a vehicle for conducting e-commerce and in the application of PKI technology, the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) have developed a set of principles and criteria for CAs, the WebTrust Principles and Criteria for Certification Authorities. Public accounting firms and practitioners who are specifically licensed by the AICPA can provide assurance services to evaluate and test whether the services provided by a particular CA meet these principles and criteria. The posting of the WebTrust seal of assurance for CAs is a symbolic representation of a practitioner's unqualified report. Similar to the WebTrust seal for business-to-consumer e-commerce, the seal of assurance also indicates that those who use the digital certificates (and certificate status information) issued by the CA, subscribers, and relying parties can click on the seal to see the practitioner's report. This seal is displayed on the CA's Web site together with links to the practitioner's report and other relevant information.

.05 This document is designed to benefit users and providers of CA e-commerce assurance services by providing a common body of knowledge that is communicated to such parties. *Suitable Trust Services Criteria and Illustrations for Certification Authorities* is consistent with standards being developed by the American National Standards Institute (ANSI) and the Internet Engineering Task Force (IETF).[2]

Overview

Electronic Commerce

.06 E-commerce involves individuals and organizations engaging in a variety of electronic business transactions, without paper documents, using computer and

---

[2] The American National Standards Institute (ANSI) X9F5 Digital Signature and Certificate Policy working group is developing the X9.79 *PKI Practices and Policy Framework* (X9.79) standard for the financial services community. This standard includes detailed Certification Authority Control Objectives against which certification authorities may be evaluated. An International Organization for Standardization (ISO) working group has been formed to standardize X9.79 based on international requirements in a new international standard. In addition, the American Bar Association's Information Security Committee (ABA-ISC) is developing the *PKI Assessment Guidelines* (PAG) which address the legal and technical requirements for certification authorities. The PAG makes reference to the Certification Authority Control Objectives that are detailed in the draft X9.79 standard and reflected in the WebTrust Principles and Criteria for Certification Authorities. The Certification Authority Control Objectives referred to in each of these documents were developed based on the existing body of ANSI, ISO, Internet Engineering Task Force (IETF), and other existing standards.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

telecommunication networks. These networks can be either private or public, or a combination of the two. Traditionally, the definition of e-commerce has been focused on electronic data interchange (EDI) as the primary means of conducting business electronically between entities with a preestablished contractual relationship. Commerce has also been conducted electronically for years in the form of credit card transactions authorized at the point of sale, debit card transactions, and cash advances from automatic teller machines. More recently, however, with the development of electronic mail, and separately, the browser and HTML, the definition of e-commerce has broadened to encompass business conducted over the Internet between entities generally not previously known to each other. This is attributable to the Web's surge in popularity and the acceptance of the Internet as a viable transport mechanism for business information. The use of a public network-based infrastructure such as the Internet can reduce costs and "level the playing field" for small and large businesses. This allows companies of all sizes to extend their reach to a broader customer base.

Public Key Infrastructure

.07 With the expansion of e-commerce, PKI is growing in importance and will probably be the most critical enterprise security investment a company will make in the next several years. PKI enables parties to an e-commerce transaction to identify one another by providing authentication with digital certificates, and allows reliable business communications by providing confidentiality through the use of encryption and authentication, data integrity, and a reasonable basis for nonrepudiation through the use of digital signatures.

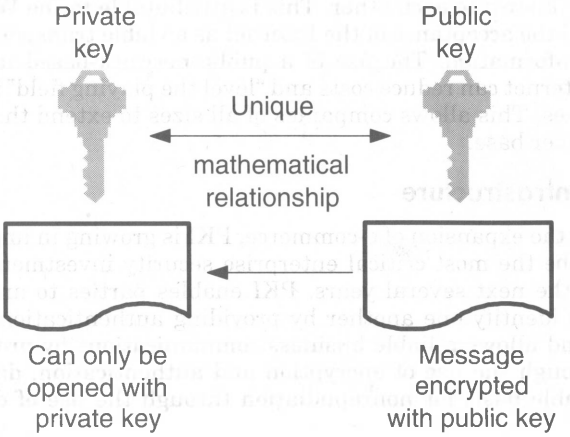
.08 PKI uses public/private-key pairs—two mathematically related keys. Typically, one of these keys is made public, by posting it on the Internet for example, while the other remains private. Public-key cryptography works in such a way that a message encrypted with the public key can be decrypted only with the private key, and, conversely, a message signed with a private key can only be verified with the public key. This technology can be used in different ways to provide the four ingredients required for trust in e-commerce transactions, namely confidentiality, authentication, integrity, and nonrepudiation.

.09 Using PKI, a subscriber (that is, an end entity or individual whose public key is cryptographically bound to his or her identity in a digital certificate) has an asymmetric cryptographic key pair (that is, a public key and a private key). The subscriber's private key must be kept secret, whereas the public key may be made widely available, usually presented in the form of a digital certificate to ensure that relying parties know with confidence the identity to which the public key belongs. Using public key cryptography, the subscriber can send a message signed with his or her private key. The signature can be validated by the message recipient using the subscriber's public key. The subscriber can also encrypt a message using the recipient's public key. The message can be decrypted only with the recipient's private key.

.10 A subscriber first obtains a public/private key pair (generated by the subscriber or for the subscriber as a service). The subscriber then goes through a registration process by submitting his or her public key to a certification authority or a registration authority (RA), which acts as an agent for the CA. The CA or RA verifies the identity of the subscriber in accordance with the CA's established business practices (that may be contained in a certification practice statement), and then issues a digital certificate. The certificate includes the subscriber's public key and identity information, and is digitally signed by the CA,

which binds the subscriber's identity to that public key. The CA also manages the subscriber's digital certificate through the certificate life cycle (that is, from registration through revocation or expiration). In some circumstances, it remains important to manage digital certificates even after expiry or revocation so digital signatures on stored documents held past the revocation or expiry period can be validated at a later date.

.11 The following diagram illustrates the relationship between a subscriber's public and private keys, and how they are used to secure messages sent to a relying party.



.12 A transaction submitted by a customer to an online merchant via the Internet can be encrypted with the merchant's public key and therefore can only be decrypted by that merchant using the merchant's private key—ensuring a level of confidentiality. Confidentiality can also be achieved through the use of Secure Socket Layer (SSL), Secure/Multipurpose Internet Mail Extensions (S/MIME), and other protocols, such as Secure Electronic Transaction (SET).

Digital Signature

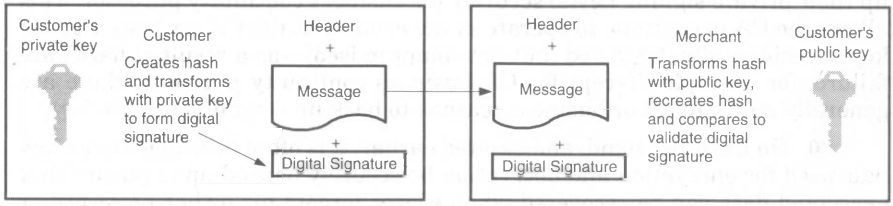
.13 Digital signatures can be used to provide authentication, integrity, and nonrepudiation. Generally speaking, if a customer sends a digitally signed message to a merchant, the customer's private key is used to generate the digital signature and the customer's public key can be used by the merchant to verify the signature. The mathematical processes employed differ somewhat depending on the kind of asymmetric cryptographic algorithm employed. For example, the processes are slightly different for reversible algorithms (that is, those that can be readily used to support digital signatures as well as encryption), such as Rivest Shamir Adleman (RSA), and irreversible algorithms, such as the Digital Signature Algorithm (DSA).

.14 The following example illustrates the digital signature generation and verification process for a reversible asymmetric cryptographic algorithm (such as RSA). Suppose a customer wants to send a digitally signed message to a merchant. The customer runs the message through a hash function (that is, a mathematical function that converts a message into a fixed-length block of data—the hash—in such a fashion that the hash uniquely reflects the message; in effect, is the message's "fingerprint." The customer then transforms the hash using the algorithm and the customer's private key to create

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

the digital signature, which is appended to the message. A header is also added, indicating the merchant's e-mail address, the sender's e-mail address, and other information such as the time the message is sent. The message header, the message itself, and the digital signature are then sent to the merchant. The customer has the option to send his or her public key certificate to the merchant in the message itself. All of this is usually done by the e-mail software in such a way that the process is transparent to the user.

.15 The following diagram illustrates the process of using a subscriber's key pair to ensure the integrity and authenticity of a message sent by the customer (subscriber) to a merchant.



.16 To determine whether the message came from the customer (that is, authentication) and to determine whether the message has not been modified (that is, integrity), the merchant validates the digital signature. To do so, the merchant must obtain the customer's public key certificate. If the customer did not send his or her public key certificate as part of the message, the merchant would typically obtain the customer's public key certificate from an online repository (maintained by the CA, another party acting as the agent of the CA, or any other source even if unrelated to the CA). The merchant then validates that the customer's digital certificate (containing the customer's public key) was signed by a recognized CA to ensure that the binding between the public key and the customer represented in the certificate has not been altered. Next, the merchant extracts the public key from the certificate and uses that public key to transform the digital signature to reveal the original hash. The merchant then runs the message as received through the same hash function to create a hash of the received message. To verify the digital signature, the merchant compares these two hashes. If they match, the digital signature validates and the merchant knows that the message came from the customer and it was not modified from the time the signature was made. If the hashes do not match, the merchant knows that the message was either modified in transit or the message was not signed with the customer's private key. As a result, the merchant cannot rely on the digital signature.

.17 Digital signatures can also be used to provide a basis for nonrepudiation (that is, that the signer cannot readily deny having signed the message). For example, an online brokerage customer who purchases 1,000 shares of stock using a digitally signed order via the Internet should have a difficult task if he or she later tries to deny (that is, repudiate) having authorized the purchase.

Differences Between Encryption Key Pairs and Signing Key Pairs

.18 As stated earlier, establishing a reasonable basis for nonrepudiation requires that the private key used to create a digital signature (that is, the

signing private key) be generated and stored securely under the sole control of the user. In the event a user forgets his or her password or loses, breaks, or destroys his or her signing private key, it is acceptable to generate a new signing key pair for use from that point forward with minimal impact on the subscriber. Previously signed documents can still be verified with the user's old signature verification public key. Documents subsequently signed with the user's new signing private key must be verified with the user's new signature verification public key.

.19 Extra care is required to secure the CA's signing private key, which is used for signing user certificates. The trustworthiness of all certificates issued by a CA depends upon the CA protecting its private signing key. CAs often back up their private signing key(s) securely for business continuity purposes. This allows the CA to continue to operate in the event that the CA's private signing key is accidentally destroyed (but not compromised)—as a result of hardware failure, for example. Except for CA business continuity purposes, there are generally no technical or business reasons to back up a signing private key.

.20 On the other hand, and as cited earlier, it is often desirable that a key pair used for encryption and decryption be securely backed up to ensure that encrypted data can be recovered when a user forgets his or her password or otherwise loses access to his or her decryption key. This is analogous to requiring that the combination to a safe be backed up in case the user forgets it or becomes incapacitated. As a result, a PKI typically requires two key pairs for each user: one key pair for encryption and decryption and a second key pair for signing and signature verification.

Certification Authority

.21 For these technologies to enable parties to securely conduct e-commerce, one important question must be answered: How can a user in the digital world know that an individual's public key actually belongs to that individual? A digital certificate, which is an electronic document containing information about an individual and his or her public key, is the answer. This document is digitally signed by a trusted organization, the CA. The basic premise is that the CA is vouching for the link between an individual's identity and his or her public key. The CA provides a level of assurance that the public key contained in the certificate does indeed belong to the entity named in the certificate. The digital signature placed on the public key certificate by the CA provides the cryptographic binding between the entity's public key, the entity's name, and other information in the certificate, such as a validity period. For a relying party to determine whether the certificate was issued by a legitimate CA, the relying party must verify the issuing CA's signature on the certificate by using the CA's public key. The public keys of many common root CAs (defined in paragraph .29) are preloaded into standard Web browser software (for example, Netscape Navigator and Microsoft Internet Explorer).

.22 The purpose of a CA is to manage the certificate life cycle, which includes generation and issuance, distribution, renewal and rekey, revocation, and suspension of certificates. The CA frequently delegates the initial registration of subscribers to RAs, which act as agents for the CA. In some cases, the CA may perform registration functions directly. The CA is also responsible for providing certificate status information though the issuance of certificate revocation lists (CRLs), the maintenance of an online status-checking mechanism, or both. Typically, the CA posts the certificates and CRLs that it has issued to a repository (such as an online directory) that is accessible to relying parties.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

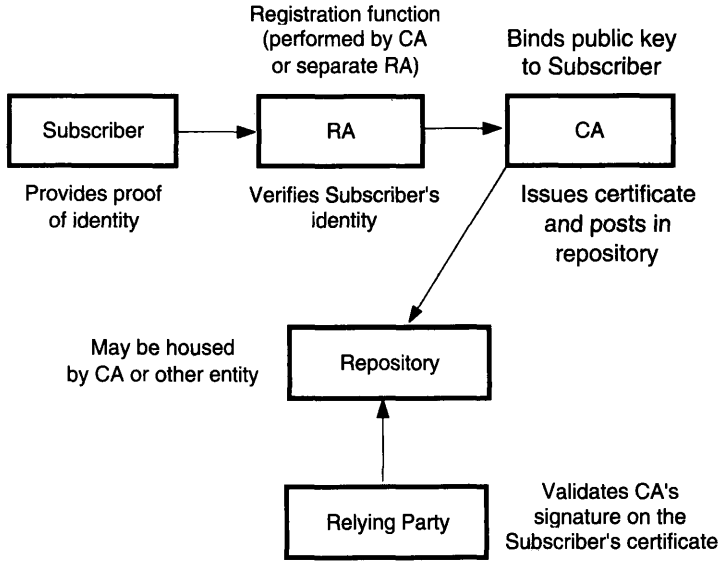
Registration Authority

.23 An RA is an entity that is responsible for the identification and authentication of subscribers, but does not sign or issue certificates. In some cases, the CA performs the subscriber registration function internally. In other cases, the CA delegates the RA function to external registration authorities (sometimes referred to as local registration authorities, or LRAs) that may or may not be part of the same legal entity as the CA. In still other cases, a customer of a CA (for example, a company) arranges with that CA to perform the RA function itself or using its agent. These external RAs are required to comply with the relevant provisions of the CA's business practices disclosures, often documented in a certification practice statement (CPS) and applicable certificate policy(s) (CPs). In performing a WebTrust for certification authorities engagement, the practitioner must consider how the CA handles the RA function and whether the RA function is within the scope of the examination. For example, a CA that provides CA services to several banks might delegate the subscriber registration function to RAs that are specifically designated functional groups within each bank. The functions performed by these specific groups would typically be outside the scope of the WebTrust for Certification Authorities examination performed for the CA. In this case management's assertion should specify those aspects of the registration process that are not handled by the CA.

.24 The initial registration process for a subscriber is as follows, although the steps may vary from CA to CA and also depend upon the certificate policy under which the certificate is to be issued. The subscriber first generates his or her own public/private key pair. (In some implementations, a CA may generate the subscriber's key pair and deliver it to the subscriber securely, but this is normally done only for encryption key pairs, not signature key pairs.) Then, the subscriber produces proof of identity in accordance with the applicable certificate policy requirements and demonstrates that he or she holds the private key corresponding to the public key without disclosing the private key (typically by digitally signing a piece of data with the private key, with the subscriber's digital signature then verified by the CA). Once the association between a person and a public key is verified, the CA issues a certificate. The CA digitally signs each certificate that it issues with its private key to provide the means for establishing authenticity and integrity of the certificate.

.25 The CA then notifies the subscriber of certificate issuance and gives the subscriber an opportunity to review the contents of the certificate before it is made public. Assuming the subscriber approves the accuracy of the certificate, the subscriber will publish the certificate, have the CA publish it and make it available to other users, or both. A repository is an electronic certificate database that is available online. The repository may be maintained by the CA or a third party contracted for that purpose by the subscriber or by any other party. Subscribers may obtain certificates of other subscribers and certificate status information from the repository. For example, if a subscriber's certificate was revoked, the repository would indicate that the subscriber's certificate has been revoked and should not be relied upon. The ability to update the repository is typically retained by the CA. Subscribers and other relying parties have read-only access to the repository. Because the certificates stored in the repository are digitally signed by the CA, they cannot be maliciously changed without detection, even if someone were to hack into the repository.

.26 The following diagram illustrates the relationship between the subscriber and the RA and CA functions.



Certification Practice Statements and Certificate Policies

.27 A CPS is a statement of the practices that a CA employs in issuing and managing certificates. A CP is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate the applicability of a type of certificate to the authentication of EDI transactions for the trading of goods within a given price range.

The Difference Between Licensed and Nonlicensed CAs

.28 Many countries, states, and other governmental jurisdictions have enacted or are developing digital signature laws. In those jurisdictions that have digital signature laws and provide for certification authority licensing, certificates issued by licensed CAs typically have a higher level of legal recognition than those issued by nonlicensed CAs. For a number of jurisdictions, the use of certificates issued by licensed CAs is provided specific recognition in those jurisdictions' digital signature laws. In the United States, for example, several state digital signature laws require that audits of CAs be performed as a requirement for licensing. One of the purposes of this document is to provide suitable criteria that would meet the requirements of various governmental jurisdictions and the marketplace.

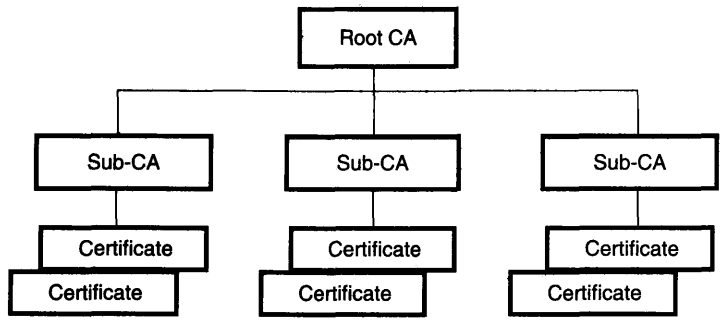
The Hierarchical and Cross-Certified CA Models

.29 CAs may be linked using two basic architectures, hierarchical and cross-certified (shared trust), or a hybrid of the two. In a hierarchical model, a highest level (or "root") CA is deployed and subordinate CAs may be set up for various business units, domains, or communities of interest. The root CA validates the subordinate CAs, which in turn issue certificates to lower-tier CAs or directly to subscribers. Such a root CA typically has more stringent security requirements than a subordinate CA. Although it is difficult for an attacker to access the root CA (which in some implementations is online only in the rare event that it must issue, renew, or revoke subordinate CA certificates), one drawback to this model is that the root CA represents a single point

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

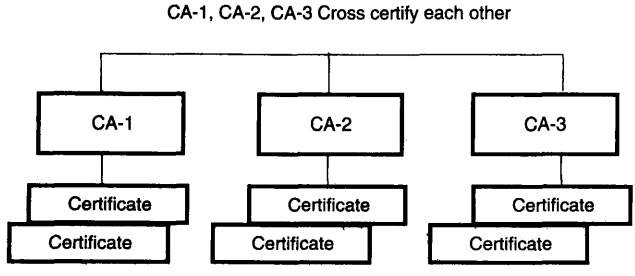
of failure. In the hierarchical model, the root CA maintains the established "community of trust" by ensuring that each entity in the hierarchy conforms to a minimum set of practices. Adherence to the established policies may be tested through audits of the subordinate CAs and, in a number of cases, the RAs.

