Strafford

Presenting a live 110-minute teleconference with interactive Q&A

Preparing SOC 1, SOC 2 or SOC 3 Reports: Best Practices

Meeting Challenges Arising From SSAE 16, ISAE 3402 and Other Service Company Control Standards

WEDNESDAY, MARCH 7, 2012

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Suzanne Nersessian, Director, National Service Organization Controls Reporting, **Deloitte & Touche**, Boston

David Palmer, Managing Director, **KPMG**, Chicago

Nargiz Yusupova, Manager, **P&N Consulting**, Baton Rouge, La.

Ryan Buckner, Shareholder, **BrightLine CPAs & Assoc.**, Atlanta

For this program, attendees must listen to the audio over the telephone.

Please refer to the instructions emailed to the registrant for the dial-in information. Attendees can still view the presentation slides online. If you have any questions, please contact **Customer Service at1-800-926-7926 ext. 10**.

AT Section 101

Attest Engagements

Source: SSAE No. 10; SSAE No. 11; SSAE No. 12; SSAE No. 14.

See section 9101 for interpretations of this section.

Effective when the subject matter or assertion is as of or for a period ending on or after June 1, 2001, unless otherwise indicated.

Applicability

.01 This section applies to engagements, except for those services discussed in paragraph .04, in which a certified public accountant in the practice of public accounting[1] (hereinafter referred to as a *practitioner*) is engaged to issue or does issue an examination, a review, or an agreed-upon procedures report on subject matter, or an assertion about the subject matter (hereafter referred to as *the assertion*), that is the responsibility of another party.[2]

.02 This section establishes a framework for attest[3] engagements performed by practitioners and for the ongoing development of related standards. For certain subject matter, specific attestation standards have been developed to provide additional requirements for engagement performance and reporting.

.03 When a practitioner undertakes an attest engagement for the benefit of a government body or agency and agrees to follow specified government standards, guides, procedures, statutes, rules, and regulations, the practitioner is obliged to follow those governmental requirements as well as the applicable attestation standards.

.04 Professional services provided by practitioners that are not covered by this SSAE include the following:

a. Services performed in accordance with Statements on Auditing Standards (SASs)

b. Services performed in accordance with Statements on Standards for Accounting and Review Services (SSARSs)

c. Services performed in accordance with the Statement on Standards for Consulting Services (SSCS), such as engagements in which the practitioner's role is solely to assist the client (for example, acting as the company accountant in preparing information other than financial statements), or engagements in which a practitioner is engaged to testify as an expert witness in accounting, auditing, taxation, or other matters, given certain stipulated facts

---

[1] For a definition of the term *practice of public accounting*, see *Definitions* [ET section 92.25].

[2] See section 301, *Financial Forecasts and Projections*,paragraph .02, for additional guidance on applicability when engaged to provide an attest service on a financial forecast or projection.

[3] The term *attest* and its variants, such as *attesting* and *attestation,* are used in a number of state accountancy laws, and in regulations issued by state boards of accountancy under such laws, for different purposes and with different meanings from those intended by this section. Consequently, the definition of *attest engagements* set out in paragraph .01, and the attendant meaning of *attest* and *attestation* as used throughout the section, should not be understood as defining these terms and similar terms, as they are used in any law or regulation, nor as embodying a common understanding of the terms which may also be reflected in such laws or regulations.

d. Engagements in which the practitioner is engaged to advocate a client's position—for example, tax matters being reviewed by the Internal Revenue Service

e. Tax engagements in which a practitioner is engaged to prepare tax returns or provide tax advice

.05 An attest engagement may be part of a larger engagement, for example, a feasibility study or business acquisition study may also include an examination of prospective financial information. In such circumstances, these standards apply only to the attest portion of the engagement.

.06 Any professional service resulting in the expression of assurance must be performed under AICPA professional standards that provide for the expression of such assurance. Reports issued by a practitioner in connection with other professional standards should be written to be clearly distinguishable from and not to be confused with attest reports. For example, a practitioner performing an engagement which is intended solely to assist an organization in improving its controls over the privacy of client data should not issue a report as a result of that engagement expressing assurance as to the effectiveness of such controls. Additionally, a report that merely excludes the words, " ...was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants..." but is otherwise similar to an examination, a review or an agreed-upon procedures attest report may be inferred to be an attest report.

