1-1-2008

# Proposed statement on standards for attestation engagements: reporting on controls at a service organization; Exposure draft (American Institute of Certified Public Accountants), 2008, November 17

American Institute of Certified Public Accountants. Auditing Standards Board

# EXPOSURE DRAFT

# PROPOSED STATEMENT ON STANDARDS FOR ATTESTATION ENGAGEMENTS

## *REPORTING ON CONTROLS AT A SERVICE ORGANIZATION*

**(*To supersede the guidance for service auditors in AU section 324*, Service Organizations *[AICPA*, Professional Standards, *vol. 1])***

## November 17, 2008

## Comments are requested by February 17, 2009.

**Prepared by the AICPA Auditing Standards Board for comment from persons interested in auditing, attestation, and reporting issues.**

**Comments should be addressed to Sharon Macey at smacey@aicpa.org or Audit and Attest Standards, AICPA, 1211 Avenue of the Americas, New York, NY 10036-8775**

## EXPLANATORY MEMORANDUM

## CONTENTS

## EXPLANATORY MEMORANDUM

### Introduction

This memorandum provides background for the proposed Statement on Standards for Attestation Engagements (SSAE), *Reporting on Controls at a Service Organization.* The proposed SSAE would supersede the requirements and guidance for auditors reporting on controls at service organizations (service auditors) in AU section 324, *Service Organizations* (AICPA, *Professional Standards*, vol. 1). The guidance in AU section 324 for auditors of the financial statements of entities that use a service organization (user auditors) is being revised, renamed *Audit Considerations Relating to an Entity Using a Service Organization,* and retained in AU section 324. The proposed Statement on Auditing Standards (SAS) that would replace the guidance for user auditors is being exposed for comment concurrently with this proposed SSAE.

### How the Proposed SSAE Would Affect Existing Standards

The proposed SSAE would affect AU section 324 in the following ways:

- As a condition of engagement performance, management of the service organization would be required to provide the service auditor with a written assertion about (1) the fairness of the presentation of the description of the service organization's system, (2) the suitability of the design of the controls to achieve the related control objectives stated in the description, and, in a type 2 engagement, (3) the operating effectiveness of those controls to achieve the related control objectives stated in the description.

- A service auditor would be able to report on controls at a service organization other than controls that are relevant to user entities' financial reporting, for example, controls related to user entities' regulatory compliance, production, or quality control.

- In a type 2 report, the service auditor's opinion on the fairness of the presentation of the description of the service organization's system and on the suitability of the design of the controls would be for a period rather than as of a specified date, as it currently is in AU section 324.

- When obtaining an understanding of the service organization's system, the service auditor would be required to obtain information to identify risks that the description of the service organization's system is not fairly presented or that the control objectives stated in the description were not achieved due to intentional acts by service organization personnel.

- Indicates that when assessing the operating effectiveness of controls in a type 2 engagement, evidence obtained in prior engagements about the satisfactory operation of controls in prior periods does not provide a basis for a reduction in testing, even if supplemented with evidence obtained during the current period.

- A service auditor's type 2 report would identify the customers to whom use of the report is restricted as "customers of the service organization's system during some or all of the period covered by the service auditor's report," and in a service auditor's type 1 report, as, "customers as of the date of the service organization's description covered by the report."

## Background

### Clarity

To address concerns over the clarity, length, and complexity of its standards, the Auditing Standards Board (ASB) is undertaking a significant effort to clarify its standards.[1] In March 2007, the ASB issued a discussion paper, "Improving the Clarity of ASB Standards."[2] In response to the feedback received on the discussion paper and subsequent discussions with interested parties, the ASB established clarity drafting conventions and began to revise its standards in accordance with those conventions. The clarity drafting conventions include the following:

- Establishing objectives for each of the standards
- Including a definitions section in each standard, where relevant
- Separating requirements from application and other explanatory material
- Numbering application and other explanatory material paragraphs using an *A-* prefix and presenting them in a separate section that follows the requirements section
- Using formatting techniques, such as bulleted lists, to enhance readability
- Including, where appropriate, special considerations relevant to audits of smaller, less complex entities
- Including, where appropriate, special considerations relevant to audits of governmental entities

### Convergence

Consistent with the ASB's strategy to converge its standards with those of the International Auditing and Assurance Standards Board (IAASB),[3] the proposed SSAE has been drafted using the December 2007 exposure draft of International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Third Party Service Organization,* as a base. Differences between the proposed SSAE and the ISAE 3402 exposure draft, for which the ASB believes there is no compelling reason, have been eliminated. Any differences in objectives, definitions, or requirements between the proposed SSAE and the ISAE 3402 exposure draft are identified in exhibit E.

The ASB has made various changes to the language in the proposed ISAE, including replacing terms or phrases used in the proposed ISAE with those more commonly used in the United States, and tailoring examples and guidance so that they are more appropriate for the U.S. environment. Where the ASB believes that such changes in language have resulted in a substantive difference, these differences have been identified in exhibit E.

---

[1] The pamphlet, "Clarification and Convergence," provides information about the Auditing Standards Board's (ASB) clarity project and can be viewed at www.aicpa.org/download/auditstd/ASB_Clarity_%20and_Convergence_(8.5x11).pdf.

[2] The discussion paper, "Improving the Clarity of ASB Standards," can be viewed at www.aicpa.org/download/auditstd/Clarity_of_ASB_Standards_Discussion_Memo.pdf.

[3] The paper, "AICPA's Auditing Standards Board International Convergence Plan," can be viewed at www.aicpa.org/download/auditstd/ASB_Convergence_Plan.pdf.

**Issues for Consideration**

Effective Date

The ASB plans to make most of its clarified standards effective at the same time (no earlier than periods beginning on or after December 15, 2010). The effective date of the ISAE has not yet been determined. However, if the ISAE and the SSAE were to become effective at different times, two different standards resulting in two different reports, that frequently are used by auditors in multiple jurisdictions, would be available at the same time. To avoid the confusion that might result from that situation, the ASB has proposed making the SSAE effective concurrently with the ISAE. Accordingly, if the ISAE is effective for periods beginning earlier than December 15, 2010, the effective date for this proposed SSAE may be before, and not tied to, the effective date of the aforementioned proposed SAS, *Audit Considerations Relating to an Entity Using a Service Organization*. The ASB is seeking specific comments on an appropriate effective date. Should the effective date of the proposed SSAE precede the effective date of the other converged standards?

Management's Assertion

The proposed SSAE requires management of the service organization to provide the service auditor with a written assertion about the fair presentation of the description of the service organization's system, the suitability of the design of the controls and, in the case of a type 2 report, the operating effectiveness of the controls (an assertion-based engagement). Management's written assertion would accompany the description of the service organization's system, as required by paragraph 8(c) of the proposed SSAE. The ASB believes that an assertion-based engagement is more appropriate than the alternative, a direct-reporting engagement, in which the subject matter of the engagement is included in the service auditor's report, and no management assertion accompanies the report. An assertion-based engagement includes an explicit acknowledgement by management of its responsibility for the matters addressed in its assertion. Assertion-based engagements are prevalent in some jurisdictions; in others, direct-reporting engagements are more common.

It should be noted that the nature, timing, and extent of the service auditor's procedures ordinarily would be the same regardless of whether the engagement to report on controls at a service organization is an assertion-based or direct-reporting engagement. Further, in the case of a direct-reporting engagement, a service auditor would be required to obtain representations from management of the service organization that contain confirmations equivalent to the assertions outlined in the proposed SSAE. The ASB is seeking views on whether there are situations in which it would not be possible or practicable for management of the service organization to provide an assertion.

**Guide for Respondents**

In addition to the aforementioned specific areas on which the ASB is seeking comments, the ASB is seeking comments on the effect of applying the clarity drafting conventions to the proposed SSAE and of converging it with the ISAE 3402 exposure draft. Respondents are asked to comment in particular on the appropriateness of

1. the objectives stated in the proposed SSAE to be achieved by the service auditor.

2. the revisions made to the existing standard to converge it with the ISAE 3402 exposure draft.

3. the differences between the proposed SSAE and the ISAE 3402 exposure draft identified in exhibit E, and other language changes.

4. the manner in which considerations for audits of smaller, less complex entities and governmental entities have been dealt with.

Comments are most helpful when they refer to specific paragraphs, include the reasons for the comments, and, where appropriate, make specific suggestions for any proposed changes to wording. When a respondent agrees with proposals in the exposure draft, it is helpful if the ASB is made aware of this view.

The comment period for the exposure draft ends on February 17, 2009. Written comments on the exposure draft will become part of the public record of the AICPA and will be available for public inspection at the offices of the AICPA after March 17, 2009, for one year. Responses should be sent to Sharon Macey at smacey@aicpa.org or mailed to Audit and Attest Standards, AICPA, 1211 Avenue of the Americas, New York, NY 10036-8775 in time to be received by February 17, 2009.

**Supplement to the Exposure Draft**

To assist respondents in commenting on the proposed SSAE, the Audit and Attest Standards staff has prepared the following supplementary material:

- A table comparing the ISAE 3402 exposure draft to the proposed SSAE. The table is a paragraph-by-paragraph comparison that contains the following four columns:

  1. The December 2007 exposure draft of ISAE 3402

  2. A marked draft of the ISAE 3402 exposure draft showing changes made to that draft to arrive at the proposed SSAE

  3. The related paragraphs in extant AU section 324

  4. Explanations of substantive changes to the ISAE 3402 ED and other comments

- A table showing how the paragraphs in extant AU section 324, *Service Organizations*, are reflected in the proposed SAS and in the proposed SSAE. This table is a paragraph-by-paragraph comparison that contains the following three columns:

  1 The paragraphs in extant AU section 324

  2. The related paragraphs in the proposed SAS and in the proposed SSAE

  3. Comments and explanations

This staff-prepared supplementary material is for informational purposes only and is not a part of the exposure draft. However, it may be useful to respondents in formulating comments and is available on the AICPA Web site at www.aicpa.org/Professional+Resources/Accounting+and+Auditing/Audit+and+Attest+Standards/Improving+the+Clarity+of+ASB+Standards.htm.

**Comment Period**

The comment period for this exposure draft ends on February 17, 2009.

## Auditing Standards Board
**(2007–2008)**

Harold L. Monk, Jr., *Chair*
Sheila M. Birch
Jacob J. Cohen
Walton T. Conn, Jr.
Anthony J. Costantini
Robert D. Dohrer
Charles E. Frazier
Nicholas J. Mastracchio, Jr.
Jorge Milo
Andrew M. Mintzer
Keith O. Newton
Patricia P. Piteo
Douglas F. Prawitt
Randy C. Roberts
Darrel R. Schubert
Thomas M. Stemlar
Stephanie A. Westington
Arthur M. Winstead, Jr.
Megan F. Zietsman

## Service Organizations Task Force

George H. Tucker, *Chair*
Walton T. Conn, Jr.
Robert Dacey
Susan Jones
Susan E. Kenney
James R. Merrill
Suzanne Nersessian
Thomas Wallace
Megan F. Zietsman

## AICPA Staff

Charles E. Landes
*Vice President*
*Professional Standards and Services*

Judith M. Sherinsky
*Technical Manager*
*Audit and Attest Standards*

**PROPOSED STATEMENT ON STANDARDS FOR ATTESTATION ENGAGEMENTS,**
***REPORTING ON CONTROLS AT A SERVICE ORGANIZATION***

**CONTENTS**

**Proposed Statement on Standards for Attestation Engagements,**
***Reporting on Controls at a Service Organization***

## Introduction

### Scope of this Statement on Standards for Attestation Engagements

**1**. This Statement on Standards for Attestation Engagements (SSAE) addresses examination engagements undertaken by a service auditor to report on controls at organizations that provide services to user entities when those controls are likely to be part of the user entities' information and communication systems relevant to financial reporting. It complements proposed AU section 324, *Audit Considerations Relating to an Entity Using a Service Organization* (AICPA, *Professional Standards*, vol. 1), in that reports prepared in accordance with this SSAE may provide appropriate evidence under AU section 324.