.30 The following diagram illustrates the structure and relationships between CAs and subscribers operating in a hierarchical model.



.31 In an alternative model, cross-certified CAs are built on a peer-to-peer model. Rather than deploying a common root CA, the cross-certification model shares trust among CAs known to one another. Cross-certification is a process in which two CAs certify the trustworthiness of the other's certificates. If two CAs, CA1 and CA2, cross-certify, CA1 creates and digitally signs a certificate containing the public key of CA2 (and vice versa). Consequently, users in either CA domain are assured that each CA trusts the other and therefore subscribers in each domain can trust each other. Cross-certified CAs are not subject to the single point of failure in the hierarchical model. However, the network is only as strong as the weakest CA, and requires continual policing. In the cross-certified model, to establish and maintain a community of trust, audits may be performed to ensure that each cross-certified CA conforms to a minimum set of practices as agreed upon by the members of the community of trust.

.32 The following diagram illustrates the structure and relationships between CAs and subscribers operating in a cross-certified (shared trust) model.



.33 In a hybrid model, both a hierarchical structure and cross-certification are employed. For example, two existing hierarchical communities of trust may want to cross-certify each other, so that members of each community can rely upon the certificates issued by the other to conduct e-commerce.

Business Issues Associated With CAs

.34 Unless they are subject to governmental licensing and regulation, CAs may use different standards or procedures to verify the identity of persons to whom they issue certificates. Thus, a digital signature is only as reliable as

the CA is trustworthy in performing its functions. Consequently, a relying party needs some way to gauge how much reliance it should place on a digital signature supported by a certificate issued by a particular CA.

.35 CA topology (for example, use of a hierarchical, a cross-certified, or a hybrid model) is a developing issue. Which model is most appropriate depends on business circumstances. Although it is important that public keys be certified, the issuance of nonstandard certificates can be a concern. For example, if the broadly recognized International Telecommunications Union-Telecommunication Standardization Sector's (ITU-T) X.509 data format standard[3] is not used, subscribers and relying parties may be unable to process such certificates. Implementing the cross-certified CA model (discussed previously) would also be very difficult. For these reasons, major entities such as the U.S. and Canadian governments are using or plan to use X.509 certificates for their internal and external activities.

The WebTrust Seal of Assurance for Certification Authorities

.36 The Web has captured the attention of businesses and consumers, causing the number and kinds of electronic transactions to grow rapidly. Nevertheless, many believe that e-commerce will not reach its full potential until customers perceive that the risks of doing business electronically have been reduced to an acceptable level. Customers may have legitimate concerns about confidentiality, authentication, integrity, and nonrepudiation. In e-commerce, participants need the assurance of an objective third party. This assurance can be provided by an independent and objective practitioner and demonstrated through the display of a WebTrust seal for CAs on the CA's Web site.

.37 The WebTrust seal of assurance for CAs symbolizes to potential relying parties that a qualified practitioner has evaluated the CA's business practices and controls to determine whether they are in conformity with the AICPA/CICA WebTrust Principles and Criteria for Certification Authorities, and has issued a report with an unqualified opinion indicating that such principles are being followed in conformity with the WebTrust for Certification Authorities criteria. See Appendix A [paragraph .67], "Illustrative Examples of Practitioner Reports." These principles and criteria reflect fundamental rules for the operation of a CA organization or function.

Practitioners as Assurance Professionals

.38 Practitioners are in the business of providing assurance services, the most publicly recognized of which is the audit of financial statements. An audit opinion signed by a qualified practitioner is valued because these professionals are experienced in assurance matters and financial accounting subject matter and are recognized for their independence, integrity, discretion, and objectivity. Practitioners also follow comprehensive ethics rules and professional standards in providing their services. However, financial statement assurance is only one of the many kinds of assurance services that can be provided by a practitioner. Practitioners also provide assurance about controls and compliance with specified criteria.

---

[3] International Telecommunications Union-Telecommunication Standardization Sector's (ITU-T) Recommendation X.509 (1997) was also standardized by International Organization for Standardization (ISO) as ISO/IEC 9594-8.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.39 In general, the business and professional experience, subject matter expertise (e-commerce information systems security, privacy, auditability, and control), and professional characteristics (independence, integrity, discretion, and objectivity) needed for such projects are the same key elements that enable a practitioner to comprehensively and objectively assess the risks, controls, and business disclosures associated with e-commerce.

Obtaining and Keeping the WebTrust Seal of Assurance for Certification Authorities

The Assurance Process

.40 The CA's management will make assertions along the following lines:

Management has assessed the controls over its CA operations. Based on that assessment, in ABC Certification Authority, Inc. (ABC-CA) Management's opinion, in providing its certification authority (CA) services at [*location*], ABC-CA, during the period from [*Month, day, year*] through [*Month, day, year*]:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
  - The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
  - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
  - The continuity of key and certificate life cycle management operations was maintained; and
  - CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria.

.41 For an initial representation, the historical period covered should be at least two months or more as determined by the practitioner. For established CAs and CA functions, two months may be quite sufficient, while for new CAs and CA functions, the practitioner may believe that a longer initial period would be more appropriate. For subsequent representations, the period covered should begin with the end of the prior period, to provide continuous representation. Reports should be issued at least every 12 months. In some situations, given the business needs or expectations of relying parties, the practitioner may believe a shorter subsequent period would be more appropriate.

.42 To have a basis for such assertions, the CA's management should have made a risk assessment and implemented appropriate controls for its CA operations. The WebTrust for Certification Authorities criteria and illustrative controls provide a basis for a risk assessment and a minimum set of CA controls.

.43 An independent, objective, and knowledgeable practitioner will perform tests of these representations under AICPA professional standards[4] and provide a professional opinion, which adds to the credibility of management's representations.

Comparison of a WebTrust for Certification Authorities Examination With Service Auditor Reports

.44 Professional standards currently exist for auditors to report on controls of third-party service providers (a service auditor's engagement). Guidance for these engagements is set out in the AICPA's Statement on Auditing Standards (SAS) No. 70, *Service Organizations* (AICPA, *Professional Standards*, vol. 1, AU sec. 324), as amended. A WebTrust for Certification Authorities engagement differs from a service auditor's engagement in a number of ways, including the following:

- *Purpose.* WebTrust for Certification Authorities provides a new framework for reporting activities of CAs through auditor communication to interested parties, including business partners and existing or potential customers. SAS No. 70 (service auditor reports) was designed for auditor-to-auditor communication to assist the user auditor in reporting on the financial statements of a customer of the service organization.
- *Target of evaluation.* WebTrust for Certification Authorities was designed specifically for the examinations of CA business activities. Service auditor reports were designed for service organizations in general.
- *Type of engagement.* WebTrust for Certification Authorities requires reporting on compliance with the AICPA/CICA WebTrust Principles and Criteria for Certification Authorities. Service auditor reports were designed for reporting on the design and existence of controls and the effective operation of those controls when the report covers a period of time.
- *Examination standards.* WebTrust for Certification Authorities follows the AICPA Statements on Standards for Attestation Engagements (SSAEs). Service auditor reports follow generally accepted auditing standards.
- *Coverage of activities.* WebTrust for Certification Authorities requires coverage of specific areas as defined herein, including CA business practices disclosure, service integrity (including key and certificate life cycle management activities), and CA environmental controls. Service auditor reports were designed for reporting upon controls related to financial information.
- *Linkage to authoritative standards.* WebTrust for Certification Authorities provides uniform rules derived from the draft ANSI X9.79 standard (which is intended to be submitted to the International Organ-

[4] These services are performed in the United States under Chapter 1, "Attest Engagements," of Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101). Practitioners will need the appropriate skills and experience, training in the WebTrust for Certification Authorities service offering, and a WebTrust business license from the AICPA, CICA, or other authorized national accounting institute to provide the WebTrust for Certification Authorities services to their clients. The practitioner needs to perform an "examination" (audit) level engagement in order to award the WebTrust seal for certification authorities. A review level engagement is not sufficient.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

ization for Standardization [ISO] for international standardization). Standards underlying service auditor reports do not specify the control objectives that must be covered by the report.

- *Period of coverage of review.* WebTrust for Certification Authorities encourages continuous coverage from the point of initial qualification and requires continuous coverage to retain the seal. Qualification after compliance can be tested over a minimum two-month period, with updates over a specified period (currently one-year maximum). Service auditor reports cover a period of time specified by the service organization, but do not require continuous coverage.

.45 In addition, this approach maintains consistency in the professional standards used for the Suitable Trust Services Criteria and Illustrations. Both WebTrust and SysTrust use Chapter 1, "Attest Engagements," of SSAE No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101), as amended, as the reporting standards.

.46 A table highlighting the differences between a WebTrust for Certification Authorities engagement and SAS No. 70 and Section 5900 engagements is provided in Appendix E [paragraph .71].

Obtaining the WebTrust Seal

.47 To obtain the WebTrust seal of assurance, the CA must meet all the WebTrust for Certification Authorities principles as measured by the WebTrust for Certification Authorities criteria associated with each of these principles. In addition, the entity must (*a*) engage a practitioner who has a WebTrust business license from the AICPA, CICA, or other authorized national accounting institute to provide the WebTrust service, and (*b*) obtain an unqualified report from such practitioner.

Keeping the WebTrust Seal

.48 Once the seal is obtained, the CA will be able to continue displaying it on its Web site provided the following are performed.

a. The CA's WebTrust practitioner updates his or her assurance examination of the assertion on a regular basis. The CA must continue to obtain an unqualified report from such practitioner. The interval between such updates will depend on matters such as the following:

(1) The nature and complexity of the CA's operations

(2) The frequency of significant changes to the CA's operations

(3) The relative effectiveness of the entity's monitoring and change-management controls for ensuring continued conformity with the applicable WebTrust for Certification Authorities criteria as such changes are made

(4) The practitioner's professional judgment

For example, an update may be required more frequently for a CA that is expanding operations, changing extensively and rapidly, or issuing high-assurance certificates that are used for very sensitive transmissions or high-value transactions, as compared to a CA that issues few certificates and has a relatively stable operation. In no event should the interval between updates exceed 12 months; this interval often may be shorter. For example, in the situation of a start-up CA or CA function, it may be more appropriate that the initial examination period be established at 3 months, with the next review being performed 6 months after the WebTrust seal for CAs is

awarded, thereafter moving to a 12-month review cycle. To provide continuous coverage and retain the seal, the period covered for update reports should begin with either the end of the prior period or the start of the period in the initial report.

b. During the period between updates, the CA undertakes to inform the practitioner of any significant changes in its business policies, practices, processes, and controls, particularly if such changes might affect the CA's ability to continue meeting the WebTrust Principles and Criteria for Certification Authorities, or the manner in which they are met. Such changes may trigger the need for an assurance update or, in some cases, removal of the seal until an update examination by the practitioner can be made. If the practitioner becomes aware of such a change in circumstances, he or she determines whether the seal needs to be removed until an update examination is completed and the updated auditor's report is issued.

The Seal Management Process

.49 The WebTrust seal of assurance for the CA will be managed by a seal manager along the following lines.

- Upon becoming a WebTrust licensee, the WebTrust practitioner obtains a registration number (ID and password) from the WebTrust licensing authority. With this the practitioner can issue a WebTrust seal to the CA.
- When the practitioner is prepared to issue a WebTrust seal, he or she accesses the WebTrust secure server system. Upon payment of the registration fee, the practitioner receives passwords and IDs unique to the engagement. The seal manager issues these to the practitioner in pairs. One set allows the practitioner to read and write to the secure server (see below) and the other permits the CA to preview the presentation.
- The practitioner prepares a draft of the practitioner's report and provides it along with management's assertions for posting to the preview site.
- The seal manager then delivers the seal to the CA with the appropriate links to the preview site. Notification of delivery is provided to the practitioner.
- When the practitioner and CA have agreed that the seal should become active, the practitioner notifies the seal manager to transfer the information from the preview site to the active WebTrust site and provides the appropriate expiration date.
- The seal remains valid for the period provided by the practitioner plus a one-month grace period, unless removed for cause. The one-month period is to allow sufficient time to complete the engagement and other open items. For example, if the seal expires on June 30, 20XX, the practitioner has 30 days to complete open items and prepare new documents for posting with the seal manager. The subsequent examination period begins July 1, 20XX.
- If the practitioner determines that the seal should be removed from the CA's Web site, the practitioner will immediately notify the CA and request that the seal be removed from the CA's site. The practitioner will then notify the seal manager to remove all the relevant information and to replace it with a statement that the WebTrust seal for this site is no longer valid.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- The seal manager will notify the practitioner 30 days prior to expiration that the seal needs to be renewed. The seal manager may revoke seals if the registration fee for the seal is unpaid or for other sufficient cause.

WebTrust Seal Authentication

.50 To verify whether the seal displayed on a CA's Web site is authentic, the customer can:

- Click on the seal, which links the customer through a secure connection to a WebTrust seal verification page hosted by the seal manager. It identifies the CA and confirms that the CA is entitled to display the WebTrust seal. It also provides links to the appropriate principle(s) (that is, the WebTrust for Certification Authorities principles) and other relevant information.
- Access the list of entities that have received a WebTrust seal; the list is maintained by the seal manager at www.webtrust.org/abtseals.htm. A CA is registered on this list when the seal is issued.

WebTrust Principles and Criteria for Certification Authorities

WebTrust for Certification Authorities Principles

.51 To be understandable to the ultimate users—the subscriber and relying party—the following principles have been developed with the relying party in mind, and, as a result, are intended to be practical and nontechnical in nature.

Principle 1: CA Business Practices Disclosure

.52 The first principle is—*The certification authority discloses its key and certificate life cycle management business and information privacy practices and provides its services in accordance with its disclosed practices.*

.53 The CA must disclose its key and certificate life cycle management business and information privacy practices. Information regarding the CA's business practices should be made available to all subscribers and all potential relying parties, typically by posting on its Web site. Such disclosure may be contained in a certificate policy (CP), certification practice statement (CPS), or other informative materials that are available to users (subscribers and relying parties).

Principle 2: Service Integrity

.54 The second principle is—*The certification authority maintains effective controls to provide reasonable assurance that:*

- *Subscriber information was properly authenticated (for the registration activities performed by ABC-CA).*
- *The integrity of keys and certificates it manages is established and protected throughout their life cycles.*

.55 Effective key management controls and practices are essential to the trustworthiness of the public key infrastructure. Cryptographic key management controls and practices cover CA key generation; CA key storage, backup, and recovery; CA public key distribution (especially when done in the form of self-signed "root" certificates); CA key escrow (optional); CA key usage; CA key destruction; CA key archival; the management of CA cryptographic hardware through its life cycle; and CA-provided subscriber key management services

(optional). Strong key life cycle management controls are vital to guard against key compromise that can damage the integrity of the public key infrastructure.

.56 The user certificate life cycle is at the core of the services provided by the CA. The CA establishes its standards and practices by which it will deliver services in its published CPS and CPs. The user certificate life cycle includes the following:

- Registration (that is, the identification and authentication process related to binding the individual subscriber to the certificate)
- The renewal of certificates (optional)
- The rekey of certificates
- The revocation of certificates
- The suspension of certificates (optional)
- The timely publication of certificate status information (through certificate revocation lists or some form of online certificate status protocol)
- The management of integrated circuit cards (ICCs) holding private keys through their life cycle (optional)

.57 Effective controls over the registration process are essential, as poor identification and authentication controls jeopardize the ability of subscribers and relying parties to rely on the certificates issued by the CA. Effective revocation procedures and timely publication of certificate status information are also essential elements, as it is critical for subscribers and relying parties to know when they are unable to rely on certificates that have been issued by the CA.

Principle 3: CA Environmental Controls

.58 The third principle is—*The certification authority maintains effective controls to provide reasonable assurance that:*

- *Subscriber and relying party information is restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;*
- *The continuity of key and certificate life cycle management operations is maintained; and*
- *CA systems development, maintenance, and operation are properly authorized and performed to maintain CA systems integrity.*

.59 The establishment and maintenance of a trustworthy CA environment is essential to the reliability of the CA's business processes. Without strong CA environmental controls, strong key and certificate life cycle management controls are severely diminished in value. CA environmental controls include CPS and CP management, security management, asset classification and management, personnel security, physical and environmental security of the CA facility, operations management, system access management, systems development and maintenance, business continuity management, monitoring and compliance, and event journaling.

WebTrust for Certification Authorities Criteria

.60 To provide more specific guidance on meeting the WebTrust for Certification Authorities principles, the WebTrust for Certification Authorities criteria have been developed. These provide a basis against which a CA can make

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

a self-assessment of its conformity with the criteria, and a consistent set of measurement criteria for practitioners to use in testing and evaluating CA practices.

.61 The WebTrust for Certification Authorities criteria are presented under the three principles listed above (Principle 1, CA Business Practices Disclosure; Principle 2, Service Integrity, including key and certificate life cycle management controls; and Principle 3, CA Environmental Controls. Each principle contains a series of criteria that the CA's management asserts it has achieved. Depending on the scope of services provided by the CA, a number of the criteria may not be applicable. Criteria considered optional, depending on whether the CA provides the related services, are key escrow, certificate renewal, certificate suspension, the use of integrated circuit cards (ICCs), and the provision of subscriber key management services. If any of these services are provided by the CA, the criteria are applicable and must be tested by the practitioner. If any of these services are not provided by the CA, the criteria are not applicable and no modification of the standard report is necessary. In some situations, some RA services may be performed by another party that is not controlled by the CA, and therefore those activities are not included in the examination of the CA. In these circumstances the standard report should be modified to specify the exclusion of the specific RA activities from the scope of the examination, as shown in Appendix A [paragraph .67], Example 2. This may be accomplished by reference to the CA's business practice disclosures in which the CA specifies which RA activities it does not control. In all instances some RA activities will be performed by the CA and should be tested by the practitioner for compliance with the controls disclosed under Principle 1 and the criteria specified in Principle 2.[5]

.62 In performing a WebTrust for Certification Authorities engagement, the practitioner must gain an understanding of the CA's business model and services provided to determine which control criteria may not be applicable. For each of the disclosure and control criteria, there is a detailed list of illustrative disclosures and control procedures that might be followed by the CA to meet the related criteria. The illustrative disclosures and controls do not necessarily need to be in place for a criterion to be met in a given business circumstance and alternatives may be sufficient.

.63 The CA Business Practices Disclosure criteria were derived primarily from the Internet Engineering Task Force's (IETF) Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework—Request For Comments Draft (RFC 2527), which has been incorporated into Annex A of the draft ANSI X9.79 standard. For specific key and certificate life cycle management (Principle 2) and CA environmental illustrative controls (Principle 3), in which the CA's implemented controls may vary depending on the CA's business practices, such illustrative controls refer to specifically required CA business practices disclosures included in Principle 1.

---

[5] As indicated herein, during development of this document, the AICPA/CICA Electronic Commerce Assurance Task Force considered the situations in which subscriber registration is performed by the certification authority (CA) itself or by external registration authorities (RAs). This document has been written such that the RA function may be "carved out" or considered outside the scope of the WebTrust for certification authorities examination when registration activities are performed by parties external to the CA. For the purpose of some end users, this approach may not address all requirements for the independent verification of such end users. The Task Force was aware of this situation and concluded that the issuance and use of this document was desirable and that the impact of a third-party registration function was beyond the scope of this document.

