2001

AICPA/CICA SysTrust : principles and criteria for systems reliability : version 2.0 January 2001

American Institute of Certified Public Accountants (AICPA)

Canadian Institute of Chartered Accountants

AICPA/CICA SysTrust™

Principles and Criteria for Systems Reliability

Version 2.0

January 2001

AICPA

Chartered
Accountants
of Canada

SYSTRUST LICENSE AGREEMENT

By using the SysTrust Principles and Criteria annexed hereto to provide SysTrust Services, you ("Practitioner") agree to be bound by the terms and conditions of this license. IF YOU DO NOT AGREE TO BE BOUND BY THESE TERMS AND CONDITIONS, YOU MAY RETURN THE SYSTRUST PRINCIPLES AND CRITERIA TO THE AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS ("AICPA"), AT 1211 AVENUE OF THE AMERICAS, NEW YORK, NY 10036, FOR A FULL REFUND.

1. Definitions:

"**Agreed-Upon Procedure Level**": an engagement under the Attestation Standards in which a practitioner performs procedures, agreed-upon by the practitioner and users, and issues a report on the practitioner's finding. The users assume responsibility for the sufficiency of the procedures. No opinion or assurance is provided.

"**Attestation Standards**": AICPA's *Statements on Standards for Attestation Engagements* and applicable standards referred to therein, as revised by AICPA from time to time.

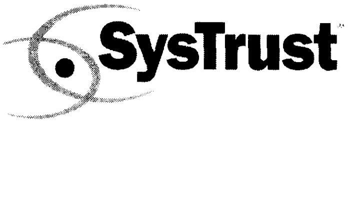
"**CICA**": Canadian Institute of Chartered Accountants.

"**Examination Level**": the highest level of assurance that can be provided under the Attestation Standards (*i.e.*, procedures sufficient to assure low level attestation risk and result in a positive opinion).

"**Report**": Practitioner's report, based on an engagement performed under the Attestation Standards at either the Examination Level or Agreed-Upon Procedure Level, attesting that client's assertion that a defined system meets one or more of the SysTrust Principles and Criteria is fairly stated, and stating the SysTrust Principles and Criteria were issued by AICPA/CICA.

"**System of Quality Control**": the policies, standards and procedures established by Practitioner to ensure it complies with the Attestation Standards and this Agreement, and its own policies and procedures, including an independent inspection of Practitioner's SysTrust Services, its related quality assurance process and its annual license renewal representations pursuant to the AICPA Professional Standards, sections on *Statements on Quality Control Standards, Bylaws, Code of Professional Conduct and Ethics Rulings and Statement on Standards for Consulting Services*, as revised by AICPA from time to time.

"**SysTrust Marks**": SYSTRUST and the CPA SYSTRUST logo:



"**SysTrust Principles and Criteria**": the *AICPA/CICA SysTrust^{TM} Principles and Criteria for Systems Reliability*, as revised from time-to-time. Information on how to obtain the current version can be found at <http://www.aicpa.org> or through the AICPA's Assurance Services Team at (212) 596-6200.

"**SysTrust Program**": AICPA's promulgation of SysTrust Principles and Criteria and licensing of the SysTrust Marks and Practitioner's provision of SysTrust Services and submission to the System of Quality Control.

"**SysTrust Services**": Practitioner's examination of clients' systems and issuing of Reports based on the SysTrust Principles and Criteria and/or consulting services related to the SysTrust Principles and Criteria.

2. Grant and Qualifications: Subject to the terms of this Agreement, AICPA grants Practitioner a non-exclusive license to use the SysTrust Marks in the United States in connection with providing SysTrust Services or to sublicense Practitioner's clients to use SysTrust Marks: (i) as icons on the client's web site linking to the Practitioner's report; and (ii) in advertising to indicate the client's systems have been examined under the SysTrust Program. Practitioner agrees, during the term of this Agreement, to maintain membership in good-standing in AICPA and to enroll in an AICPA approved practice-monitoring program.

3. Quality Control:

Standards: Practitioner shall provide SysTrust Services only as an Examination Level or Agreed-Upon-Procedure Level service under appropriate Attestation Standards, using as measurement criteria the current version of the SysTrust Principles and Criteria.

Advertising: Practitioner shall have the right, in the United States, for the sole purpose of advertising, promoting or marketing the SysTrust Services, to use and to sublicense its clients to use the SysTrust Marks in high-quality promotional and advertising materials in a manner prescribed by AICPA Professional Standards, section on *Code of Professional Conduct*, provided neither Practitioner nor its sublicensee uses the SysTrust Marks in any manner that, in AICPA's opinion, may harm, dilute or reflect adversely on AICPA or the SysTrust Marks. Practitioner shall submit to AICPA's Assurance Services Team representative samples of all new advertising and promotional materials using the SysTrust Marks for approval prior to publication or distribution, which AICPA may withhold in its sole discretion. Materials submitted shall be deemed approved if AICPA does not disapprove such materials within seven (7) business days after receipt.

System of Quality Control. Practitioner shall provide SysTrust Services under a System of

(*continued on inside back cover*)

SysTrust℠

AICPA/CICA SysTrust™

Principles and Criteria for Systems Reliability

Version 2.0

January 2001

AICPA

CA Chartered Accountants of Canada

NOTICE TO READERS

AICPA/CICA SysTrust™ Principles and Criteria for Systems Reliability is an authoritative issuance of both the Assurance Services Executive Committee in the United States and the Assurance Services Development Board in Canada, which are senior technical committees authorized to speak for the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants in matters of assurance. By purchasing this publication, members are expected to comply with the principles and criteria herein and with the terms of the licensing agreement on the inside covers.

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

SUMMARY

This is version 2.0 of the SysTrust™ Principles and Criteria for Systems Reliability, which provide the basis for the SysTrust assurance service developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). The focus of the SysTrust service is to increase the confidence of management, customers, and business partners in systems that support a business or a particular activity. The principal differences between version 1.0 (November 1999) and version 2.0 of this document include, but are not limited to, the following:

1. **Revision to the reporting guidance to permit reports on any one of the four SysTrust principles of availability, security, integrity or maintainability.** In version 1.0, a practitioner could not accept a SysTrust engagement to report on less than all four principles and related criteria. In version 2.0, an engagement can be undertaken to report on any one or more of the four principles.

2. **Clarification of the extent to which the security principle covers the issue of privacy.** Privacy concerns related to restricting access to and use of confidential information are addressed by the SysTrust security principle. Version 2.0 clarifies that a practitioner performing a SysTrust engagement need only examine issues related to privacy to the extent that the entity discloses its privacy policy in the system description or is affected by privacy-related laws and regulations.

3. **Provision for engagements for systems in the preimplementation phase.** Version 2.0 provides guidance for engagements to test the suitability of the design of controls for systems that have not been placed into operation. The related report for these engagements would be for a point in time rather than for a period of time.

4. **Expansion of the guidance to address agreed-upon procedures and consulting engagements.** Version 2.0 includes agreed-upon procedures and consulting engagements in the range of services encompassed by SysTrust.

5. **Additional examples of practitioners' reports and modifications to other reports to improve their readability.** Added examples of practitioners' reports include—

   - Reporting on an assertion about the effectiveness of controls related to one of the principles (examples 4 and 10).
   - Reporting on an assertion about the suitability of the design of controls for systems in the preimplementation phase (examples 5 and 11).
   - Reporting on an agreed-upon procedures/specified auditing procedures engagement (examples 6 and 12).

The task force has endeavored to ensure that the principles and criteria reflect current professional standards, technical and operational practices, and market needs. However, future revisions may be needed to update these criteria and related materials. This document is effective upon issuance. Early implementation was permitted based on the guidance in the exposure draft of the *AICPA/CICA SysTrust Principles and Criteria* Version 2.0 dated July 2000.

TABLE OF CONTENTS

Committee and Task Force Members

AICPA Assurance Services Executive Committee

Robert L. Bunting, *Chair*
Diana Chant
Gari Fails
Everett C. Johnson, Jr.
John W. Lainhart
George Lewis
Edward F. Rockman
Susan C. Rucker
J. W. Mike Starr
Wendy E. Visconty
Darwin Voltin

AICPA Staff
Alan W. 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 P. McPhie
Steven E. Salterio
David W. Stephen
Keith S. Vance

CICA Staff
Greg Shields
Director, Assurance Services Development

AICPA/CICA Systems Reliability Task Force

Doug P. McPhie, *Chair*
J. Efrim Boritz
M. Marcel Labelle
John W. Lainhart
Robert J. Reimer
George H. Tucker
Fred Umbach
Miklos A. Vasarhelyi
Thomas E. Wallace
Sander Wechsler
Dan White

CICA Staff
Bryan Walker
Principal, Assurance Services Development

AICPA Staff
Erin P. Mackler
Technical Manager
Assurance Services
Judith M. Sherinsky
Technical Manager
Audit and Attest Standards

Introduction

Developments in information technology (IT) are making far greater power available to entities at far lower costs. The systems supported by this technology are not just doing bookkeeping—they are running businesses, producing products and services, and communicating with customers and business partners. As a result, IT permeates all areas of organizations, differentiates them in the marketplace, and consumes increasing amounts of human and financial capital. As business dependence on IT increases, tolerance decreases for systems that are unsecured, unavailable when needed, and unable to produce accurate information on a consistent basis. Like the weak link in a chain, an unreliable system can cause a succession of events that negatively affect a company and its customers, suppliers, and business partners.

Consequently, the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) have introduced a professional service to provide assurance on the reliability of systems. The development of this service is part of a broader future vision to supply real-time assurance on informational databases and systems. System reliability is a fundamental building block in the profession's goal to provide continuous assurance, as discussed in the AICPA/CICA research report "Continuous Auditing."

The SysTrust^{SM} service[1] is an assurance service developed by the Assurance Services Executive Committee (ASEC) of the AICPA and the Assurance Services Development Board (ASDB) of the CICA to be provided by a certified public accountant or a chartered accountant (hereinafter, referred to as a practitioner). It is designed to increase the comfort of management, customers, and business partners with the systems that support a business or a particular activity.

[1] The SysTrust service has been trademarked and servicemarked in the United States by the AICPA and trademarked in Canada by the CICA. The terms and conditions of the SysTrust licensing agreement are included in this document.

The SysTrust service entails a practitioner providing an assurance service in which he or she tests and evaluates whether a system is reliable when measured against four essential principles: availability, security, integrity, and maintainability. Page 16 of this document presents guidance on performing various types of SysTrust engagements, for example, engagements that address only selected SysTrust principles.

Potential users of this service are shareholders, creditors, bankers, business partners, users who outsource functions to other entities, stakeholders, and anyone who in some way relies on the continued availability, security, integrity, and maintainability of a system. The SysTrust service will help differentiate entities from their competitors because entities that undergo the rigors of a SysTrust engagement will be better service providers—attuned to the risks posed by their environment, equipped with the controls that address those risks, and able to provide assurance to users regarding those controls.

This document explains the SysTrust service; the SysTrust principles, criteria, and illustrative controls; and the various reports a practitioner may issue.

What Is a System?

A system consists of five key components organized to achieve a specified objective. Business systems typically are organized to transform data inputs into information outputs using the following five components:

1. *Infrastructure*—The physical and hardware components of a system, including facilities, mainframes, servers, networks, and related components
2. *Software*—The programs and operating software of a system, including operating systems, utilities, business applications software such as Enterprise Resource Planning (ERP), and financial systems
3. *People*—The personnel involved in the operation and use of a system, including IT personnel such as programmers and operators, users of the system, and management

4. *Procedures*—The programmed and manual procedures involved in the operation of a system, including IT procedures such as back-up and maintenance, and user-based procedures such as data entry

5. *Data*—The information used and supported by a system, including transaction streams, files, databases, and tables

A system may be as simple as one consisting of a personal-computer-based payroll application with a single user, or as complex as one consisting of a multiapplication, multicomputer banking system accessed by a virtually unlimited number of users within and outside an entity, such as the system described in appendix B of this document.