**2**. The focus of this SSAE is on engagements to report on controls at service organizations relevant to financial reporting by user entities. It also may be applied, adapted as necessary, to engagements to report on

*a*. a service organization's controls other than those that are part of user entities' information and communication systems relevant to financial reporting, for example, controls that affect user entities' regulatory compliance,[1] production, or quality control.

*b*. controls at a shared service center that provides services to a group of related entities.

**3**. In addition to performing an examination of a service organization's controls, a service auditor may be engaged to (*a*) report on a user entity's transactions or balances[2] maintained by a service organization, or (*b*) perform agreed upon procedures[3] related to the controls of a service organization or to transactions or balances of a user entity maintained by a service organization. However, these engagements are not dealt with in this SSAE.

**4**. Paragraph .09 of AT section 101, *Attest Engagements* (AICPA, *Professional Standards*, vol. 1), indicates that a practitioner may report on either management's written assertion or directly on the subject matter to which it relates. The reporting guidance in this SSAE is based on the premise that management will provide the service auditor with a written assertion that is included in management's description of the service organization's system, except in the circumstances described in paragraph 9 of this SSAE.

### Effective Date

**5**. This SSAE is effective for service auditors' reports for periods beginning on or after [*date*]. [*] Earlier implementation is permitted.

### Objectives

[1] AT section 601, *Compliance Attestation* (AICPA, *Professional Standards*, vol. 1), of Statements on Standards for Attestation Engagements (SSAE) is applicable if a practitioner is reporting on an entity's own regulatory compliance.
[2] Paragraphs .11–.13 of AU section 623, *Special Reports* (AICPA, *Professional Standards*, vol. 1), address engagements to report on specified elements, accounts, or items of a financial statement.
[3] AT section 201, *Agreed-Upon Procedures Engagements* (AICPA, *Professional Standards*, vol. 1), addresses engagements in which a practitioner reports on agreed upon procedures.
[*] See the discussion of the effective date under "Issues for Consideration."

**6**. The objectives of the service auditor are to

*a*. obtain reasonable assurance about whether, in all material respects, based on suitable criteria[4]

(1) management's description of the service organization's system is fairly presented.

(2) the controls are suitably designed to achieve the control objectives stated in management's description of the service organization's system.

(3) when included in the scope of the engagement, the controls operated effectively throughout the specified period to achieve the control objectives stated in management's description of the service organization's system.

*b*. report in accordance with the service auditor's findings.

**Definitions**

**7.** For purposes of this SSAE, the following terms have the meanings attributed in the subsequent text:

**Carve-out method.** Method of dealing with the services provided by a subservice organization whereby the description of the service organization's system identifies the nature of the services performed by the subservice organization and excludes from the description and from the scope of the service auditor's engagement, the subservice organization's relevant control objectives and related controls. The description of the service organization's system and the scope of the service auditor's engagement include controls at the service organization for monitoring the effectiveness of controls at the subservice organization, which may include the service organization's review of a service auditor's report on controls at the subservice organization.

**Complementary user entity controls.** Controls that the service organization assumes, in the design of its service, will be implemented by user entities, and which, if necessary to achieve the control objectives stated in the description of the service organization's system, are identified as such in that description.

**Control objectives.** The aim or purpose of specified controls at the service organization. Control objectives ordinarily address the risks that controls are intended to mitigate. In the context of internal control over financial reporting, a control objective generally relates to one or more relevant assertions for a significant account or disclosure in user entities' financial statements and addresses the risk that the controls in a specific area will not provide reasonable assurance that a misstatement or omission in that relevant assertion is prevented or detected and corrected on a timely basis.

**Controls at a service organization.** The policies and procedures at a service organization that are likely to be relevant to user entities' internal control over financial reporting. These policies and procedures are designed, implemented, and maintained by the service organization to provide reasonable assurance about the achievement of the control objectives relevant to the services covered by the service auditor's report (Ref: par. A1)

**Controls at a subservice organization.** The policies and procedures designed, implemented, and maintained by a subservice organization to provide reasonable assurance about the

achievement of control objectives that are relevant to the services covered by the service auditor's report.

**Criteria.** The standards or benchmarks used to measure and present the subject matter and against which the service auditor evaluates the subject matter. Management is responsible for selecting the criteria. Suitable criteria are required for reasonably consistent evaluation or measurement of a subject matter. Criteria need to be available to the intended users to enable them to understand how the subject matter has been evaluated or measured. Information about suitable criteria is provided in paragraphs .23–.34 of AT section 101. Paragraphs 15–17 of this SSAE discuss the criteria for evaluating the fairness of the presentation of management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls.

**Inclusive method.** Method of dealing with the services provided by a subservice organization whereby the service organization's description of its system includes a description of the nature of the services provided by the subservice organization as well as the subservice organization's relevant control objectives and related controls included in the scope of the service auditor's engagement. (Ref: par. A2)

**Internal audit function.** The service organization's internal auditors and others (for example, a compliance or risk department) who perform activities similar to those performed by internal auditors.

**Report on a description of a service organization's system and the suitability of the design of controls** (referred to in this SSAE as a *type 1 report*). (Ref: par. A3). A report that comprises

*a.* a description of the service organization's system prepared by management of the service organization.

*b.* a written assertion by the service organization's management about whether, in all material respects, and based on suitable criteria

(1) the description of the service organization's system fairly presents the service organization's system that was designed and implemented as of a specified date.

(2) the controls related to the control objectives stated in the description were suitably designed to achieve those control objectives as of the specified date.

*c.* a service auditor's report that expresses an opinion on the matters in *b*1–2.

**Report on a description of a service organization's system and the suitability of the design and operating effectiveness of controls** (referred to in this SSAE as a *type 2 report*) (Ref: par. A3). A report that comprises

*a.* a description of the service organization's system prepared by management of the service organization.

*b.* a written assertion by the service organization's management, about whether in all material respects, and based on suitable criteria

(1) the description of the service organization's system fairly presents the service organization's system that was designed and implemented throughout the specified period.

(2) the controls related to the control objectives stated in the description of the service organization's system were suitably designed throughout the specified period to achieve those control objectives.

(3) the controls related to the control objectives stated in the description of the service organization's system operated effectively throughout the specified period to achieve those control objectives.

*c*. a service auditor's report that

(1) expresses an opinion on the matters in *b*1–3.

(2) includes a description of the service auditor's tests of controls and the results thereof.

**Service auditor.** A practitioner who reports on controls at a service organization.

**Service organization.** An organization or segment of an organization that provides services to user entities that are part of those user entities' information and communication systems relevant to financial reporting.

**Service organization's system.** The policies and procedures designed, implemented, and maintained by the service organization to provide user entities with the services covered by the service auditor's report. The description of the service organization's system, prepared by management of the service organization, identifies the services covered, the period to which the description relates, the control objectives specified by management or an outside party, the party specifying the control objectives (if not specified by management), and the related controls.

**Subservice organization.** A service organization used by another service organization to perform some of the services provided to user entities that are part of those user entities' information and communication systems relevant to financial reporting.

**Test of controls.** A procedure designed to evaluate the operating effectiveness of controls in preventing or detecting and correcting deficiencies in internal control that could result in the nonachievement of the control objectives stated in the description of the service organization's system.

**User auditor.** An auditor who audits and reports on the financial statements of a user entity.

**User entity.** An entity that uses a service organization.

**Requirements**

**Acceptance and Continuance** (Ref: par. A4–A6)

**8.** Unless the service auditor is required by law or regulation to continue (or accept as applicable) an engagement to report on controls at a service organization, the service auditor should continue (or accept as applicable) a service auditor's engagement only if

*a.* the service auditor's preliminary knowledge of the engagement circumstances indicates that

(1) the criteria to be used will be suitable and available to the intended users;

(2) the service auditor will have access to sufficient, appropriate evidence to the extent necessary; and

(3) the scope of the engagement and the description of the service organization's system will not be so limited that they are unlikely to be useful to user entities and their auditors.

*b.* in agreeing to the terms of the engagement, management of the service organization acknowledges and accepts responsibility for the following:

(1) Preparing and presenting the description of the service organization's system and the accompanying assertion, including the completeness, accuracy, and method of presentation of the description and assertion

(2) Selecting the criteria used and stating them in the assertion

(3) Specifying the control objectives, stating them in the description of the service organization's system, and, if the control objectives are specified by law, regulation, or another party (for example, a user group or a professional body), identifying in the description the party specifying the control objectives

(4) Identifying the risks that threaten the achievement of the control objectives

(5) Designing, implementing, and maintaining controls to provide reasonable assurance that the control objectives stated in the description of the service organization's system will be achieved

(6) Providing the service auditor with the following:

(a) All information relevant to the preparation and presentation of the description of the service organization's system and accompanying assertion, such as information contained in records and documentation

(b) Any additional relevant information that the service auditor may request

(c) Unrestricted access to personnel within the service organization from whom the service auditor determines it is necessary to obtain evidence relevant to the service auditor's engagement

(d) Written representations at the conclusion of the engagement

*c.* Management of the service organization provides a written assertion that will accompany the description of the service organization's system provided to user entities (Ref: par. A5).

**9.** If management subsequently refuses to furnish a written assertion, the service auditor should withdraw from the engagement. If law or regulation does not allow the service auditor to withdraw from the engagement, the service auditor should disclaim an opinion.

**10**. When the service auditor plans to disclaim an opinion, the limited procedures performed by the service auditor may cause the service auditor to conclude that certain aspects of the description of the service organization's system are not fairly presented in all material respects; that certain controls were not suitably designed to provide reasonable assurance that the control objectives stated in the description would be achieved if the controls operated as described; or, in the case of a type 2 report, certain controls did not operate effectively throughout the specified period to achieve the control objectives stated in the description. In such instances, the service auditor's report also should identify the aspects of the description that are not fairly presented; the controls that were not suitably designed to achieve the control objectives stated in the description; and, in the case of a type 2 report, the controls that were not

operating effectively throughout the specified period to achieve the control objectives stated in the description.

**11.** The service auditor's inability to obtain a written assertion from management represents a scope limitation. When disclaiming an opinion because of a scope limitation, the service auditor should state that he or she does not express an opinion on the fairness of the presentation of the description of the service organization's system or on the suitability of the design or operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description. In a separate paragraph of the service auditor's report, the service auditor should state the substantive reasons for the disclaimer. The auditor should not identify the procedures that were performed nor include statements describing the characteristics of a service auditor's engagement; to do so might overshadow the disclaimer.

**12**. If management requests a change in the scope of the engagement before the completion of the engagement, the service auditor should be satisfied, before agreeing to the change, that there is reasonable justification for the change (Ref: par. A4).