WebTrust Principles and Criteria for Certification Authorities

Principle 1: CA Business Practices Disclosure

.64 The certification authority discloses its key and certificate life cycle management business and information privacy practices and provides its services in accordance with its disclosed practices.

Criteria	*Illustrative Disclosures*
1.1 CA Business Practices Disclosure The certification authority (CA) discloses its business practices, including but not limited to the following:	
General	
Identification of each certificate policy (CP) and certification policy statement (CPS) for which the CA issues certificates	1 The CA issues certificates in accordance with the CA's certification policy statement (CPS) dated [*date*]. The CA issues certificates that support the following certificate policies: CA's Class 1 Certificate Policy, CA's Class 2 Certificate Policy, CA's Class 3 Certificate Policy, and the Bank Consortium's Certificate Policy.
Community and applicability, including a description of the types of entities within the public key infrastructure (PKI) and the applicability of certificates issued by the CA	2 The CA is established to provide certificate services for a variety of external customers. The organization operates a single CA, which issues user certificates to all CA customers. The CA makes use of customer designated personnel to act as agents to verify the identity of subscribers, in accordance with the indicated certificate policy. Subscribers include all parties who contract with the CA for digital certificate services. All parties who may rely upon the certificates issued by the CA are considered relying parties. This certification policy statement (CPS) (or other CA business practices disclosure) is applicable to all certificates issued by the CA. The practices described in the CPS (or other CA business practices disclosure) apply to the issuance and use of certificates and certificate revocation lists (CRLs) for users within the CA domain.
Contact details and administrative provisions, including: • Contact person • Identification of policy authority	3 This CPS (or other CA business practices disclosure) is administered by the CA operations manager. The CA's certificate policies are administered by the CA's policy authority. Contact information is listed below.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria		*Illustrative Disclosures*
• Street address • Version and effective date(s) of each CP and CPS		The contact details for this CPS are: CA Operations Manager [*Address*] [*Telephone*] [*Fax*] [*E-mail*] The contact details for the CA's certificate policy are: Policy Authority [*Address*] [*Telephone*] [*Fax*] [*E-mail*]
Any applicable provisions regarding apportionment of liability	4	Except as expressly provided otherwise in this CPS, applicable CP, or by statute or regulation, the CA's total liability per breach of any express warranties made under this CPS and/or applicable CP is limited to direct damages having a maximum dollar amount (that is, a liability cap) of $10,000. The liability cap set forth in this CPS or applicable CP shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate. Additionally, in the event the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall the CA be obligated to pay more than the aggregate liability cap for each certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.
Financial responsibility, including: • Indemnification by relying parties • Fiduciary relationships	5	By their applying for and being issued certificates, or otherwise relying upon such certificates, subscribers and relying parties agree to indemnify, defend, and hold harmless the CA, and its personnel, organizations, entities, subcontractors, suppliers, vendors, representatives, and agents from any errors, omissions, acts, failures to act, or negligence resulting in liability, losses, damages, suits, or expenses of any kind, due to or otherwise proximately caused by the use or publication of a certificate that arises from the subscriber's failure to provide the CA with current, accurate, and complete information at the time of certificate application or the subscriber's errors, omissions, acts, failures to act, and negligence. The CA and its registration authorities (RAs) are not the agents, fiduciaries, trustees, or other representatives of subscribers or relying parties.

(continued)

Criteria	*Illustrative Disclosures*
Interpretation and enforcement, including: • Governing law • Severability, survival, merger, and notice • Dispute resolution procedures	6 Governing Law: The laws of [*jurisdiction*] shall govern the enforceability and construction of this CPS (or other CA business practices disclosure) to ensure uniform procedures and interpretation for all users. Severability, Survival, Merger, Notice: Severance or merger may result in changes to the scope, management, and/or operations of this CA. In such an event, this CPS may require modification as well. Changes to the operations will occur consistently with the CA's disclosed CPS management processes. Dispute Resolution Procedures: In the event of any dispute involving the services or provisions covered by this CPS (or other CA business practices disclosure), the aggrieved party shall first notify the CA and all other relevant parties regarding the dispute. The CA will involve the appropriate personnel to resolve the dispute.
Fees, including: • Certificate issuance or renewal fees • Certificate access fees • Revocation or status information access fees • Fees for other services, such as policy information • Refund policy	7 The CA may charge subscribers fees for their use of the CA's services. A current schedule of such fees is available from the CA's repository at [*URL*]. Such fees are subject to change seven (7) days following their posting in the CA's repository.
Publication and repository requirements, including: • Publication of CA information • Frequency of publication • Access controls	8 The CA's CPS (or other CA business practices disclosure) is available at [*URL*]. The CA's certificate policies can be found at [*URL*]. Upon issuance, all public key certificates and CRLs issued by the CA are published in the CA's directory. All subscribers and relying parties have access to the CA's repository.
Compliance audit requirements, including: • Frequency of entity compliance audit • Auditor's relationship to audited party • Topics covered by audit • Actions taken as a result of deficiency • Communication of results	9 An annual audit is performed by an independent external auditor to assess the adequacy of the CA's business practices disclosure and the effectiveness of the CA's controls over its CA operations. Topics covered by the annual audit include the following: • CA business practices disclosure • Service integrity (including key and certificate life cycle management controls) • CA environmental controls

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Disclosures*
	Significant deficiencies identified during the compliance audit will result in a determination of actions to be taken. This determination is made by the auditor with input from CA management. The CA is responsible for seeing that corrective action is taken within 60 days. Should a severe deficiency be identified that might compromise the integrity of the CA, CA management considers, with input from the auditor, whether suspension of the CA's operation is warranted. Compliance audit results are communicated to the board of directors of the CA, CA management, and the CA's policy authority, as well as others deemed appropriate by CA management.
Description of the conditions for applicability of certificates issued by the CA that reference a specific CP, including: • Specific permitted uses for the certificates if such use is limited to specific applications • Limitations on the use of certificates if there are specified prohibited uses for such certificates	10 Certificates issued under the CA's certificate policy are limited to use in connection with [*bank's*] Consumer Internet Banking application. Certificates issued by the CA may not be used for any other purpose.
CA and/or registration authority (RA) obligations: • Notification of issuance of a certificate to the subscriber who is the subject of the certificate being issued • Notification of issuance of a certificate to others than the subject of the certificate • Notification of revocation or suspension of a certificate to the subscriber whose certificate is being revoked or suspended • Notification of revocation or suspension of a certificate to others than the subject whose certificate is being revoked or suspended	11 The CA is obligated to: • Conform its operations to the CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the CA repository • Issue and publish certificates in a timely manner in accordance with the relevant certificate policy • Revoke certificates issued by the CA, upon receipt of a valid request to revoke the certificate from a person authorized to request revocation • Publish CRLs on a regular basis, in accordance with the applicable certificate policy and with provisions described in the CA's disclosed business practices (Principle 1, item 35 [paragraph .64]) • Notify subscribers via e-mail (1) that certificates have been generated for them and (2) how the subscribers may retrieve the certificates • In the event the CA is not successful in validating the subscriber's application in accordance with the requirements for that class of certificate the CA shall notify the subscriber that the application has been rejected

(continued)

Criteria	*Illustrative Disclosures*
	• Notify subscribers via e-mail that the subscriber's certificate has been revoked • Notify other participants in the PKI of certificate issuance revocation through access to certificates and CRLs in the CA repository
RA obligations, including: • Identification and authentication of subscribers • Validation of revocation and suspension requests • Verification of subscriber renewal or rekey requests	12 The RAs (or the CA's RA function) are obligated to: • Verify the accuracy and authenticity of the information provided by the subscriber at the time of application, in accordance with the relevant certificate policy. • Validate and securely send a revocation request to the CA upon receipt of a request to revoke a certificate, in accordance with the relevant certificate policy. • Verify the accuracy and authenticity of the information provided by the subscriber at the time of renewal or rekey, in accordance with the relevant certificate policy.
Repository obligations, including: • Timely publication of certificates and certificate revocation lists (CRLs)	13 The CA's repository function is obligated to publish certificates and certificate revocation lists in a timely manner.
Subscriber obligations, including: • Accuracy of representations in certificate application • Protection of the subscriber's private key • Restrictions on private key and certificate use • Notification upon private key compromise	14 Subscribers are obligated to: • Provide information to the CA that is accurate and complete to the best of the subscribers' knowledge and belief regarding information in their certificates and identification and authentication information and promptly notify the CA of any changes to this information. • Safeguard their private key from compromise. • Use certificates exclusively for legal purposes and in accordance with the relevant certificate policy and this CPS (or other CA business practices disclosure). • Promptly request that the CA revoke a certificate if the subscriber has reason to believe there has been a compromise of their private key corresponding to the public key listed in the certificate.
Relying party obligations, including: • Purposes for which certificate is used • Digital signature verification responsibilities	15 Relying parties are obligated to: • Restrict reliance on certificates issued by the CA to the purposes for those certificates, in accordance with the relevant certificate policy and with this CPS (or other CA business practices disclosure).

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Disclosures*
• Revocation and suspension checking responsibilities • Acknowledgment of applicable liability caps and warranties	• Verify the status of certificates at the time of reliance. • Agree to be bound by the provisions of limitations of liability as described in the CPS (or other CA business practices disclosure) upon reliance on a certificate issued by the CA.
Key Life Cycle Management	
Any applicable reliance or financial limits for certificate usage.	16 Certificates issued under the CA's certificate policy may only be used in connection with transactions having a dollar value of no more than $100,000.
CA key pair generation, including: • What key sizes are required • What key generation algorithm is required • Whether key generation is performed in hardware or software • What standards are required for the module used to generate the keys (for example, the required ISO 15782-1/FIPS 140-1/ANSI X9.66 level of the module) • For what purposes the key may be used • For what purposes usage of the key should be restricted • The usage periods or active lifetimes for the CA public and the private key, respectively	17 The CA's signing key pair is 1024 bit using the RSA algorithm. Hardware key generation is used and is compliant to at least FIPS 140-1 level 3. The CA's signing key is used to sign certificates and CRLs. The lifetime of the CA signing key pair is five years.
CA private key protection including: • What standards are required for the module used to store the CA private signature key (for example, the required ISO 15782-1/FIPS 140-1/ANSI X9.66 level of the module) • Whether the CA private key is maintained under m out of n multiperson control • Whether the CA private signature key is escrowed • Whether the CA private signing key is backed up • Whether the CA private and public signature keys are archived	18 Hardware cryptographic modules for generating and storing the CA's root key are certified to FIPS 140-1 level 3. There is a separation of physical and logical access to the CA's root private key. Two individuals provide dual control over physical access to the hardware modules; m of n secret shares held by other, separate custodians on removable media are required for logical activation of the private keys. The CA's private signing key is backed up only on hardware certified to FIPS 140-1 level 3 and is stored with two-person control enforced. Escrow of CA private keys by an external third party is not performed. The CA's private signing key and expired (and revoked) CA public key certificates are archived.

(continued)

Criteria	*Illustrative Disclosures*
Whether the CA provides subscriber key management services and a description of the services provided	19 The CA provides subscriber key management services including the following: • Subscriber key generation • Subscriber key storage, backup, and recovery • Subscriber key archival • Subscriber key destruction
CA public key distribution, including a description of how the CA's public key is provided securely to subscribers and relying parties	20 The CA's public key is delivered in a self-signed certificate to subscribers using an encrypted session between the CA and the subscriber's client software, with an authorization code as a shared secret. Authenticity and integrity protection is based on a MAC key derived from the authorization code.
Key changeover, including a description of the procedures used to provide a new public key to a CA's users	21 The CA root signing private key has a lifetime of two years and the corresponding public key certificate has a lifetime of four years. Upon the end of the private key's lifetime, a new CA signing key pair is generated and all subsequently issued certificates and CRLs are signed with the new private signing key. The corresponding new CA public key certificate is securely provided to subscribers and relying parties.
Subscriber key pair generation (if the CA provides subscriber key pair generation services), including: • How the subscriber's private key is provided securely to the subscriber • What key sizes are required • What key generation algorithm is required • Whether key pair generation is performed in hardware or software • What standards are required for the module used to generate the keys (for example, the required ISO 15782-1/FIPS 140-1/ANSI X9.66 level of the module) • For what purposes the key may be used • For what purposes usage of the key should be restricted	22 For subscribers, the CA creates an encryption key pair and the corresponding encryption public key certificate. For subscribers, the encryption key pair is provided securely to the user via an encrypted session between the CA and the subscriber's client software. Subscriber encryption key pairs are 1024 bit using the RSA algorithm. The CA's process for generating subscriber encryption key pairs uses the CA system software and is designed to comply with FIPS 140-1 level 1.
Subscriber private key protection (if the CA provides subscriber key management services), including: • Whether the subscriber's decryption private key is backed up • Whether the subscriber's decryption private key is archived	23 Subscriber encryption private keys generated by the CA are backed up in the CA database. The CA database is encrypted and its integrity is protected by master keys. Subscriber signature private keys are generated by the subscriber and are not known or stored by the CA.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Disclosures*
• Under what conditions a subscriber's private key can be destroyed • Whether subscriber private decryption keys are escrowed by the CA	The encryption key pair history for all users, including a complete history of all decryption private keys, is stored encrypted in the CA database. Subscriber encryption private keys stored by the CA are not destroyed. Escrow of subscriber private keys is not performed by the CA.
Certificate Life Cycle Management	
Whether certificate suspension is supported	24 The CA does not support suspension of certificates.
Initial registration, including a description of the CA's requirements for the identification and authentication of subscribers and validation of certificate requests during entity registration or certificate issuance: • Types of names assigned to the subject and rules for interpreting various name forms • Whether names have to be meaningful or not • Whether names have to be unique • How name claim disputes are resolved • Recognition, authentication, and role of trademarks • If and how the subject must prove possession of the companion private key for the public key being provided for a certificate • How the subscriber's public key is provided securely to the CA for issuance of a certificate • Authentication requirements for organizational identity of subject • Authentication of individual identity • Required certificate request data • How the CA verifies the authority of the subscriber to request a certificate • How the CA verifies the accuracy of the information included in the subscriber's certificate request	25 The CA has established a single naming hierarchy utilizing the X.500 Distinguished Name form. In all cases, names of subjects must be meaningful. Generally, the name by which a subscriber is commonly known to the CA should be used. The CA does not support the use of pseudonyms in subscriber common names. All subjects in the CA's PKI are unambiguously identified in the naming hierarchy. When there is a conflict in distinguished names, such as a second "John Doe," then a middle initial, middle name, or other modification acceptable to the subscriber may be used to make the name unique. The CA issues certificates within a closed PKI. Trademarks and related naming issues will generally not apply to certificates issued within this space. Possession of a private key is proved by a certificate applicant by providing check values as defined in the certificate policy. If organizational identity is considered important based upon the certificate policy, the organization identity is verified using a method approved by the certificate policy. The requirements for authentication of individual identity are defined by the certificate policy [*hot link to certificate policy*]. In submitting a certificate application, at least the following information must be submitted to the CA: subscriber's public key, subscriber's distinguished name, and other information required on the CA's certificate application form.

(continued)

Criteria		*Illustrative Disclosures*
• Whether the CA checks certificate requests for errors or omissions		If required by the certificate policy, the CA verifies the authority of the subscriber to request a certificate by checking whether the subscriber is an employee of a particular organization or association through inquiry of the organization's HR department or the association's membership department. The CA verifies the accuracy of the information included in the subscriber's certificate request through validation against a third-party database. The CA checks certificate requests for errors or omissions.
Registration requirements where external RAs are used, including the CA's procedures for: • Validating the identity of external RAs • Authorizing external RAs • Requirements for the external RA to secure that part of the certificate application, certificate renewal, and certificate rekey processes for which the RA assumes responsibility • How the CA verifies the authenticity of certificate request submissions received from an external RA	26	The CA requires that external registration authorities (RAs) physically present themselves along with two forms of identification to an employee of the CA. The CA authorizes external RAs upon successful identification and authentication, and approval of the external RA enrollment and certificate application forms. External RAs are responsible for identification and authentication of subscribers and must secure their private signing keys used for signing certificate applications, securely forward certificate applications to the CA, and securely store any subscriber information collected. The CA verifies the authenticity of certificate request submissions received from an external RA by validating the RA's digital signature on the submission.
Certificate renewal, including a description of the CA's procedures for the following: • Notifying subscribers of the need for renewal • Identification and authentication • Renewal request verification	27	The certificate renewal process is similar to an application for a new certificate. However, the subscriber needs to provide only information that has changed.
Routine rekey, including a description of the identification and authentication and rekey request verification procedures	28	Authentication of the individual's identity as defined in the CA's identification and authentication requirements for initial registration need not be repeated unless required by the applicable certificate policy. Subscribers will be limited to rekeying no more than twice before repeating the authentication process defined in identification and authentication requirements for initial registration.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Disclosures*
Rekey after revocation or expiration, including a description of the identification and authentication and rekey request verification procedures for rekey after the subject certificate has been revoked	29 For subscribers whose certificates have been revoked or have expired, rekey is permitted if the identification and authentication requirements for initial registration are repeated.
Certificate issuance, including a description of the requirements regarding the following: • Issuance of a certificate • Notification to the applicant of such issuance • Certificate format requirements • Validity period requirements • Extension field requirements (that is, what extension fields are honored, and how they are to be populated)	30 Certificates are issued to the subscribers upon successful processing of the application and the acceptance of the certificates by the subscribers. Certificate format, validity period, extension field, and key usage extension field requirements are specified in accordance with the CA's disclosed certificate profile.
Certificate acceptance, including a description of the requirements regarding acceptance of an issued certificate and for consequent publication of certificates	31 Once a certificate has been generated, it is maintained in a secure remote repository until it is retrieved by the subscriber. Upon retrieval of the certificate from the secure remote repository, the certificate status is updated to reflect its status as accepted and valid.
Certificate distribution, including a description of the CA's established mechanism (for example, a repository such as a directory) for making available to relying parties the certificates and CRLs that it issues	32 A single repository is operated for all subscribers and relying parties. All certificates issued by the CA and all certificate revocation lists (CRLs) relating thereto, shall be published in the repository. The repository for this CA is provided by an X.500 directory system. The protocol used to access the directory is the Lightweight Directory Access Protocol (LDAP) version 2.
Certificate revocation, including: • Circumstances under which a certificate may or must be revoked • Identification and authentication procedures required for revocation requests • Procedures used for initiation, authorization, and verification of certificate revocation requests • Revocation request grace period available to the subscriber	33 A certificate can be revoked for several reasons, including suspected or actual compromise of control of the private key that relates to the public key contained in the certificate, hardware or software failures that render the private key inoperable, or failure of a subscriber to meet the obligations of this certification policy statement (CPS) and the related certificate policy (CP). Other circumstances for revocation may be stipulated in the particular CP and may relate to changes in a subscriber's relationship with the CA, such as a change in customer or employee status or a change in the particular role of an employee.