In a SysTrust engagement, management prepares a description of the aspects of the system covered by the engagement so that the boundaries of the system are clear to report users. The system description is attached to the practitioner's report. Although the practitioner performs procedures to determine whether the system description describes the boundaries of the system covered by the engagement, the practitioner does not examine the description or express an opinion on it. A clear definition of the system's boundaries is important because some systems receive and process data from sources outside the defined system, whereas other systems include only data from sources within the defined system. For example, a payroll processing system may receive information inputs in a ready-to-process state from an employer outside the boundaries of a system, limiting the scope of the system to processing inputs provided by the employer to produce checks or direct bank deposits to specified bank accounts. However, another system, such as an automated teller system, may include the data sources within the boundaries of the system, encompassing the data inputs provided by automatic teller machine (ATM) users and all related processing, validation, database updating, and reporting functions.

If laws and regulations affect system requirements (for example, laws regarding privacy), it may be useful for management to identify such laws and regulations in its system description.

Principles, Criteria, and Illustrative Controls for a Reliable System

Principles of a Reliable System

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 following four principles are used to evaluate whether a system is reliable:

1. *Availability. The system is available for operation and use at times set forth in service-level statements or agreements.*

   System users must be able to input new or revised information into a system. If system unavailability prevents users from doing so, the system processing may contain errors. In turn, users who access information from the system for decision-making purposes are hampered by a system that is unavailable when needed. Another aspect of availability involves system accessibility by support personnel who monitor system performance and make changes to the system when needed.

   Although there is a connection between *system availability, system functionality*, and *system usability*, the SysTrust 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 the availability principle, which relates to whether the information stored in a system is accessible for routine processing, monitoring, and maintenance.

2. *Security. The system is protected against unauthorized physical and logical access.*

   Access to a system must be restricted to authorized users. The access restriction applies to the physical components of the system as well as the logic functions the system performs. Restricting access to a system helps prevent potential abuse of system components, theft of system resources, misuse of system software, and improper access to, use, alteration, destruction, or disclosure of information. The terms *security* and *privacy* are sometimes used interchangeably; however, they may have very different meanings and implications depending on the definitions used.

Privacy relates to (*a*) the nature and extent of the personally identifiable information a system requests, stores, and uses in providing services, and (*b*) the degree of intrusiveness a system imposes on users, for example, when an advertiser sends unsolicited advertisements to users of a system. Some privacy concerns may be related to local customs or legislative initiatives, as when a jurisdiction regulates the kinds of personal information that may be sent across borders.

As defined in this document, the security principle addresses access to the system and the methods used to protect access to system information. Privacy concerns related to restricting access to and protecting the personally identifiable information contained in the system are addressed by the SysTrust security principle. However, the security principle does not address other aspects of privacy, such as the dissemination of information captured by the system and the subsequent reuse of that information by parties outside the system.

When there are laws and regulation governing such matters, a system would be expected to comply with them.

3. *Integrity. System processing is complete, accurate, timely, and authorized.*

In this document, system *integrity* refers to the completeness, accuracy, timeliness, and authorization of system processing. System integrity exists if a system performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation of the system. System processing integrity addresses all of the system components as well as the procedures to initiate, record, process, and report the information that is the subject of the SysTrust engagement.

If a system processes information inputs from sources outside the system's boundaries, an entity can establish only limited controls over the completeness, accuracy, authorization, and timeliness of the information submitted for processing because, for the most part, procedures at external sites are beyond the entity's control. Thus, when the information source is explicitly excluded from the boundaries of the system that define the SysTrust 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 system description.

It is also important to recognize that system integrity does not automatically imply that the information stored by the system is complete, accurate, current, and authorized. This is because errors may have been introduced into system data at some previous time (for example, at initial data conversion) and those errors could still be present in the data even though current system processing may be complete, accurate, timely, and authorized.

System integrity differs from *data integrity.* In this document, data integrity refers to the completeness, accuracy, currency, and authorization of data. Data integrity exists if information and programs can be changed only in a specified and authorized manner. Data integrity depends on system integrity, and system integrity depends on controls over system components and the risks affecting those components in the system's business context. Although system integrity and data integrity are related, the focus of a SysTrust engagement is on system integrity.

Because SysTrust is a controls-based engagement, ordinarily it would not provide sufficient evidence to enable a practitioner to provide examination-level assurance about data integrity. This is due to the following inherent limitations of controls:

- The possibility of circumvention, either by employee collusion or management override
- The trade-off between operating efficiency and complex controls that may reduce exposure
- The practical materiality limits below which it is impractical to implement controls
- Changing conditions in entities that may lead controls to deteriorate or to become inappropriate
- The reliance on human judgment in the design, implementation, and monitoring of controls, any of which may lead to control breakdowns

Because of the inherent limitations of controls, evidence about the effectiveness of controls over system integrity ordinarily would not provide sufficient evidence about data integrity to reduce attestation risk to a sufficiently low level. Thus, although evidence about the effectiveness of controls over system integrity may be very persuasive, it would be necessary to perform procedures beyond those performed in a SysTrust examination to reduce attestation risk about data integrity to a level required by examination-level attestation standards.

4. *Maintainability. The system can be updated when required in a manner that continues to provide for system availability, security, and integrity.*

   Systems frequently must be updated and modified to keep them current. If a system is not updated to correct faults, errors, or failures, it cannot be considered reliable.

   Resources must be available to maintain a system in accordance with the documented requirements of authorized users and management's documented objectives, policies, and standards. In addition, resources must be available to manage, schedule, and document all changes to the system.

Only authorized, tested, and documented changes should be made to a system and related data. All planned and completed changes should be communicated to information systems management and authorized users.

Criteria for Assessing Whether the Principles Have Been Met

For each of the four principles, criteria have been established against which a system can be evaluated. The criteria address the following features that contribute to system reliability.

1. *Definition and documentation of an entity's performance objectives, policies, and standards* as they relate to (*a*) system performance expectations and service level commitments, and (*b*) communication of the objectives, policies, and standards to applicable personnel (Performance objectives, policies, and standards reflect management's awareness and commitment to a level of performance and control at the entity. *Performance objectives* are the overall goals that an entity wishes to achieve. *Policies* are rules that provide a formal direction for achieving the objectives and that enable enforcement. *Standards* are required procedures that are implemented to meet the policies. In some entities, policies and standards represent separate items; in other entities, they are terms that are used interchangeably.)

2. *Procedures* an entity implements for all system components to achieve its performance objectives in accordance with its established policies and standards

3. *System monitoring activities and monitoring of the surrounding environment* to enable an entity to identify potential impairments to system reliability and to take appropriate action to achieve compliance with objectives, policies, and standards

The SysTrust criteria are designed to be complete, relevant, objective, and measurable and to address all of the system components and the relationships among them. In some cases, for evidence-gathering purposes, the criteria may need to be broken down, for example, by system component, to address infrastructure, software, people, procedures, and data or by system development phase, which includes investigation, acquisition, implementation, operation, and maintenance. In reporting on a SysTrust engagement, it should be noted that—

- All of the SysTrust criteria for all four principles must be satisfied for a system to be deemed reliable.
- For engagements that address only certain of the four principles, all of the criteria related to the principle(s) under examination must be satisfied. In addition, the report must indicate which principles were not examined in the engagement. See pages 16, 48, and 57 of this document for performance and reporting guidance for such engagements.
- In determining whether a deviation from a specified criterion is material to that criterion, due consideration should be given to the anticipated users of the information and the kinds of decisions they are expected to make based on the information provided by the system.

Illustrative Controls That Provide for System Reliability

A SysTrust engagement is based on the premise that system controls that are operating effectively enable a system to perform reliably. An example of such a control is the use of personal identification numbers (PINs) to prevent unauthorized access to a system. An entity may adopt such a control in its written policies, but that control will not achieve the entity's objectives unless the control is operating effectively. The operating effectiveness of a control is a function of the suitability of its design, how the control is applied, the consistency with which it is applied, and by whom it is applied. In a SysTrust engagement, the practitioner obtains evidence about whether the controls over the system were operating with sufficient effectiveness during the period covered by the examination to enable the system to meet the criteria related to the principle(s) being reported on. If the practitioner deems an entity's controls over its system to have been operating with sufficient effectiveness to meet the criteria related to the principle(s) covered by the engagement, the practitioner will be able to issue an unqualified attestation/assurance report like some of the reports shown in appendix A of this document.

A list of illustrative controls that support system reliability is presented in this document; however, the list is not intended to be comprehensive, nor are all of the controls in the list required for every system. In each engagement, the practitioner should tailor the list to the circumstances of the particular engagement. Other controls in place at an entity, not included in the list, may support specified criteria, and some of the listed controls may not be applicable to all systems. Although entities would be expected to have some of the listed controls in each area, the choice and number of those controls would be based on the entity's management style, philosophy, size, and industry. The list of illustrative controls was developed by the Systems Reliability Task Force (task force) using a variety of sources including leading control frameworks, such as the Information Systems Audit and Control Foundation's *Control Objectives for Information and related Technology* (COBIT™) and the CICA's *Information Technology Control Guidelines*, other relevant research, and the task force's practical experiences. Additional guidance on controls is available in material developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in the United States and the Criteria of Control Board (CoCo) in Canada. The task force engaged in lengthy debate and discussion to arrive at a complete yet concise set of principles, criteria, and illustrative controls. However, it is anticipated that future revisions may be required to update and refine these principles, criteria, and illustrative controls.

The CPA and CA as Assurance Professionals

CPAs and CAs are in the business of providing assurance services, the most publicly recognized of which is the audit of financial statements. An audit report signed by a CPA or CA is valued because these professionals are knowledgeable about financial accounting and assurance matters and are recognized for their independence, integrity, objectivity, and discretion. Financial statement assurance is only one of the many kinds of assurance services that CPAs and CAs provide. They also provide assurance on internal control and compliance with specified criteria. The business and professional experience, subject matter expertise (information systems security and control), and professional characteristics (independence, integrity, objectivity, and discretion) needed for such engagements are the same key attributes that enable a CPA or CA to comprehensively and objectively assess the risks and controls associated with systems reliability. In addition, CPAs and CAs are required to follow comprehensive ethics rules and professional standards when providing professional services.

SysTrust Examination/Audit Engagement

Objective of a SysTrust Examination/Audit Engagement

In general, the objective of a SysTrust engagement is for the practitioner to issue a report on whether management maintained effective controls over its system based on the fifty-eight criteria presented on pages 15 through 37 of this document. The practitioner determines whether controls over the system exist and performs tests to determine whether those controls were operating effectively during the period covered by the attestation/assurance report.

The objective of a SysTrust engagement varies depending on the nature of the engagement. Variations of SysTrust engagements are described on pages 16 through 19 of this document.

Management's Assertion

Under AICPA attestation standards, management must provide the practitioner with an assertion regarding the availability, security, integrity, and maintainability of the system—specifically, management's assertion that during the period covered by the report and based on the AICPA/CICA SysTrust criteria for system reliability, the entity maintained effective controls over its system to provide reasonable assurance that—

1. The system was available for operation and use at times set forth in service-level statements or agreements.
2. The system was protected against unauthorized physical and logical access.
3. The system processing was complete, accurate, timely, and authorized.
4. The system could be updated when required in a manner that continued to provide for system availability, security, and integrity.

For engagements covering only selected principles, management's assertion should address only the principle(s) covered by the engagement.

When the practitioner reports on the assertion, the assertion should accompany the practitioner's report. Appendix C of this document contains an example of a management assertion.

Under both AICPA and CICA standards, the practitioner may report on either of the following:

1. Management's assertion that it maintained effective controls over the reliability of the system during the period covered by the report
2. The subject matter—that is, the effectiveness of the controls over the reliability of the system during the period covered by the report

Under CICA assurance standards, the practitioner would seek management's acknowledgement of responsibility for the subject matter, but a written assertion is not mandatory. If no assertion is provided, the practitioner would report directly on the subject matter.

If one or more criteria have not been achieved, the practitioner would issue 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. Under CICA standards, when one or more criteria have not been achieved and the practitioner is reporting directly on the subject matter, the practitioner would issue a qualified or adverse report. However, under CICA standards, when the practitioner is reporting on management's assertion, and that assertion appropriately describes a departure from the criteria, the practitioner would not issue a qualified or adverse report, but would emphasize this departure by referring to it in the paragraph of his or her report containing the practitioner's conclusion, and by describing the departure in a separate paragraph following the practitioner's conclusion.