**13.** If management of the service organization will not provide the service auditor with a written assertion, this SSAE precludes the service auditor from performing a service auditor's engagement under AT section 101, *Attest Engagements* (Ref: par. A5).

**Assessing the Suitability of the Criteria** (Ref: par. A7–A8)

**14.** As required by paragraph .23 of AT section 101, the service auditor should assess whether management has used suitable criteria in preparing and presenting the description of the service organization's system; evaluating whether controls were suitably designed to achieve the control objectives stated in the description; and in the case of a type 2 report, evaluating whether controls operated effectively throughout the specified period to achieve the control objectives stated in the description.

**15.** Suitable criteria for evaluating whether the description of the service organization's system is fairly presented should include, at a minimum, whether the description

*a.* presents how the service organization's system made available to user entities was designed and implemented to process relevant transactions, including the following information about the service organization's system:

(1) The classes of transactions processed

(2) The procedures, within both automated and manual systems, by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and reported to user entities

(3) The related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities

(4) How the service organization's system captures significant events and conditions, other than transactions

(5) The process used to prepare reports provided to user entities

(6) The specified control objectives and controls designed to achieve those objectives

(7) Other aspects of the service organization's control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to achieving the control objectives stated in the description of the service organization's system.

*b.* does not omit or distort information relevant to the scope of the service organization's system, while acknowledging that the description of the service organization's system is presented to meet the common needs of a broad range of user entities and their auditors, and may not, therefore, include every aspect of the service organization's system that each individual user entity and its auditor may consider important in its own particular environment.

**16.** Suitable criteria for evaluating whether controls are suitably designed to provide reasonable assurance that the control objectives stated in the description of the service organization's system would be achieved if the controls operated effectively should include, at a minimum, whether

*a.* the risks that threaten the achievement of the control objectives stated in the description have been identified.

*b.* the identified controls would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

**17.** Suitable criteria for evaluating whether controls operated effectively to provide reasonable assurance that the control objectives stated in the description of the service organization's system would be achieved should include, at a minimum, whether the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

**Materiality** (Ref: par. A9–A10)

**18.** When planning and performing the engagement, the service auditor should evaluate materiality with respect to the fair presentation of the description of the service organization's system, the suitability of the design of controls to achieve the related control objectives stated in the description and, in the case of a type 2 report, the operating effectiveness of the controls to achieve the related control objectives stated in the description.

**Using the Work of an Internal Audit Function**

*Obtaining an Understanding of the Internal Audit Function* (Ref: par. A11–A12)

**19.** The service auditor should obtain an understanding of the aspects of the internal audit function that are relevant to the engagement.

*Planning to Use the Work of the Internal Audit Function*

**20**. When the service auditor intends to use the work of the internal audit function, the service auditor should evaluate the following:

*a.* The objectivity and technical competence of members of the internal audit function

*b.* Whether the internal audit function is carried out with due professional care

*c.* The effect of any constraints or restrictions placed on the internal audit function by management or those charged with governance

**21**. In making judgments about the effect of the internal audit function's work on the service auditor's procedures, the service auditor should evaluate the following:

*a.* The significance of that work to the service auditor's conclusions

*b.* The degree of subjectivity involved in the evaluation of the evidence gathered in support of those conclusions

*Using the Work of the Internal Audit Function*

**22.** When the service auditor uses specific work of the internal audit function or the internal audit function provides direct assistance to the service auditor, the service auditor should perform procedures to evaluate the adequacy of that work.

**23.** When evaluating specific work performed by the internal audit function, the service auditor should consider the adequacy of the scope of the work and whether the evaluation of the internal audit function remains appropriate. The service auditor should evaluate whether

*a.* the work is performed by persons having appropriate skill and expertise.

*b.* the work is properly supervised, reviewed, and documented.

*c.* sufficient, appropriate evidence is obtained to be able to draw reasonable conclusions.

*d.* conclusions reached are appropriate in the circumstances, and any reports prepared are consistent with the results of the work performed.

*e.* any exceptions or unusual matters disclosed by the internal audit function are properly resolved.

*Effect on the Service Auditor's Report*

**24.** If the work of the internal audit function has been used, the service auditor should make no reference to that work in the service auditor's opinion. Notwithstanding its degree of autonomy and objectivity, the internal audit function is not independent of the service organization. The service auditor has sole responsibility for the opinion expressed in the service auditor's report and, accordingly, that responsibility is not reduced by the service auditor's use of the work of the internal audit function.

**25.** In the case of a type 2 report, if the work of the internal audit function has been used in performing tests of controls, the service auditor's description of tests of controls and results thereof should include a description of the internal auditor's work and of the service auditor's procedures with respect to that work.

**Using the Work of a Service Auditor's Specialist**

*The Capabilities, Competence, and Objectivity of the Service Auditor's Specialist*

**26.** If the service auditor intends to use the work of a specialist, the service auditor should evaluate whether the service auditor's specialist has the necessary capabilities, competence, and objectivity for the service auditor's purposes. In evaluating the specialist's objectivity, the service auditor should inquire about interests and relationships that may create a threat to that specialist's objectivity.

*Obtaining an Understanding of the Field of Expertise of the Service Auditor's Specialist*

**27.** The service auditor should obtain a sufficient understanding of the field of expertise of the service auditor's specialist to enable the service auditor to

*a.* determine the nature, scope, and objectives of that specialist's work for the service auditor's purposes.

*b.* evaluate the adequacy of that work for the service auditor's purposes.

*Establishing an Understanding With the Service Auditor's Specialist*

**28.** The service auditor should establish a written understanding with the service auditor's specialist regarding the following matters:

*a.* The nature, scope, and objectives of that specialist's work

*b.* The respective roles of the service auditor and that specialist

*c.* The nature, timing, and extent of communication between the service auditor and that specialist, including the form of any report to be provided by that specialist

*Evaluating the Adequacy of the Work of the Service Auditor's Specialist*

**29**. The service auditor should evaluate the adequacy of the work of the service auditor's specialist for the service auditor's purposes.

*Effect on the Service Auditor's Report*

**30.** If the work of the service auditor's specialist has been used, the service auditor should make no reference to that work in the section of the service auditor's report that contains the service auditor's opinion. The service auditor has sole responsibility for the opinion expressed in the service auditor's report and, accordingly, that responsibility is not reduced by the service auditor's use of the work of a service auditor's specialist.

**Obtaining an Understanding of the Service Organization's System**
(Ref: par. A13–A19)

**31.** The service auditor should obtain an understanding of the service organization's system, including controls that are included in the scope of the engagement (Ref: par. A13–A14).

**32.** When obtaining an understanding of the service organization 's system, the service auditor should obtain information for use in identifying risks that the description of the service organization's system is not fairly presented or that the control objectives stated in that description were not achieved due to intentional acts by service organization personnel (Ref: par. A15–A19).

**Obtaining Evidence Regarding the Description of the Service Organization's System** (Ref: par. A20–A24)

**33.** The service auditor should obtain and read the description of the service organization's system and should evaluate whether those aspects of the description that are included in the scope of the engagement are presented fairly, including whether

*a.* the control objectives stated in the description are reasonable in the circumstances.

*b.* controls identified in the description were implemented.

*c.* complementary user entity controls, if any, are adequately described.

*d.* services performed by a subservice organization, if any, are adequately described, including whether the inclusive method or the carve-out method has been used.

**34.** The service auditor should determine, through inquiries of management and other service organization personnel in combination with other procedures, whether the service organization's system described in management's description has been implemented.

**Obtaining Evidence Regarding the Design of Controls** (Ref: par. A25–A27)

**35.** The service auditor should determine which of the controls at the service organization are necessary to achieve the control objectives stated in the description of the service organization's system and should assess whether they were suitably designed to achieve those control objectives by

*a.* identifying the risks that threaten the achievement of the control objectives stated in the description.

*b.* evaluating the linkage of the controls identified in the description with those risks.

**Obtaining Evidence Regarding the Effectiveness of Controls** (Ref: par. A28–A34)

**36.** When performing a type 2 engagement, the service auditor should test those controls that the service auditor has determined are necessary to achieve the control objectives stated in the description of the service organization's system and should assess their operating effectiveness throughout the period. Evidence obtained in prior engagements about the satisfactory operation of controls in prior periods does not provide a basis for a reduction in testing, even if it is supplemented with evidence obtained during the current period.

**37.** The service auditor should inquire about changes in the service organization's controls that were implemented during the period covered by the service auditor's report. If the service auditor believes the changes would be considered significant by user entities and their auditors, those changes should be included in the description of the service organization's system. If such changes are not included in the description, the service auditor should describe the changes in his or her report. If the superseded controls are relevant to the achievement of the control objectives stated in the description, the service auditor should determine from management whether it is possible for the controls to be tested before and after the change, and if it is not possible, to determine the effect on the service auditor's report.

**38.** When designing and performing tests of controls, the service auditor should

*a.* perform other procedures in combination with inquiry to obtain evidence about the following:

(1) How the control was applied

(2) The consistency with which the control was applied

(3) By whom or by what means the control was applied

*b.* determine whether the controls to be tested depend on other controls, and if so, whether it is necessary to obtain evidence supporting the operating effectiveness of those other controls.

*c.* determine an effective method for selecting the items to be tested to meet the objectives of the procedure.

**39.** When determining the extent of tests of controls and whether sampling is appropriate, the service

auditor should consider the characteristics of the population of the controls to be tested, including the nature of the controls, the frequency of their application (for example, monthly, daily, many times per day), and the expected rate of deviation. If the service auditor determines that sampling is appropriate, the service auditor should refer to AU section 350, *Audit Sampling* (AICPA, *Professional Standards*, vol.1).

*Nature and Cause of Deviations*

**40.** The service auditor should investigate the nature and cause of any deviations identified, including considering whether the deviations may be the result of intentional acts by service organization personnel and should determine whether

*a.* identified deviations are within the expected rate of deviation and are acceptable. If so, the testing that has been performed provides an appropriate basis for concluding that the control operated effectively throughout the specified period.

*b.* additional testing of the control or of compensating controls is necessary to reach a conclusion about whether the controls related to the control objectives stated in the description of the service organization's system operated effectively throughout the specified period. Compensating controls, if effective, may limit the severity of a deficiency and prevent it from being a significant deficiency or a material weakness.

*c.* the testing that has been performed provides an appropriate basis for concluding that the control did not operate effectively throughout the specified period.

**41.** When the service auditor considers a deviation discovered in a sample to be an anomaly, and no compensating controls have been identified, the service auditor should obtain a high degree of certainty that such deviation is not representative of the population. The service auditor should obtain this degree of certainty by performing additional procedures to obtain sufficient, appropriate evidence that such deviations do not exist in the remainder of the population.

**Written Representations** (Ref: par. A35–A37)

**42.** The service auditor should ask management to provide written representations, based on its knowledge and belief

*a.* that reaffirm the assertion accompanying the description of the service organization's system.

*b.* about whether all records, documentation, unusual matters of which they are aware, and other information relevant to the engagement have been made available to the service auditor.