(continued)

Criteria	*Illustrative Disclosures*
• Any variations on the preceding stipulations in the event that the revocation is the result of private key compromise (as opposed to other reasons for revocation) • Procedures to provide a means of rapid communication to facilitate the secure and authenticated revocation of (1) one or more certificates of one or more entities; (2) the set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates; and (3) all certificates issued by a CA, regardless of the public/private key pair used • Procedures for notifying the subscriber upon revocation of the subscriber's certificate • Whether the external RA is notified upon the revocation of a subscriber's certificate for which the revocation request was processed by the external RA • How and when the subscriber's certificate status information is updated upon certificate revocation	Revocation may be requested by the subscriber, registration authority, or CA. Requests by RA personnel to revoke a certificate require sufficient RA system access rights. Requests by subscribers to revoke their own certificates require one of the following: • A digitally signed message from the subscriber to the RA • Personal presentation of the subscriber to the RA with a personal photo ID card • Presentation of the pass phrase created by the subscriber at the point of initial application • Other means as provided in the CP A subscriber can request a certificate revocation online, via e-mail, or by telephone to the CA. If the request is made online and the end entity supplies the correct pass phrase, the certificate is revoked immediately. Certificate revocation requests made via e-mail or telephone are processed on a daily basis by the CA after the validity of such requests is ascertained. Validation procedures for telephone and e-mail revocation requests are defined in the CP. Validated certificate revocation requests will be processed no more than 24 hours after receipt. The CP may define a shorter time period for the processing of revocation requests. Revocation requests for reasons other than key compromise must be placed within a maximum of 48 hours of the event necessitating revocation. In the case of suspected or known private key compromise, revocation request should be made immediately upon identification of the event. The CA's certificate revocation process supports the secure and authenticated revocation of one or more certificates of one or more entities and provides a means of rapid communication of such revocation through the issuance of daily CRLs (or, if necessary, more frequent CRLs). The CA's system and processes provide the capability to revoke (1) the set of all certificates issued by the CA that have been signed with a single CA private signing key or (2) groups of certificates issued by the CA that have been signed with different CA private signing keys. Upon revocation of the subscriber's certificate, the subscriber is notified via e-mail.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Disclosures*
	When a revocation request has been processed by an external registration authority, the external RA is also notified upon the revocation of a subscriber's certificate. Upon the revocation of a subscriber's certificate, the newly revoked certificate is recorded in the next CRL that is issued.
Certificate suspension, including: • Circumstances under which a certificate may or must be suspended • Identification and authentication procedures required for revocation requests • Procedures used for initiation, authorization, and verification of certificate suspension requests • How long the suspension may last • Circumstances under which the suspension of a certificate may or must be lifted • Authorization criteria to request the lifting of a certificate suspension • Any variations on the preceding stipulations if the suspension is the result of private key compromise (as opposed to other reasons for suspension) • Procedures to provide a means of rapid communication to facilitate the secure and authenticated suspension of (1) one or more certificates of one or more entities; (2) the set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates; and (3) all certificates issued by a CA, regardless of the public/private key pair used • Procedures for notifying the subscriber upon suspension of the subscriber's certificate • Whether the external RA is notified upon the suspension of a subscriber's certificate for which the suspension request was processed or submitted by the external RA	34 The CA does not support certificate suspension.

(continued)

Criteria	*Illustrative Disclosures*
• How and when the subscriber's certificate status information is updated upon certificate suspension and the lifting of a certificate suspension	
Provision of certificate status information, including: • What mechanism is used (CRLs, online certificate status protocol [OCSP], other) • If a CRL mechanism is used, the issuance frequency • Requirements on relying parties to check CRLs • Online revocation and status checking availability • Requirements on relying parties to perform online revocation and status checks • Other forms of revocation advertisements available • Requirements on relying parties to check other forms of revocation advertisements • Any variations on the above stipulations when the suspension or revocation is the result of private key compromise (as opposed to other reasons for suspension or revocation) • The CA's requirements for archival and retention of CRLs or other certificate status information • Whether copies of all certificates issued (including all expired, revoked, or suspended certificates) are retained and disclosure of the retention period • If an online status mechanism is used (for example, OCSP), certificate status request content requirements • If an online status mechanism is used (for example, OCSP), definitive response message data content requirements • What key is used to digitally sign definitive response messages	35 The CA issues CRLs once a day at 11:59 PM. In addition, the CA may issue interim CRLs in the event that personnel of the CA deem it necessary (that is, in the event of a serious private key compromise) or as dictated by certificate policy (CP). As stated in the CP, CRL checking is required for all relying parties. A subscriber is notified of the revocation of his or her certificate by e-mail, postal mail, or telephone. The CP may define other forms of revocation advertisements. The CA archives and retains all certificates and CRLs issued by the CA for a period not less than 10 years. The CA also supports online certificate revocation checking using OCSP. The CA requires that OCSP requests contain the following data: • Protocol version • Service request • Target certificate identifier • Optional extensions which may be processed by the OCSP responder. Definitive OCSP response messages include the following: • Version of the response syntax • Name of the responder • Responses for each of the certificates in a request (including target certificate identifier, certificate status value, response validity interval, and optional extensions) • Optional extensions • Signature algorithm OID • Signature computed across hash of the response All definitive response messages are digitally signed with a key belonging to the CA that issued the certificate in question. When the CA returns an error message in response to a certificate status request, the error message is not digitally signed.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Disclosures*
• Whether the CA signs error messages when returned in response to certificate status requests	
Certificate profile, including: • Version number(s) supported • Certificate extensions populated and their criticality • Cryptographic algorithm object identifiers • Name forms (that is, naming hierarchy used to ensure that the certificate subject can be uniquely identified—if required) used for the CA, RA, and subscribers names • Name constraints used and the name forms used in the name constraints • Applicable certificate policy object identifier(s) • Usage of the policy constraints extension • Policy qualifiers syntax and semantics • Processing semantics for the critical certificate policy extension	36 The following fields in the X.509 certificate format are utilized in the CA's PKI: • Version—Set to v3 • Serial number—Unique values for each certificate in the CA domain • Signature algorithm identifier—The algorithm used by the CA for signing the certificate • Issuer—Identification of the certificate issuer • Validity—Start date and end date of the validity period are defined • Subject—Certificate subject's distinguished name • Public key information—Algorithm identifier (that is, RSA with SHA-1) and public key • Issuer unique identifier • Subject unique identifier • Extensions
CRL profile, including: • Version numbers supported for CRLs • CRL and CRL entry extensions populated and their criticality	37 The following fields of the X.509 CRL format are utilized by the CA: • Version—v2 • Signature—Identifies algorithm used to sign CRL • Issuer—Identification of the CA issuing the CRL • This update—Time of CRL issue • Next update—Time of next anticipated CRL issue • Revoked certificates—Listing of information for revoked certificates The CA may alternatively support online certificate status and revocation checking services.
Integrated circuit card (ICC) life cycle management, including: • Whether ICCs are issued by the CA (or RA) • If supported, a description of the CA's ICC life cycle management processes, including a description of the ICC distribution process	38 The CA does not issue smart cards to subscribers. Subscribers may, at their own discretion, purchase smart cards and readers for purposes of key generation and storage.

(continued)

Criteria	*Illustrative Disclosures*
CA Environmental Controls	
CPS and CP administration: • CPS and CP change control procedures • Publication and notification policies • CPS and CP approval procedures	39 Some revisions to this certification policy statement (CPS) may be deemed by the CA's policy authority to have minimal or no impact on subscribers and relying parties using certificates and CRLs issued by CA. Such revisions may be made without notice to users of the CPS and without changing the version number of this CPS. Revisions to the certificate policies supported by this CPS, as well as revisions to the CPS which are deemed by the CA's policy authority to have significant impact on the users of this CPS, may be made with 45 days notice to the users and a change in version number for this CPS. The CA's policy authority will provide notification of upcoming changes on the CA's Web site 45 days prior to significant revisions to this CPS. This CPS and any subsequent changes are approved by the CA's policy authority.
CA termination, including a description of the CA's procedures for termination and for termination notification of a CA or RA, including the identity of the custodian of CA and RA archival records	40 The CA can only be terminated by the board of directors of the CA. In the event the CA is terminated, all certificates issued under the CA will be revoked and the CA will cease to issue certificates. The CA will provide no less than one month notice to all business units utilizing the services of the CA. Upon termination, the records of the CA will be archived and transferred to a specified custodian.
Confidentiality, including: • Applicable statutory or regulatory requirements to keep information confidential • Kinds of information to be kept confidential • Kinds of information not considered confidential • Disclosure of information concerning certificate revocation and suspension • Release to law enforcement officials • Release as part of civil discovery • Disclosure upon owner's request • Other information release circumstances	41 Information which is not considered by the CA to be public domain information is to be kept confidential. Confidential information includes: • Subscribers' private signing keys are confidential and are not provided to the CA or RA. • Information specific to the operation and control of the CA, such as security parameters and audit trails, is maintained confidentially by the CA and is not released outside of the CA organization unless required by law. • Information about subscribers held by the CA or RAs, excluding that which is published in certificates, CRLs, certificate policies, or this CPS, is considered confidential and shall not be released outside of the CA except as required by certificate policy or otherwise required by law.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria		*Illustrative Disclosures*
		• Generally, the results of annual audits are kept confidential, unless disclosure is deemed necessary by CA management. Nonconfidential information includes: • Information included in certificates and CRLs issued by the CA is not considered confidential. • Information in the certificate policies supported by this CA is not considered confidential. • Information in the CA's disclosed CPS (or other CA business practices disclosure) is not considered confidential. • When the CA revokes a certificate, a revocation reason is included in the CRL entry for the revoked certificate. This revocation reason code is not considered confidential and can be shared with all other subscribers and relying parties. However, no other details concerning the revocation are normally disclosed. The CA will comply with legal requirements to release information to law enforcement officials. The CA may disclose to another party information pertaining to the owner of such information upon the owner's request.
Intellectual property rights	42	Public key certificates and CRLs issued by the CA are the property of the CA. This CPS and the related certificate policies are the property of the CA.
Physical security controls, including: • Site location and construction • Physical access controls, including authentication controls to control and restrict access to CA facilities • Power and air conditioning • Water exposures • Fire prevention and protection • Media storage • Waste disposal • Off-site backup	43	All critical CA operations take place within a physically secure facility with at least four layers of security to access sensitive hardware or software. Such systems are physically separated from the organization's other systems so that only authorized employees of the CA can access them. Physical access to the CA systems is strictly controlled. Only trustworthy individuals with a valid business reason are provided such access. The access control system is always functional and utilizes proximity cards and biometrics for access. All CA systems have industry standard power and air conditioning systems to provide a suitable operating environment.

(continued)

Criteria		*Illustrative Disclosures*
		All CA systems have reasonable precautions taken to minimize the impact of water exposure. All CA systems have industry standard fire prevention and protection mechanisms in place. Media storage at the CA third-party processor is subject to the same degree of protection as the CA hardware. Media storage under the control of the CA is subject to the normal media storage requirements of the company. Waste is disposed of in accordance with the organization's normal waste disposal requirements. Cryptographic devices are physically destroyed or zeroized in accordance with the manufacturers' guidance prior to disposal. Off-site backups are stored in a physically secure manner by a bonded third-party storage facility.
Business continuity management controls, including: • Whether the CA has business continuity plans to maintain or restore the CA's business operations in a reasonably timely manner following interruption to or failure of critical business processes • Whether the CA's business continuity plans define an acceptable system outage and recovery time and disclosure of the defined time period(s) • How frequently backup copies of essential business information and software are taken • Proximity of recovery facilities to the CA's main site	44	The CA has a business continuity plan to restore the CA's business operations in a reasonably timely manner following interruption to, or failure of, critical business processes. The CA's business continuity plan defines 24 hours as an acceptable system outage time in the event of a major natural disaster or CA private key compromise. Copies of essential business information and CA system software are performed daily. The CA maintains a recovery site which is located approximately 50 miles from the CA's primary site.
Event logging, including the following: • How frequently the CA archives event journal data • How frequently event journals are reviewed	45	As part of the CA's scheduled system backup procedures, audit trail files are backed up to media on at least a daily basis. Audit trail files are archived by the system administrator on a weekly basis. Event journals are reviewed at least on a weekly basis by CA management.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Principle 2: Service Integrity

.65 The certification authority maintains effective controls to provide reasonable assurance that:

- Subscriber information was properly authenticated (for the registration activities performed by ABC-CA) and
- The integrity of keys and certificates it manages is established and protected throughout their life cycles.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
2.1 Key Life Cycle Management Controls	
2.1.1 CA Key Generation	**Such controls generally include but are not limited to the following:**
The certification authority (CA) maintains controls to provide reasonable assurance that CA key pairs are generated in accordance with industry standards.	1 CA key generation occurs within a secure cryptographic device meeting the appropriate ISO 15782-1/FIPS 140-1/ANSI X9.66 level requirement as disclosed in the CA's business practices (see Principle 1, item 18 [paragraph .64]). 2 CA key generation by the CA requires dual control by properly authorized personnel. 3 The CA generates its own key pair in the same cryptographic device in which it will be used or the key pair is injected directly from the device where it was generated into the device in which it will be used. 4 Key generation uses a random number generator (RNG) or pseudo random number generator (PRNG) as specified in an ANSI X9 or ISO standard. 5 Key generation uses a prime number generator as specified in an ANSI X9 or ISO standard. 6 Key generation uses a key generation algorithm as specified in an ANSI X9 or ISO standard as disclosed in the CA's business practices (Principle 1, item 18 [paragraph .64]). 7 Key generation results in key sizes as disclosed in the CA's business practices (Principle 1, item 18 [paragraph .64]). 8 The integrity of the hardware and software used for key generation and the interfaces to the hardware and software are tested before usage.

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
2.1.2 CA Key Storage, Backup, and Recovery The CA maintains controls to provide reasonable assurance that CA private keys remain confidential and maintain their integrity.	**Such controls generally include but are not limited to the following:** 1 The CA's private signing key is stored within a secure cryptographic device meeting the appropriate ISO 15782-1/FIPS 140-1/ANSI X9.66 level requirement as disclosed in the CA's business practices (Principle 1, item 17 [paragraph .64]). 2 If the CA private key is not exported from a secure cryptographic module and moved to secure storage for purposes of offline processing or backup and recovery, then the CA private key is generated and used within the same cryptographic module and is never exported outside of the cryptographic module. 3 If the CA private key is exported from a secure cryptographic module and moved to secure storage for purposes of offline processing or backup and recovery, then the private key is exported in a secure key management scheme including any of the following: *a.* As ciphertext using dual control *b.* As encrypted key fragments using dual control and split knowledge/ownership *c.* In another secure cryptographic module such as a key transportation device using dual control 4 The CA private key is backed up, stored, and recovered by authorized personnel using dual control in a physically secured environment. 5 If the CA's private signing key is backed up, backup copies of the CA private keys are subject to the same or greater level of security controls as keys currently in use. 6 If the CA's private signing key is backed up, recovery of the CA private key is conducted in the same secure schema used in the backup process, using dual control.
2.1.3 CA Public Key Distribution The CA maintains controls to provide reasonable assurance that the integrity and authenticity of the CA public key and any associated parameters are maintained during initial and subsequent distribution.	**Such controls generally include but are not limited to the following:** 1 The CA provides a mechanism for detecting the modification of the CA's public key during the initial distribution process (for example, using a self-signed certificate).

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
	2 The initial distribution mechanism for the CA's public key is controlled as disclosed in the CA's business practices (Principle 1, item 20 [paragraph .64]).
	3 CA public keys are initially distributed using one of the following methods as disclosed in any one of the following CA's business practices (Principle 1, item 20 [paragraph .64]) *a.* Machine readable media (for example, smart card) *b.* Embedding in an entity's cryptographic module *c.* Other secure means
	4 The CA's public key is changed (rekeyed) periodically as disclosed in the CA's business practices (Principle 1, item 21 [paragraph .64]).
	5 The subsequent distribution mechanism for the CA's public key is controlled as disclosed in the CA's business practices (Principle 1, item 21 [paragraph .64]).
	6 If an entity already has an authenticated copy of the CA's public key, a new CA public key is distributed using one of the following methods as disclosed in the CA's business practices (Principle 1, item 21[paragraph .64): *a.* Direct electronic transmission from the CA *b.* Placing into a remote cache or directory *c.* Loading into a cryptographic module *d.* Any of the methods used for initial distribution
2.1.4 CA Key Escrow (Optional)	**Such controls generally include but are not limited to the following:**
The CA maintains controls to provide reasonable assurance that escrowed CA private signing keys remain confidential.	1 If a third party provides CA private key escrow services, a contract outlining the liabilities and remedies between the parties exists.
	2 If CA private signing keys are held in escrow, escrowed copies of the CA private signing keys are subject to the same or greater level of security controls as keys currently in use.

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
2.1.5 CA Key Usage The CA maintains controls to provide reasonable assurance that CA keys are used only for their intended functions in their intended locations.	**Such controls generally include but are not limited to the following:** 1 The activation of the CA private signing key is performed using multiparty control (that is, *m* of *n*). 2 If necessary based on a risk assessment, the activation of the CA private signing key is performed using multi-factor authentication (for example, smart card and password, biometric, and password). 3 The CA ceases to use a key pair at the end of the cryptoperiod or when the compromise of the private key is known or suspected.
2.1.6 CA Key Destruction The CA maintains controls to provide reasonable assurance that CA keys are completely destroyed at the end of the key pair life cycle.	**Such controls generally include but are not limited to the following:** 1 Authorization to destroy a CA private key and how the CA's private key is destroyed (for example, token surrender, token destruction, or key overwrite) are limited as disclosed in the CA's business practices (Principle 1, item 17 [paragraph .64]). 2 All copies and fragments of the CA's private key are destroyed at the end of the key pair life cycle. 3 If a secure cryptographic device is accessible and known to be permanently removed from service, all CA private keys stored within the device that have ever been or potentially could be used for any cryptographic purpose are destroyed. 4 If a CA cryptographic device is being permanently removed from service, any key contained within the device that has been used for any cryptographic purpose is erased from the device. 5 If a CA cryptographic device case is intended to provide tamper-evident characteristics and the device is being permanently removed from service, the case is destroyed.
2.1.7 CA Key Archival The CA maintains controls to provide reasonable assurance that archived CA keys remain confidential and are never put back into production.	**Such controls generally include but are not limited to the following:** 1 Archived CA keys are subject to the same or greater level of security controls as keys currently in use. 2 All archived CA keys are destroyed at the end of the archive period using dual control in a physically secure site.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
	3 Archived keys are never put back into production. 4 Archived keys are recovered for the shortest time period technically permissible. 5 Archived keys are periodically verified to ensure that they are properly destroyed at the end of the archive period.
2.1.8 CA Cryptographic Hardware Life Cycle Management The CA maintains controls to provide reasonable assurance that access to CA cryptographic hardware is limited to properly authorized individuals.	*For purposes of this section, CA cryptographic hardware refers to devices containing CA private signing keys.* **Such controls generally include but are not limited to the following:** 1 Policies and procedures require that CA cryptographic hardware be sent from the manufacturer via registered mail using tamper-evident packaging. 2 Upon the receipt of CA cryptographic hardware from the manufacturer, authorized CA personnel inspect the tamper-evident packaging to determine whether the seal is intact. 3 To prevent tampering, CA cryptographic hardware is stored in a secure site, with access limited to authorized personnel, having the following characteristics: *a.* Inventory control processes and procedures to manage the origination, arrival, condition, departure, and destination of each device *b.* Access control processes and procedures to limit physical access to authorized personnel *c.* All successful or failed access attempts to the CA facility and device storage mechanism (for example, a safe) recorded in an event journal *d.* Incident processes and procedures to handle abnormal events, security breaches, and investigation and reports *e.* Audit processes and procedures to verify the effectiveness of the controls 4 CA cryptographic hardware is stored in tamper-resistant packages. 5 The handling of CA cryptographic hardware is performed in the presence of no less than two trusted employees. 6 The installation of CA cryptographic hardware is performed in the presence of no less than two trusted employees.