Definitions and Underlying Concepts

Subject Matter

.07 The subject matter of an attest engagement may take many forms, including the following:

a. Historical or prospective performance or condition (for example, historical or prospective financial information, performance measurements, and backlog data)

b. Physical characteristics (for example, narrative descriptions, square footage of facilities)

c. Historical events (for example, the price of a market basket of goods on a certain date)

d. Analyses (for example, break-even analyses)

e. Systems and processes (for example, internal control)

f. Behavior (for example, corporate governance, compliance with laws and regulations, and human resource practices)

The subject matter may be as of a point in time or for a period of time.

Assertion

.08 An assertion is any declaration or set of declarations about whether the subject matter is based on or in conformity with the criteria selected.

.09 A practitioner may report on a written assertion or may report directly on the subject matter. In either case, the practitioner should ordinarily obtain a written assertion in an examination or a review engagement. A written assertion may be presented to a practitioner in a number of ways, such as in a narrative description, within a schedule, or as part of a representation letter appropriately identifying what is being presented and the point in time or period of time covered.

.10 When a written assertion has not been obtained, a practitioner may still report on the subject matter; however, the form of the report will vary depending on the circumstances and its use should be restricted.[4] In this section, see paragraphs .58 and .60 on gathering sufficient evidence and paragraphs .73 to .75 and .78 to .80 for reporting guidance.

Responsible Party

.11 The *responsible party* is defined as the person or persons, either as individuals or representatives of the entity, responsible for the subject matter. If the nature of the subject matter is such that no such party exists, a party who has a reasonable basis for making a written assertion about the subject matter may provide such an assertion (hereinafter referred to as the *responsible party*).

.12 The practitioner may be engaged to gather information to enable the responsible party to evaluate the subject matter in connection with providing a written assertion. Regardless of the procedures performed by the practitioner, the responsible party must accept responsibility for its assertion and the subject matter and must not base its assertion solely on the practitioner's procedures.[5]

.13 Because the practitioner's role in an attest engagement is that of an *attester*, the practitioner should not take on the role of the responsible party in an attest engagement. Therefore, the need to clearly identify a responsible party is a prerequisite for an attest engagement. A practitioner may accept an engagement to perform an examination, a review or an agreed-upon procedures engagement on subject matter or an assertion related thereto provided that one of the following conditions is met.

a. The party wishing to engage the practitioner is responsible for the subject matter, or has a reasonable basis for providing a written assertion about the subject matter if the nature of the subject matter is such that a responsible party does not otherwise exist.

b. The party wishing to engage the practitioner is not responsible for the subject matter but is able to provide the practitioner, or have a third party who is responsible for the subject matter provide the practitioner, with evidence of the third party's responsibility for the subject matter.

.14 The practitioner should obtain written acknowledgment or other evidence of the responsible party's responsibility for the subject matter, or the written assertion, as it relates to the objective of the engagement. The responsible party can acknowledge that responsibility in a number of ways, for example, in an engagement letter, a representation letter, or the presentation of the subject matter, including the notes thereto, or the written assertion. If the practitioner is not able to directly obtain written acknowledgment, the practitioner should obtain other evidence of the responsible party's responsibility for the subject matter (for example, by reference to legislation, a regulation, or a contract).

---

[4] When the practitioner is unable to perform the inquiry and analytical or other procedures that he or she considers necessary to achieve the limited assurance contemplated by a review, or when the client is the responsible party and does not provide the practitioner with a written assertion, the review will be incomplete. A review that is incomplete is not an adequate basis for issuing a review report and, accordingly, the practitioner should withdraw from the engagement.

[5] See paragraph .112 regarding the practitioner's assistance in developing subject matter or criteria.

Applicability to Agreed-Upon Procedures Engagements

.15 An agreed-upon procedures attest engagement is one in which a practitioner is engaged to issue a report of findings based on specific procedures performed on subject matter. The general, fieldwork, and reporting standards for attest engagements set forth in this section are applicable to agreed-upon procedures engagements. Because the application of these standards to agreed-upon procedures engagements is discussed in section 201, *Agreed-Upon Procedures Engagements*, such engagements are not discussed further in this section.