*c.* that they have disclosed to the service auditor any of the following of which they are aware:

(1) Instances of noncompliance with laws and regulations or uncorrected errors attributable to the service organization's management or employees that may affect one or more user entities

(2) Knowledge of any actual, suspected, or alleged intentional acts by the service organization's management or employees, such as overrides of controls or misappropriation of user entity assets, that could adversely affect the fairness of the presentation of the description of the service organization's system or the completeness or achievement of the control objectives stated in the description

(3) Design deficiencies in controls, including those for which management believes the cost of corrective action may exceed the benefits

(4) Instances where controls have not operated as described

(5) Subsequent events regarding the services covered by the engagement that could have a significant effect on user entities

**43.** If a service organization uses a subservice organization, and the description of the service organization's system uses the inclusive method, the service auditor also should obtain the written representations identified in paragraph 42 from management of the subservice organization.

**44.** These written representations should be in the form of a representation letter addressed to the service auditor and should be as of the same date as the date of the service auditor's report.

**45.** If management does not provide one or more of the written representations requested by the service auditor, the service auditor should

*a*. discuss the matter with management.

*b.* consider the assessment of the integrity of management and determine the effects on the engagement.

*c.* take appropriate actions, including determining the possible effect on the opinion in the service auditor's report (also see paragraph .62 of AT section 101).

### Other Information

**46.** The service auditor should read other information, if any, included in a document containing the description of the service organization's system and the service auditor's report to identify material inconsistencies, if any, with that description. While reading the other information for the purpose of identifying material inconsistencies, the service auditor may become aware of an apparent misstatement of fact in the other information.

**47.** If the service auditor becomes aware of a material inconsistency or an apparent misstatement of fact in the other information, the service auditor should discuss the matter with management. If the service auditor concludes that there is a material inconsistency or a misstatement of fact in the other information that management refuses to correct, the service auditor should take further appropriate action.

### Subsequent Events

**48.** The service auditor should inquire whether management is aware of any events subsequent to the period covered by the description of the service organization's system up to the date of the service auditor's report that could have a significant effect on the controls at the service organization or on the service auditor's report. If so, and information about that event is not disclosed by the service organization in its description, the service auditor should disclose it in the service auditor's report.

**49.** The service auditor has no obligation to perform any procedures regarding the description of the service organization's system or the suitability of the design or operating effectiveness of the controls after the date of the service auditor's report.

### Documentation

**50.** The service auditor should prepare documentation that would enable an experienced service auditor, having no previous connection with the engagement, to understand the following:

*a.* The nature, timing, and extent of the procedures performed to comply with this SSAE and with applicable legal and regulatory requirements

*b.* The results of the procedures and the evidence obtained

*c.* Significant matters arising during the engagement, the conclusions reached thereon, and significant professional judgments made in reaching those conclusions

**51.** In documenting the nature, timing, and extent of procedures performed, the service auditor should record the following:

*a.* The identifying characteristics of the specific items or matters tested

*b.* Who performed the procedures and the date such procedures were completed

*c.* Who reviewed the work performed and the date and extent of such review

**52**. The service auditor should document discussions with service organization personnel and others of significant matters, including when and with whom the discussions took place.

**53.** If the service auditor has identified information that is inconsistent with the service auditor's final conclusion regarding a significant finding or issue, the service auditor should document how the service auditor addressed the inconsistency in forming the final conclusion.

**54.** The service auditor should complete the assembly of the final engagement file on a timely basis after the date of the service auditor's report.

**55.** After the assembly of the final engagement file has been completed, the service auditor should not delete or discard documentation before the end of its retention period.

**56.** If the service auditor finds it necessary to modify existing engagement documentation or add new documentation after the assembly of the final engagement file has been completed, the service auditor should, regardless of the nature of the modifications or additions, document the following:

*a.* When and by whom they were made, and where applicable, reviewed

*b.* The specific reasons for making them

*c.* Their effect, if any, on the service auditor's conclusions

**Preparing the Service Auditor's Report**

*Content of the Service Auditor's Report* (Ref: par. A38–A41)

**57.** The service auditor's report should include the following elements:

*a.* A title that clearly indicates that the report is an independent service auditor's report

*b.* An addressee

c. Identification of the following:

(1) The description of the service organization's system prepared by management of the service organization, and management's assertion about the matters identified in the definitions, in paragraph 7, of "report on a description of a service organization's system and the suitability

of the design of controls" and "report on a description of a service organization's system and the suitability of the design and operating effectiveness of controls."

(2) If parts of the description of the service organization's system are not covered by the service auditor's report, an identification of those parts

(3) If the description of the service organization's system refers to the need for complementary user entity controls, a statement that the service auditor has not evaluated the suitability of the design or operating effectiveness of complementary user entity controls, and that the control objectives stated in the description can be achieved only if complementary user entity controls are suitably designed and operating effectively, along with the controls at the service organization

(4) If services are performed by a subservice organization, an identification of those services and whether the inclusive method or the carve-out method was used in relation to them. If the carve-out method was used, a statement that the description of the service organization's system excludes the control objectives and related controls at relevant subservice organizations, and that the service auditor's procedures do not extend to the subservice organization. If the inclusive method has been used, a statement that the description of the service organization's system includes the subservice organization's specified control objectives and related controls, and that the service auditor's procedures included procedures at or related to the subservice organization

*d.* Identification of the criteria

*e.* A statement of the inherent limitations of the potential effectiveness of controls at the service organization and of the risk of projecting to the future any evaluation of the description of the service organization's system or any conclusions about the effectiveness of controls in achieving the related control objectives stated in the description

*f.* A description of the service organization's and the service auditor's responsibilities, including a statement that management of the service organization is responsible for the following:

(1) Preparing and presenting the description of the service organization's system and the accompanying assertion, including the completeness, accuracy, and method of presentation of the description and assertion

(2) Providing the services covered by the description of the service organization's system

(3) Specifying the control objectives and stating them in the description of the service organization's system. If the control objectives are specified by law, regulation, or another party (for example, a user group or a professional body), management is responsible for identifying, in the description, the party specifying the control objectives

(4) Designing, implementing, and maintaining controls to achieve the related control objectives stated in the description of the service organization's system

(5) Selecting the criteria

*g.* A statement that the engagement was performed in accordance with Statements on Standards for Attestation Engagements

*h.* A summary of the service auditor's procedures to obtain reasonable assurance and, in the case of a type1 report, a statement that the service auditor has not performed any procedures regarding the operating effectiveness of controls and, therefore, expresses no opinion thereon

*i.* The service auditor's opinion on whether, in all material respects, based on the criteria specified in management's assertion

(1) in the case of a type 2 report,

(a) the description of the service organization's system fairly presents the service organization's system that was designed and implemented throughout the specified period.

(b) the controls related to the control objectives stated in the description of the service organization's system were suitably designed to provide reasonable assurance that those control objectives would be achieved if the controls operated effectively throughout the specified period.

(c) the controls the service auditor tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the specified period.

(2) in the case of a type 1 report,

(a) the description of the service organization's system fairly presents the service organization's system that was designed and implemented as of the specified date.

(b) the controls related to the control objectives stated in the description of the service organization's system were suitably designed to provide reasonable assurance that those control objectives would be achieved if the controls operated effectively as of the specified date.

*j.* A paragraph at the end of the report that contains the following elements (Ref: par. A39):

(1) In the case of a type 2 report,

(a) a statement restricting the use of the service auditor's report and description of tests of controls and results thereof to management of the service organization, customers of the service organization's system during some or all of the period covered by the service auditor's report and their auditors.

(b) a statement that the report is not intended to be and should not be used by anyone other than these specified parties.

(2) In the case of a type 1 report,

(a) a statement restricting the use the service auditor's report to management of the service organization, customers of the service organization's system as of the end of the period covered by the service auditor's report, and their auditors.

(b) a statement that the report is not intended to be and should not be used by anyone other than these specified parties.

*k.* The date of the service auditor's report

*l.* The name of the service auditor and the city where the service auditor maintains the office that has responsibility for the engagement

**58.** If the application of complementary user entity controls is necessary to achieve the control objectives stated in the description of the service organization's system, the service auditor should add the phrase,

- "and customers applied the complementary user entity controls contemplated in the design of XYZ Service Organization's controls throughout the period [*date*] to [*date*]," at the end of subparagraph 57*i* (1)(b) of the opinion paragraph of a type 2 report.

- "if customers applied the complementary user entity controls contemplated in the design of XYZ Service Organization's controls throughout the period [*date*] to [*date*]," at the end of subparagraph 57i (1)(c) of the opinion paragraph of a type 2 report.

- "and customers applied the complementary user entity controls contemplated in the design of XYZ Service Organization's controls as of [*date*]" at the end of subparagraph 57*i* (2)(b) of the opinion paragraph in a type 1 report.

*Description of the Service Auditor's Tests of Controls and the Results Thereof* (Ref: par. A40)

**59.** In the case of a type 2 report, the service auditor's report should include a separate section after the opinion or an attachment that describes the service auditor's tests of controls and the results thereof. In describing the tests of controls, the service auditor should clearly indicate which controls were tested, the period covered by the testing, whether the items tested represent all or a selection of the items in the population, and the nature of the tests in sufficient detail to enable user auditors to determine the effect of such tests on their risk assessments. If deviations have been identified, the service auditor should include the extent of testing performed by the service auditor that led to the identification of the deviations, the nature of the deviations, and the number of deviations noted. The service auditor should report deviations even if, on the basis of tests performed, the service auditor concludes that the related control objective was achieved, or if the control that was tested is subsequently removed from the description of the service organization's system.

*Modified Opinions*

**60.** If the service auditor concludes that (Ref: par. A41)

*a.* management's description of the service organization's system is not fairly presented in all material respects,

*b.* the controls are not suitably designed to provide reasonable assurance that the control objectives stated in the description of the service organization's system would be achieved if the controls operated as described,

*c.* in the case of a type 2 report, the controls did not operate effectively throughout the specified period to achieve the related control objectives stated in the description,

*d.* the service auditor is unable to obtain sufficient, appropriate evidence,

the service auditor's opinion should be modified, and the service auditor's report should contain a clear description of all the reasons for the modification.

**61.** The service auditor also should modify the report if information, irrespective of specified control objectives, comes to the service auditor's attention that causes him or her to conclude (1) that design deficiencies exist that could adversely affect the ability of the service organization to initiate, authorize, record, process, or report financial data to user organizations without error, and (2) that user organizations would not generally be expected to have controls in place to mitigate such design deficiencies.

### Other Communication Responsibilities

**62.** A service auditor may become aware of incidents of noncompliance with laws and regulations, fraud, or uncorrected errors attributable to the service organization that are not clearly trivial and that may affect one or more user entities. In those circumstances, the service auditor should determine the effect of such incidents on the description of the service organization's system, the achievement of the control objectives, and the service auditor's report. Additionally, the service auditor should determine whether this information has been communicated appropriately to affected user entities. If the information has not been so communicated, and management of the service organization is unwilling to do so, the service auditor should take appropriate action, which could, depending on the significance of the matter, include withdrawing from the engagement and communicating the reasons for withdrawal to those charged with governance (Ref: par: A42).

## Application and Other Explanatory Material

### Definitions

**A1.** The policies and procedures referred to in the definition of "controls at a service organization" in paragraph 7 invariably include aspects of user entities' information and communication systems maintained by the service organization and also aspects of one or more of the other components of internal control at the service organization. For example, it may include aspects of the service organization's control environment, monitoring, and control activities that relate to the services provided. It does not, however, include controls at a service organization that are not related to the achievement of the control objectives stated in the description of the service organization's system, for example, controls related to the preparation of the service organization's own financial statements (Ref: par. 7).