Use of a SysTrust Report

The SysTrust criteria are available to any user of a SysTrust report;[2] accordingly, the criteria do not have to be stated in the assertion, and the report's use need not be restricted to specified parties. However, a practitioner may restrict the use of any report. The SysTrust criteria require that the entity's performance objectives, policies, and standards be communicated to authorized users; however, they do not have to be communicated to unauthorized users of the system, such as potential customers of the service. For security purposes, an entity may not wish to disclose such information to unauthorized users. Users of the report who do not have access to the policies, objectives, and standards may still find the report useful. Appendix A of this document presents examples of practitioners' reports.

[2] The SysTrust criteria are posted on the AICPA's and CICA's Web sites.

Period of Coverage

Management's assertion (when required) and the practitioner's report should always specify the time period covered by the assertion and report, respectively. Because the concept of system reliability is dynamic rather than static, SysTrust reports cover a historical period of time as opposed to a point in time (except for SysTrust engagements that cover systems in the preimplementation phase). The determination of an appropriate period should be at the discretion of the practitioner and the reporting entity.

Factors to be considered in establishing the reporting period include—

- 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.
- The cyclical nature of processing within the system.
- Historical information about the reliability of the system.
- The period of time needed to provide sufficient and appropriate evidence regarding the operating effectiveness of the controls.

Subsequent Events

Changes in controls or other factors that might significantly affect controls over the reliability of a system may occur subsequent to the period covered by management's assertion[3] but before the date of the practitioner's report. Such events may have a significant effect on controls over system reliability and therefore may require disclosure by management. Such occurrences are referred to as *subsequent events*. In performing a SysTrust 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:

[3] As stated previously, a practitioner may report on management's assertion or on the subject matter. For simplicity, this document refers to reports on an assertion; however, the guidance is equally applicable to reports on the subject matter.

1. Events that provide additional information about conditions that existed during the period covered by management's assertion. This information should be used by a practitioner in determining whether controls over system reliability were operating effectively based on the SysTrust criteria and whether those events may affect management's assertion or the practitioner's report.
2. Events that provide information about conditions that arose subsequent to the period covered by management's assertion that are of such a nature and significance that their disclosure is necessary to keep users from being misled. This type of information ordinarily will not affect the practitioner's report if the information is appropriately disclosed.

In a SysTrust engagement performed under Statement on Standards for Attestation Engagements (SSAE) No. 1, *Attestation Engagements* (AICPA, *Professional Standards*, vol. 1, AT sec. 100), a practitioner has no responsibility to obtain evidence regarding subsequent events. However, a practitioner should inquire of management as to whether it is aware of any subsequent events through the date of the practitioner's report that would have a significant effect on management's assertion about controls over the system. The practitioner should also consider obtaining a representation from management regarding subsequent events.

The Assurance Process

In the United States a SysTrust attestation engagement is performed under AICPA professional standards, and in Canada a SysTrust assurance engagement is performed under CICA professional standards.[4] An independent, objective, knowledgeable

[4] In the United States, SysTrust examination and agreed-upon procedures engagements are performed under Statement on Standards for Attestation Engagements (SSAE) No. 1, *Attestation Standards* (AICPA, *Professional Standards*, vol. 1, AT sec. 100). However, in January, 2001 the AICPA' s Auditing Standards Board will issue SSAE No. 10, *Attestation Standards: Revision and Recodification*, which supersedes SSAE Nos. 1 through 9. SSAE No. 10 is effective when the subject matter or assertion is as of or for a period ending on or after June 1, 2001; early application is permitted. In Canada a SysTrust audit engagement is performed under the *CICA Handbook—Assurance*, Section 5025, "Standards for Assurance Engagements." A SysTrust-specified auditing procedures engagement is not an assurance engagement-practitioners should refer to Section 5025, appendix A, for guidance on this type of engagement. Practitioners will need the appropriate skills and experience to perform a SysTrust engagement.

practitioner performs tests of either management's assertion or the subject matter to which the assertion relates. The practitioner gathers evidence about the subject matter's conformity with the criteria in the same way as is commonly done in other audit engagements, by performing procedures such as inspection, observation, inquiry, confirmation, computation, and analysis to verify the achievement of system reliability criteria. The practitioner expresses an opinion on management's assertion or on the subject matter to which it relates. The practitioner's report provides value to management because it increases the credibility of management's assertion and helps distinguish the entity from other service providers.

How a SysTrust Engagement Differs From Certain Other Engagements

There are a number of similarities and important differences between a SysTrust engagement and other AICPA/CICA engagements, such as a service auditor's engagement and a WebTrust engagement. Refer to appendix D for a summary of how SysTrust differs from a service auditor's engagement and a WebTrust engagement, and for information about the applicability of these engagements.

Variations of a SysTrust Engagement

This document so far has described how the SysTrust Principles and Criteria may be used in examination/audit level attestation engagements for systems in production. The SysTrust Principles and Criteria may also be used in other types of engagements to meet client needs, as long as the applicable professional standards and the SysTrust licensing agreement are observed. Following are examples of other types of SysTrust engagements a practitioner might perform.

Reporting on Selected SysTrust Principles

A client may request a report that covers selected SysTrust principles, for example, a system owner may primarily be concerned with the availability of a system. A practitioner may report on one principle or any combination of principles. An illustrative report on the availability principle is presented in examples 4 and 10 of appendix A. All of the relevant SysTrust criteria related to the principle(s) being reported on must be satisfied.

During an engagement involving selected SysTrust principles, information about control or system deficiencies related to principles and criteria *not* included in the defined scope of the engagement may come to the practitioner's attention. For example, while engaged to report on controls related to the system availability principle, a practitioner may become aware of information related to the system security principle—a principle not covered by the practitioner's report because it is not part of the defined scope of the engagement. A practitioner's report on a specified principle(s) does not address the interdependence of the principles; accordingly, a practitioner is not responsible for searching for such information. Nevertheless, a practitioner should consider such information that comes to his or her attention and evaluate whether the information indicates the existence of significant system deficiencies. If the practitioner concludes that such deficiencies exist, he or she should communicate them to management in writing.

The practitioner also should consider whether users of the system would be expected to have knowledge of these deficiencies. If not, the practitioner should request that management disclose this additional information in the system description, which is attached to the practitioner's SysTrust report. Even if management agrees to disclose this information in the system description, the practitioner should consider the business risk entailed in being associated with such a report. If management is unwilling to disclose such information, and the practitioner concludes that the omission of this information would be material to users of the report, the practitioner should consider what course of action to take. If the practitioner concludes that omission of the information would be material to users of the report, and management is unwilling to disclose the additional information in the system description, the practitioner should consider withdrawing from the engagement.

Engagements for Systems in the Preimplementation Phase

A client may request a SysTrust engagement for a system that is in the preimplementation phase. As stated on page 6, the operating effectiveness of a control is a function of the suitability of its design, how the control is applied, the consistency with which it is applied, and by whom it is applied. Suitability of design is measured according to whether controls, if effectively implemented, would prevent or detect material error, fault, or failure of the system in a specified environment. If a system has not yet been placed in operation, a practitioner would be unable to perform all of the tests necessary to report on the operating effectiveness of controls; however, a practitioner could test the suitability of the design of the controls. The report would be at a point in time rather than for a period of time. Such a report should indicate that the system has not been placed in operation. The system description attached to the practitioner's report should identify the version of the system being reported on or contain other appropriate identifiers of the system being examined. Illustrative reports on the suitability of the design of controls are presented in examples 5 and 11 of appendix A.

Agreed-Upon Procedures Engagements

A client may request that a practitioner perform an agreed-upon procedures engagement related to the SysTrust Principles and Criteria. In such an engagement, the practitioner performs specified procedures, agreed to by the specified parties,[5] and reports his or her findings. Because users' needs may vary widely, the nature, timing, and extent of the agreed-upon procedures may vary as well; consequently, the users assume responsibility for the sufficiency of the procedures because 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

[5] The specified users and the practitioner agree upon the procedures to be performed by the practitioner.

or negative assurance about the assertion or subject matter.[6] The practitioner's report on agreed-upon procedures is in the form of procedures and findings. Illustrative agreed-upon procedures reports are presented in examples 6 and 12 of appendix A. The use of an agreed-upon procedures report is restricted to the specified parties who agreed upon the procedures.

Consulting Engagements

A practitioner may perform a consulting engagement related to the SysTrust Principles and Criteria. For example, a practitioner may be engaged by a client to evaluate its readiness for a SysTrust engagement. In the United States, Statements on Standards for Consulting Services govern such engagements.

Other Reporting Guidance

A practitioner should also adhere to the following guidance:

- All SysTrust engagements should be performed in accordance with the applicable professional standards and the SysTrust license agreement.
- All SysTrust reports should make reference to the *SysTrust Principles and Criteria*, as required by item 7 of the SysTrust license agreement.
- A practitioner may not issue a review-level SysTrust attestation report.

[6] In the United States, agreed-upon procedures engagements are performed under SSAE No. 4, *Agreed-Upon Procedures* (AICPA, *Professional Standards*, vol. 1, AT sec. 600). However, in January, 2001 the AICPA's Auditing Standards Board will issue SSAE No. 10, *Attestation Standards: Revision and Recodification*, which supersedes SSAE Nos. 1 through 9. SSAE No. 10 is effective when the subject matter or assertion is as of or for a period ending on or after June 1, 2001; early application is permitted. In Canada, "agreed upon procedures" engagements are referred to as "specified auditing engagements." Practitioners should refer to *CICA Handbook—Assurance*, Section 5025, appendix A, for guidance on this type of engagement.

Availability: The system is available for operation and use at times set forth in service-level statements or agreements.

Criteria		Illustrative Controls
A1	***The entity has defined and communicated performance objectives, policies, and standards for system availability.***	
A1.1	The system availability requirements of authorized users, and system availability objectives, policies, and standards, are identified and documented.	Procedures exist to identify and document authorized users of the system and their availability requirements. User requirements are documented in service-level agreements or other documents.
A1.2	Documented system availability objectives, policies, and standards have been communicated to authorized users.	There is formal communication of system availability objectives, policies, and standards to authorized users through means such as memos, meetings, and manuals. Procedures exist to log and review requests from authorized users for changes and additions to system availability objectives, policies, and standards.
A1.3	Documented system availability objectives, policies, and standards are consistent with system availability requirements defined in contractual, legal, and other service-level agreements and applicable laws and regulations.	A formal process exists to identify and review contractual, legal, and other service-level agreements and applicable laws and regulations that could affect system availability objectives, policies, and standards. Procedures exist to review any new or changing contractual, legal, or other service-level agreements and applicable laws and regulations for their impact on current system availability objectives, policies, and standards.
A1.4	Responsibility and accountability for system availability have been assigned.	One or more positions exist that have formal responsibility and accountability for system availability, as indicated by a documented job description and organization chart.
A1.5	Documented system availability objectives, policies, and standards are communicated to entity personnel responsible for implementing them.	Documented system availability objectives, policies, and standards are communicated to personnel responsible for implementing them through such means as memos, meetings, and manuals. Additions and changes to system availability objectives, policies, and standards are communicated on a timely basis to entity personnel responsible for implementing and monitoring them.

Criteria	Illustrative Controls
A2 The entity uses procedures, people, software, data, and infrastructure to achieve system availability objectives in accordance with established policies and standards.	
A2.1 The acquisition, implementation, configuration and management of system components[7] related to system availability are consistent with documented system availability objectives, policies, and standards.	Existing system availability features are compared to documented system objectives, policies, and availability standards. System availability features are regularly tested and variances are recorded and followed up. The effects of development, additions, or changes to system components are compared to system availability objectives, policies, and standards.
A2.2 There are procedures to protect the system against potential risks 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, excessive heat and humidity, and labor problems have been considered. Preventive measures are implemented based on the level of risk identified. Vendor warranty specifications are complied with and tested to determine if the system is properly configured.
A2.3 Continuity provisions address minor processing errors, minor destruction of records, and major disruptions of system processing that might impair system availability.	Procedures to address minor processing errors, outages, and destruction of records are documented. Operations personnel are familiar with operations procedures. Procedures exist for the identification, documentation, escalation, resolution, and review of problems. Disaster recovery and contingency plans are documented. Disaster recovery and contingency plans are tested on a regular basis, with a frequency appropriate for the business environment.