The Relationship of Attestation Standards to Quality Control Standards

.16 The practitioner is responsible for compliance with the American Institute of Certified Public Accountants' (AICPA's) Statements on Standards for Attestation Engagements (SSAEs) in an attest engagement. Rule 202, *Compliance With Standards*, of the Code of Professional Conduct [ET section 202.01], requires members to comply with such standards when conducting professional services.

.17 A firm of practitioners has a responsibility to adopt a system of quality control in the conduct of a firm's attest practice.[6] Thus, a firm should establish quality control policies and procedures to provide it with reasonable assurance that its personnel comply with the attestation standards in its attest engagements. The nature and extent of a firm's quality control policies and procedures depend on factors such as its size, the degree of operating autonomy allowed its personnel and its practice offices, the nature of its practice, its organization, and appropriate cost-benefit considerations. [As amended, effective September 2002, by SSAE No. 12.]

.18 Attestation standards relate to the conduct of individual attest engagements; quality control standards relate to the conduct of a firm's attest practice as a whole. Thus, attestation standards and quality control standards are related and the quality control policies and procedures that a firm adopts may affect both the conduct of individual attest engagements and the conduct of a firm's attest practice as a whole. However, deficiencies in or instances of noncompliance with a firm's quality control policies and procedures do not, in and of themselves, indicate that a particular engagement was not performed in accordance with attestation standards. [As amended, effective September 2002, by Statement on Standards for Attestation Engagements No. 12.]

General Standards

Training and Proficiency

.19 The first general standard is—*The practitioner must have adequate technical training and proficiency to perform the attestation engagement.* [As amended, effective when the subject matter or assertion is as of or for a period

---

[6] The elements of a system of quality control are identified in Statement on Quality Control Standards (SQCS) No. 7, *A Firm's System of Quality Control* [QC section 10A]. A system of quality control consists of policies designed to provide the firm with reasonable assurance that the firm and its personnel comply with professional standards and applicable legal and regulatory requirements and that reports issued by the firm are appropriate in the circumstances, and the procedures necessary to implement and monitor compliance with those policies. [As amended, effective September 2002, by SSAE No. 12. Footnote amended due to the issuance of SQCS No. 7, December 2008.]

ending on or after December 15, 2006, by Statement on Standards for Attestation Engagements No. 14.]

.20 Performing attest services is different from preparing and presenting subject matter or an assertion. The latter involves collecting, classifying, summarizing, and communicating information; this usually entails reducing a mass of detailed data to a manageable and understandable form. On the other hand, performing attest services involves gathering evidence to support the subject matter or the assertion and objectively assessing the measurements and communications of the responsible party. Thus, attest services are analytical, critical, investigative, and are concerned with the basis and support for the subject matter or the assertion.

Adequate Knowledge of Subject Matter

.21 The second general standard is—*The practitioner must have adequate knowledge of the subject matter.* [As amended, effective when the subject matter or assertion is as of or for a period ending on or after December 15, 2006, by Statement on Standards for Attestation Engagements No. 14.]

.22 A practitioner may obtain adequate knowledge of the subject matter through formal or continuing education, including self-study, or through practical experience. However, this standard does not necessarily require a practitioner to personally acquire all of the necessary knowledge in the subject matter to be qualified to express a conclusion. This knowledge requirement may be met, in part, through the use of one or more specialists on a particular attest engagement if the practitioner has sufficient knowledge of the subject matter (*a*) to communicate to the specialist the objectives of the work and (*b*) to evaluate the specialist's work to determine if the objectives were achieved.

Suitability and Availability of Criteria

.23 The third general standard is—*The practitioner must have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users.* [As amended, effective when the subject matter or assertion is as of or for a period ending on or after December 15, 2006, by Statement on Standards for Attestation Engagements No. 14.]

Suitability of Criteria

.24 Criteria are the standards or benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter.[*] Suitable criteria must have each of the following attributes:

- *Objectivity*—Criteria should be free from bias.
- *Measurability*—Criteria should permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
- *Completeness*—Criteria should be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted.
- *Relevance*—Criteria should be relevant to the subject matter.