**A2.** As indicated in the definition of "inclusive method" in paragraph 7, a service organization that uses a subservice organization may present its description of the service organization's system by using the inclusive method. When the inclusive method is used, performing procedures at the subservice organization entails coordination and communication between the service organization, the subservice organization, and the service auditor. The inclusive method generally is feasible if the service organization and the subservice organization are related, or if the contract between the service organization and the subservice organization provides for issuance of such a report.

**A3.** The terms *type 1 report* and *type 2 report,* referred to in the definitions in paragraph 7 of "report on a description of a service organization's system and the suitability of the design of controls" and "report on a description of a service organization's system and the suitability of the design and operating effectiveness of controls," have the same meaning as the terms *type A report* and *type B report, respectively,* that are used in International Standards on Auditing and International Standards for Assurance Engagements issued by the International Auditing and Assurance Standards Board (Ref: par. 7)

### Acceptance and Continuance

**A4.** A request to change the scope of the engagement may not have a reasonable justification if, for example, the request is made (Ref: par. 12)

- to exclude certain controls at the service organization from the scope of the engagement because of the likelihood that the service auditor's opinion would be modified with respect to those controls.

- to change the report from a type 2 to a type 1 report because of the likelihood that the service auditor's opinion would be modified with respect to the operating effectiveness of controls.

**A5.** A recent change in management or the appointment of the service auditor by a party other than management are examples of situations that might cause management to be unwilling to provide the service auditor with a written assertion. However, there may be other members of management who are in a position to, and will agree to, sign the assertion so that the service auditor can meet the requirement of paragraph 8(c) (Ref: par. 13).

**A6.** In performing a service auditor's engagement, the service auditor need not be independent of each user entity.

**Assessing the Suitability of the Criteria** (Ref: par. 14–17)

**A7.** AT section 101 requires a practitioner, among other things, to determine whether the subject matter is capable of evaluation against criteria that are suitable and available to users. As indicated in paragraph .27 of AT section 101, regardless of who establishes or develops the criteria, management is responsible for selecting the criteria and for determining whether the criteria are appropriate. The subject matter is the underlying condition of interest to intended users of an attestation report. The following table identifies the subject matter and minimum criteria for each of the opinions in type 2 and type 1 reports.

| | Subject matter | Criteria | Comment |
|---|---|---|---|
| ***Opinion on the fair presentation of the description of the service organization's system (type 1 and type 2 reports).*** | Management's description of the service organization's system that is relevant to services covered by the service auditor's report, and the service organization's assertion about whether the description is fairly presented. | The description of the service organization's system is fairly presented if it<br><br>*a*. presents how the service organization's system made available to user entities has been designed and implemented to process relevant transactions including the matters identified in paragraph 15*a*.<br><br>*b*. does not omit or distort information relevant to the scope of the service organization's system, while acknowledging that the description is presented to meet the common needs of a broad range of user entities and may not, therefore, include every aspect of the service organization's system that each individual user entity may consider important in its own particular environment. | The specific wording of the criteria for this opinion may need to be tailored to be consistent with criteria established by, for example, law, regulation, user groups, or a professional body. Criteria for evaluating the description of the service organization's system are provided in paragraph 15. Paragraphs 33–34 and A20–A24 offer further guidance on determining whether these criteria are met. |

| | Subject matter | Criteria | Comment | |
|---|---|---|---|---|
| ***Opinion on suitability of design and operating effectiveness (type 2 reports).*** | The design and operating effectiveness of the controls that are necessary to achieve the control objectives stated in the description that are relevant to the services covered by the service auditor's report. | The controls were suitably designed and operating effectively to achieve the control objectives stated in the description if<br><br>*a*. the risks that threaten the achievement of the control objectives stated in the description of the service organization's system have been identified.<br><br>*b*. the identified controls would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.<br><br>*c*. the controls necessary for achieving the control objectives stated in the description were consistently applied as designed. This includes whether manual controls were applied by individuals who have the appropriate competence and authority. | When the criteria for this opinion is met, controls will have provided reasonable assurance that the related control objectives stated in the description were achieved throughout the specified period. | The control objectives stated in the description of the service organization's system are part of the criteria for these opinions. The control objectives stated in the description will differ from engagement to engagement. If the service auditor concludes that the control objectives stated in the description are not fairly presented because they are not suitable (for example, they are incomplete or not appropriate for the service being described), then those control objectives would not be suitable as part of the criteria for forming an opinion on the design and operating effectiveness of the controls. |
| ***Opinion on suitability of design (type 1 reports).*** | The suitability of the design of the controls necessary to achieve the control objectives stated in the description of the service organization's system and relevant to the services covered by the service auditor's report. | The controls are suitably designed to achieve the control objectives stated in the description of the service organization's system if<br><br>*a*. the risks that threaten the achievement of the control objectives stated in the description have been identified.<br><br>*b*. the identified controls would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved. | Meeting this criterion does not, of itself, provide any assurance that the control objectives stated in the description were achieved because no evidence has been obtained about the operating effectiveness of the controls. | |

**A8.** The requirement to include in the description of the service organization's system "other aspects of the service organization's control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls, that are relevant to achieving the control objectives stated in the description" is also applicable to the internal

control components of subservice organizations used by the service organization when the inclusive method is used (Ref: par. 15 (a)(7)).

**Materiality** (Ref: par. 18)

**A9.** Paragraph .67 of AT section 101 requires the practitioner to consider materiality in applying AT section 101. It indicates that the practitioner should deem an omission or a misstatement to be material if the omission or misstatement—individually or when aggregated with others—is such that a reasonable person would be influenced by the omission or misstatement. In the context of a service auditor's engagement, a reasonable person would be, for example, a member of the user entity's management or the user auditor. AT section 101 requires the practitioner to consider both qualitative and quantitative aspects of omissions and misstatements.

**A10.** In an engagement to report on controls at a service organization, the concept of materiality relates to the information being reported on, not the financial statements of user entities. The service auditor plans and performs procedures to determine whether the description of the service organization's system is fairly presented in all material respects; whether controls at the service organization are suitably designed in all material respects to achieve the control objectives stated in the description; and in the case of a type 2 report, whether controls at the service organization operated effectively throughout the specified period in all material respects to achieve the control objectives stated in the description. In applying the concept of materiality, the service auditor recognizes that the service auditor's report provides information about the service organization's system to meet the common information needs of a broad range of user entities and their auditors who have an understanding of the manner in which the system is being used by a particular user entity for financial reporting. Materiality with respect to the fair presentation of the description, and with respect to the design of controls, primarily includes the consideration of qualitative factors, for example, whether

- the description includes the significant aspects of the processing of significant transactions.
- the description omits or distorts relevant information.
- the controls have the ability, as designed, to provide reasonable assurance that the control objectives stated in the description would be achieved.

Materiality with respect to the operating effectiveness of controls includes the consideration of both quantitative and qualitative factors, for example, the tolerable rate and observed rate of deviation of a quantitative matter, and the nature and cause of any observed deviations of a qualitative matter.

**Using the Work of an Internal Audit Function**

*Obtaining an Understanding of the Internal Audit Function* (Ref: par. 19)

**A11.** An internal audit function may be responsible for providing analyses, evaluations, assurances, recommendations, and other information to management and those charged with governance. An internal audit function at a service organization may perform activities related to the service organization's internal control or activities related to the services and systems, including controls that the service organization provides to user entities.

**A12.** The scope and objectives of an internal audit function vary widely and depend on the size and structure of the service organization and the requirements of management and those charged with governance. Internal audit function activities may include one or more of the following:

- Monitoring the service organization's internal control or the application processing systems. This may include controls relevant to the services provided to user entities. The internal audit function

may be assigned specific responsibility for reviewing controls, monitoring their operation, and recommending improvements thereto.

- Examination of financial and operating information. The internal audit function may be assigned to review the means by which the service organization identifies, measures, classifies, and reports financial and operating information; to make inquiries about specific matters; and to perform other procedures including detailed testing of transactions, balances, and procedures.

- Evaluation of the economy, efficiency, and effectiveness of operating activities including nonfinancial activities of the service organization.

- Evaluation of compliance with laws, regulations, and other external requirements and with management policies, directives, and other internal requirements.

**Obtaining an Understanding of the Service Organization's System** (Ref: par. 31–32).

**A13.** Obtaining an understanding of the service organization's system, including related controls, assists the service auditor in the following:

- Identifying the boundaries of the system and how it interfaces with other systems

- Assessing whether the description of the service organization's system fairly presents the service organization's system that has been designed and implemented

- Determining which controls are necessary to achieve the control objectives stated in the description, whether controls were suitably designed to achieve those control objectives, and, in the case of a type 2 report, whether controls were operating effectively throughout the period to achieve those control objectives

**A14.** Procedures to obtain this understanding may include the following:

- Inquiring of management and others within the service organization who, in the service auditor's judgment, may have relevant information

- Observing operations and inspecting documents, reports, and printed and electronic records of transaction processing

- Inspecting a selection of agreements between the service organization and user entities to identify their common terms

- Reperforming the application of a control

**A15.** Procedures the service auditor may perform to obtain information to be used in identifying risks that the description of the service organization's system is not fairly presented or that the control objectives stated in that description were not achieved due to intentional acts by service organization personnel include the following:

- Discussing, among the members of the service auditor's team, factors at the service organization that could affect the risks that the description is not fairly presented or that the control objectives stated in the description were not achieved due to intentional acts by service organization personnel, such as management override of controls

- Making inquiries of management and others within the service organization to obtain their views about such risks and how they are addressed

- Considering whether factors exist at the service organization that increase such risks

- Considering other information that comes to the service auditor's attention that may be helpful in the identification of such risks

**A16.** The procedures and controls that the service organization implements to address the risks that the description of the service organization's system is not fairly presented or that the control objectives were not achieved due to intentional acts by service organization personnel may include relevant aspects of the control environment, risk assessment, monitoring, the information and communication systems used to process user transactions, and control activities.

**A17.** In addition to management override of controls at the service organization, other intentional acts by service organization personnel that may affect the fairness of the presentation of the description of the service organization's system or the completeness or achievement of the control objectives stated in that description include the following:

- Misappropriation of user entity assets by service organization personnel

- Creation, by service organization personnel, of false or misleading documents or records of user organization transactions processed by the service organization

**A18.** The risk of management override and the risk of misappropriation of user entity assets may result in false or misleading records or documents being provided to user entities. Factors that may increase the risk of management override include unrealistic processing schedules, significant increases in processing volumes that exceed normal processing capacity, or an environment in which established procedures and controls are not consistently followed. Depending on the nature of the services provided by the service organization and the extent to which the service organization initiates, authorizes, records, processes, and reports transactions for user entities, a significant risk of misappropriation of user entity assets by service organization personnel may exist. Factors that may increase the risk of misappropriation of assets include inadequate supervision or monitoring, processing or maintaining records of large amounts of cash or investments, inadequate segregation of duties or independent checks, and inadequate physical or electronic safeguards over cash or investments. The service auditor's procedures are affected by the service auditor's risk assessment and the extent to which management has identified and addressed the identified risks through monitoring or other controls, and the nature and extent of the identified risks.