(continued)

[7] System components are categorized as follows: infrastructure (facilities, equipment, and networks), software (systems, applications, and utilities), people (developers, operators, users, and managers), procedures (automated and manual), and data (transaction streams, files, databases, and tables).

Criteria	Illustrative Controls
	Preventive maintenance agreements or procedures are in place for key system hardware components. An alternative system processing capability has been developed or other arrangements have been put into place that reflect the system availability objectives, policies, and standards. On a regular basis, software and data are backed up and stored offsite in accordance with system availability objectives, policies, and standards. Insurance has been obtained to address key system availability risks. Physical and logical security controls are implemented to reduce the opportunity for unauthorized actions that could impair system availability
A2.4 There are procedures to ensure that personnel responsible for the design, development, implementation, and operation of system availability features are qualified to fulfil their responsibilities.	Hiring procedures exist to employ personnel who meet job description requirements. All new personnel are subject to background checks, reference validation, and so on. Personnel receive training and development in system availability concepts and issues. Personnel responsible for system availability have relevant experience. Procedures are in place to provide alternate personnel for key system availability functions in case of absence or departure. Personnel periodically are reminded of their responsibilities. Periodic performance appraisals are performed regularly.
A3 The entity monitors the system and takes action to achieve compliance with system availability objectives, policies, and standards.	
A3.1 System availability performance is periodically reviewed and compared with documented system availability requirements of authorized users and contractual, legal, and other service-level agreements.	Procedures exist for regular comparisons of existing system availability against objectives, policies, and standards and for reporting of the results. Variances are recorded and followed up.

Criteria	Illustrative Controls
	In the event of incidents, the actions of personnel are reviewed. The internal audit function includes system availability reviews in its annual audit plan. Problem logs are reviewed and trends are analyzed to identify the potential impact on system availability objectives.
A3.2 There is a process to identify potential impairments to the system's ongoing ability to address the documented system availability objectives policies, and standards and to take appropriate action.	Procedures exist for the documentation, escalation, resolution, and review of problems. Problem logs are reviewed and trends are analyzed to identify their potential impact on system availability objectives. System workload versus current capacity is monitored to facilitate increases in capacity when needed.
A3.3 Environmental and technological changes are monitored and their impact on system availability is periodically assessed on a timely basis.	A risk assessment has been prepared and is 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, excessive heat and humidity, and labor problems are considered. Changes to system components are assessed for their impact on documented system availability objectives, policies, and standards.

Security: The system is protected against unauthorized physical and logical access.

Criteria	Illustrative Controls
S1 The entity has defined and communicated performance objectives, policies, and standards for system security.	
S1.1 The system security requirements of authorized users, and the system security objectives, policies, and standards, are identified and documented.	There is a framework for classifying access privileges based on an assessment of the business impact of the loss of security and confidentiality. Objectives, policies, and standards exist that support the implementation, operation, and maintenance of security measures. Security levels are defined for each of the data classifications identified above the level of "no protection required." These security levels represent the appropriate (minimum) set of security and control measures for each of the classifications. A risk assessment approach has been established that defines the scope and boundaries and the methodology to be adopted for risk. The risk assessment approach focuses on the examination of the essential elements of risk such as assets, threats, vulnerabilities, safeguards, consequences, and likelihood of threat.
S1.2 Documented system security objectives, policies, and standards have been communicated to authorized users.	System security objectives, policies, and standards are communicated to all authorized personnel within the entity. A security awareness program communicates the information security policy to each user. Employees sign an agreement at the time of hiring acknowledging that they will adhere to the security policy. The entity discloses its information privacy practices, including the specific kinds and sources of information being collected, the use of that information, and possible third-party distribution of that information.
S1.3 Documented system security objectives, with policies, and standards are consistent system security requirements defined in contractual, legal, and other service-level agreements and applicable laws and regulations.	A formal process exists to identify and review contractual, legal, and other service-level agreements and applicable laws and regulations that could have an impact system on security objectives, policies, and standards.

Criteria	Illustrative Controls
	Procedures exist to review any new or changing contractual, legal, or other service-level agreements and applicable laws and regulations for their impact on current system security objectives, policies, and standards.
S1.4 Responsibility and accountability for system security have been assigned.	One or more positions exist that have formal responsibility and accountability for system security, as indicated by a documented job description and organization chart. 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. Responsibility for the logical and physical security of the entity's information assets is assigned to appropriate individuals. Defined responsibility exists for developing and maintaining a policy that establishes the entity's overall approach to security.
S1.5 Documented system security objectives, policies, and standards are communicated to entity personnel responsible for implementing them.	Documented system security objectives, policies, and standards are communicated to the personnel responsible for implementing them through means such as memos, meetings, and manuals. Additions and changes to system security objectives, policies, and standards are communicated on a timely basis to the entity personnel responsible for implementing and monitoring them.
S2 The entity uses procedures, people, software, data, and infrastructure to achieve system security objectives in accordance with established policies and standards.	
S2.1 The acquisition, implementation, configuration, and management of system components related to system security are consistent with documented system security objectives, policies, and standards.	Procedures exist to regularly compare existing system security features to documented system security objectives, policies, and standards. The effects of development, additions, or changes to system components are compared with system security objectives, policies, and standards. The access control and operating system facilities have been appropriately installed, including the implementation of appropriate options and parameters to restrict access in accordance with the security objectives, policies, and standards.

(continued)

Criteria	Illustrative Controls
	The owners of information and data classify the sensitivity of the information and data to determine the level of protection required to maintain an appropriate level of confidentiality. The operators, users, and custodians of system components implement and comply with procedures and controls that meet the security objectives, policies, and standards.
S2.2 There are procedures to identify and authenticate all users authorized to access the system.	All paths that allow access to significant information resources are controlled by the access control system and operating system facilities. To the extent possible, unique user IDs are assigned to individual users. Passwords are used to validate such user IDs. Users are held accountable for maintaining the confidentiality of their passwords and for any system activity performed with their user IDs. Procedures exist to ensure timely action relating to requesting, establishing, issuing, suspending, and closing user accounts and access privileges.
S2.3 There are procedures to grant system access privileges to users in accordance with the policies and standards for granting such privileges.	Data owners are responsible for authorizing access to data and systems, and proper segregation of duties is considered in granting authorization. The appropriate security administrator(s) is notified when personnel leave the entity or change assignments and immediately removes or changes the access capabilities of those individuals. Access to utility programs that can read, add, change, or delete data or programs is restricted to authorized individuals. The entity implements security procedures that provide access security control based on an individual's demonstrated need to read, add, change, or delete data.
S2.4 There are procedures to restrict access to computer processing output to authorized users.	Access to computer processing output is based on the classification of the information and the kind of output.

Criteria	Illustrative Controls
	Processing outputs are stored in an area that reflects the classification of the information.
S2.5 There are procedures to restrict access to files on offline storage media to authorized users.	Access to offline storage media is based on the classification of the information and the kind of media. Offline storage media are stored in an area that reflects the classification of the information.
S2.6 There are procedures to protect external access points against unauthorized logical access.	External access points are designed to manage threats of loss or damage to the integrity and confidentiality of resources, and to control the navigation available to users accessing the resources from outside the enterprise. If connection to the Internet or other public networks exists, adequate firewalls or other procedures are operative to protect against unauthorized access to the internal resources. Private information is protected during transmission by using encryption technology. Procedures exist to verify the authenticity of the counterparty providing electronic instructions or transactions through trusted exchange of passwords, tokens, or cryptographic keys.
S2.7 There are procedures to protect the system against infection by computer viruses, malicious codes, and unauthorized software.	Regarding malicious software, such as computer viruses or "Trojan horses," a framework of adequate preventative, detective, and corrective control measures is established. There are periodic checks of the entity's computers for unauthorized software.
S2.8 Threats of sabotage, terrorism, vandalism and other physical attacks have been considered when locating the system.	System components are protected from threats of sabotage, terrorism, vandalism, and other physical attacks by being located in areas away from hazardous or combustible materials and by other mechanisms such as fire and smoke detection equipment, and fire extinguishing equipment. When IT resources are located in public areas, they are appropriately protected to prevent or deter loss or damage from theft or vandalism.

(continued)

Criteria	Illustrative Controls
	When IT equipment is located in decentralized areas, precautions are taken commensurate with the value of the equipment, the criticality of the equipment to the enterprise's operations, the sensitivity of the stored data, and the inherent threats of sabotage, vandalism, and terrorism.
S2.9 There are procedures to segregate incompatible functions within the system through security authorizations.	The level of user access (for example, read, add, update, or delete) is appropriate based on the user's job function and supports segregation of incompatible functions (for example, data entry is segregated from transaction review and approval). An assignment of responsibility is maintained that ensures that no single individual has the authority to read, add, change, or delete an information asset without an independent review of that activity.
S2.10 There are procedures to protect the system against unauthorized physical access.	Access to the computers, disk and tape storage devices, communications equipment, and control console is restricted to authorized personnel. Appropriate physical security and access control measures are established for IT facilities.
S2.11 There are procedures to ensure that personnel responsible for the design, development, implementation, and operation of system security arequalified to fulfil their responsibilities.	Hiring procedures exist to hire personnel who meet the job description requirements. All new personnel are subject to background checks, reference validation, and so on. Personnel receive training and development in system security concepts and issues. Personnel responsible for system security have relevant experience. Procedures are in place to provide alternate personnel for key system security functions in case of absence or departure. Personnel are periodically reminded of their responsibilities. Periodic performance appraisals are performed regularly.

Criteria		Illustrative Controls
S3	***The entity monitors the system and takes action to achieve compliance with system security objectives, policies, and standards.***	
S3.1	System security performance is periodically reviewed and compared with documented system security requirements of authorized users and contractual, legal, and other service-level agreements.	Procedures exist for regular comparisons of existing system security against objectives, policies, and standards, and for reporting of results. Variances are recorded and followed up. In the event of security incidents, the actions of personnel are reviewed. The internal audit function includes system security reviews in its annual audit plan. Problem logs are reviewed and trends are analyzed to identify their potential impact on system security objectives.
S3.2	There is a process to identify potential impairments to the system's ongoing ability to address the documented system security objectives, policies, and standards, and to take appropriate action.	Standard procedures exist for the documentation, escalation, resolution, and review of problems. Problem logs are reviewed and trends are analyzed to identify their potential impact on system security objectives.
S3.3	Environmental and technological changes are monitored and their impact on system security is periodically assessed on a timely basis.	A risk assessment has been prepared and is reviewed on a regular basis or when a significant change occurs in either the internal or external environment. Changes to system components are assessed for their impact on documented system security objectives, policies, and standards.

Integrity: System processing is complete, accurate, timely, and authorized.

Criteria	Illustrative Controls
I1 The entity has defined and communicated performance objectives, policies, and standards for system processing integrity.	
I1.1 The system processing integrity requirements of authorized users and the system processing integrity objectives, policies, and standards are identified and documented.	The entity has created a positive control environment throughout the entity by addressing aspects such as— • Integrity, ethical values, and competence of personnel. • Management philosophy and operating style. • Accountability. • Attention and direction provided by executive management and the board. Procedures exist to identify and document authorized users of the system and their integrity requirements. User requirements are documented in service-level agreements or other documents.
I1.2 Documented system processing integrity objectives, policies, and standards have been communicated to authorized users.	There is formal communication of system processing integrity objectives, policies, and standards to authorized users through means such as memos, meetings, and manuals. Procedures exist to log and review requests from authorized users for changes and additions to system processing integrity objectives, policies, and standards.
I1.3 Documented system processing integrity objectives, policies, and standards are consistent with system processing integrity requirements defined in contractual, legal, and other service-level agreements and applicable laws and regulations.	A formal process exists to identify and review contractual, legal, and other service-level agreements and laws and regulations that could have an impact on system processing integrity objectives, policies, and standards. Procedures exist to review any new or changing contractual, legal, or other service-level agreements and applicable laws and regulations to determine their impact on current system processing integrity objectives, policies, and standards.
I1.4 Responsibility and accountability for system processing integrity have been assigned.	One or more positions exist that have formal responsibility and accountability for system processing integrity, as indicated by a documented job description and organization chart.