.25 Criteria that are established or developed by groups composed of experts that follow due process procedures, including exposure of the proposed

---

[*] An example of suitable criteria are the Trust Services criteria (includes WebTrust and SysTrust) developed by the AICPA's Assurance Services Executive Committee. These criteria may be used when the subject matter of the engagement is the security, availability, processing integrity, or confidentiality of a system or an entity's privacy. The Trust Services criteria are presented in TSP sections 100 and 200 of the AICPA's *Technical Practice Aids*. [Footnote added by the Assurance Services Executive Committee, January 2003. Footnote revised, May 2006, to reflect conforming changes necessary due to the issuance of Generally Accepted Privacy Principles.]

criteria for public comment, ordinarily should be considered suitable. Criteria promulgated by a body designated by the AICPA Governing Council under the AICPA Code of Professional Conduct are, by definition, considered to be suitable.

.26 Criteria may be established or developed by the client, the responsible party, industry associations, or other groups that do not follow due process procedures or do not as clearly represent. the public interest. To determine whether these criteria are suitable, the practitioner should evaluate them based on the attributes described in paragraph .24.

.27 Regardless of who establishes or develops the criteria, the responsible party or the client is responsible for selecting the criteria and the client is responsible for determining that such criteria are appropriate for its purposes.

.28 The use of suitable criteria does not presume that all persons or groups would be expected to select the same criteria in evaluating the same subject matter. There may be more than one set of suitable criteria for a given subject matter. For example, in an engagement to express assurance about customer satisfaction, a responsible party may select as a criterion for customer satisfaction that all customer complaints are resolved to the satisfaction of the customer. In other cases, another responsible party may select a different criterion, such as the number of repeat purchases in the three months following the initial purchase.

.29 In evaluating the measurability attribute as described in paragraph .24, the practitioner should consider whether the criteria are sufficiently precise to permit people having competence in and using the same measurement criterion to be able to ordinarily obtain materially similar measurements. Consequently, practitioners should not perform an engagement when the criteria are so subjective or vague that reasonably consistent measurements, qualitative or quantitative, of subject matter cannot ordinarily be obtained. However, practitioners will not always reach the same conclusion because such evaluations often require the exercise of considerable professional judgment.

.30 For the purpose of assessing whether the use of particular criteria can be expected to yield reasonably consistent measurement and evaluation, consideration should be given to the nature of the subject matter. For example, *soft information*, such as forecasts or projections, would be expected to have a wider range of reasonable estimates than *hard* data, such as the calculated investment performance of a defined portfolio of managed investment products.

.31 Some criteria may be appropriate for only a limited number of parties who either participated in their establishment or can be presumed to have an adequate understanding of the criteria. For instance, criteria set forth in a lease agreement for override payments may be appropriate only for reporting to the parties to the agreement because of the likelihood that such criteria would be misunderstood or misinterpreted by parties other than those who have specifically agreed to the criteria. Such criteria can be agreed upon directly by the parties or through a designated representative. If a practitioner determines that such criteria are appropriate only for a limited number of parties, the use of the report should be restricted to those specified parties who either participated in their establishment or can be presumed to have an adequate understanding of the criteria.

.32 The third general standard in paragraph .23 applies equally regardless of the level of the attest service to be provided. Consequently, it is inappropriate to perform a review engagement if the practitioner concludes that an examination cannot be performed because competent persons using the same criteria would not be able to obtain materially similar evaluations.

Availability of Criteria

.33 The criteria should be available to users in one or more of the following ways:

a. Available publicly

b. Available to all users through inclusion in a clear manner in the presentation of the subject matter or in the assertion

c. Available to all users through inclusion in a clear manner in the practitioner's report

d. Well understood by most users, although not formally available (for example, "The distance between points A and B is twenty feet;" the criterion of distance measured in feet is considered to be well understood)

e. Available only to specified parties; for example, terms of a contract or criteria issued by an industry association that are available only to those in the industry

.34 If criteria are only available to specified parties, the practitioner's report should be restricted to those parties who have access to the criteria as described in paragraphs .78 and .80.

Independence

.35 The fourth general standard is—*The practitioner must maintain independence in mental attitude in all matters relating to the engagement.*[7] [As amended, effective when the subject matter or assertion is as of or for a period ending on or after December 15, 2006, by Statement on Standards for Attestation Engagements No. 14.]