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
	7 The removal of CA cryptographic hardware from production is performed in the presence of no less than two trusted employees.
	8 The process whereby CA cryptographic hardware is serviced or repaired with new hardware, firmware, or software is performed in the presence of no less than two trusted employees.
	9 The service or repair site is a secure site with inventory control and access limited to authorized personnel.
	10 The process whereby CA cryptographic hardware is disassembled and permanently removed from use is performed in the presence of no less than two trusted employees.
The CA maintains controls to provide reasonable assurance that CA cryptographic hardware is functioning correctly.	11 Upon the receipt of CA cryptographic hardware from the manufacturer, acceptance testing and verification of firmware settings is performed.
	12 Upon the receipt of CA cryptographic hardware that has been serviced or repaired, acceptance testing and verification of firmware settings is performed.
	13 Devices used for private key storage and recovery and the interfaces to these devices are tested before usage for integrity.
	14 Correct processing of CA cryptographic hardware is verified on a periodic basis.
	15 Diagnostic support is provided during troubleshooting of CA cryptographic hardware in the presence of no less than two trusted employees.
2.1.9 CA-Provided Subscriber Key Management Services (Optional)	*For purposes of this section, subscriber includes external registration authorities (RAs).*
	Such controls generally include but are not limited to the following:
The CA maintains controls to provide reasonable assurance that subscriber keys generated by the CA (or registration authority [RA]) are generated in accordance with industry standards.	1 Subscriber key generation performed by the CA (or RA) occurs within a secure cryptographic device meeting the appropriate ISO 15782-1/FIPS 140-1/ANSI X9.66 level requirement as disclosed in the CA's business practices (Principle 1, item 18 [paragraph .64]).
	2 Subscriber key generation performed by the CA (or RA) uses a random number generator (RNG) or pseudo random number generator (PRNG) as specified in an ANSI X9 or ISO standard.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
	3 Subscriber key generation performed by the CA (or RA) uses a prime number generator as specified in an ANSI X9 or ISO standard.
	4 Subscriber key generation performed by the CA (or RA) uses a key generation algorithm as specified in an ANSI X9 or ISO standard as disclosed in the CA's business practices (Principle 1, item 18 [paragraph .64]).
	5 Subscriber key generation performed by the CA (or RA) results in key sizes as disclosed in the CA's business practices (Principle 1, item 18 [paragraph .64]).
	6 Subscriber key generation performed by the CA (or RA) is performed by authorized personnel as disclosed in the CA's business practices (Principle 1, item 18 [paragraph .64]).
	7 When subscriber key generation is performed by the CA (or RA), the CA (or RA) securely (confidentially) delivers the key pair(s) generated by the CA (or RA) on behalf of the subscriber to the subscriber as disclosed in the CA's business practices (Principle 1, item 18 [paragraph .64]).
The CA maintains controls to provide reasonable assurance that subscriber private keys stored by the CA remain confidential and maintain their integrity.	8 Subscriber private keys stored by the CA are stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and the business requirements of the CA.
	9 If the CA generates key pair(s) on behalf of a subscriber, the CA ensures that subscriber's private keys are not disclosed to any entity other than the owner of the keys.
	10 If the CA generates public/private digital signature key pair(s), the CA does not maintain a copy of any digital signature private key, once that key is delivered to the subscriber.
	11 If the CA provides subscriber key storage, backup, and recovery, subscriber private key backup and recovery is performed only by authorized personnel.
	12 If the CA provides subscriber key storage, backup, and recovery, controls exist to ensure that the integrity of the subscriber's private key is maintained throughout its life cycle.

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
The CA maintains controls to provide reasonable assurance that subscriber keys stored by the CA are completely destroyed at the end of the key pair life cycle.	13 If the CA provides subscriber key storage, authorization to destroy a subscriber's private key and the means to destroy the subscriber's private key (for example, key overwrite) are limited as disclosed in the CA's business practices (Principle 1, item 22 [paragraph .64]).
	14 If the CA provides subscriber key storage, all copies and fragments of the subscriber's private key are destroyed at the end of the key pair life cycle.
The CA maintains controls to provide reasonable assurance that subscriber keys archived by the CA remain confidential.	15 Subscriber private keys archived by the CA are stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and the business requirements of the CA.
	16 If the CA provides subscriber key archival, all archived subscriber keys are destroyed at the end of the archive period.
The CA maintains controls to provide reasonable assurance that subscriber keys escrowed by the CA remain confidential.	17 Subscriber private keys escrowed by the CA are stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and the business requirements of the CA.

2.2 Certificate Life Cycle Management Controls

2.2.1 Subscriber Registration

Note: A requesting entity may be a subscriber requesting a certificate from an RA or CA, an RA requesting a certificate from a CA, or a subordinate CA requesting a certificate from a root CA or superior CA.

Such controls generally include but are not limited to the following:

The CA maintains controls to provide reasonable assurance that subscribers are properly identified and authenticated.	1 The CA verifies or requires that the external RA verify the identity of the entity requesting a certificate as disclosed in the CA's business practices (Principle 1, item 25 [paragraph .64]).
	2 The CA requires that an entity requesting a certificate must prepare and submit the appropriate certificate request data (registration request) to an RA (or the CA) as disclosed in the CA's business practices (Principle 1, item 25 [paragraph .64]).
	3 The CA verifies or requires that the external RA verify the authority of the entity requesting a certificate as disclosed in the CA's business practices (Principle 1, item 25 [paragraph .64]).

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
	4 The CA verifies or requires that the external RA verify the accuracy of the information included in the requesting entity's certificate request as disclosed in the CA's business practices (Principle 1, item 25 [paragraph .64]).
	5 If external RAs are used, the CA validates the identity of external RAs as disclosed in the CA's business practices (Principle 1, item 26 [paragraph .64]).
	6 If external registration authorities are used, the CA authorizes external RAs as disclosed in the CA's business practices (Principle 1, item 26 [pargraph .64]).
The CA maintains controls to provide reasonable assurance that subscriber certificate requests are accurate, authorized, and complete.	7 The CA requires that an entity requesting a certificate prepare and submit the appropriate certificate request data to the CA or an external RA as disclosed in the CA's business practices (Principle 1, item 25 [paragraph .64]).
	8 The CA requires that the requesting entity submit its public key in a signed message to the CA for certification. The CA requires that the requesting entity digitally sign the registration request using the private key that relates to the public key contained in the registration request in order to: *a.* Allow the detection of errors in the certificate application process. *b.* Prove possession of the companion private key for the public key being registered.
	9 The CA uses the public key contained in the requesting entity's certificate request to verify the requesting entity's signature on the certificate request submission.
	10 If an external RA is used, the CA requires that the external RA submits the requesting entity's certificate request data to the CA in a message (certificate request) signed by the RA.
	11 If an external RA is used, the CA requires that the RA secure that part of the certificate application process for which it (the RA) assumes responsibility as disclosed in the CA's business practices (Principle 1, item 26 [paragraph .64]).
	12 If an external RA is used, the CA requires that the external RA records its actions in an event journal.

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
	13 If an external RA is used, the CA verifies the authenticity of the submission by the RA as disclosed in the CA's business practices (Principle 1, item 26 [paragraph .64]).
	14 If an external RA is used, the CA verifies the RA's signature on the certificate request.
	15 The CA or RA checks the certificate request for errors or omissions as disclosed in the CA's business practices (Principle 1, item 25 [paragraph .64]).
	16 The CA verifies the uniqueness of the requesting entity's distinguished name within the CA's domain.
	17 The CA accepts the certificate request from the requesting entity whose identity has been validated.
	18 When the CA detects duplicate public keys, the certificate request is rejected and the original certificate is revoked.
2.2.2 Certificate Renewal (Optional)	**Such controls generally include but are not limited to the following:**
The CA maintains controls to provide reasonable assurance that certificate renewal requests are accurate, authorized, and complete.	1 The subscriber's certificate renewal request includes at least the subscriber's distinguished name, the serial number of the certificate (or other information that identifies the certificate), and the requested validity period to allow the CA or the RA to identify the certificate to renew.
	2 The CA requires that the requesting entity digitally sign the certificate renewal request using the private key that relates to the public key contained in the requesting entity's existing public key certificate.
	3 The CA or the RA processes the certificate renewal data to verify the identity of the requesting entity and identify the certificate to be renewed.
	4 The CA or the RA validates the signature on the certificate renewal request.
	5 The CA or the RA verifies the existence and validity of the certificate to be renewed.
	6 The CA or the RA verifies that the request, including the extension of the validity period, meets the requirements as disclosed in the CA's business practices (Principle 1, item 28 [paragraph .64]).

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
	7 If an external RA is used, the CA requires that the external RA submits the requesting entity's certificate request data to the CA in a message (certificate renewal request) signed by the RA.
	8 When an external RA is used, the RA secures that part of the certificate renewal process for which it (the RA) assumes responsibility as disclosed in the CA's business practices (Principle 1, item 26 [paragraph .64]).
	9 If an external RA is used, the CA requires that the external RAs record its actions in an event journal.
	10 If an external RA is used, the CA verifies the authenticity of the submission by the RA.
	11 If an external RA is used, the CA verifies the RA's signature on the certificate renewal request.
	12 The CA or RA checks the certificate renewal request for errors or omissions.
	13 The CA or RA notifies subscribers prior to the expiration of their certificate of the need for renewal as disclosed in the CA's business practices (Principle 1, item 27 [paragraph .64]).
	14 Prior to certificate generation and issuance of renewed certificates, the CA or RA verifies the following: *a.* The signature on the certificate renewal data submission *b.* The existence and validity of the certificate to be renewed *c.* That the request, including the extension of the validity period, meets the requirements as disclosed in the CA's business practices (Principle 1, item 27 [paragraph .64])
2.2.3 Certificate Rekey The CA maintains controls to provide reasonable assurance that certificate rekey requests are accurate, authorized, and complete.	**Such controls generally include but are not limited to the following:** 1 The subscriber's certificate rekey request includes at least the subscriber's distinguished name, the serial number of the certificate, and the requested validity period to allow the CA or the RA to identify the certificate to rekey. 2 The CA requires that the requesting entity digitally sign the certificate rekey request using the private key that relates to the public key contained in the requesting entity's existing public key certificate.

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
	3 The CA or the RA processes the certificate rekey request to verify the identity of the requesting entity and identify the certificate to be rekeyed.
	4 The CA or the RA validates the signature on the certificate rekey request.
	5 The CA or the RA verifies the existence and validity of the certificate to be rekeyed.
	6 The CA or the RA verifies that the certificate rekey request meets the requirements as disclosed in the CA's business practices (Principle 1, item 28 [paragraph .64]).
	7 If an external RA is used, the CA requires that the external RA submits the requesting entity's certificate rekey request to the CA in a message signed by the RA.
	8 If an external RA is used, the CA requires that the RA secure that part of the certificate rekey process for which it (the RA) assumes responsibility as disclosed in the CA's business practices (Principle 1, item 26 [paragraph .64]).
	9 If an external RA is used, the CA requires that the external RA records its actions in an event journal.
	10 If an external RA is used, the CA verifies the authenticity of the submission by the RA.
	11 If an external RA is used, the CA verifies the RA's signature on the certificate rekey request.
	12 The CA or the RA checks the certificate rekey request for errors or omissions.
	13 The CA or RA notifies subscribers prior to the expiration of their certificate of the need for rekey.
	14 Prior to the generation and issuance of rekeyed certificates, the CA or RA verifies the following: *a.* The signature on the certificate renewal data submission *b.* The existence and validity of the certificate to be renewed *c.* That the request, including the extension of the validity period, meets the requirements as disclosed in the CA's business practices (Principle 1, item 28 [paragraph .64])

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
The CA maintains controls to provide reasonable assurance that certificate rekey requests following certificate revocation or expiration are accurate, authorized, and complete.	15 Following the revocation or expiration of a subscriber's existing certificate, the subscriber is required to follow the CA's subscriber registration procedures to obtain a new rekeyed certificate (as specified in §2.2.1, Subscriber Registration) as disclosed in the CA's business practices (Principle 1, item 29 [paragraph .64]).
2.2.4 Certificate Issuance	**Such controls generally include but are not limited to the following:**
The CA maintains controls to provide reasonable assurance that new, renewed, and rekeyed certificates are generated and issued in accordance with the CA's disclosed business practices.	1 The CA generates certificates using the appropriate certificate format as disclosed in the CA's business practices (Principle 1, item 30 [paragraph .64]). 2 The CA generates certificates in accordance with ISO 9594/X.509 as disclosed in the CA's business practices (Principle 1, item 30 [paragraph .64]). 3 Validity periods are set in accordance with ISO 9594/X.509 as disclosed in the CA's business practices (Principle 1, item 30 [paragraph .64]). 4 Extension fields are set in accordance with ISO 9594/X.509 as disclosed in the CA's business practices (Principle 1, item 30 [paragraph .64]). 5 Key usage extension fields are set in accordance with ISO 9594/X.509 as disclosed in the CA's business practices (Principle 1, item 30 [paragraph .64]). 6 The CA signs the requesting entity's certificate with the CA's private signing key. 7 The CA issues the certificate after the certificate has been accepted by the requesting entity as disclosed in the CA's business practices (Principle 1, item 31 [paragraph .64]). 8 When an RA is used, the CA notifies the RA when a certificate is issued to a subscriber for whom the RA submitted a certificate request. 9 For certificate renewals, the CA generates and signs a new instance of the certificate, differing from the previous certificate only by the validity period and the CA signature, only if the CA has approved the certificate renewal request as specified in §2.2.2, Certificate Renewal.

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
	10 For rekeyed certificates, the CA generates and signs a new certificate only if the CA has approved the certificate rekey request as specified in §2.2.3, Certificate Rekey.
	11 The CA issues an out-of-band notification to the requesting entity when a certificate is issued.
2.2.5 Certificate Distribution	**Such controls generally include but are not limited to the following:**
The CA maintains controls to provide reasonable assurance that, upon issuance, complete and accurate certificates are available to subscribers and relying parties in accordance with the CA's disclosed business practices.	1 The CA makes the certificates issued by the CA available to relying parties using an established mechanism (for example, a repository such as a directory) as disclosed in the CA's business practices (Principle 1, item 32 [paragraph .64]). 2 Upon certificate issuance, the CA posts certificates to the repository or alternative distribution mechanism as disclosed in the CA's business practices (Principle 1, item 32 [paragraph .64]). 3 Only authorized CA personnel may administer the CA's repository or alternative distribution mechanism. 4 The performance of the CA's repository or alternative distribution mechanism is monitored and managed. 5 The integrity of the repository or alternative distribution mechanism is maintained.
2.2.6 Certificate Revocation	**Such controls generally include but are not limited to the following:**
The CA maintains controls to provide reasonable assurance that certificates are revoked based on authorized and validated certificate revocation requests.	1 As disclosed in the CA's business practices (Principle 1, item 33 [paragraph .64]), the CA provides a means of rapid communication to facilitate the secure and authenticated revocation of the following: *a.* One or more certificates of one or more entities *b.* The set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates *c.* All certificates issued by a CA, regardless of the public/private key pair used 2 The CA verifies or requires that the external RA verify the identity and authority of the entity requesting revocation of a certificate as disclosed in the CA's business practices (Principle 1, item 33 [paragraph .64]).

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
	3 If an external RA accepts revocation requests, the CA requires that the RA submit certificate revocation requests to the CA in an authenticated manner as disclosed in the CA's business practices (Principle 1, item 33 [paragraph .64]).
	4 If an external RA accepts and forwards revocation requests to the CA, the CA provides an authenticated acknowledgment of the revocation to the requesting RA as disclosed in the CA's business practices (Principle 1, item 33 [paragraph .64]).
	5 The CA updates the certificate revocation list (CRL) and other certificate status mechanisms upon certificate revocation as disclosed in the CA's business practices (Principle 1, item 33 [paragraph .64]).
	6 The CA records all certificate revocation requests and their outcome in an event journal.
	7 The CA or RA provides an authenticated acknowledgement of the revocation to the entity whose certificate has been revoked as disclosed in the CA's business practices (Principle 1, item 33 [paragraph .64]).
	8 Where certificate renewal is supported, when a certificate is revoked all valid instances of the certificate are also revoked.
2.2.7 Certificate Suspension (Optional) The CA maintains controls to provide reasonable assurance that certificates are suspended based on authorized and validated certificate suspension requests.	**Such controls generally include but are not limited to the following:** 1 As disclosed in the CA's business practices (Principle 1, item 34 [paragraph .64]), the CA provides a means of rapid communication to facilitate the secure and authenticated suspension of the following: *a.* One or more certificates of one or more entities *b.* The set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates *c.* All certificates issued by a CA, regardless of the public/private key pair used 2 The CA verifies or requires that the external RA verify the identity and authority of the entity requesting suspension of a certificate as disclosed in the CA's business practices (Principle 1, item 34 [paragraph .64]).

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
	3 If an external RA accepts suspension requests, the RA submits certificate suspension requests to the CA in an authenticated manner as disclosed in the CA's business practices (Principle 1, item 34 [paragraph .64]).
	4 The CA or RA notifies the end entity in the event of a certificate suspension as disclosed in the CA's business practices (Principle 1, item 34 [paragraph .64]).
	5 Certificate suspension requests are processed and validated as disclosed in the CA's business practices (Principle 1, item 34 [paragraph .64]).
	6 The CA updates the certificate revocation list (CRL) and other certificate status mechanisms upon certificate suspension as disclosed in the CA's business practices (Principle 1, item 34 [paragraph .64]).
	7 Certificates are suspended only for the allowable length of time as disclosed in the CA's business practices (Principle 1, item 34 [paragraph .64]).
	8 Once a certificate suspension (hold) has been issued, the suspension is handled in one of the following three ways: *a.* An entry for the suspended certificate remains on the CRL with no further action, causing users to reject transactions issued during the hold period *b.* The CRL entry for the suspended certificate is replaced by a revocation entry for the same certificate *c.* The suspended certificate is explicitly released and the entry removed from the CRL
	9 A certificate suspension (hold) entry remains on the CRL until the expiration of the underlying certificate or the expiration of the suspension, whichever is first.
	10 The CA updates the CRL and other certificate status mechanisms upon the lifting of a certificate suspension as disclosed in the CA's business practices (Principle 1, item 34 [paragraph .64]).
	11 The CA verifies or requires that the external RA verify the identity and authority of the entity requesting that the suspension of a certificate be lifted.
	12 Certificate suspensions and the lifting of certificate suspensions are recorded in an event journal.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
2.2.8 Certificate Status Information Processing The CA maintains controls to provide reasonable assurance that timely, complete, and accurate certificate status information (including certificate revocation lists [CRLs] and other certificate status mechanisms) is made available to subscribers and relying parties.	**Such controls generally include but are not limited to the following:** 1 Certificate status information is made available to all relevant entities as disclosed in the CA's business practices (Principle 1, item 35 [paragraph .64]). 2 The CA makes each certificate revocation list (CRL) issued by the CA available to relying parties using an established mechanism (for example, a repository such as a directory) as disclosed in the CA's business practices (Principle 1, item 35 [paragraph .64]). 3 The CA digitally signs each CRL that it issues so that entities can validate the integrity of the CRL and the date of issuance. 4 The CA issues CRLs at regular intervals, even if no changes have occurred since the last issuance, as disclosed in the CA's business practices (Principle 1, item 35 [paragraph .64]). 5 At a minimum, a CRL entry identifying a revoked certificate remains on the CRL until the end of the certificate's validity period. 6 If certificate suspension is supported, a certificate suspension (hold) entry with its original action date and expiration date remains on the CRL until the normal expiration of the certificate. 7 CRLs are archived as disclosed in the CA's business practices (Principle 1, item 35 [paragraph .64]). 8 CAs include a monotonically increasing sequence number for each CRL issued by that CA (for example, 1, 2, 3). 9 The CRL contains entries for all revoked unexpired certificates issued by the CA. 10 Old CRLs are retained for the appropriate period of time as disclosed in the CA's business practices (Principle 1, item 35 [paragraph .64]). 11 Whether certificates expire, are revoked, or are suspended, copies of certificates are retained for the appropriate period of time as disclosed in the CA's disclosed business practices (Principle 1, item 35 [paragraph .64]).