	Criteria	Illustrative Controls
I1.5	Documented system processing integrity objectives, policies, and standards are communicated to entity personnel responsible for implementing them.	Documented system processing integrity objectives, policies, and standards are communicated to personnel responsible for implementing them through such means as memos, meetings, and manuals. Additions and changes to system processing integrity objectives, policies, and standards are communicated on a timely basis to entity personnel responsible for implementing and monitoring them.
I2	***The entity uses procedures, people, software, data, and infrastructure to achieve system processing integrity objectives in accordance with established policies and standards.***	
I2.1	The acquisition, implementation, configuration, and management of system components related to system processing integrity are consistent with documented system processing integrity objectives, policies, and standards.	Existing system processing integrity requirements are regularly compared with documented system processing integrity objectives, policies, and standards. System processing integrity features are regularly tested, and variances are recorded and followed up. Strategic plans as well as annual budgets are prepared, and reviewed and approved by executive management and the board. Changes to hardware, software, and personnel responsibilities are reviewed, monitored, and approved by IT management. Hardware and software acquisitions and implementations are subjected to extensive testing before acceptance in production. The effects of additions or changes to system components are compared with system processing integrity objectives, policies, and standards.
I2.2	The information processing integrity procedures related to information inputs are consistent with the documented system processing integrity requirements.	Software design methodologies contain standards for the integration of controls in the system development life cycle (SDLC) methodology that address the documented system processing integrity requirements. The entity has established data preparation procedures to be followed by user departments. Input form design should help assure that errors and omissions are minimized.

(continued)

Criteria	Illustrative Controls
	The entity ensures that source documents are properly prepared by authorized personnel who are acting within their authority and that an adequate segregation of duties is in place regarding the origination and approval of source documents.
	The entity's procedures ensure that all authorized source documents are complete and accurate, properly accounted for, and transmitted in a timely manner.
	Error handling procedures during data origination reasonably ensure that errors and irregularities are detected, reported, and corrected.
	Procedures exist to ensure that original source documents are retained or are reproducible by the entity for an adequate amount of time to facilitate the retrieval or reconstruction of data as well as to satisfy legal requirements.
	Appropriate procedures exist to ensure that data input is performed only by authorized personnel.
	Transaction data entered for processing (people-generated, system-generated, or interfaced inputs) are subjected to a variety of controls to check for accuracy, completeness, and validity.
	Procedures exist to ensure that input data are edited and validated as close to the point of origination as possible.
	Procedures exist for the correction and resubmission of data that was erroneously input.
	The entity ensures that adequate protection of sensitive information from unauthorized access, modification, and misaddressing is provided during transmission and transport.
I2.3 There are procedures to ensure that system processing is complete, accurate, timely, and authorized.	There is an appropriate segregation of incompatible duties with respect to the handling of production data.
	There is an appropriate segregation of incompatible duties within the information services function of the entity.
	Appropriate SDLC methodologies are employed in the development of applications and such methodologies contain appropriate controls for user involvement,

Criteria	Illustrative Controls
	testing, conversion, and management approvals of system processing integrity features. Computer operations procedures exist, are documented, and contain procedures and instructions for operations personnel regarding system processing integrity objectives, policies, and standards. Job scheduling procedures exist, are documented, and require appropriate review and approval to ensure that only authorized jobs are introduced into the production environment. Applications contain extensive edit and validation routines to check for incomplete or inaccurate data. Errors are logged, investigated, corrected, and resubmitted for input on a timely basis. Error logs are regularly reviewed to ensure that all errors are corrected on a timely basis. End-of-day procedures exist to reconcile all transactions accepted to control reports, file update/status reports, or other control mechanisms. Files received from users are balanced to control totals, record counts, and so on, and are subject to the same edit and validation checks as online submissions. End-of-day procedures exist to reconcile number of records accepted to number of records processed to number of records output. Procedures exist to ensure that application programs contain provisions that routinely verify the tasks performed by the software to help ensure data integrity, and that provide for the restoration of the integrity through rollback or other means. See the security principle for additional illustrative controls relating to "authorized" system processing.
I2.4 The information processing integrity procedures related to information outputs are consistent with the documented system processing integrity requirements.	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 control totals daily, on both a system-wide and an indvidual

(*continued*)

Criteria	Illustrative Controls
	customer basis. Exceptions are resolved before acceptance of the applicable transaction set. Procedures exist for assuring that the accuracy of output reports is reviewed by the provider and the relevant users. Procedures exist for controlling errors contained in output reports. Procedures exist for assuring that the security of output reports is maintained for those awaiting distribution, as well as for those already distributed to users. The entity ensures that adequate protection from unauthorized access, modification, and misaddressing of sensitive information is provided during transmission and transport.
I2.5 There are procedures to ensure that personnel responsible for the design, development, implementation, and operation of the system are qualified to fulfil their responsibilities.	Hiring procedures exist to hire personnel who meet job description requirements. All new personnel are subjected to background checks, reference validation, and so on. Personnel receive training and development in system processing integrity concepts and issues. Personnel responsible for system processing integrity have relevant experience. Procedures are in place to provide alternate personnel for key system processing integrity functions in case of absence or departure. Personnel are periodically reminded of their responsibilities. Periodic performance appraisals are regularly performed.
I2.6 There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.	The SDLC methodology requires that adequate mechanisms to enable tracing of information inputs from their source to their final disposition and vice versa (audit trails) are available or can be developed for the solution identified and selected. All input transactions are date/time stamped by the system, and identified with the submitting source (terminal, transmission line).

Criteria	Illustrative Controls
	System logs record all system-related events with a unique transaction identifier. Transaction logs record each transaction along with a unique transaction identifier. User documentation includes flow of transactions, including input, processing, and output, and a description of key processing functions.
I3 The entity monitors the system and takes action to achieve compliance with system processing integrity objectives, policies, and standards.	
I3.1 System processing integrity performance is periodically reviewed and compared with documented system processing integrity requirements of authorized users and contractual, legal, and other service-level agreements.	Procedures exist for regular comparisons of existing system processing integrity against objectives, policies, and standards and for reporting of the results. Variances are recorded and followed up. In the event of incidents, the actions of personnel are reviewed. The internal audit function includes system processing integrity reviews in the annual audit plan. Supervisory personnel review and approve end-of-day activities, including reconciliations, system logs, and problem management reports. Problem management escalation procedures exist to address incidents that have a potential global impact on system processing integrity.
I3.2 There is a process to identify potential impairments to the system's ongoing ability to address the documented system processing integrity objectives, policies, and standards and to take appropriate action.	Procedures exist for the identification, documentation, escalation, resolution, and review of problems. Problem logs are reviewed and trends are analyzed to identify the potential impact on system processing integrity objectives. Internal audit procedures exist and include tests of data acceptance and validation routines to identify potential sources of corrupt data. There is a documented business resumption plan that addresses the recovery of the system processing facilities. The plan is periodically tested.

(*continued*)

Criteria		Illustrative Controls
I3.3	Environmental and technological changes are monitored and their impact on system processing integrity is periodically assessed on a timely basis.	A risk assessment has been prepared and is reviewed on a regular basis or when a significant change occurs in either the internal or external environment. Changes to system components are assessed for their impact on documented system processing integrity objectives, policies, and standards. The entity maintains a research and development group whose charter is to assess the impact of emerging technologies. Users are proactively invited to contribute to initiatives to improve system processing integrity through the use of new technologies. Proposed changes in the system Configuration are analyzed to identify their impact on system processing integrity.

Maintainability: The system can be updated when required in a manner that continues to provide for system availability, security, and integrity.

Criteria	Illustrative Controls
M1 The entity has defined and communicated performance objectives, policies, and standards for system maintainability.	
M1.1 Documented system maintainability objectives, policies, and standards address all areas affected by system changes.	There is a formal SDLC methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology. The methodology is appropriate for the systems to be developed, acquired, implemented, and maintained and SDLC standards are observed. User requirements are documented in service-level agreements or other documents. There is routine and periodic hardware maintenance to reduce the frequency and impact of performance failures.
M1.2 Documented system maintainability objectives, policies, and standards have been communicated to authorized users.	There is formal communication of system maintainability objectives, policies, and standards to authorized users through means such as memos, meetings, and manuals. There is a "help desk" function that provides user support. Individuals responsible for performing the function closely interact with problem management personnel. There is an annual budgeting process in which system and user resource requirements are allocated for expected maintenance on some basis such as business unit, department, or application. There is a relationship between the basis used for current allocations and prior allocations.
M1.3 Documented system maintainability objectives, policies, and standards are consistent with system maintainability requirements defined in contractual, legal, and other service-level agreements and applicable laws and regulations.	A formal process exists to identify and review contractual, legal, and other service-level agreements and applicable laws and regulations that could have an impact on system maintainability objectives, policies, and standards. Procedures exist to review any new or changing contractual, legal, or other service-level agreements and applicable laws and regulations for their impact on

(*continued*)

Criteria	Illustrative Controls
	current system maintainability objectives, policies, and standards.
M1.4 Responsibility and accountability for system maintainability have been assigned.	One or more positions exist that have formal responsibility and accountability for system maintainability, as indicated by a documented job description and organization chart. There is a process in place to regularly verify that personnel performing specified tasks are qualified to perform those tasks based on their education, training, and experience, as required. Management encourages personnel to obtain membership in professional organizations. All requests for changes are assessed in a structured way to determine their possible impact on the operational system and its functionality.
M1.5 Documented system maintainability objectives, policies, and standards are communicated to entity personnel responsible for implementing them.	Formal change control processes and procedures exist and responsibilities are identified. These procedures contribute to the segregation of duties. There is a budget allocation for emergency or unanticipated maintenance requirements. Emergency changes that require deviations from standard procedures are logged and reviewed, and approved after the fact by management.
M2 The entity uses procedures, people, software, data, and infrastructure to achieve system maintainability objectives in accordance with established policies and standards.	
M2.1 Resources available to maintain the system are consistent with the documented requirements of authorized users and documented objectives, policies, and standards.	Staffing requirement evaluations are performed regularly to provide the information services function with a sufficient number of competent IT personnel. Hardware and infrastructure requirements are periodically evaluated to provide adequate resources for maintenance activities. Software requirements are periodically evaluated to provide adequate resources for maintenance activities. Key component requirements are evaluated at least annually or whenever there are major changes to the business, operational, or informational technology environment.

Criteria	Illustrative Controls
	Results of the evaluation are acted upon promptly to ensure adequate current and future resources.
M2.2 Procedures to manage, schedule, and document all planned changes to the system are applied to modifications of system components to maintain documented system availability, security, and integrity consistent with documented objectives, policies, and standards.	Procedures exist to initiate, review, and approve change requests. Changes to system components are assessed to determine their impact on system availability, security, and integrity objectives, policies, and standards. All requests for changes, system maintenance, and supplier maintenance are standardized and subject to formal change management procedures. Changes are categorized and ranked according to priority, and specific 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/test environment before implementation into production. The impact on system availability, security, and integrity objectives, policies, and standards of emergency changes or any deviation in change procedures is assessed before implementation. Backout plans are developed before implementation of changes. Software change management, control, and distribution are properly integrated with a comprehensive configuration management system. Correct software elements are distributed to the right place, with integrity, in a timely manner and with adequate audit trails.
M2.3 There are procedures to ensure that only authorized, tested, and documented changes are made to the system and related data.	Formal change control processes exist such that when system changes are implemented, the associated documentation and procedures are updated accordingly. Maintenance personnel have specific assignments and their work is properly monitored. In addition, their system access rights are controlled to avoid the risk of unauthorized access to systems and related data.