**A19.** Although AU section 316, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1), is not applicable to engagements performed under this SSAE, it, nonetheless, provides a framework that may be useful to the service auditor for identifying and responding to risks that the description of the service organization's system is not fairly presented or that control objectives stated in that description would not be achieved due to intentional acts by service organization personnel.

**Obtaining Evidence Regarding the Description of the Service Organization's System** (Ref: par. 33–34)

**A20.** Considering the following questions may assist the service auditor in determining whether the description of the service organization's system is fairly presented in all material respects:

- Does the description address the major aspects of the service provided and included in the scope of the engagement that could reasonably be expected to be relevant to the common needs of a broad range of user auditors in planning their audits of user entities' financial statements?

- Is the description presented at a level of detail that could reasonably be expected to provide a broad range of user auditors with sufficient information to obtain an understanding of internal control in accordance with AU section 314, *Understanding the Entity and Its Environment and*

*Assessing the Risks of Material Misstatement* (AICPA, *Professional Standards*, vol. 1). The description need not address every aspect of the service organization's processing or the services provided to user entities and need not be so detailed that it would potentially enable a reader to compromise security or other controls at the service organization.

- Is the description prepared and presented in a manner that does not omit or distort information that might affect the decisions of a broad range of user auditors; for example, does the description contain any significant omissions or inaccuracies regarding processing of which the service auditor is aware?

- Have the controls identified in the description actually been implemented?

- Are complementary user entity controls, if any, adequately described? In most cases, the control objectives stated in the description are worded so that they are capable of being achieved through the effective operation of controls implemented by the service organization alone. In some cases, however, the control objectives stated in the description cannot be achieved by the service organization alone because their achievement requires particular controls to be implemented by user entities. This may be the case when, for example, the control objectives are specified by a regulatory authority. When the description includes complementary user entity controls, they are separately identified as such.

**A21.** The service auditor's procedures to evaluate the fair presentation of the description of the service organization's system may include the following:

- Considering the nature of the user entities and how the services provided by the service organization are likely to affect them, for example, the predominant types of user entities, and whether the user entities are regulated by government agencies.

- Reading standard contracts or standard terms of contracts with user entities to gain an understanding of the service organization's contractual obligations

- Observing procedures performed by service organization personnel

- Reviewing the service organization's policy and procedure manuals and other documentation of the system, for example, flowcharts and narratives

- Performing walkthroughs of transactions through the service organization's system

**A22.** Paragraph 33(a) requires the service auditor to evaluate whether the control objectives stated in the description of the service organization's system are reasonable in the circumstances. Considering the following questions may assist the service auditor in this evaluation:

- Have the control objectives stated in the description been designated by management of the service organization or by outside parties, such as regulatory authorities, a user group, a professional body, or others?

- Do the control objectives stated in the description and designated by management relate to the types of assertions commonly embodied in the broad range of user entities' financial statements to which controls at the service organization could reasonably be expected to relate? Although the service auditor ordinarily will not be able to determine how controls at a service organization specifically relate to the assertions embodied in individual user entities' financial statements, the service auditor's understanding of the nature of the service organization's system, including controls, and the services being provided is used to identify the types of assertions to which those controls are likely to relate.

- Are the control objectives stated in the description and designated by management complete? A complete set of control objectives can provide a broad range of user auditors with a framework for assessing the effect of controls at the service organization on assertions commonly embodied in user entities' financial statements. If the control objectives are specified by an outside party, including control objectives specified by law or regulation, the outside party is responsible for their completeness and reasonableness.

**A23.** Other procedures that the service auditor may use in combination with inquiry of management and other service organization personnel to determine whether the system described by the service organization has been implemented include observation, inspection of records and other documentation, as well as reperformance of the manner in which transactions are processed through the system and controls are applied.

**A24.** If the inclusive method has been used, it is important that the description of the service organization's system adequately differentiate between controls at the service organization and controls at the subservice organization. If the carve-out method has been used, it is important that the description identify the functions that are performed by the subservice organization, but need not describe the detailed processing or controls at the subservice organization.

**Obtaining Evidence Regarding the Design of Controls** (Ref: par. 35)

**A25.** From the viewpoint of a *user auditor*, a control is suitably designed to achieve the control objectives stated in the description of the service organization's system if individually or in combination with other controls, it would, when complied with satisfactorily, provide reasonable assurance that material misstatements, whether due to fraud or error, are prevented or detected and corrected. A *service auditor*, however, is not aware of the circumstances at individual user entities that would affect whether or not a misstatement resulting from a control deficiency is material to those user entities. Therefore, from the viewpoint of a service auditor, a control is suitably designed if individually or in combination with other controls, it would, when complied with satisfactorily, provide reasonable assurance that the control objective stated in the description of the service organization's system is achieved.

**A26.** A service auditor may consider using flowcharts, questionnaires, or decision tables to facilitate understanding the design of the controls.

**A27.** Controls may consist of a number of integrated activities directed at the achievement of various control objectives. Consequently, if the service auditor evaluates certain activities as being ineffective in achieving a particular control objective, the existence of other activities, sometimes known as *compensating controls* may, nonetheless, enable the service auditor to conclude that controls related to the control objective stated in the description of the service organization's system are suitably designed to achieve those control objectives.

**Obtaining Evidence Regarding the Effectiveness of Controls**

*Assessing Operating Effectiveness* (Ref: par. 36–41)

**A28.** From the viewpoint of a *user auditor*, a control is operating effectively if individually or in combination with other controls, it provides reasonable assurance that material misstatements, whether due to fraud or error, are prevented or detected and corrected. A *service auditor*, however, is not aware of the circumstances at individual user entities that would determine whether or not a misstatement resulting from a deficiency in internal control is material. Therefore, from the viewpoint of a service auditor, a control is operating effectively if individually or in combination with other controls, it provides reasonable assurance that the control objectives stated in the description of the service organization's system are achieved. Similarly, a service auditor is not in a position to determine whether any observed deficiency in

internal control would result in a material misstatement from the viewpoint of an individual user entity.

**A29.** Obtaining an understanding of controls sufficient to opine on the suitability of their design is not sufficient evidence regarding their operating effectiveness unless there is some automation that provides for the consistent operation of the controls as they were designed and implemented. For example, obtaining information about the implementation of a manual control at a point in time does not provide evidence about operation of the control at other times. However, because of the inherent consistency of IT processing, performing procedures to determine the design of an automated control and whether it has been implemented may serve as evidence of that control's operating effectiveness, depending on the service auditor's assessment and testing of controls such as those over program changes.

**A30.** To be useful to user auditors, a type 2 report ordinarily covers a minimum period of six months. If the period is less than six months, the service organization's description of the system may describe the reasons for the shorter period, and the service auditor's report may include that information as well. Circumstances that may result in a report covering a period of less than six months include the following:

*a.* The service auditor was engaged close to the date by which the report on controls is to be issued, and controls cannot be tested for operating effectiveness for a six month period.

*b.* The service organization or a particular system or application has been in operation for less than six months.

*c.* Significant changes have been made to the controls, and it is not practicable either to wait six months before issuing a report or to issue a report covering the system both before and after the changes.

**A31.** Certain control procedures may not leave evidence of their operation that can be tested at a later date and, accordingly, the service auditor may find it appropriate to test the operating effectiveness of such control procedures at various times throughout the reporting period.

**A32.** Determining the effect of changes in the service organization's controls that were implemented during the period covered by the service auditor's report involves gathering information about the nature and extent of such changes, how they affect processing at the service organization, and how they might affect assertions in the user entities' financial statements.

**A33.** Evidence about the satisfactory operation of controls in prior periods does not provide a basis for a reduction in the testing of controls in the current period because the service auditor expresses an opinion on the effectiveness of controls throughout each period. Therefore, sufficient, appropriate evidence about the operating effectiveness of controls throughout the current period is required for the service auditor to express that opinion.

**A34.** A service auditor may decide to test less than 100 percent of the executions of a control, for example, a control that is designed to be performed daily, to enable the service auditor to project the results of his or her tests to the population of controls. In those circumstances, the guidance in AU section 350 is applicable.

**Written Representations** (Ref: par. 42–45)

**A35.** Written representations reaffirming management's assertion about the effective operation of controls may be based on ongoing monitoring activities, separate evaluations, or a combination of the two. Ongoing monitoring activities are often built into the normal recurring activities of a service organization and include regular management and supervisory activities. Internal auditors or personnel performing similar functions may contribute to the monitoring of a service organization's activities. Monitoring activities also may include using information obtained through communications from external parties, such as customer complaints and regulator comments that may indicate problems or highlight areas in need of

improvement.

**A36.** In certain circumstances, a service auditor may obtain written representations from parties in addition to management of the service organization, such as those charged with governance.

**A37.** The written representations required by paragraph 42 are separate from, and in addition to, the assertion accompanying the service organization's description of the system required by paragraph 8(c).

### Preparing the Service Auditor's Report

*Content of the Service Auditor's Report* (Ref: par. 57)

**A38.** Examples of service auditors' reports are contained in exhibits B–D, and illustrative assertions by management of the service organization are presented in exhibit A.

*Use of the Service Auditor's Report* (Ref: par. 57(j))

**A39.** Paragraph .79 of AT section 101 requires that use of a practitioner's report be restricted to specified parties when the criteria used to evaluate or measure the subject matter are available only to specified parties or appropriate only for a limited number of parties who either participated in their establishment or can be presumed to have an adequate understanding of the criteria. The criteria used for engagements to report on controls at a service organization are relevant only for the purpose of providing information about the service organization's system, including controls, to those who have an understanding of how the system is used for financial reporting by user entities and, accordingly, the service auditor's report states that the report and the description of tests of controls are intended only for use by management of the service organization, customers of the service organization ("during some or all of the period covered by the report" for a type 2 report) ("as of the ending date of the period covered by the report" for a type 1 report), and their financial statement auditors. (The illustrative service auditor's reports in exhibit A illustrate language for a paragraph restricting the use of a service auditor's report.)

*Description of the Service Auditor's Tests of Controls* (Ref: par. 59)

**A40.** In describing the service auditor's tests of controls for a type 2 report, it assists readers if the service auditor's report includes information about causative factors for identified deviations, to the extent the service auditor has identified such factors.

*Modified Opinions* (Ref: par. 60–61)

**A41.** Examples of elements of modified service auditor's reports are presented in exhibit C.

### Other Communication Responsibilities (Ref: par. 62)

**A42.** The following are actions that a service auditor may take when he or she becomes aware of noncompliance with laws and regulations, fraud, or uncorrected errors at the service organization, giving additional consideration to instances in which the service organization has not appropriately communicated this information to affected user entities, and management of the service organization is unwilling to do so:

- Obtaining legal advice about the consequences of different courses of action
- Communicating with those charged with governance of the service organization
- Modifying the service auditor's opinion or adding an emphasis of a matter paragraph

- Communicating with third parties, for example, a regulator, when required to do so
- Withdrawing from the engagement

**A43**.

**Exhibit A**

**Illustrative Management Assertions**

The following illustrative management assertions are for guidance only and are not intended to be exhaustive or applicable to all situations.