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
	12 If an online certificate status mechanism (for example, OCSP) is used, the CA requires that certificate status inquiries (for example, OCSP requests) contain all required data as disclosed in the CA's business practices (Principle 1, item 35 [paragraph .64]).
	13 Upon the receipt of a certificate status request (for example, an OCSP request) from a relying party, the CA returns a definitive response to the relying party if: *a.* The request message is well formed; *b.* The responder is configured to provide the requested service; and *c.* The request contains the information needed by the responder as disclosed in the CA's business practices (Principle 1, item 35 [paragraph .64]).
	14 All definitive response messages are digitally signed as disclosed in the CA's business practices (Principle 1, item 35 [paragraph .64]).
	15 Definitive response messages include all required data as disclosed in the CA's business practices (Principle 1, item 35 [paragraph .64]).
	16 If any of the three conditions (specified in item 13) are not met, the CA produces a signed or unsigned error message as disclosed in the CA's business practices (Principle 1, item 35 [paragraph .64]).
2.2.9 Integrated Circuit Card (ICC) Life Cycle Management (Optional)	*Note: For purposes of this section, integrated circuit cards (for example, smart cards) include devices that may hold a subscriber's private key(s) and certificate(s).*
	Such controls generally include but are not limited to the following:
The CA maintains controls to provide reasonable assurance that ICC preparation is securely controlled by the CA (or RA).	1 The CA (or RA), as the card issuer, controls ICC personalization (the loading of common data file (CDF) data and its related cryptographic keys).
	2 Common data that identify the ICC, the card issuer, and the cardholder are stored by the card issuer in the ICC CDF). CDF activation is performed by the CA (or RA), as the card issuer, using a securely controlled process.
	3 After CDF activation, the ICC indicates a CDF activated status.
	4 The CA (or RA) logs ICC personalization and CDF activation.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANS8.79 Standard)*
The CA maintains controls to provide reasonable assurance that ICC application data file (ADF) preparation is securely controlled by the CA (or RA).	5 Specific application supplier data stored in the ICC is located in the application data file (ADF). ADF allocation (the allocation of memory areas in an integrated circuit) is securely controlled by the CA, as the card issuer.
	6 The CA, as the application supplier, controls ADF personalization (the loading of ADF related keys and data).
	7 The CA, as the card issuer, controls ADF activation (preparation of an ADF for use by the cardholder) using a securely controlled process.
	8 An ADF can only be activated when the CDF is either in an activated or a reactivated state.
	9 After ADF activation, the ICC indicates an ADF activated status.
	10 The CA logs ADF allocation, personalization, and activation.
The CA maintains controls to provide reasonable assurance that ICC usage is enabled by the CA (or RA) prior to ICC issuance.	11 An ICC is not issued unless the card has been personalized.
	12 An ICC is unusable unless the CDF is in an activated or a reactivated state.
The CA maintains controls to provide reasonable assurance that ICCs are securely stored and distributed by the CA (or RA).	13 ICCs are securely stored prior to distribution.
	14 Receipt, activation, and distribution of ICCs are logged in an event journal. An inventory of ICCs and their status is maintained.
	15 ICCs are securely distributed as disclosed in the CA's business practices (Principle 1, item 38 [paragraph .64]).
The CA maintains controls to provide reasonable assurance that ICC deactivation and reactivation are securely controlled by the CA (or RA).	16 ADF deactivation can be performed only by the CA, as the application supplier.
	17 CDF deactivation can be performed only by the CA, as the card issuer.
	18 CDF reactivation is conducted under the control of the CA, as the card issuer.
	19 ADF reactivation is conducted under the control of the CA, as the application supplier.
	20 ADF deactivation, CDF deactivation, CDF reactivation, and ADF reactivation are logged.
The CA maintains controls to provide reasonable assurance that the use of ICCs is securely terminated for ICCs returned to the CA (or RA).	21 The CA, as the application supplier, controls ADF termination.
	22 CDF termination is controlled by the CA, as the card issuer.

Principle 3: CA Environmental Controls

.66 The certification authority maintains effective controls to provide reasonable assurance that:

- Subscriber and relying party information is restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
- The continuity of key and certificate life cycle management operations is maintained; and
- CA systems development, maintenance, and operation are properly authorized and performed to maintain CA systems integrity.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
3.1 Certification Practice Statement and Certificate Policy Management The CA maintains controls to provide reasonable assurance that the CA's certification policy statement (CPS) and certificate policy (CP) management controls are effective.	**Such controls generally include but are not limited to the following:** 1 The CA organization has a management group with final authority and responsibility for specifying and approving the CA's certification practice statement (CPS). 2 There is a policy management authority with final authority and responsibility for specifying and approving certificate policy(s) (CPs). 3 The policy management authority (or equivalent group) has performed an assessment to evaluate business risks and determine the security requirements and operational procedures to be included in the applicable CP and/or CPS for the following: *a.* Key life cycle management controls *b.* Certificate life cycle management controls *c.* CA environmental controls 4 The CA's CPS is approved and modified in accordance with a defined review process, including responsibilities for maintaining the CPS. 5 The CA makes available its public CPS to all appropriate subscribers and relying parties. 6 Revisions to the CA's CPS are made available to subscribers and relying parties. 7 CPs are approved and modified in accordance with a defined review process, including responsibilities for maintaining the CPs. 8 A defined review process exists to ensure that CPs are supported by the CA's CPS.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
	9 The CA makes available the CPs supported by the CA to all appropriate subscribers and relying parties.
	10 Revisions to CPs supported by the CA are made available to subscribers and relying parties.
3.2 Security Management	**Such controls generally include but are not limited to the following:**
The CA maintains controls to provide reasonable assurance that management direction and support for information security is provided.	1 An information security policy document (*security policy*) is approved by management, published, and communicated, as appropriate, to all employees.
	2 The security policy contains a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing.
	3 The security policy contains a statement of management intent, supporting the goals and principles of information security.
	4 The security policy contains an explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including the following: *a.* Compliance with legislative and contractual requirements *b.* Security education requirements *c.* Prevention and detection of viruses and other malicious software *d.* Business continuity management *e.* The consequences of security policy violations
	5 The security policy contains a definition of general and specific responsibilities for information security management, including reporting security incidents.
	6 The security policy contains references to documentation which supports the policy.
	7 There is a defined review process, including responsibilities and review dates, for maintaining the security policy.
The CA maintains controls to provide reasonable assurance that information security is properly managed within the organization.	8 Senior management and/or a high level management information security committee ensures there is clear direction and visible management support for security initiatives.
	9 A management group or security committee exists to coordinate the implementation of information security measures.

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
	10 Responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined.
	11 A management authorization process for new information processing facilities exists and is followed.
The CA maintains controls to provide reasonable assurance that the security of CA facilities, systems, and information assets accessed by third parties is maintained.	12 Procedures exist and are followed to control physical and logical access to CA facilities and systems by third parties including on-site contractors and trading partners or joint ventures.
	13 If there is a business need for the CA to allow third-party access to CA facilities and systems, a risk assessment is performed to determine security implications and specific control requirements.
	14 Arrangements involving third-party access to CA facilities and systems are based on a formal contract containing all necessary security requirements.
The CA maintains controls to provide reasonable assurance that the security of information is maintained when the responsibility for CA functions has been outsourced to another organization or entity.	15 If the CA outsources the management and control of all or some of its information systems, networks, or desktop environments, the security requirements of the CA are addressed in a contract agreed to by the parties.
	16 A CA service provider may choose to delegate a portion of the CA roles and respective functions, and the CA service provider is ultimately responsible for the completion of the identified functions that it performs and the definition and maintenance of a statement of its certification practices (that is, certification practice statement).
3.3 Asset Classification and Management	**Such controls generally include but are not limited to the following:**
The CA maintains controls to provide reasonable assurance that CA assets and information receive an appropriate level of protection.	1 Owners are identified for all major CA assets and assigned responsibility for the maintenance of appropriate controls.
	2 Inventories of important CA assets are maintained.
	3 The CA has implemented information classification and associated protective controls for information that take account of business needs for sharing or restricting information, and the business impacts associated with such needs.
	4 Procedures are defined to ensure that information labeling and handling is performed in accordance with the CA's information classification scheme.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
3.4 Personnel Security The CA maintains controls to provide reasonable assurance that personnel and hiring practices enhance and support the trustworthiness of the CA's operations.	**Such controls generally include but are not limited to the following:** 1 Security roles and responsibilities, as specified in the organization's security policy, are documented in job descriptions. 2 Verification checks on permanent staff are performed at the time of job application. The CA's policies and procedures specify the background checks and clearance procedures required for the personnel filling the trusted roles, and other personnel, including janitorial staff. 3 Employees sign a confidentiality (nondisclosure) agreement as part of their initial terms and conditions of employment. 4 Contracting personnel controls include the following: *a.* Bonding requirements on contract personnel *b.* Contractual requirements including indemnification for damages due to the actions of the contractor personnel *c.* Audit and monitoring of contractor personnel 5 All employees of the organization and, where relevant, third-party users, receive appropriate training in organizational policies and procedures. The CA's policies and procedures specify the following: *a.* The training requirements and training procedures for each role *b.* Any retraining period and retraining procedures for each role 6 Periodic reviews occur to verify the continued trustworthiness of personnel involved in the activities related to key management and certificate management. 7 A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures. The CA's policies and procedures specify the sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems. 8 Appropriate and timely actions are taken when an employee is terminated so that controls and security are not impaired by such an occurrence.

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
3.5 Physical and Environmental Security The CA maintains controls to provide reasonable assurance that physical access to CA facilities is limited to properly authorized individuals and CA facilities are protected from environmental hazards.	**Such controls generally include but are not limited to the following:** 1 Physical protection is achieved through the creation of clearly defined security perimeters (meaning, physical barriers) around the business premises and CA facilities. 2 The perimeter of the building or site containing the CA facility is physically sound (that is, there should be no gaps in the perimeter where a break-in could easily occur). 3 A manned reception area or other means to control physical access is in place to restrict access to the building or site housing CA operations to authorized personnel only. 4 To prevent unauthorized entry and environmental contamination, proper physical barriers are in place (for example, extended from real floor to real ceiling as opposed to raised floor to suspended ceiling) as disclosed in the CA's business practices (Principle 1, item 43 [paragraph .64]). 5 All fire doors on security perimeters around the CA facilities are alarmed and slam shut. 6 Intruder detection systems are installed and regularly tested to cover all external doors of the building housing the CA facility and the CA facility itself. 7 The CA facility is alarmed when unoccupied. 8 The CA facility is physically locked and periodically checked when vacant. 9 Unsupervised working in secure CA facilities is not allowed both for safety reasons and to prevent opportunities for malicious activities. 10 All personnel are required to wear visible identification and are encouraged to challenge anyone not wearing visible identification. 11 Access to CA facilities is controlled and restricted to authorized persons through the use of authentication controls as disclosed in the CA's business practices (Principle 1, item 43 [paragraph .64]). 12 All personnel entering and leaving the CA facility are logged (that is, an audit trail of all access is securely maintained). 13 Visitors to the CA facility are supervised and their date and time of entry and departure recorded.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
	14 Third-party support services personnel are granted restricted access to secure CA facilities only when required and such access is authorized and monitored.
	15 Access rights to the CA facility are regularly reviewed and updated.
The CA maintains controls to provide reasonable assurance that loss, damage, or compromise of assets and interruption to business activities are prevented.	16 Equipment is sited or protected such as to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
	17 Equipment is protected from power failures and other electrical anomalies.
	18 Power and telecommunications cabling carrying data or supporting CA services is protected from interception or damage.
	19 Equipment is maintained in accordance with the manufacturer's instructions and/or other documented procedures to ensure its continued availability and integrity.
	20 All items of equipment containing storage media (that is, fixed hard disks) are checked to determine whether they contain any sensitive data prior to disposal or reuse. Storage devices containing sensitive information are physically destroyed or securely overwritten prior to disposal or reuse.
The CA maintains controls to provide reasonable assurance that compromise or theft of information and information processing facilities are prevented.	21 Sensitive or critical business information is locked away when not required and when the CA facility is vacated.
	22 Personal computers and workstations are not left logged on when unattended and are protected by key locks, passwords, or other controls when not in use.
	23 Equipment, information, and software belonging to the organization cannot be taken off-site without authorization.
3.6 Operations Management	**Such controls generally include but are not limited to the following:**
The CA maintains controls to provide reasonable assurance that the correct and secure operation of CA information processing facilities is ensured.	1 CA operating procedures are documented and maintained.
	2 Formal management responsibilities and procedures exist to control all changes to CA equipment, software, and operating procedures.
	3 Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorized modification or misuse of information or services.

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
	4 Development and testing facilities are separated from operational facilities.
	5 Prior to using external facilities management services, risks are identified and appropriate controls are agreed upon with the contractor and incorporated into the contract.
The CA maintains controls to provide reasonable assurance that the risk of CA systems failure is minimized.	6 Capacity demands are monitored and projections of future capacity requirements are made to ensure that adequate processing power and storage are available.
	7 Acceptance criteria for new information systems, upgrades, and new versions are established and suitable tests of the system are carried out prior to acceptance.
The CA maintains controls to provide reasonable assurance that the integrity of CA systems and information is protected against viruses and malicious software.	8 Detection and prevention controls to protect against viruses and malicious software and appropriate user awareness procedures are implemented.
	9 A formal reporting procedure exists and is followed, together with an incident response procedure, setting out the action to be taken on receipt of an incident report.
The CA maintains controls to provide reasonable assurance that damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures.	10 Users of CA systems are required to note and report observed or suspected security weaknesses in or threats to systems or services.
	11 Procedures exist and are followed for reporting software malfunctions.
	12 Procedures exist and are followed to ensure that faults are reported and corrective action is taken.
	13 The types, volumes, and costs of incidents and malfunctions are quantified and monitored.
	14 Incident management responsibilities and procedures exist and are followed to ensure a quick, effective, and orderly response to security incidents.
The CA maintains controls to provide reasonable assurance that media are securely handled to protect media from damage, theft, and unauthorized access.	15 Procedures for the management of removable computer media require the following: *a.* If no longer required, the previous contents of any reusable media that are to be removed from the organization are erased. *b.* Authorization is required for all media removed from the organization and a record of all such removals is kept, to maintain an audit trail. *c.* All media are stored in a safe, secure environment, in accordance with manufacturers' specifications.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
	16 Media is disposed of securely and safely when no longer required.
	17 Procedures for the handling and storage of information exist and are followed in order to protect such information from unauthorized disclosure or misuse.
	18 System documentation is protected from unauthorized access.
3.7 System Access Management	**Such controls generally include but are not limited to the following:**
	User access management
The CA maintains controls to provide reasonable assurance that CA system access is limited to properly authorized individuals.	1 Business requirements for access control are defined and documented in an access control policy which includes at least the following: *a.* Roles and corresponding access permissions *b.* Identification and authentication process for each user *c.* Segregation of duties *d.* Number of persons required to perform specific CA operations (that is, *m of n* rule)
	2 A formal user registration and deregistration procedure for granting access to CA information systems and services is followed.
	3 The allocation and use of privileges is restricted and controlled.
	4 The allocation of passwords is controlled through a formal management process.
	5 Users' access rights are reviewed at regular intervals.
	6 Users are required to follow defined policies and procedures in the selection and use of passwords.
	7 Users are required to ensure that unattended equipment has appropriate protection.
	Network access control
	8 Users are provided direct access only to the services that they have been specifically authorized to use.
	9 The path from the user terminal to computer services is controlled.
	10 If permitted, access by remote users is subject to authentication.
	11 Connections to remote computer systems are authenticated.
	12 Access to diagnostic ports is securely controlled.

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
	13 Controls (for example, firewalls) are in place to protect the CA's internal network domains from external network domains accessible by third parties.
	14 Controls are in place to limit the services (for example, HTTP, FTP) available to users in accordance with the CA's access control policies.
	15 Routing controls are in place to ensure that computer connections and information flows do not breach the access control policy of the organization's business applications.
	16 The security attributes of all network services used by the organization are documented by the CA.
	Operating system access control
	17 Automatic terminal identification is used to authenticate connections to specific locations and to portable equipment.
	18 Access to CA systems uses a secure logon process.
	19 All users have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual.
	20 A password management system is in place to provide an effective, interactive facility which ensures quality passwords.
	21 Use of system utility programs is restricted and tightly controlled.
	22 If required based on a risk assessment, duress alarms are provided for users who might be the target of coercion.
	23 Inactive terminals serving CA systems time out after a defined period of inactivity to prevent access by unauthorized persons.
	24 Restrictions on connection times are used to provide additional security for high-risk applications.
	Application access control
	25 Access to information and application system functions is restricted in accordance with the access control policy.
	26 Sensitive systems require a dedicated (isolated) computing environment.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
3.8 Systems Development and Maintenance The CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are properly authorized to maintain CA system integrity.	**Such controls generally include but are not limited to the following:** 1 Business requirements for new systems or enhancements to existing systems specify the requirements for controls. 2 Change control procedures exist and are followed for the implementation of software on operational systems. 3 Change control procedures exist and are followed for scheduled software releases and modifications. 4 Change control procedures exist and are followed for emergency software fixes. 5 Test data is protected and controlled. 6 Strict control is maintained over access to program source libraries. 7 The implementation of changes is strictly controlled by the use of formal change control procedures to minimize the risk of corruption of information systems. 8 Application systems are reviewed and tested when operating system changes occur. 9 Modifications to software packages are discouraged and essential changes strictly controlled. 10 The purchase, use, and modification of software is controlled and checked to protect against possible covert channels and Trojan code. 11 Controls are in place to secure outsourced software development.
3.9 Business Continuity Management The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster.	**Such controls generally include but are not limited to the following:** 1 The CA has a managed process for developing and maintaining its business continuity plans. 2 The CA has a business continuity planning strategy based on an appropriate risk assessment. 3 The CA has business continuity plans to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes as disclosed in the CA's business practices (Principle 1, item 44 [paragraph .64]).