(*continued*)

Criteria	Illustrative Controls
	As part of the change control policies and procedures, there is a formal "promotion" process (for example, from "test" to "staging" to "production"). Changes to system infrastructure and software are developed and tested in a separate development/test environment before implementation into production. When changes are made to "mission critical" systems, there is a "back-out" plan for use in the event of major interruption(s). There is adequate off-site storage of maintenance resources, particularly program libraries, to enable reconstruction in the event of a loss of on-site resources. Senior management implements a division of roles and responsibilities that prevents a single individual from subverting a critical process. In particular, a segregation of duties is maintained among the following functions: • Computer operation • Network management • System administration • System development and maintenance • Change management • Security administration The level of user access (for example, read, add, change, or delete) is appropriate based on the user's job function and supports segregation of incompatible functions (for example, data entry is segregated from transaction review and approval). An assignment of responsibility is maintained that ensures that no single individual has the authority to read, add, change, or delete an information asset without an independent review of that activity.
M2.4 There are procedures to communicate planned and completed system changes to information systems management and to authorized users.	Annual budget resources are allocated for planned changes. There is periodic communication of changes.
M2.5 There are procedures to allow for and control emergency changes.	Emergency changes that require exception processing require appropriate management approval and leave an audit trail.

Criteria	Illustrative Controls
M3 The entity monitors the system and takes action to achieve compliance with maintainability objectives, policies, and standards.	
M3.1 System maintainability performance is periodically reviewed and compared with documented system maintainability requirements of authorized users and contractual, legal, and other service-level agreements.	Procedures exist for regular comparisons of existing system maintainability against objectives, policies, and standards and for reporting of the results. Variances are recorded and followed up.
	Requests for changes and system maintenance are standardized and subject to formal change management procedures. Changes are categorized and prioritized, and specific procedures are in place to handle urgent matters. Change requestors are kept informed of the status of their requests.
	The internal audit function includes system maintainability reviews in the annual audit plan.
	Problem logs are reviewed and trends are analyzed to identify the potential impact on system maintainability objectives.
M3.2 There is a process to identify potential impairments to the system's ongoing ability to address the documented system maintainability objectives, policies, and standards and to take appropriate action.	IT management seeks audit involvement in a proactive manner before finalizing IT service solutions.
	The responsibilities assigned to the quality assurance personnel include a review of general adherence to the information services function's standards and procedures.
	The quality assurance function reviews the extent to which particular systems and application development activities have achieved the objectives of the information services function.
	The quality assurance function prepares review reports and submits them to the management of the user departments and the information services function.
	The entity's SDLC methodology requires that a postimplementation review of operational information system requirements (for example, capacity, throughput) be conducted to assess whether the users' needs are being met by the system.

(*continued*)

Criteria	Illustrative Controls
	At least annually, users are involved in assessing whether specific systems meet their current and anticipated business needs. Where possible, this process includes a competitive analysis.
M3.3 Environmental and technological changes are monitored and their impact on system maintainability is periodically assessed on a timely basis.	A risk assessment has been prepared and is reviewed on a regular basis or when a significant change occurs in either the internal or external environment. Internal audit periodically prepares reports that compare actual maintenance and updating requirements to budgeted requirements and then analyzes the results. Before developing or changing the strategic IT plan, management of the information services function assesses the existing information systems in terms of degree of business automation, functionality, stability, complexity, cost, strengths, and weaknesses to determine the degree to which the existing systems support the entity's business requirements.

APPENDIX A

Examples of Practitioners' Reports

This appendix presents illustrative reports for SysTrust engagements. Examples 1 through 6 are prepared in accordance with the AICPA's attestation standards and examples 7 through 12 are prepared in accordance with the CICA's assurance standards or other relevant standards.

In all engagements, management prepares a system description that delineates the boundaries of the system covered by the practitioner's report. For engagements that require an assertion, management prepares an assertion that is attached to the practitioner's report.

A practitioner's report should conform to the applicable professional standards and the SysTrust license agreement.

Reports Based on AICPA Standards

Example 1—Reporting on an Assertion About the Effectiveness of Controls Based on AICPA Standards: Unqualified Opinion

Independent Accountant's Report

To [*Specify the party to whom the report is addressed*]:

We have examined the accompanying assertion by the management of ABC Corporation regarding the effectiveness of its controls over the availability, security, integrity, and maintainability of the Financial Services System during the period Month X, 200X, to Month XX, 200X, based on the SysTrust™ Principles and Criteria established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), which are available at www.aicpa.org/assurance.

This assertion is the responsibility of the management of ABC Corporation. Our responsibility is to express an opinion on the aforementioned assertion based on our examination.

Management's description of the aspects of the Financial Services System covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the AICPA and accordingly, included (1) obtaining an understanding of the controls related to the availability, security, integrity, and maintainability of the Financial Services System, (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.

Because of the inherent limitations of 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 changes made to the system or controls, changes in processing requirements, or the failure to make changes to the system when required may alter the validity of such conclusions.

In our opinion, management's assertion that ABC Corporation maintained effective controls over the availability, security, integrity, and maintainability of the Financial Services System to provide reasonable assurance that—

- The system was available for operation and use at times set forth in service-level statements or agreements,
- The system was protected against unauthorized physical and logical access,
- The system processing was complete, accurate, timely, and authorized, and
- The system could be updated when required in a manner that continued to provide for system availability, security, and integrity

during the period Month X, 200X, to Month XX, 200X, based on the SysTrust™ Principles and Criteria established by the AICPA and the CICA, is fairly stated in all material respects.

[*Signature*]

[*Date*]

Example 2—Reporting on the Subject Matter (the Effectiveness of Controls) Based on AICPA Standards: Unqualified Opinion

Independent Accountant's Report

To [*Specify the party to whom the report is addressed*]:

We have examined the accompanying assertion by the management of ABC Corporation regarding the effectiveness of its controls over the availability, security, integrity, and maintainability of the Financial Services System during the period Month X, 200X, to Month XX, 200X, based on the SysTrust™ Principles and Criteria established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), which are available at www.aicpa.org/assurance. This assertion is the responsibility of the management of ABC Corporation. Our responsibility is to express an opinion on the aforementioned assertion based on our examination.

Management's description of the aspects of the Financial Services System covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the AICPA and accordingly, included (1) obtaining an understanding of the controls related to the availability, security, integrity, and maintainability of the Financial Services System, (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.

Because of the inherent limitations of 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 changes made to the system or controls, changes in processing requirements, or the failure to make changes to the system when required may alter the validity of such conclusions.

In our opinion, ABC Corporation maintained effective controls over the availability, security, integrity, and maintainability of the Financial Services System to provide reasonable assurance that—

- The system was available for operation and use at times set forth in service-level statements or agreements,
- The system was protected against unauthorized physical and logical access,
- The system processing was complete, accurate, timely, and authorized, and
- The system could be updated when required in a manner that continued to provide for system availability, security, and integrity

during the period Month X, 200X, to Month XX, 200X, based on the SysTrust™ Principles and Criteria established by the AICPA and the CICA.

[*Signature*]

[*Date*]

Example 3—Reporting on the Subject Matter (the Effectiveness of Controls) Based on AICPA Standards: Qualified Opinion

Independent Accountant's Report

To [*Specify the party to whom the report is addressed*]:

We have examined the accompanying assertion by the management of ABC Corporation regarding the effectiveness of its controls over the availability, security, integrity, and maintainability of the Financial Services System during the period Month X, 200X, to Month XX, 200X, based on the SysTrust™ Principles and Criteria established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), which are available at www.aicpa.org/assurance. This assertion is the responsibility of the management of ABC Corporation. Our responsibility is to express an opinion on the aforementioned assertion based on our examination.

Management's description of the aspects of the Financial Services System covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the AICPA and accordingly, included (1) obtaining an understanding of the controls related to the availability, security, integrity, and maintainability of the Financial Services System, (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.

Because of the inherent limitations of 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 changes made to the system or controls, changes in processing requirements, or the failure to make changes to the system when required may alter the validity of such conclusions.

The SysTrust criteria require that a reliable system have continuity provisions that address minor processing errors, minor destruction of records, and major disruptions of system processing that might impair system availability. In the course of our examination, we noted that ABC Corporation had not fully implemented recovery plans addressing major disruptions of system processing. Accordingly, the criterion related to continuity provisions was not met.

In our opinion, except for the effects of the matter discussed in the preceding paragraph, ABC Corporation maintained effective controls over the availability, security, integrity, and maintainability of the Financial Services System to provide reasonable assurance that—

- The system was available for operation and use at times set forth in service-level statements or agreements,
- The system was protected against unauthorized physical and logical access,
- The system processing was complete, accurate, timely, and authorized, and
- The system could be updated when required in a manner that continued to provide for system availability, security, and integrity

during the period Month X, 200X, to Month XX, 200X, based on the SysTrust™ Principles and Criteria established by the AICPA and the CICA.

[*Signature*]

[*Date*]

Example 4—Reporting on an Assertion About the Effectiveness of Controls Over the Availability of a System Based on AICPA Standards

Independent Accountant's Report

To [*Specify the party to whom the report is addressed*]:

We have examined the accompanying assertion by the management of ABC Corporation regarding the effectiveness of its controls over the availability of the Financial Services System during the period Month X, 200X, to Month XX, 200X, based on the availability principle in the SysTrust™ Principles and Criteria established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), which are available at www.aicpa.org/assurance. This assertion is the responsibility of the management of ABC Corporation. Our responsibility is to express an opinion on the aforementioned assertion based on our examination.

The SysTrust™ Principles and Criteria include four principles: availability, security, integrity, and maintainability. This report covers only the availability principle and does not address the remaining three principles or the effect they may have on the availability principle. Management's description of the aspects of the Financial Services System covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the AICPA and accordingly, included (1) obtaining an understanding of the controls related to the availability of the Financial Services System, (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.

Because of the inherent limitations of 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 changes made to the system or controls, changes in processing requirements, or the failure to make changes to the system when required may alter the validity of such conclusions.

In our opinion, management's assertion that ABC Corporation maintained effective controls over the availability of the Financial Services System to provide reasonable assurance that the system was available for operation and use at times set forth in service-level statements or agreements during the period Month X, 200X, to Month XX, 200X, based on the availability principle of the SysTrust™ Principles and Criteria established by the AICPA and the CICA, is fairly stated in all material respects.

[*Signature*]

[*Date*]

Example 5—Reporting on an Assertion About the Suitability of the Design of Controls for Systems in the Preimplementation Phase Based on AICPA Standards

Independent Accountant's Report

To [*Specify the party to whom the report is addressed*]:

We have examined the accompanying assertion by the management of ABC Corporation regarding the suitability of the design of the controls over the availability, security, integrity, and maintainability of the Financial Services System as of Month XX, 200X, based on the SysTrust™ Principles and Criteria established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), which are available at www.aicpa.org/assurance. This assertion is the responsibility of the management of ABC Corporation. Our responsibility is to express an opinion on the aforementioned assertion based on our examination.

Management's description of the aspects of the Financial Services System covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the AICPA and accordingly, included (1) obtaining an understanding of the controls related to the availability, security, integrity, and maintainability of the Financial Services System, (2) evaluating the suitability of the design of the controls as of Month XX, 200X, 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.

Because of the inherent limitations of 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 changes made to the system or controls, changes in processing requirements, or the failure to make changes to the system when required may alter the validity of such conclusions.

The ABC system has not been placed in operation; accordingly, additional changes may be made to the design of the controls before the system is implemented. Furthermore, because the system has not yet been placed in operation, we were unable to and did not test the operating effectiveness of the controls.

In our opinion, management's assertion that the controls over the availability, security, integrity, and maintainability of the Financial Services System were suitably designed as of Month XX, 200X, based on the SysTrust™ Principles and Criteria established by the AICPA and the CICA, is fairly stated in all material respects.

[*Signature*]

[*Date*]

Example 6—Reporting on an Agreed-Upon Procedures Engagement Based on AICPA Standards

Independent Accountant's Report

To [*Specify the party to whom the report is addressed*]:

We have performed the procedures enumerated below, which were agreed to by the management of ABC Corporation and XYZ User Corporation, solely to assist you in evaluating certain controls over the availability of ABC Corporation's Financial Services System during the period Month X, 200X, to Month XX, 200X, based on the SysTrust™ Principles and Criteria established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) for the availability principle. ABC Corporation is responsible for controls over the availability of the Financial Services System. This agreed-upon procedures engagement was performed in accordance with standards established by the AICPA. The sufficiency of these procedures is solely the responsibility of the parties specified in this report. Consequently, we make no representation regarding the sufficiency of the procedures described below either for the purpose for which this report has been requested or for any other purpose.