**Example 1: Management Assertion for a Type 2 Report**

Management's Assertion

We have prepared the accompanying description of XYZ Service Organization's [*type or name of*] system for customers of the system during some or all of the period [*date*] to [*date*], and their financial statement auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by customers of the system themselves, when assessing the risks of material misstatements of customers' financial statements. We confirm, to the best of our knowledge and belief, that

*a.* the accompanying description on pages [*bb–cc*] fairly presents the [*type or name of*] system made available to customers of the system during some or all of the period [*date*] to [*date*] for processing their transactions. The criteria we used in making this assertion were that the accompanying description

(1) presents how the system was designed and implemented to process relevant transactions, including

- the classes of transactions processed.
- the procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to customers of the system.
- the related accounting records, supporting information, and specific accounts involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to customers of the system.
- how the system captures significant events and conditions, other than transactions.
- the process used to prepare reports provided to customers of the system.
- specified control objectives and controls designed to achieve those objectives.
- other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of customers of the system.

(2) does not omit or distort information relevant to the scope of the [*type or name of*] system, while acknowledging that the description is presented to meet the common needs of a broad range of customers of the system and their auditors, and may not, therefore, include every aspect of the [*type or name of*] system that each individual customer and its auditor may consider important in its own particular environment.

*b.* the controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period [*date*] to [*date*] to achieve the control objectives stated in the description. The criteria we used in making this assertion were that

(1) the risks that threaten the achievement of the control objectives stated in the description have been identified;

(2) the identified controls would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

(3) the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

*Management's signature*

**Example 2: Management Assertion for a Type 1 Report**

Management's Assertion

We have prepared the accompanying description of XYZ Service Organization's [*type or name of*] system for customers of the system as of [*date*], and their financial statement auditors who have a sufficient understanding to consider it, along with other information including information about controls implemented by customers themselves, when obtaining an understanding of customers' information and communication systems relevant to financial reporting. We confirm, to the best of our knowledge and belief, that

*a.* the accompanying description, on pages [*bb–cc*], fairly presents our [*type or name of*] system made available to customers of the system as of [*date*] for processing their transactions. The criteria we used in making this assertion were that the accompanying description

(1) presents how the system made available to customers of the system was designed and implemented to process relevant transactions, including

- the classes of transactions processed.
- the procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to customers of the system.
- the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports provided to customers of the system.
- how the system captures significant events and conditions, other than transactions.
- the process used to prepare reports provided to customers of the system.
- specified control objectives and controls designed to achieve those objectives.
- other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of

customers of the system.

(2) does not omit or distort information relevant to the scope of the [*type or name of*] system, while acknowledging that the description is presented to meet the common needs of a broad range of customers of the system and their auditors, and may not, therefore, include every aspect of the [*type or name of*] system that each individual customer of the system and its auditor may consider important in its own particular environment.

*b.* the controls related to the control objectives stated in the accompanying description were suitably designed as of [*date*] to achieve those control objectives. The criteria we used in making this assertion were that

(1) the risks that threaten achievement of the control objectives stated in the description have been identified.

(2) the identified controls would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

*Management's signature*

**A44**.

**Exhibit B**

**Illustrative Service Auditor's Reports**

The following illustrative reports are for guidance only and are not intended to be exhaustive or applicable to all situations.

**Example 1: Type 2 Service Auditor's Report**

**Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls**

To: XYZ Service Organization

*Scope*
We have examined XYZ Service Organization's description on pages [*bb–cc*] of the [*type or name of*] system made available to customers of the system throughout the period [*date*] to [*date*] for processing their transactions and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description.

*Management's responsibilities*
Management of XYZ Service Organization is responsible for preparing and presenting the description and accompanying assertion on page [*aa*], including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, selecting the criteria, and designing, implementing, and maintaining controls to achieve the control objectives stated in the description.

*Service auditor's responsibilities*
Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our procedures. We conducted our examination in accordance with Statements on Standards for Attestation Engagements issued by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our procedures to obtain reasonable assurance about whether the description is fairly presented and whether the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period [*date*] to [*date*] in all material respects.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls involves performing procedures to obtain evidence about the fairness of the presentation of the description and about the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description, whether due to fraud or error. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated in the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

*Inherent limitations*

Because of their nature, controls at a service organization may not prevent or detect and correct all errors or omissions in processing or reporting transactions. The description of XYZ Service Organization's [*type or name of*] system and information about tests of the operating effectiveness of specific controls covers the period [*date*] to [*date*]. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at the Service Organization is subject to inherent limitations and, accordingly, fraud or error may occur and not be detected. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

*Opinion*
In our opinion, based on the criteria described in management's assertion on page [*aa*], in all material respects

*a.* the description of XYZ Service Organization's system fairly presents the [*type or name of*] system that was designed and implemented throughout the period [*date*] to [*date*].

*b.* the controls related to the control objectives stated in the description of XYZ Service Organization's system were suitably designed to provide reasonable assurance that those control objectives would be achieved if the controls operated effectively throughout the period [*date*] to [*date*].

*c.* the controls we tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description of XYZ Service Organization's system were achieved, operated effectively throughout the period [*date*] to [*date*].

*Description of tests of controls*
The specific controls that were tested and the nature, timing, and results of those tests are listed on pages [*yy–zz*].

*Restricted use*
This report and the description of tests of controls on pages [*yy–zz*] are intended solely for the information and use of management of XYZ Service Organization, customers of the [*type or name of*] system during some or all of the period [*date*] to [*date*], and their financial statement auditors, who have a sufficient understanding to consider it, along with other information including information about controls implemented by customers themselves, when assessing the risks of material misstatements of customers' financial statements. This report is intended to be and should not be used by anyone other than these specified parties.

[*Service auditor's signature*]
[*Date of the service auditor's report*]
[*Service auditor's city*]

Following is a modification of subparagraphs 57*i* (1)(b) and 57i (1)(c) of the opinion paragraph of a type 2 report if the application of complementary controls by user entities is necessary to achieve the control objectives stated in the description of the service organization's system (New language is shown in boldface italics):

*b.* The controls related to the control objectives stated in the description of XYZ Service Organization's system were suitably designed to provide reasonable assurance that those control objectives would be achieved if the controls operated effectively throughout the period [*date*] to [*date*] ***and customers applied the complementary user entity controls contemplated in the design of XYZ Service Organization's controls throughout the period [date] to [date]***.

*c.* The controls we tested, which were those necessary to provide reasonable assurance that the

related control objectives stated in the description were achieved, operated effectively throughout the period [*date*] to [*date*] ***if customers applied the complementary user entity controls contemplated in the design of XYZ Service Organization's controls throughout the period [date] to [date]***.

Following is a modification of the paragraph that describes management's responsibilities to be used in a type 1 or type 2 report when the control objectives have been specified by an outside party. (New language is shown in boldface italics):

> Management of XYZ Service Organization is responsible for preparing and presenting the description of its [*type or name of*] system and accompanying assertion on page [*aa*], including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, selecting the criteria, and designing, implementing, and maintaining controls to achieve the control objectives stated in the description. ***The control objectives have been specified by [name of party specifying the control objectives] and are stated on page [aa] of the description***.

**Example 2: Type 1 Service Auditor's Report**

**Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design of Controls**

To: XYZ Service Organization

*Scope*
We have examined XYZ Service Organization's description on pages [*bb–cc*] of the [*type or name of*] system made available to customers of the system for processing their transactions as of [*date*], and the suitability of the design of controls to achieve the related control objectives stated in the description.

*Management's responsibilities*
Management of XYZ Service Organization is responsible for preparing and presenting the description and accompanying assertion on page [*aa*], including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, selecting the criteria, and designing, implementing, and maintaining controls to achieve the related control objectives stated in the description.

*Service auditor's responsibilities*
Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design of controls in achieving the related control objectives stated in the description, based on our procedures. We conducted our examination in accordance with Statements on Standards for Attestation Engagements issued by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our procedures to obtain reasonable assurance about whether the description is fairly presented and the controls are suitably designed to achieve the related control objectives stated in the description as of [*date*] in all material respects.

An examination of a description of a service organization's system and the suitability of the design of controls in achieving the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description of the system and the suitability of the design of the controls to achieve the related control objectives stated in the description. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated in the description.

We did not perform any procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, do not express an opinion thereon.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

*Inherent limitations*
Because of their nature, controls at a service organization may not prevent or detect and correct all errors or omissions in processing or reporting transactions. The description of controls at XYZ Service Organization is as of [*date*] and any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at the Service Organization is subject to inherent limitations and, accordingly, fraud or error 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 may alter the validity of such conclusions.

*Opinion*
In our opinion, based on the criteria described in management's assertion on page [*aa*], in all material respects

*a.* the description of XYZ Service Organization's system fairly presents the [*type or name of*] system that was designed and implemented as of [*date*], and

*b.* the controls related to the control objectives stated in the description of XYZ Service Organization's system were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively as of [*date*].

*Restricted use*
This report is intended solely for the information and use of management of XYZ Service Organization, customers of XYZ Service Organization's [*type or name of*] system as of [date], and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls implemented by customers themselves, when obtaining an understanding of customers' information and communication systems relevant to financial reporting. This report is not intended to be and should not be used by anyone other than these specified parties.

[*Service auditor's signature*]
[*Date of the service auditor's report*]
[*Service auditor's city*]

Following is a modification of subparagraph "b" of the opinion paragraph in a type 1 report if the application of complementary user entity controls is necessary to achieve the control objectives stated in the description of the service organization's system (New language is shown in boldface italics):

*b.* The controls related to the control objectives stated in the description of XYZ Service Organization's [*type or name of*] system were suitably designed to provide reasonable assurance that those control objectives would be achieved if the controls operated effectively as of [*date*] ***and customers applied the complementary user entity controls contemplated in the design of XYZ Service Organization's controls as of [date].***

**A45**.

**Exhibit C**

**Illustrative Modified Service Auditor's Reports**

The following examples of modified service auditors' reports are for guidance only and are not intended to be exhaustive or applicable to all situations. They are based on the illustrative reports in exhibit B.

**Example 1: Qualified opinion for a type 2 report— the description of the service organization's system is not fairly presented in all material respects**

[*Illustrative explanatory paragraph that would be inserted before the modified opinion paragraph. All other report paragraphs are unchanged.*]

*Explanatory paragraph*
The accompanying description of the [*type or name of*] system states on page [*mn*] that XYZ Service Organization uses operator identification numbers and passwords to prevent unauthorized access to the system. Based on inquiries of staff personnel and observation of activities, we have determined that operator identification numbers and passwords are employed in applications A and B but are not required to access the system in applications C and D.

*Opinion*
In our opinion, except for the matter described in the preceding paragraph, and based on the criteria described in management's assertion on page *[aa]*, in all material respects.

**Example 2: Qualified opinion—the controls are not suitably designed to provide reasonable assurance that the control objectives stated in the description of the service organization's system would be achieved if the controls operated effectively**

[*Illustrative explanatory paragraph that would be inserted before the modified opinion paragraph. All other report paragraphs are unchanged.*]

*Explanatory paragraph*
As discussed at page [*mn*] of the accompanying description, from time to time, XYZ Service Organization makes changes in application programs to correct deficiencies or to enhance capabilities. The procedures followed in determining whether to make changes, in designing the changes, and in implementing them do not include review and approval by authorized individuals who are independent from those involved in making the changes. There are also no specified requirements to test such changes or provide test results to an authorized reviewer prior to implementing the changes.