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
	4 The CA has a business continuity planning framework which requires that business continuity plans address the following: *a.* The conditions for activating the plans *b.* Emergency procedures *c.* Fallback procedures *d.* Resumption procedures *e.* A maintenance schedule *f.* Awareness and education requirements *g.* The responsibilities of the individuals
	5 Business continuity plans are tested regularly to ensure that they are up-to-date and effective.
	6 Business continuity plans are maintained by regular reviews and updates to ensure their continuing effectiveness.
	7 Business continuity plans define an acceptable system outage time, recovery time, and the average time between failures as disclosed in the CA's business practices (Principle 1, item 44 [paragraph .64]).
	8 The CA's business continuity plans include disaster recovery processes for all critical components of a CA system, including the hardware, software, and keys, in the event of a failure of one or more of these components.
	9 The CA's business continuity plans address the recovery procedures used if computing resources, software, or data are corrupted or suspected to be corrupted.
	10 The CA's business continuity plans include procedures for securing its facility during the period of time following a natural or other disaster and before a secure environment is reestablished either at the original site or a remote hot site.
	11 Back-up copies of essential business information and software are regularly taken as disclosed in the CA's business practices (Principle 1, item 44 [paragraph .64]). The security requirements of these copies are consistent with the controls for the information backed up.
	12 Fallback equipment and backup media are sited at a safe distance to avoid damage from disaster at the main site as disclosed in the CA's business practices (Principle 1, item 44 [paragraph .64]).

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
The CA maintains controls to provide reasonable assurance of continuity of operations in the event of the compromise of the CA's private signing key.	13 The CA's business continuity plans address the compromise or suspected compromise of a CA's private signing key as a disaster. 14 In the event of the compromise or suspected compromise of a CA's private key, disaster recovery procedures include the revocation and reissuance of all certificates that were signed with the CA's private key. 15 The recovery procedures used if the CA's private key is compromised and the CA's public key is revoked include the following: *a.* How a secure environment is reestablished *b.* How the CA's old public key is revoked *c.* How the CA's new public key is provided to the users *d.* How the subjects are recertified 16 In the event that the CA has to replace its CA root private key, procedures are in place for the secure and authenticated revocation of the following: *a.* The old CA root public key *b.* The set of all certificates issued by a CA based on the compromised private key *c.* Any subordinate CA private keys and corresponding certificates 17 The CA's business continuity plan for key compromise addresses who is notified and what actions are taken with system software and hardware, symmetric and asymmetric keys, previously generated signatures, and encrypted data.
The CA maintains controls to provide reasonable assurance that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services.	18 The CA maintains procedures for the termination and notification of affected entities, and for transferring relevant archived CA records to a custodian as disclosed in the CA's business practices (Principle 1, item 40 [paragraph .64]).
3.10 Monitoring and Compliance The CA maintains controls to provide reasonable assurance that the CA complies with legal requirements.	**Such controls generally include but are not limited to the following:** 1 All relevant statutory, regulatory, and contractual requirements are explicitly defined and documented for each information system. 2 Appropriate procedures are implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights, and on the use of proprietary software products as disclosed in the CA's business practices (Principle 1, item 42 [paragraph .64]).

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
	3 Important records of an organization are protected from loss, destruction, and falsification.
	4 Controls are applied to protect personal information in accordance with relevant legislation.
	5 Management authorizes the use of information processing facilities and controls are applied to prevent the misuse of such facilities.
	6 Controls are in place to ensure compliance with national agreements, laws, regulations, or other instruments to control the access to or use of cryptographic controls.
	7 As disclosed in the CA's business practices (Principle 1, item 41 [paragraph .64]), the CA's confidentiality policies and procedures address the following: *a.* The kinds of information that must be kept confidential by the CA or RA *b.* The kinds of information that are not considered confidential *c.* Who is entitled to be informed of reasons for revocation and suspension of certificates *d.* The policy on release of information to law enforcement officials *e.* Information that can be revealed as part of civil discovery *f.* The conditions upon which the CA or RA may disclose information upon the owner's request *g.* Any other circumstances under which confidential information may be disclosed
The CA maintains controls to provide reasonable assurance that compliance with the CA's security policies and procedures is ensured.	8 Managers are responsible for ensuring that security procedures within their area of responsibility are carried out correctly.
	9 The CA's operations are subject to regular review to ensure compliance with security policies and standards.
	10 CA systems are periodically checked for compliance with security implementation standards.
The CA maintains controls to provide reasonable assurance that the effectiveness of the system audit process is maximized and interference to and from the system audit process is minimized.	11 Audits of operational systems are planned and agreed to such as to minimize the risk of disruptions to business processes.
	12 Access to system audit tools is protected to prevent possible misuse or compromise.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
The CA maintains controls to provide reasonable assurance that unauthorized CA system usage is detected.	13 Procedures for monitoring the use of CA systems are established and the results of the monitoring activities are reviewed regularly.
3.11 Event Journaling	**Such controls generally include but are not limited to the following:**
The CA maintains controls to provide reasonable assurance that significant CA environmental, key management, and certificate management events are logged accurately and completely.	1 The CA generates automatic (electronic) and manual event journals as appropriate. 2 All journal entries include the following elements: *a.* Date and time of the entry *b.* Serial or sequence number of entry (for automatic journal entries) *c.* Kind of entry *d.* Source of entry (for example, terminal, port, location, customer) *e.* Identity of the entity making the journal entry 3 The CA logs the following key life cycle management related events: *a.* CA (and subscriber, if applicable) key generation *b.* Installation of manual cryptographic keys and its outcome (with the identity of the operator) *c.* CA (and subscriber, if applicable) key backup *d.* CA (and subscriber, if applicable) key storage *e.* CA (and subscriber, if applicable) key recovery *f.* CA (and subscriber, if applicable) key escrow activities (optional) *g.* CA key usage *h.* CA (and subscriber, if applicable) key archival *i.* Withdrawal of keying material from service *j.* CA (and subscriber, if applicable) key destruction *k.* Identity of the entity authorizing a key management operation *l.* Identity of the entity handling any keying material (such as key components or keys stored in portable devices or media) *m.* Custody of keys and of devices or media holding keys *n.* Compromise of a private key

(continued)

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
	4 The CA logs the following certificate life cycle management related events: *a.* Receipt of requests for certificate(s)—including initial certificate requests, renewal requests, and rekey requests *b.* Submissions of public keys for certification *c.* Change of affiliation of an entity *d.* Generation of certificates *e.* Distribution of the CA's public key *f.* Certificate revocation requests *g.* Certificate suspension requests (if applicable) *h.* Generation and issuance of certificate revocation lists *i.* Actions taken upon expiration of a certificate
	5 The CA logs the following cryptographic device life cycle management related events: *a.* Device receipt *b.* Entering or removing a device from storage *c.* Device usage *d.* Device deinstallation *e.* Designation of a device for service and repair *f.* Device retirement
	6 The CA logs (or requires that the RA log) the following certificate application information: *a.* Kind of identification document(s) presented by the applicant *b.* Record of unique identification data, numbers, or a combination thereof (for example, applicant's driver's license number) of identification documents, if applicable *c.* Storage location of copies of applications and identification documents *d.* Identity of entity accepting the application *e.* Method used to validate identification documents, if any *f.* Name of receiving CA or submitting RA, if applicable
	7 The CA logs the following security-sensitive events: *a.* Security-sensitive files or records read or written, including the event journal *b.* Deletion of security-sensitive data *c.* Security profile changes

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Criteria	*Illustrative Controls (Based on the CA Control Procedures Detailed in the Draft ANSI X9.79 Standard)*
	d. Use of identification and authentication mechanisms, both successful and unsuccessful (including multiple failed authentication) *e.* System crashes, hardware failures, and other anomalies *f.* Actions taken by computer operators, system administrators, and system security officers *g.* Change of affiliation of an entity *h.* Decisions to bypass encryption or authentication processes or procedures *i.* Access to the CA system or any component thereof
	8 Event journals do not record the plain text values of any private keys.
	9 CA computer system clocks are synchronized for accurate recording.
The CA maintains controls to provide reasonable assurance that the confidentiality and integrity of current and archived event journals are maintained.	10 Current and archived event journals are maintained in a form that prevents unauthorized modification or destruction.
	11 Current and archived automated event journals are protected from modification or substitution.
	12 The private key used for signing event journals is not used for any other purpose.
The CA maintains controls to provide reasonable assurance that event journals are archived completely and confidentially in accordance with disclosed business practices.	13 The CA archives event journal data on a periodic basis as disclosed in the CA's business practices (Principle 1, item 45 [paragraph .64]).
	14 A risk assessment has been performed to determine the appropriate length of time for retention of archived event journals.
	15 The CA maintains archived event journals at a secure off-site location for a predetermined period.
The CA maintains controls to provide reasonable assurance that event journals are reviewed periodically by authorized personnel.	16 Current and archived event journals may only be retrieved by authorized individuals for valid business or security reasons.
	17 Event journals are reviewed periodically as disclosed in the CA's business practices (Principle 1, item 45 [paragraph .64]).
	18 The review of current and archived event journals includes a validation of the event journals' integrity, and the identification and follow-up of exceptional, unauthorized, or suspicious activity.

.67

Appendix A

Illustrative Examples of Practitioner Reports

A1. This appendix presents three illustrative reports for WebTrust® for Certification Authorities engagements, all prepared in accordance with the American Institute of Certified Public Accountants' (AICPA's) attestation standards.

A2. Under the attestation standards, the first paragraph of the practitioner's report will state that the practitioner has performed an examination of management's assertion about disclosures of its business practices and effectiveness of its controls in conformity with the WebTrust Principles and Criteria for Certification Authorities. The practitioner may opine (1) on management's assertion or (2) directly on the subject matter. Samples of both kinds of reports are provided.

Example 1

A3. The following is an example of a practitioner report for use when all WebTrust for Certification Authorities criteria are applicable.

Report of Independent Certified Public Accountant

To the Management of ABC Certification Authority, Inc.:

We have examined the assertion by the management of ABC Certification Authority, Inc. (ABC-CA) [*hot link to management's assertion*] that in providing its certification authority (CA) services at [*location*], ABC-CA, during the period from [*Month, day, year*] through [*Month, day, year*]:

- Disclosed its key and certificate life cycle management business and information privacy practices [*hot link to CA business practices disclosure*] and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
  - — Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
  - — The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
  - — Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
  - — The continuity of key and certificate life cycle management operations was maintained; and
  - — CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria [*hot link to WebTrust for Certification Authorities criteria*].

ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of ABC-CA's key and certificate life cycle management business and information privacy practices and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

and certificate life cycle management operations, and over development, maintenance, and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business and information privacy practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, for the period [*Month, day, year*] through [*Month, day, year*], ABC-CA management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the AICPA/CICA WebTrust for Certification Authorities criteria.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

The WebTrust seal of assurance for certification authorities on ABC-CA's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust for Certification Authorities criteria, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

Example 2

A4. The following is an example of a practitioner report for use when external registration authorities are used and the certification authority (CA) does not support key escrow, certificate renewal, certificate suspension, the use of integrated circuit cards, or the provision of subscriber key management services.

Report of Independent Certified Public Accountant

To the Management of
ABC Certification Authority, Inc.:

We have examined the assertion by the management of ABC Certification Authority, Inc. (ABC-CA) [*hot link to management's assertion*] that in providing its certification authority (CA) services at [*location*], ABC-CA, during the period from _____ through _____:

- Disclosed its key and certificate life cycle management business and information privacy practices [*hot link to CA business practices disclosure*] and provided such services in accordance with its disclosed practices

- Maintained effective controls to provide reasonable assurance that:
  - — Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
  - — The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
  - — Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
  - — The continuity of key and certificate life cycle management operations was maintained; and
  - — CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria [*hot link to WebTrust for Certification Authorities criteria*].

ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

ABC-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in ABC-CA's business practice disclosures. Our examination did not extend to the controls of external registration authorities.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

The WebTrust seal of assurance for certification authorities on ABC-CA's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at external registration authorities and individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at external registration authorities and individual subscriber and relying party locations.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust for Certification Authorities criteria, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Example 3

A5. The following is an example of a direct report for use when all criteria are applicable.

Report of Independent Certified Public Accountant

To the Management of
ABC Certification Authority, Inc.:

We have examined the assertion [*hot link to management's assertion*] by the management of ABC Certification Authority, Inc. (ABC-CA) regarding the disclosure of its key and certificate life cycle management business and information privacy practices on its Web site and the effectiveness of its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over development, maintenance, and operation of systems integrity, based on the AICPA/CICA WebTrust for Certification Authorities criteria [*hot link to WebTrust for Certification Authorities criteria*], during the period [*Month, day, year*] through [*Month, day, year*].

These disclosures and controls are the responsibility of ABC-CA's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of ABC-CA's key and certificate life cycle management business and information privacy practices and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over development, maintenance, and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business and information privacy practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, during the period from [*Month, day, year*] through [*Month, day, year*], ABC-CA, in all material respects:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that subscriber information was properly authenticated (for the registration activities performed by ABC-CA) and the integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure; the continuity of key and certificate life cycle management operations was maintained; and CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria [*hot link to WebTrust for Certification Authorities criteria*].

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required

because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

The WebTrust seal of assurance for Certification Authorities on ABC-CA's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust for Certification Authorities criteria, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.68

Appendix B

Illustrative Examples of Management's Assertion

Example 1

B1. The following is an example of management's assertion for use when all criteria are applicable.

Assertion of Management as to its Disclosure of its Business Practices and its Controls Over its Certification Authority Operations during the period from [*Month, day, year*] through [*Month, day, year*]

[*Date*]

ABC Certification Authority, Inc. operates as a certification authority (CA) known as ABC-CA. ABC-CA, as a root CA [*or as a subordinate CA of DEF Certification Authority, Inc.*], provides the following CA services:

- Subscriber key management services
- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution (using an online repository)
- Certificate revocation
- Certificate suspension
- Certificate status information processing (using an online repository)
- Integrated circuit card life cycle management

Management of ABC-CA is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure [*hot link to CA business practices disclosure*], service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to ABC-CA's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its CA operations. Based on that assessment, in ABC Certification Authority, Inc. (ABC-CA) management's opinion, in providing its CA services at [*location*], ABC-CA, during the period from [*Month, day, year*] through [*Month, day, year*]:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
  - — Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
  - — The integrity of keys and certificates it managed was established and protected throughout their life cycles

- Maintained effective controls to provide reasonable assurance that:

  — Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;

  — The continuity of key and certificate life cycle management operations was maintained; and

  — CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria [*hot link to WebTrust for Certification Authorities criteria*], including the following:

CA Business Practices Disclosure

Service Integrity

Key Life Cycle Management Controls

CA Key Generation
CA Key Storage, Backup, and Recovery
CA Public Key Distribution
CA Key Escrow
CA Key Usage
CA Key Destruction
CA Key Archival
CA Cryptographic Hardware Life Cycle Management
CA-Provided Subscriber Key Management Services

Certificate Life Cycle Management Controls

Subscriber Registration
Certificate Renewal
Certificate Rekey
Certificate Issuance
Certificate Distribution
Certificate Revocation
Certificate Suspension
Certificate Status Information Processing
Integrated Circuit Card Life Cycle Management

CA Environmental Controls

Certification Practice Statement and Certificate Policy Management
Security Management
Asset Classification and Management
Personnel Security
Physical and Environmental Security
Operations Management
System Access Management
Systems Development and Maintenance
Business Continuity Management
Monitoring and Compliance
Event Journaling

[*Name*]
[*Title*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Example 2

B2. The following is an example of management's assertion for use when external registration authorities are used and the certification authority (CA) does not support key escrow, certificate renewal, certificate suspension, the use of integrated circuit cards, or the provision of subscriber key management services.

Assertion of Management as to its Disclosure of its Business Practices and its Controls Over its Certification Authority Operations during the period from [*Month, day, year*] through [*Month, day, year*]

[*Date*]

ABC Certification Authority, Inc. operates as a certification authority (CA) known as ABC-CA. ABC-CA, as a root CA [*or as a subordinate CA of DEF Certification Authority, Inc.*], provides the following CA services:

- Certificate rekey
- Certificate issuance
- Certificate distribution (using an online repository)
- Certificate revocation
- Certificate status information processing (using an online repository)

ABC-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in ABC-CA's business practice disclosures.

Management of ABC-CA is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure [*hot link to CA business practices disclosure*], service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective internal controls can provide only reasonable assurance with respect to ABC-CA's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its CA operations. Based on that assessment, in ABC Certification Authority, Inc. (ABC-CA) management's opinion, in providing its CA services at [*location*], ABC-CA, during the period from [*Month, day, year*] through [*Month, day, year*]:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
  - — Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
  - — The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
  - — Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
  - — The continuity of key and certificate life cycle management operations was maintained; and

— CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria [*hot link to WebTrust for Certification Authorities criteria*], including the following:

CA Business Practices Disclosure

Service Integrity

Key Life Cycle Management Controls

CA Key Generation
CA Key Storage, Backup, and Recovery
CA Public Key Distribution
CA Key Usage
CA Key Destruction
CA Key Archival
CA Cryptographic Hardware Life Cycle Management

Certificate Life Cycle Management Controls

Subscriber Registration
Certificate Rekey
Certificate Issuance
Certificate Distribution
Certificate Revocation
Certificate Status Information Processing

CA Environmental Controls

Certification Practice Statement and Certificate Policy Management
Security Management
Asset Classification and Management
Personnel Security
Physical and Environmental Security
Operations Management
System Access Management
Systems Development and Maintenance
Business Continuity Management
Monitoring and Compliance
Event Journaling

[*Name*]
[*Title*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.69

Appendix C

Illustrative Examples of Management's Representation

Example 1

C1. The following is an example of a management representation for use when all criteria are applicable.

[*Date*]

[*Name of CPA firm*]
[*Address*]

Dear Members of the Firm:

Management confirms its understanding that your examination of our assertion related to ABC Certification Authority, Inc.'s (ABC-CA) business practices disclosure and controls over its certification authority (CA) operations during the period from [*Month, day, year*] through [*Month, day, year*] was made for the purpose of expressing an opinion as to whether our assertion is fairly presented, in all material respects, and that your opinion is based on criteria for effective controls as stated in our assertion document. We are responsible for our assertion. In connection with your examination, management:

a. Acknowledges its responsibility for establishing and maintaining effective controls over its CA operations at [*location*], including CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls.

b. Has performed an assessment and believes that ABC-CA's CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls met the minimum requirement of the criteria described in our assertion document during the period from [*Month, day, year*] through [*Month, day, year*].

c. Believes the stated criteria against which our assertion has been assessed are reasonable and appropriate.

d. Has disclosed to you that there are no significant deficiencies in the design or operation of the controls which could adversely affect the Company's ability to comply with the control criteria related to ABC-CA's CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls, consistent with the assertions of management.

e. Has made available to you all significant information and records related to our assertion.

f. Has responded fully to all inquiries made to us by you during your examination.

g. Has disclosed to you any changes occurring or planned to occur subsequent to _____, in controls or other factors that might significantly affect the controls, including any corrective actions taken by management with regard to significant deficiencies.