[*Include paragraphs that enumerate the procedures and findings.*]

We were not engaged to, and did not, perform an examination, the objective of which is the expression of an opinion on the controls over the availability of ABC Corporation's Financial Services System during the period Month X, 200X, to Month XX, 200X, based on the SysTrusttm Principles and Criteria for the availability principle. 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 Corporation and XYZ User Corporation, and is not intended to be and should not be used by anyone other than these specified parties.

[*Signature*]

[*Date*]

Reports Based on CICA Standards

Example 7—Attest Report on the Effectiveness of Controls Based on CICA Standards: Report Without Reservation

Auditor's Report

To [*Specify the party to whom the report is addressed*]:

We have audited the accompanying assertion by the management of ABC Corporation regarding the effectiveness of its controls over the availability, security, integrity, and maintainability of the Financial Services System during the period Month X, 200X, to Month XX, 200X. This assertion is the responsibility of the management of ABC Corporation. Our responsibility is to express an opinion, based on our audit, on the conformity of management's assertion with the SysTrust™ Principles and Criteria established by the American Institute of Certified Public Accountants

(AICPA) and the Canadian Institute of Chartered Accountants (CICA), which are available at www.cica.ca.

Our audit was conducted in accordance with standards for assurance engagements established by the CICA. Those standards require that we plan and perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of the controls related to the availability, security, integrity, and maintainability of the Financial Services System, (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 audit provides a reasonable basis for our opinion.

In our opinion, management's assertion that ABC Corporation maintained effective controls over the availability, security, integrity, and maintainability of the Financial Service System to provide reasonable assurance that—

- The system was available for operation and use at times set forth in service-level statements or agreements,
- The system was protected against unauthorized physical and logical access,
- The system processing was complete, accurate, timely, and authorized, and
- The system could be updated when required in a manner that continued to provide for system availability, security, and integrity

during the period Month X, 200X, to Month XX, 200X, is fairly stated in all material respects in accordance with the SysTrust™ Principles and Criteria established by the AICPA and the CICA.

Management's description of the aspects of the Financial Services System covered by its assertion is attached. We did not audit this description, and accordingly, we do not express an opinion on it.

Because of the inherent limitations of 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 changes made to the system or controls, changes in processing requirements, or the failure to make changes to the system when required may alter the validity of such conclusions.

[Signature]

[Date]

Example 8—Direct Report on the Effectiveness of Controls Based on CICA Standards: Report Without Reservation

Auditor's Report

To [*Specify the party to whom the report is addressed*]:

We have audited the effectiveness of ABC Corporation's controls over the availability, security, integrity, and maintainability of the Financial Services System during the period Month X, 200X, to Month XX, 200X. The effectiveness of these controls is the responsibility of the management of ABC Corporation. Our responsibility is to express an opinion, based on our audit, on whether these controls were effectively maintained in accordance with the SysTrust™ Principles and Criteria established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), which are available at www.cica.ca.

Our audit was conducted in accordance with standards for assurance engagements established by CICA. Those standards require that we plan and perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of the controls related to the availability, security, integrity, and maintainability of the Financial Services System, (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 audit provides a reasonable basis for our opinion.

In our opinion, ABC Corporation maintained effective controls over the availability, security, integrity, and maintainability of the Financial Services System to provide reasonable assurance that—

- The system was available for operation and use at times set forth in service-level statements or agreements,
- The system was protected against unauthorized physical and logical access,
- The system processing was complete, accurate, timely, and authorized, and
- The system could be updated when required in a manner that continued to provide for system availability, security, and integrity

during the period Month X, 200X, to Month XX, 200X in accordance, in all material respects, with the SysTrust™ Principles and Criteria established by the AICPA and the CICA.

Management's description of the Financial Services System is attached. We did not audit this description, and accordingly, we do not express an opinion on it.

Because of the inherent limitations of 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 changes made to the system or controls, changes in processing requirements, or the failure to make changes to the system when required may alter the validity of such conclusions.

[Signature]

[Date]

Example 9—Direct Report on the Effectiveness of Controls Based on CICA Standards: Report With Reservation

Auditor's Report

To [*Specify the party to whom the report is addressed*]:

We have audited the effectiveness of ABC Corporation's controls over the availability, security, integrity, and maintainability of the Financial Services System during the period Month X, 200X, to Month XX, 200X. The effectiveness of these controls is the responsibility of the management of ABC Corporation. Our responsibility is to express an opinion, based on our audit, on whether these controls were effectively maintained in accordance with the SysTrust™ Principles and Criteria established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), which are available at www.cica.ca.

Our audit was conducted in accordance with standards for assurance engagements established by CICA. Those standards require that we plan and perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of the controls related to the availability, security, integrity, and maintainability of the Financial Services System, (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 audit provides a reasonable basis for our opinion.

The SysTrust™ criteria require that a reliable system have continuity provisions that address minor processing errors, minor destruction of records, and major disruptions of system processing that might impair system availability. In the course of our audit, we noted that ABC Corporation had not fully implemented recovery plans addressing major disruptions of system processing. Accordingly, the criterion related to continuity provisions was not met.

In our opinion, except for the effect of the failure to fully implement recovery plans described in the preceding paragraph, ABC Corporation maintained effective controls over the availability, security, integrity, and maintainability of the Financial Services System to provide reasonable assurance that—

- The system was available for operation and use at times set forth in service-level statements or agreements,
- The system was protected against unauthorized physical and logical access,

- The system processing was complete, accurate, timely, and authorized, and
- The system could be updated when required in a manner that continued to provide for system availability, security, and integrity

during the period Month X, 200X, to Month XX, 200X in accordance, in all material respects, with the SysTrust™ Principles and Criteria established by the AICPA and the CICA.

Management's description of the aspects of the Financial Services System is attached. We did not audit this description, and accordingly, we do not express an opinion on it.

Because of the inherent limitations of 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 changes made to the system or controls, changes in processing requirements, or the failure to make changes to the system when required may alter the validity of such conclusions.

[*Signature*]

[*Date*]

Example 10—Attest Report on an Assertion About the Effectiveness of Controls Over the Availability of a System Based on CICA Standards: Report Without Reservation

Auditor's Report

To [*Specify the party to whom the report is addressed*]:

We have audited the accompanying assertion by the management of ABC Corporation regarding the effectiveness of its controls over the availability of the Financial Services System during the period Month X, 200X, to Month XX, 200X. This assertion is the responsibility of the management of ABC Corporation. Our responsibility is to express an opinion, based on our audit, on the conformity of management's assertion with the availability principle of the SysTrust™ Principles and Criteria established by the American Institute of Certified Public

Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), which are available at www.cica.ca.

The SysTrust™ Principles and Criteria include four principles: availability, security, integrity, and maintainability. This report covers only the availability principle and does not address the remaining three principles.

Our audit was conducted in accordance with standards for assurance engagements established by the CICA. Those standards require that we plan and perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of the controls related to the availability of the Financial Services System, (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 audit provides a reasonable basis for our opinion.

In our opinion, management's assertion that ABC Corporation maintained effective controls over the availability of the Financial Service System to provide reasonable assurance that the system was available for operation and use at times set forth in service-level statements or agreements during the period Month X, 200X, to Month XX, 200X, is fairly stated, in all material respects, in accordance with the SysTrust™ Principles and Criteria established by the AICPA and the CICA.

Management's description of the aspects of the Financial Services System covered by its assertion is attached. We did not audit this description, and accordingly, we do not express an opinion on it.

Because of the inherent limitations of 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 changes made to the system or controls, changes in processing requirements, or the failure to make changes to the system when required may alter the validity of such conclusions.

[*Signature*]

[*Date*]

Example 11—Attest Report on an Assertion About the Suitability of the Design of Controls Based on CICA Standards: Report Without Reservation

Auditor's Report

To [*Specify the party to whom the report is addressed*]:

We have audited the accompanying assertion by the management of ABC Corporation regarding the suitability of the design of the controls over the availability, security, integrity, and maintainability of the Financial Services System as of Month XX, 200X. This assertion is the responsibility of the management of ABC Corporation. Our responsibility is to express an opinion, based on our audit, on the conformity of management's assertion with the SysTrust™ Principles and Criteria established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), which are available at www.cica.ca.

Our audit was conducted in accordance with standards for assurance engagements established by the CICA. Those standards require that we plan and perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of the controls related to the availability, security, integrity, and maintainability of the Financial Services System, (2) evaluating the suitability of the design of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, management's assertion that ABC Corporation suitably designed the controls over the availability, security, integrity, and maintainability of the Financial Service System as of Month XX, 200X, is fairly stated, in all material respects, in accordance with the SysTrust™ Principles and Criteria established by the AICPA and the CICA.

Management's description of the aspects of the Financial Services System covered by its assertion is attached. We did not audit this description, and accordingly, we do not express an opinion on it.

The ABC system has not been placed in operation; accordingly, additional changes may be made to the design of the controls before the system is implemented. Further, because the system has not yet been placed in operation, we were unable to and did not test the operating effectiveness of the controls.

Because of the inherent limitations of 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 changes made to the system or controls, changes in processing requirements, or the failure to make changes to the system when required may alter the validity of such conclusions.

[*Signature*]

[*Date*]

Example 12—Report on the Results of Performing Specified Auditing Procedures Related to the Availability of a System Based on CICA Standards

Accountant's Report on System Availability

To [*Specify the party to whom the report is addressed*]:

As specifically agreed to with the managements of ABC Corporation and XYZ User Corporation, we have performed the following procedures to assist in evaluating the conformity, during the period Month X, 200X, to Month XX, 200X, of certain controls of ABC Corporation's Financial Services System with the SysTrust Principle and Criteria for availability established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

[*List the procedures performed.*]

[*Use one of the following two paragraphs.*]

As a result of applying the above procedures, we found no instance of nonconformity with the SysTrust Principle and Criteria for availability.

[*or*]

As a result of applying the above procedures, we found the following instance(s) of nonconformity with the SysTrust Principle and Criteria for availability.

[*List instances of nonconformity.*]

However, these procedures do not constitute an audit of the conformity, during the period Month X, 200X, to Month XX, 200X, of the Financial Services Systems with the SysTrust Principle and Criteria for availability established by the AICPA and CICA, and accordingly we do not express an opinion on such conformity. 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 Corporation and XYZ User Corporation, and is not intended to be and should not be used by anyone other than these specified parties.

[*Signature*]

[*Date*]

APPENDIX B

Example of a System Description

System Description of ABC Corporation's Financial Services System

The purpose of a system description is to delineate the boundaries of the Financial Services System covered by management's assertion. The system description is attached to the practitioner's report.

ABC Corporation's data center (Data Center) supports the operation of the Financial Service System (FSS) on behalf of ABC's customers. FSS processes the following transactions for deposit and loan accounts:

- Deposit accounts (savings, checking, NOW, money market, CD, IRA, Keogh)
  - Opening and closing of accounts
  - Deposits
  - Withdrawals
  - Interest calculation and posting
  - Transfers
  - Statement rendering
  - 1099 processing
- Loan accounts (mortgage, construction, student, consumer, installment, commercial)
  - Opening and closing of accounts
  - Statement and coupon rendering
  - Cash receipts and lockbox
  - Cash applications (principal/interest/escrow)
  - Escrow maintenance and payments
  - Interest calculation and posting
  - 1099 processing

The accompanying SysTrust™ report covers the processing of FSS from the point transactions are received by the Data Center (via online input, or media transfer; for example, tape or paper input), through posting to master files and reporting to customers of ABC, or their ultimate customers. The following sections define the boundaries of each of the five system components that make up the FSS.

Infrastructure

The Data Center operates an IBM 3090-400J central processor under the control of an OS 390 operating system. Various peripheral devices, such as tape cartridge silos, disk drives, and laser and impact printers, are used with the central processor. Client terminals and automated teller machines are connected to the Data Center through leased lines. Clients may select, procure, and maintain terminal and printing equipment of their choosing.

Software

The FSS application was developed by the Data Center's house programming staff. FSS provides the ability to process savings, checking, NOW, money market, certificate of deposit, IRA, and Keogh deposit accounts, and loan accounts including mortgage, construction, student, consumer, installment, and commercial loans.

FSS allows online inquiry and memo-posting of transactions through terminals and accepts monetary and maintenance transactions for batch processing that is performed each night. In addition, the applications allow input from third-party data transmissions.