*Opinion*
In our opinion, except for the matter described in the preceding paragraph, and based on the criteria described in management's assertion on page *[aa]*, in all material respects…

**Example 3: Qualified opinion for a type 2 report—the controls did not operate effectively throughout the specified period to achieve the control objectives stated in the description of the service organization's system**

[*Illustrative explanatory paragraph that would be inserted before the modified opinion paragraph. All other report paragraphs are unchanged.*]

*Explanatory paragraph*
XYZ Service Organization states in its description of the [*type or name of*] system that it has automated

controls in place to reconcile loan payments received with the various output reports. However, as noted at page [*mn*] of the description of tests of controls and results thereof, this control was not operating effectively throughout the period [*date*] to [*date*] due to a programming error. This resulted in the nonachievement of the control objective, "Controls provide reasonable assurance that loan payments received are properly recorded" throughout the period January 1, 20X1 to April 30, 20X1. Management implemented a change to the program performing the calculation as of May 1, 20X1, and our tests indicate that it was operating effectively throughout the period May 1, 20X1 to December 31, 20X1.

*Opinion*
In our opinion, except for the matter described in the preceding paragraph, and based on the criteria described in management's assertion on page [*aa*], in all material respects:…

**Example 4: Qualified opinion— the service auditor is unable to obtain sufficient appropriate evidence**

[*Illustrative explanatory paragraph that would be inserted before the modified opinion paragraph. All other report paragraphs are unchanged.*]

*Explanatory paragraph*
XYZ Service Organization states in its description of the [*type or name of*] system that it has automated controls in place to reconcile loan payments received with the output generated. However, electronic records of the performance of this reconciliation for the period from [*date*] to [*date*] were deleted as a result of a computer processing error and, therefore, we were unable to test the operation of this control for that period. Consequently, we were unable to determine whether the control objective, "Controls provide reasonable assurance that loan payments received are properly recorded" was achieved throughout the period [*date*] to [*date*].

*Opinion*
In our opinion, except for the matter described in the preceding paragraph, and based on the criteria described in management's assertion on page [*aa*], in all material respects…

**Example 5: Disclaimer of opinion on other information included in management's description of the service organization's system that is not covered by the service auditor's report.**

[*Illustrative explanatory paragraph that would be inserted following the opinion paragraph. All other report paragraphs are unchanged.*]

*Explanatory paragraph*

The information in section X describing XYZ Service Organization's inventory application is presented by management of XYZ Service Organization to provide additional information and is not a part of XYZ Service Organization's description of its [*type of name of*] system made available to customers during some or all of the period [*date*] to [*date*]. Information about XYZ Service Organization's inventory application has not been subjected to the procedures applied in the examination of the description of the [*type of name of*] system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the [*type of name of system*] and, accordingly, we express no opinion on it.

**A46**.

**Exhibit D**

**Illustrative Report Paragraphs for Service Organizations That Use a Subservice Organization**

Following are modifications of the illustrative type 2 report in example 1 of exhibit B for use in engagements in which the service organization uses a subservice organization.

*New language is shown in boldface italics; deleted language is shown by strikethrough.*

**Example 1: Carve-out method**

*Scope*
We have examined XYZ Service Organization's description on pages [*bb–cc*] of the [*type or name of*] system made available to customers of the system throughout the period [*date*] to [*date*] for processing their transactions and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. ***XYZ Service Organization uses a computer processing service organization for all of its computerized application processing. The description on pages [bb–cc] includes only the controls and related control objectives of XYZ Service Organization and excludes the control objectives and related controls of the computer processing service organization. Our examination did not extend to controls of the computer processing service organization.***

*All other report paragraphs are unchanged.*

**Example 2: Inclusive Method**

*Scope*
We have examined XYZ Service Organization's ***and ABC Subservice Organization's*** description on pages [*bb–cc*] of the [*type or name of*] system made available to customers of the system throughout the period [*date*] to [*date*] for processing their transactions and the suitability of the design and operating effectiveness of ***XYZ Service Organization's and ABC Subservice Organization's*** controls to achieve the related control objectives stated in the description. ***ABC Subservice Organization is an independent service organization that provides computer processing services to XYZ Service Organization. XYZ Service Organization's description includes a description of ABC Subservice Organization's [*****type or name of*****] system used by XYZ Service Organization to process transactions for its customers, as well as relevant control objectives and controls of ABC Subservice Organization.***

*Management's responsibilities*
Management of XYZ Service Organization ***and ABC Subservice Organization are*** ~~is~~ responsible for preparing and presenting the description and accompanying assertion at page [*aa*], including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, selecting the criteria, and designing, implementing, and maintaining controls to achieve the control objectives stated in the description.

*Inherent limitations*
Because of their nature, controls at a service organization may not prevent or detect and correct all errors or omissions in processing or reporting transactions. The description of XYZ Service Organization's [*type or name of*] system ***and ABC Subservice Organization's*** **[*****type or name of*****] system** and information about tests of the operating effectiveness of specific controls covers the period [*date*] to [*date*]. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at ~~the~~ ***XYZ***

Service Organization ***and ABC Subservice Organization*** is subject to inherent limitations and, accordingly, fraud or error may occur and not be detected. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

*Opinion*
In our opinion, based on the criteria specified in managements' assertions on page [*aa*], in all material respects

*a.* the description fairly presents ***XYZ Service Organization's*** ~~the~~ [*type or name of*] system ***and ABC Subservice Organization's* [*type or name of*] *system used by XYZ Service Organization to process transactions for its customers*** that ***were*** ~~was~~ designed and implemented throughout the period [*date*] to [*date*], and

*b.* the controls related to the control objectives ***of XYZ Service Organization and ABC Subservice Organization*** stated in the description were suitably designed to provide reasonable assurance that those control objectives stated in the description were achieved if the controls operated effectively throughout the period [*date*] to [*date*].

*c.* the controls ***of XYZ Service Organization and ABC Computer Processing Service Organization that*** we tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period [*date*] to [*date*].

*All other report paragraphs are unchanged.*

**A47.**

**Exhibit E**

**Substantive Differences Between the Proposed Statement on Standards for Attestation Engagements, *Reporting On Controls at a Service Organization,* and the Exposure Draft of International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Third-Party Service Organization***

This analysis was prepared by the AICPA Audit and Attest Standards staff to highlight substantive differences between the proposed Statement on Standards for Attestation Engagements (SSAE), *Reporting on Controls at a Service Organization,* and the December 2007 exposure draft of International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Third Party Service Organization*, and to explain the rationale for those differences. This analysis is not authoritative and is prepared for informational purposes only. It has not been acted on or reviewed by the Auditing Standards Board.

| Description of Difference | Explanation |
|---|---|
| **1. Intentional acts by service organization personnel.** Paragraph 32 of the proposed SSAE requires the auditor, when obtaining an understanding of the service organization's system, to obtain information for use in identifying risks that the description of the service organization's system is not fairly presented, or that the control objectives stated in that description were not achieved due to intentional acts by service organization personnel. The ISAE 3402 exposure draft (ED) does not contain this requirement. | Enables the service auditor to give adequate consideration to the risk that incorrect information resulting from intentional acts by service organization personnel may be reported to user entities. |
| **2. Changes in the service organization's controls.** Paragraph 37 of the proposed SSAE, which addresses type 2 reports, requires the service auditor to<br><br>• inquire about changes in the service organization's controls implemented during the period covered by the service auditor's report.<br><br>• describe the changes in his or her report if they are not included in the description of the service organization's system, and the service auditor believes the changes would be considered significant by user entities and their auditors.<br><br>• determine from management whether it is possible for the controls to be tested before and after the change, if the superseded controls are relevant to the achievement of the control objectives stated in the description during the period covered by the service auditor's report.<br><br>• determine the effect on the service auditor's report, if it is not possible for the service auditor to test the controls before and after the change.<br><br>These procedures are not required in the ISAE 3402 ED. | In a type 2 report, the service auditor's opinion on the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls covers a specified period. Information about changes in a service organization's controls implemented during the period covered by the service auditor's report could be significant to user entities and their auditors. |
| **3. Requiring an assertion** | Requiring management to provide a written |

| Description of Difference | Explanation |
|---|---|
| Paragraph 8*c* of the proposed SSAE requires the service auditor to obtain a written assertion from management regarding the fairness of the presentation of the description, the suitability of the design of the controls, and, in a type 2 report, the operating effectiveness of the controls.<br><br>Paragraph 4 of the ISAE 3402 ED states, in part, "This ISAE applies to assertion-based engagements." This sentence is not worded as a requirement and would, therefore, enable a service auditor to perform the engagement without obtaining an assertion. | assertion about the subject matter underscores the fact that management of the service organization is responsible for controls at the service organization that affect user entities' information and communication systems. |
| **4. Sampling and means of selecting items for testing**<br>Paragraph 39 of the proposed SSAE states that the service auditor should refer to AU section 350, *Audit Sampling* (AICPA, *Professional Standards*, vol. 1) if the service auditor determines that sampling is appropriate in performing tests of the operating effectiveness of controls. The ISAE 3402 ED does not contain this requirement and instead contains requirements and application guidance on this subject in paragraphs 39, A23, and A24. | Audit sampling and methods of selecting items for testing is a relatively complex topic that is more comprehensively and accurately addressed in AU section 350. |
| **5. Third party service organizations**<br>The term *third party* is used in the title of and elsewhere in the ISAE 3402 ED to describe the service organizations that are the subject of the exposure draft. That descriptive is not used in the proposed SSAE. | The term *third party* denotes a service organization that is external to the entity. Paragraph 2(b) of the ISAE 3402 ED indicates that the ISAE would also be applicable to controls at a shared service center. Use of the descriptive *third party* unnecessarily narrows the scope of the ISAE and makes it inconsistent with the statement in paragraph 2(b) and the intent of the ISAE. |
| **6. Obtaining representations from those charged with governance**<br>Paragraph 42 of the proposed SSAE requires the service auditor to ask management to provide written representations; whereas, paragraph 42 of the ISAE 3402 ED requires the service auditor to ask management and those charged with governance to provide written representations. | In practice, a service auditor is rarely engaged by and has very little interaction with those charged with governance. As a rule, a service auditor is engaged by and primarily interacts with management. |
| **7. Obtaining representations from management of the subservice organization**<br>If the service organization uses a subservice organization and the description of the service organization's system is presented using the inclusive method, paragraph 43 of the proposed SSAE requires the service auditor to obtain written representations from management of the subservice organization. The ISAE 3402 ED does not contain this requirement. | When the inclusive method is used to present the description of the service organization's system, and the subservice organization's control objectives and related controls are included in the description, that information is on the same footing as the information provided by the service organization about its own control objectives and related controls. Accordingly, the service auditor has the same responsibility for reporting on the subservice organization's information as he or she does |

| Description of Difference | Explanation |
|---|---|
| | for reporting on the service organization's information. |
| **8**. **Other Reasons for Report Modification**<br>Paragraph 61 of the proposed SSAE requires the service auditor to modify his or her report if information, regardless of specified control objectives, comes to the service auditor's attention that causes him or her to conclude that (1) design deficiencies exist that could adversely affect the ability of the service organization to initiate, authorize, record, process, or report financial data to user entities without error and (2) user entities would not generally be expected to have controls in place to mitigate such design deficiencies. The ISAE 3402 ED does not contain this requirement. | Paragraph 61 enables the service auditor to modify his or her report in circumstances other than those contemplated in paragraph 60. |