In management's opinion, ABC-CA, in providing its CA services at [*location*] during the period from [*Month, day, year*] through [*Month, day, year*]:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices

- Maintained effective controls to provide reasonable assurance that:
  - — Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
  - — The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
  - — Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
  - — The continuity of key and certificate life cycle management operations was maintained; and
  - — CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria, including the following:

CA Business Practices Disclosure

Service Integrity

Key Life Cycle Management Controls

CA Key Generation
CA Key Storage, Backup, and Recovery
CA Public Key Distribution
CA Key Escrow
CA Key Usage
CA Key Destruction
CA Key Archival
CA Cryptographic Hardware Life Cycle Management
CA-Provided Subscriber Key Management Services

Certificate Life Cycle Management Controls

Subscriber Registration
Certificate Renewal
Certificate Rekey
Certificate Issuance
Certificate Distribution
Certificate Revocation
Certificate Suspension
Certificate Status Information Processing
Integrated Circuit Card Life Cycle Management

CA Environmental Controls

Certification Practice Statement and Certificate Policy Management
Security Management
Asset Classification and Management
Personnel Security
Physical and Environmental Security
Operations Management
System Access Management
Systems Development and Maintenance
Business Continuity Management
Monitoring and Compliance
Event Journaling

Very truly yours,

[*Name*]
[*Title*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Example 2

C2. The following is an example of a management representation for use when external registration authorities are used and the certification authority (CA) does not support key escrow, certificate renewal, certificate suspension, the use of integrated circuit cards, or the provision of subscriber key management services.

[*Date*]

[*Name of CPA*]
[*Address*]

Dear Members of the Firm:

Management confirms its understanding that your examination of our assertion related to ABC Certification Authority, Inc.'s (ABC-CA) business practices disclosure and controls over its certification authority (CA) operations during the period from [*Month, day, year*] through [*Month, day, year*] was made for the purpose of expressing an opinion as to whether our assertion is fairly presented, in all material respects, and that your opinion is based on criteria for effective controls as stated in our assertion document. ABC-CA makes use of external registration authorities for specific subscriber registration activities, as disclosed in ABC-CA's business practice disclosures. We are responsible for our assertion. In connection with your examination, management:

a. Acknowledges its responsibility for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls.

b. Has performed an assessment and believes that ABC-CA's CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls, met the minimum requirement of the criteria described in our assertion document during the period from [*Month, day, year*] through [*Month, day, year*].

c. Believes the stated criteria against which our assertion has been assessed are reasonable and appropriate.

d. Has disclosed to you that there are no significant deficiencies in the design or operation of the controls which could adversely affect the Company's ability to comply with the control criteria related to ABC-CA's CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls, consistent with the assertions of management.

e. Has made available to you all significant information and records related to our assertion.

f. Has responded fully to all inquiries made to us by you during your examination.

g. Has disclosed to you any changes occurring or planned to occur subsequent to [*Month, day, year*], in controls or other factors that might significantly affect the controls, including any corrective actions taken by management with regard to significant deficiencies.

In management's opinion, ABC-CA, in providing its CA services at [*location*], ABC-CA, during the period from [*Month, day, year*] through [*Month, day, year*]:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices

- Maintained effective controls to provide reasonable assurance that:
  - — Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
  - — The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
  - — Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
  - — The continuity of key and certificate life cycle management operations was maintained; and
  - — CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria, including the following:

CA Business Practices Disclosure

Service Integrity

Key Life Cycle Management Controls

CA Key Generation
CA Key Storage, Backup, and Recovery
CA Public Key Distribution
CA Key Usage
CA Key Destruction
CA Key Archival
CA Cryptographic Hardware Life Cycle Management

Certificate Life Cycle Management Controls

Subscriber Registration
Certificate Rekey
Certificate Issuance
Certificate Distribution
Certificate Revocation
Certificate Status Information Processing

CA Environmental Controls

Certification Practice Statement and Certificate Policy Management
Security Management
Asset Classification and Management
Personnel Security
Physical and Environmental Security
Operations Management
System Access Management
Systems Development and Maintenance
Business Continuity Management
Monitoring and Compliance
Event Journaling

Very truly yours,

[*Name*]
[*Title*]

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.70

Appendix D

Comparison of WebTrust for Certification Authorities Criteria and ANSI X9.79

Draft*

WebTrust for Certification Authorities Criteria		ANSI X9.79 *(Draft) PKI Practices and Policy Framework Standard's Certification Authority Control Objectives* (CACO)	
§1	**CA Business Practices Disclosure**	**§7, §A, & §B**	**General Requirements—CP and Certification Practice Statements; PKI Practices and Policy Elements; and Certification Authority Control Objectives**
§2	**Service Integrity**	**§B.2 & B.3**	**Key and Certificate Life Cycle Management Controls**
§2.1	**Key Life Cycle Management Controls**	**§B.2**	**Key Life Cycle Management Controls**
§2.1.1	CA Key Generation	§B.2.1	CA Key Generation
§2.1.2	CA Key Storage, Backup, and Recovery	§B.2.2	CA Key Storage, Backup and Recovery
§2.1.3	CA Public Key Distribution	§B.2.3	CA Public Key Distribution
§2.1.4	CA Key Escrow	§B.2.4	CA Key Escrow
§2.1.5	CA Key Usage	§B.2.5	CA Key Usage
§2.1.6	CA Key Destruction	§B.2.6	CA Key Destruction
§2.1.7	CA Key Archival	§B.2.7	CA Key Archival
§2.1.8	CA Cryptographic Hardware Life Cycle Management	§B.2.8	CA Cryptographic Hardware Life Cycle Management
§2.1.9	CA-Provided Subscriber Key Management Services	§B.2.9	CA-Provided Subscriber Key Management Services
§2.2	**Certificate Life Cycle Management Controls**	**§B.3**	**Certificate Life Cycle Management Controls**
§2.2.1	Subscriber Registration	§B.3.1	Subscriber Registration
§2.2.2	Certificate Renewal	§B.3.2	Certificate Renewal
§2.2.3	Certificate Rekey	§B.3.3	Certificate Rekey
§2.2.4	Certificate Issuance	§B.3.4	Certificate Issuance
§2.2.5	Certificate Distribution	§B.3.5	Certificate Distribution
§2.2.6	Certificate Revocation	§B.3.6	Certificate Revocation

(continued)

* The American National Standards Institute (ANSI) X9F5 Digital signature and Certificate Policy working group is developing the X9.79 PKI Practices and Policy Framework (X9.79) standard for the financial services community. This standard includes detailed Certification Authority Control Objectives against which certification authorities may be evaluated. An International Organization for Standardization (ISO) working group has been formed to standardize X9.79 based on international requirements in a new international standard.

WebTrust for Certification Authorities Criteria		ANSI X9.79 *(Draft) PKI Practices and Policy Framework Standard's Certification Authority Control Objectives* (CACO)	
§2.2.7	Certificate Suspension	§B.3.7	Certificate Suspension
§2.2.8	Certificate Status Information Processing	§B.3.8	Certificate Status Information Processing
§2.2.9	Integrated Circuit Card (ICC) Life Cycle Management	§B.3.9	Integrated Circuit Card (ICC) Life Cycle Management
§3	**CA Environmental Controls**	**§B.1**	**CA Environmental Controls**
§3.1	Certification Practice Statement and Certificate Policy Management	§B.1.1	Certification Practice Statement and Certificate Policy Management
§3.2	Security Management	§B.1.2	Security Management
§3.3	Asset Classification and Management	§B.1.3	Asset Classification and Management
§3.4	Personnel Security	§B.1.4	Personnel Security
§3.5	Physical and Environmental Security	§B.1.5	Physical and Environmental Security
§3.6	Operations Management	§B.1.6	Operations Management
§3.7	System Access Management	§B.1.7	System Access Management
§3.8	Systems Development and Maintenance	§B.1.8	Systems Development and Maintenance
§3.9	Business Continuity Management	§B.1.9	Business Continuity Management
§3.10	Monitoring and Compliance	§B.1.10	Monitoring and Compliance
§3.11	Event Journaling	§B.1.11	Event Journaling

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

.71

Appendix E

Comparison of CICA Section 5900, AICPA SAS No. 70, and AICPA/CICA WebTrust for Certification Authorities Reviews and Reports Covering the Business Activities of Certification Authority Organizations

This document analyzes the form and content of reviews and reports performed under the indicated regulations indicating appropriate similarities and differences. For third-party reporting with respect to certification authorities (CAs), the most appropriate and relevant approach is to use the AICPA/CICA Certification Authority Trust approach wherever possible since it has been developed specifically around the reportable business activities of an organization acting as a CA.

[See table on following page.]

Content/Approach	*CICA Standards for Assurance Engagements, Section 5900 "Opinions, on Control Procedures at a Service Organization"*	*Statement on Auditing Standards No. 70,* **Service Organizations** *(AICPA,* **Professional Standards,** *vol. 1, AU sec. 324), as amended*	*AICPA/CICA WebTrust for Certification Authorities*
Purpose	— Auditor to auditor communication for obtaining reliance for audit purposes	— Auditor to auditor communication for obtaining reliance for audit purposes	— Auditor communication to interested parties including business partners and existing and potential customers
	— Covers specified applications, functions, and processing environments	— Covers specified applications, functions, and processing environments	— Mandatory coverage as noted below
	— Practical usage now results in business activity coverage	— Practical usage now results in business activity coverage	— New criteria and illustrations for reporting activities of certification authorities
Target of Evaluation	Defined by each engagement	Defined by each engagement	Certification authority business activities pre-defined in principles and criteria
Type of Engagement	— Report on design and existence of control procedures	— Report on controls placed in operation	
	— Report on design, effective operation, and continuity of control procedures	— Report on controls placed in operation and tests of operating effectiveness	— Report on compliance with WebTrust for Certification Authorities Principles and Criteria
Examination Standards	Generally accepted auditing standards	Generally accepted auditing standards	— Statements on Standards for Attestation Engagements (U.S.)
			— Standards for Assurance Engagements (Canada)

Copyright © 2003, American Institute of Certified Public Accountants, Inc.

Content/Approach	*CICA Standards for Assurance Engagements, Section 5900 "Opinions, on Control Procedures at a Service Organization"*	*Statement on Auditing Standards No. 70,* Service Organizations *(AICPA,* Professional Standards, *vol. 1, AU sec. 324), as amended*	*AICPA/CICA WebTrust for Certification Authorities*
Coverage of Activities	— No mandatory coverage — Coverage must be formulated for each engagement and defined in report scope.	— No mandatory coverage — Coverage must be formulated for each engagement and defined in report scope.	Areas of coverage defined by principles and criteria, including: — CA business practice disclosure (including the privacy of subscriber and relying party information) — Service integrity — Key life cycle management controls — Certificate life cycle management controls — CA environmental controls
Linkage to Authoritative Standards	Any linkage would need to be established as part of a specific review. Adequacy of control objectives and procedures subjectively determined by auditor based on the engagement.	Any linkage would need to be established as part of a specific review. Adequacy of control objectives and procedures subjectively determined by auditor based on engagement.	Principles and criteria linked to ANSI X9.79 standard which is intended to be submitted to the International Organization for Standardization (ISO) for international standardization. AICPA/CICA provides uniform rules which are linked to industry accepted standards.
Period of Coverage of Review	Acceptable alternatives: — Point in time (for design and existence) — Period of time (determined by client)	Acceptable alternatives: — Point in time (controls placed in operation) — Period of time (determined by client)	Continuous coverage from the point of qualification. Qualification after compliance can be tested over a minimum 90-day period, followed by updates within a specified period (currently under debate whether this would be six months, annual, or some other).

.72

Appendix F

Practitioner Policies and Guidance for Webtrust for Certification Authority Engagements

This appendix includes practitioner policies which set forth practices that practitioners must follow when conducting a WebTrust engagement. These policies are in *italic* typeface. This section also includes additional practitioner guidance on implementing these policies. This guidance is in normal typeface.

Client/Engagement Acceptance

The practitioner should not accept an engagement where the awarding of a WebTrust seal would be misleading.

The WebTrust seal implies that the entity is a reputable site that has reasonable disclosures and controls in a broad range of areas. Accordingly, the practitioner would avoid accepting a WebTrust engagement when the entity's disclosures outside the scope of the engagement are known by the practitioner to be misleading, when there are known major problems with controls not directly affecting the scope of the engagement, or when the entity is a known violator of laws or regulations.

Procedures to provide WebTrust services resulting in the awarding of a WebTrust seal should be performed at a high level of assurance (i.e., audit or examination level).

Although a practitioner can provide a variety of services related to WebTrust, such as a preliminary review of a certification authority (CA) to identify potential areas of nonconformity with the WebTrust for Certification Authorities criteria, any engagement leading to a WebTrust Seal would need to include procedures to provide a high level of assurance (that is, audit or examination level) as a basis for an unqualified opinion.

Initial Period of Coverage

The period of coverage for an initial WebTrust for Certification Authorities engagement should be at least two months or more as determined by the practitioner.

In determining the initial period of coverage, the practitioner would consider what length of period would be required to obtain sufficient competent evidential matter as a basis for his or her opinion. For example, for established CAs and CA functions, two months may be quite sufficient, while for new CAs and CA functions, the practitioner may believe that a longer initial period would be more appropriate.

Frequency of Updates

The interval between updates for the WebTrust for Certification Authorities seal should not exceed 12 months and this interval often may be considerably shorter.

In determining the interval between updates, the practitioner would consider:

- The nature and complexity of the CA's operations.
- The frequency of significant changes to the CA's operations.

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

- The relative effectiveness of the entity's monitoring and change management controls for ensuring continued conformity with the applicable WebTrust for Certification Authorities criteria as such changes are made.
- The practitioner's professional judgment.

For example, in the situation of a start-up CA or CA function, it may be more appropriate that the initial examination period be established at 3 months, with the next review being performed 6 months after the WebTrust seal for Certification Authorities is awarded, thereafter moving to a 12-month review cycle. In order to provide continuous coverage and retain the seal, the period covered for update reports should either begin with the end of the prior period or the start of the period in the initial report.

If the entity notifies the practitioner of a significant change potentially affecting conformance with the applicable WebTrust for Certification Authorities criteria included in the scope of the engagement during the period between updates, the practitioner should determine whether:

a. *An update examination would need to be performed,*
b. *The seal would need to be removed until an update examination is completed and an updated auditor's report is issued, or*
c. *No action is required at that time because of the nature of the change and/or the effectiveness of the entity's monitoring and change management controls.*

Management Assertions

Management should provide an appropriate written assertion on its Web site.

Management's assertion would ordinarily identify the specific CA covered, the period covered (which ordinarily would be the same as that covered by the practitioner's report), and include a statement along the following lines, for example for the CA model:

> Management has assessed the controls over its CA operations. Based on that assessment, in ABC Certification Authority, Inc. (ABC-CA) management's opinion, in providing its certification authority (CA) services at [*location*], ABC-CA, during the period from [*Month, day, year*] through [*Month, day, year*]:
>
> - Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
> - Maintained effective controls to provide reasonable assurance that:
> - — Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
> - — The integrity of keys and certificates it managed was established and protected throughout their life cycles
> - Maintained effective controls to provide reasonable assurance that:
> - — Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;

- The continuity of key and certificate life cycle management operations was maintained; and
- CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria.

Example management assertions are provided in Appendix B [paragraph .68].

Changes in Client Policies and Disclosures

Changes in an entity's disclosed policies need to be disclosed on its Web site. If the client appropriately discloses such changes, no mention of such change needs to be made in the practitioner's report.

Sufficient Criteria for Unqualified Opinion

In order to obtain an unqualified opinion, the entity should meet, in all material respects, all of the applicable WebTrust for Certification Authorities Criteria included in the scope of the engagement during the period covered by the report and each update period.

Subsequent Events

The practitioner should consider the effect of subsequent events up to the date of the practitioner's report. When the practitioner becomes aware of events that materially affect the subject matter, and the practitioner's conclusion, the practitioner should consider whether the disclosed practices reflect those events properly or whether those events are addressed properly in the practitioner's report.

Representation Letter

Prior to conclusion of the engagement and before the practitioner issues a report, the client will be required to provide to the practitioner a representation letter.

Example representation letters are provided in Appendix C [paragraph .69].

 Copyright © 2003, American Institute of Certified Public Accountants, Inc.

AICPA
Assurance Services Executive Committee

ROBERT L. BUNTING, *Chair*
GARI FAILS
TED HORNE
EVERETT C. JOHNSON, JR.
JOHN LAINHART
GEORGE LEWIS
EDWARD F. ROCKMAN
SUSAN C. RUCKER
J. W. MIKE STARR
WENDY E. VISCONTY
DARWIN VOLTIN
NEAL WEST

AICPA Staff

ALAN ANDERSON
Senior Vice President, Technical Services
ANTHONY J. PUGLIESE
Director, Assurance Services

CICA
Assurance Services Development Board

JOHN W. BEECH, *Chair*
DOUGLAS C. ISAAC
MARILYN KUNTZ
DOUG MCPHIE
STEPHEN E. SALTERIO
DAVID W. STEPHEN
DOUG TIMMINS
KEITH S. VANCE

CICA Staff

CAIRINE M. WILSON
Vice President, Innovation
GREGORY P. SHIELDS
Director, Assurance Services Development

AICPA/CICA
Electronic Commerce Assurance Services Task Force

EVERETT C. JOHNSON, JR., *Chair*
BRUCE R. BARRICK
JERRY R. DEVAULT
JOSEPH G. GRIFFIN
CHRISTOPHER J. LEACH, *Vice Chair*
PATRICK J. MORIARTY
WILLIAM POWERS
KERRY L. SHAKELFORD
DONALD E. SHEEHY
CHRISTIAN R. STORMER
ALFRED F. VAN RANST, JR.

Staff Contacts

BRYAN WALKER, CICA
Principal, Assurance Services Development
KARYN WALLER, AICPA
Senior Technical Manager, Trust Services
(replaced Sheryl Martin in 2001)
SHERYL MARTIN, AICPA
WebTrust Team Leader

For issues related to this release, please e-mail assure@aicpa.org.

AICPA RESOURCE: Accounting & Auditing Literature

AICPA's unique online research tool combines the power and speed of the Web with comprehensive accounting and auditing standards. *AICPA RESOURCE* includes AICPA's and FASB's literature libraries—and includes:

- AICPA Professional Standards
- AICPA Technical Practice Aids
- AICPA's Accounting Trends & Techniques
- AICPA Audit and Accounting Guides
- AICPA Audit Risk Alerts
- FASB Original Pronouncements
- FASB Current Text
- EITF Abstracts
- FASB Implementation Guides
- FASB's Comprehensive Topical Index

Search for pertinent information from both databases by keyword and get the results ranked by relevancy. Print out important *AICPA RESOURCE* segments and integrate the literature into your engagements and financial statements. Available from anywhere you have Internet access, this comprehensive reference library is packed with the A & A guidance you need—and use—the most. Both libraries are updated with the latest standards and conforming changes.

AICPA+FASB reference libraries, one-year individual online subscription
No. ORF-XX
AICPA Member $890.00
Nonmember $1,112.50

AICPA reference library, one-year individual online subscription
No. ORS-XX
AICPA Member $395.00
Nonmember $493.75

AICPA RESOURCE also offers over 50 additional subscription options—log onto www.cpa2biz.com/AICPAresource for details.

For more information or to order, log onto
www.cpa2biz.com/AICPAresource,
or call 888-777-7077

Table of Contents

How to Use Volume 2

AUD Statements of Position—Auditing and Attestation

PA Practice Alerts

STS Suitable Trust Services Criteria and Illustrations

ISO Certified 005145