The Data Center also uses a variety of system software products to maintain the operating environment and networks.

Data

Data, as defined for the FSS, constitutes the following:

- Master file data
- Transaction data
- Error/suspense logs

- Output reports
- Transmission records
- System and security files

Transaction data is processed by FSS in either online or batch modes of processing, and is used to update master files. Output reports are available either in hard copy or through a report viewing facility available to all customers of ABC.

People

The Data Center employs a staff of approximately ninety employees who support FSS. The functional areas are briefly described below:

- *Technical Services*—Provides technical assistance to clients.
- *Application Programming*—Provides application software development and testing for enhancements and modifications to FSS.
- *Product Support Specialists*—Prepares documentation manuals and training material.
- *Quality Assurance*—Monitors compliance with standards, and manages and controls the change migration process.
- *Operational Services*—Performs day-to-day operation of the computer.
- *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 ACF2 security administration, and maintains policies and procedures manuals for the FSS processing environment.
- *Voice and Data Communications*—Maintains the communication environment, monitors the network and provides assistance to clients in resolving communication problems and network planning.

Procedures

The Data Center's performance objective is to be operational seven days a week, twenty-four hours a day. The Data Center Standards Manual addresses the following key processes:

- Systems development and program maintenance
- Security administration
- Computer operations
- Business recovery planning
- FSS processing

APPENDIX C

Example of Management's Assertion

ABC Corporation's Assertion Regarding the Effectiveness of Its Controls Over the Financial Services System Based on the SysTrust™ Principles and Criteria

ABC Corporation maintained effective controls over the availability, security, integrity, and maintainability of the Financial Services System to provide reasonable assurance that—

- The system was available for operation and use at times set forth in service-level statements or agreements,
- The system was protected against unauthorized physical and logical access,
- The system processing was complete, accurate, timely, and authorized, and
- The system could be updated when required in a manner that continued to provide for system availability, security, and integrity

during the period Month X, 200X, to Month XX, 200X, based on the SysTrust™ Principles and Criteria established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). The SysTrust™ Principles and Criteria are available at www.aicpa.org/assurance or www.cica.ca.

Our attached System Description of ABC Corporation's Financial Services System identifies the aspects of the Financial Services System covered by our assertion.

[*Signature Chief Financial Officer*]

[*Signature Chief Information Officer*]

[*Signature Chief Executive Officer*]

[*Date*]

APPENDIX D

How a SysTrust Engagement Differs From Certain Other Engagements

How a SysTrust Engagement Differs From a Service Auditor's Engagement

Professional standards currently exist for auditors to report on controls of service organizations (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), and the *CICA Handbook—Assurance* Section 5900, "Opinions on Control Procedures at a Service Organization." A SysTrust engagement differs from a service auditor's engagement in a number of ways. The following table highlights the differences and is followed by a further description of the differences.

	Service Auditors' Engagements		
	AICPA—SAS No. 70	**CICA Section 5900**	**SysTrust**
Nature of the engagement	Provides a report on a service organization's controls related to financial statement assertions of user organizations	Provides a report on the design and existence of control procedures or on the design, effective operation, and continuity of control procedures at a service organization	Provides a report on system reliability using standard principles and criteria for all engagements
Are there preestablished control objectives or criteria?	No	No	Yes
Objective of the engagement	Information sharing and assurance	Information sharing	Assurance on a system

(continued)

	Service Auditors' Engagements		
	AICPA—SAS No. 70	CICA Section 5900	SysTrust
	Provides detailed information on the design of the system and controls, and an opinion on the system description and controls	Provides information about stated internal control objectives of the system and the control procedures designed to achieve those objectives	No detail on the underlying control procedures is provided
Types of systems addressed by the engagement	Financial systems	Primarily financial systems	Financial and non-financial systems
Audience for the report	Service organizations, user organizations, and auditors of the user organizations	Service organizations, user organizations, and auditors of the user organizations	Stakeholders of the system—for example, management, customers, and business partners

SAS No. 70 Engagements

SAS No. 70 is applicable when an auditor is auditing the financial statements of an entity that obtains services from another organization, and those services are part of the entity's information system.[1] Examples of service organizations are bank trust departments that invest and service assets for employee benefit plans, mortgage bankers that service mortgages for others, and application service providers that provide packaged software applications and a technology environment that customers use to process financial and operational transactions. When a user organization uses a service organization, transactions that affect the user organization's financial statements are subjected to controls that are, at least in part, physically and operationally separate from the user organization. A service auditor's engagement is designed to provide information and assurance to the auditors of the financial statements of user organizations to enable those auditors to satisfy the requirement in SAS No. 55, *Consideration of Internal Control in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 2, AU sec. 319), to obtain

[1] SAS No. 70, Service Organizations, (AU sec. 324.03) describes factors that affect whether services are part of an entity's information system.

an understanding of the entity's internal control to plan the audit and to assess control risk. A service auditor's report is primarily an auditor-to-auditor communication. The service auditor stands in the shoes of the user auditors and performs procedures that the user auditors might perform. The service auditor issues a report on the service organization's description of controls and whether the controls were placed in operation, suitably designed, and operating effectively. The report is attached to a description of the system and controls and, in certain engagements, a description of the tests performed and the results of those tests. The user auditors read the description and the results of the tests to enable them to obtain an understanding of the entity's internal control and to assess control risk for the financial statement assertions of the entity being audited.

Section 5900 Engagements

The purpose of *CICA Handbook—Assurance* Section 5900 is to provide service auditors with guidance when undertaking engagements to examine the design and existence of control procedures, or the design, effective operation, and continuity of control procedures, at a service organization. Under the provisions of this section, a service auditor is not required to evaluate whether stated internal control objectives of the system are complete or in accordance with any accepted criteria or framework or whether they are presented fairly and are relevant to a user organization's internal control structure. Reports issued under *CICA Handbook—Assurance* Section 5900 are intended for the entity operating the specified system, users of its services, and their auditors. A *CICA Handbook—Assurance* Section 5900 report is attached to an accompanying description of the system and stated internal control objectives of the system of the service organization and the control procedures designed to achieve those objectives.

SysTrust Engagements

A SysTrust engagement is designed to provide users of the report with assurance about whether the entity has maintained effective controls over the reliability of a system. In a Sys-

Trust engagement, users do not receive a detailed description of the system as they do in a service auditor's engagement. However, they do receive a description of the boundaries of the system covered by the engagement, as presented in appendix B. In a SysTrust engagement, users do not receive a description of the organization's controls, the procedures performed by the practitioner, and the results of those procedures, as they do in a service auditor's engagement, Instead, they receive a report on the effectiveness of controls over the system for the SysTrust principles being reported on.

In the United States, the information contained in a SysTrust report do not meet the needs of a user organization's auditor under SAS No. 55 and should not be used by the user organization's auditor for that purpose. In Canada, the auditor of an enterprise using a service organization may consider whether a SysTrust report of the service organization's system would meet the auditor's needs under *CICA Handbook—Assurance* Section 5310, "Audit Evidence Considerations When an Enterprise Uses a Service Organization."

How a SysTrust Engagement Differs From a WebTrust Engagement

There are a number of similarities and differences between SysTrust and another AICPA/CICA assurance service, WebTrust^{SM}. These similarities and differences may require clarification in the marketplace so that potential buyers and users of the services appreciate the respective applicability of the services and their abilities to meet the assurance needs of prospective clients.

The names themselves suggest that these services are related. Also, the structure and even the content of WebTrust and SysTrust have a number of similarities. Both services are based on current attestation standards and identify the criteria against which controls are evaluated.

Following is a table highlighting the similarities and difference of the two engagements.

	WebTrust	SysTrust
Types of systems addressed by the engagement	Web-enabled systems	All systems
Subject matter of the engagement	Electronic commerce practices and controls over Internet-supported transactions	Effectiveness of controls over the reliability of a system.
Reporting method	Web site seal and a practitioner's report.	A practitioner's report. A Web site seal is not provided.
Audience for the report	Website management, customers, and business partners of Internet-based-e-commerce sites.	Stakeholders of the system—for example, management, customers, and business partners.
Additional uses of the service	May be used as a framework for the design and implementation of systems.	May be used as a framework for the design and implementation of systems.

Quality Control. Practitioner acknowledges that it has reviewed in detail AICPA Professional Standards, sections on *Statements on Quality Control Standards, Bylaws, Code of Professional Conduct and Ethics Rulings and Statement on Standards for Consulting Services* and will maintain possession of a current copy of same.

4. Records: Practitioner shall maintain, for three (3) years following the end of the calendar year in which it performs SysTrust Services, complete and accurate working papers documenting all examinations in which Practitioner issued Reports, and shall make these records available for inspection and copying by AICPA's representatives as reasonably requested.

5. Disclaimer: Use of the SysTrust Principles and Criteria and providing of SysTrust Services are at Practitioner's sole risk. The SysTrust Principles and Criteria are provided "as is," without warranty of any kind, and AICPA EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

6. Indemnity: Practitioner shall defend and indemnify AICPA from all claims, suits, damages and costs (including attorneys' fees) arising out of: (i) false advertising, fraud, misrepresentation or other claims related to Practitioner's SysTrust Services or use by Practitioner or its sublicensee of the SysTrust Marks, other than solely that the SysTrust Marks infringe third-party rights; or (ii) Practitioner's breach of this Agreement.

7. Practitioner Undertakings: Practitioner agrees not to: (i) directly or indirectly challenge AICPA's ownership of the SysTrust Marks or the validity of this license; (ii) consent to any third-party representation concerning the SysTrust Principles and Criteria or otherwise refer to the SysTrust Marks except in connection with Practitioner's SysTrust Services; (iii) infringe AICPA's copyrights in materials relating to the SysTrust Program, provided that Practitioner may, as a licensee hereunder, reproduce and distribute without charge the SysTrust Principles and Criteria to its employees, clients and prospective clients in complete and accurate form, including AICPA's copyright notice; or (iv) violate any laws, regulations or standards established by an entity of competent jurisdiction relating to the promotion or providing of SysTrust Services. Practitioner agrees that all Reports issued pursuant to this license shall identify the SysTrust Principles and Criteria as having been issued by AICPA/CICA.

8. Termination: AICPA shall have the right to terminate this Agreement if Practitioner fails to cure any of the following within fifteen (15) days of notice from AICPA: (i) Practitioner's license to practice accountancy is revoked or suspended; (ii) Practitioner is no longer a member in good-standing of AICPA and enrolled in an AICPA-approved practice-monitoring program; (iii) Practitioner misuses the SysTrust Marks or otherwise breaches a material term or undertaking of this Agreement; or (iv) Practitioner's sublicensee misuses of SysTrust Marks. Upon termination: (A) all rights, licenses and privileges granted to Practitioner, including the right to use the SysTrust Marks, shall automatically revert to AICPA; (B) Practitioner shall immediately cease to make any representation regarding its status as a licensee; and (C) Practitioner shall execute any and all documents evidencing such automatic reversion.

9. Applicable Law; Disputes: Any dispute or claim relating to this Agreement shall be settled by arbitration before three (3) arbitrators in the State and County of New York, under the Commercial Arbitration Rules of the American Arbitration Association then existing and applying the laws of the United States and of the State of New York, without giving effect to the conflict-of-laws principles thereof. Judgment upon the award may be entered into any court of competent jurisdiction. Nonetheless, either party may bring a civil action to seek equitable relief exclusively in the state and federal courts in the State and County of New York. The parties hereby submit to the exclusive jurisdiction of and waive any objection to the propriety or convenience of venue in such courts.

10. Assignment: Practitioner shall not license, sublicense or franchise its rights hereunder, nor transfer or assign this Agreement or any rights hereunder, except as specifically provided herein, without prior, written approval of AICPA. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the parties hereto, their successors and assigns.

11. Sole Understanding. This Agreement and the SysTrust Principles and Criteria, Attestation Standards and AICPA Professional Standards, sections on *Statements on Quality Control Standards, Bylaw, Code of Professional Conduct and Ethics Rulings and Statement on Standards for Consulting Services*, which are incorporated herein by reference, comprise the entire agreement of the parties with respect to the subject matter of this Agreement and supersede all other agreements, understandings and communications with respect thereto.

060467