.36 The practitioner should maintain the intellectual honesty and impartiality necessary to reach an unbiased conclusion about the subject matter or the assertion. This is a cornerstone of the attest function.

.37 In the final analysis, independence in mental attitude means objective consideration of facts, unbiased judgments, and honest neutrality on the part of the practitioner in forming and expressing conclusions. It implies not the attitude of an advocate or an adversary but an impartiality that recognizes an obligation for fairness. Independence in mental attitude presumes an undeviating concern for an unbiased conclusion about the subject matter or an assertion no matter what the subject matter or the assertion may be.

.38 The profession has established, through the AICPA's Code of Professional Conduct, precepts to guard against the *presumption* of loss of independence. Presumption is stressed because the possession of intrinsic independence is a matter of personal quality rather than of rules that formulate certain objective tests. Insofar as these precepts have been incorporated in the profession's code, they have the force of professional law for the independent practitioner.

---

[7] The practitioner performing an attest engagement should be *independent* pursuant to Rule 101, *Independence*, of the Code of Professional Conduct [ET section 101.01]. Interpretation No. 11, "Independence and the Performance of Professional Services Under the Statements on Standards for Attestation Engagements and Statement on Auditing Standards No. 75, *Engagements to Apply Agreed-Upon Procedures to Specified Elements, Accounts, or Items of a Financial Statement*," [ET section 101.13], to rule 101 [ET section 101.01] provides guidance about its application to certain attest engagements.

Due Professional Care

.39 The fifth general standard is—*The practitioner must exercise due professional care in the planning and performance of the engagement and the preparation of the report.* [As amended, effective when the subject matter or assertion is as of or for a period ending on or after December 15, 2006, by Statement on Standards for Attestation Engagements No. 14.]

.40 Due professional care imposes a responsibility on each practitioner involved with the engagement to observe each of the attestation standards. Exercise of due professional care requires critical review at every level of supervision of the work done and the judgment exercised by those assisting in the engagement, including the preparation of the report.

.41 *Cooley on Torts*, a legal treatise, describes the obligation for due care as follows:

> Every man who offers his services to another and is employed assumes the duty to exercise in the employment such skill as he possesses with reasonable care and diligence. In all these employments where peculiar skill is requisite, if one offers his services, he is understood as holding himself out to the public as possessing the degree of skill commonly possessed by others in the same employment, and if his pretentions are unfounded, he commits a species of fraud upon every man who employs him in reliance on his public profession. But no man, whether skilled or unskilled, undertakes that the task he assumes shall be performed successfully, and without fault or error; he undertakes for good faith and integrity, but not for infallibility, and he is liable to his employer for negligence, bad faith, or dishonesty, but not for losses consequent upon mere errors of judgment.[8]

Standards of Fieldwork

Planning and Supervision

.42 The first standard of fieldwork is—*The practitioner must adequately plan the work and must properly supervise any assistants.* [As amended, effective when the subject matter or assertion is as of or for a period ending on or after December 15, 2006, by Statement on Standards for Attestation Engagements No. 14.]

.43 Proper planning and supervision contribute to the effectiveness of attest procedures. Proper planning directly influences the selection of appropriate procedures and the timeliness of their application, and proper supervision helps ensure that planned procedures are appropriately applied.

.44 Planning an attest engagement involves developing an overall strategy for the expected conduct and scope of the engagement. To develop such a strategy, practitioners need to have sufficient knowledge to enable them to understand adequately the events, transactions, and practices that, in their judgment, have a significant effect on the subject matter or the assertion.

.45 Factors to be considered by the practitioner in planning an attest engagement include the following:

a. The criteria to be used

---

[8] D. Haggard, *Cooley on Torts*, 472 (4th ed., 1932).

b. Preliminary judgments about attestation risk[9] and materiality for attest purposes

c. The nature of the subject matter or the items within the assertion that are likely to require revision or adjustment

d. Conditions that may require extension or modification of attest procedures

e. The nature of the report expected to be issued

.46 The practitioner should establish an understanding with the client regarding the services to be performed for each engagement.[10] Such an understanding reduces the risk that either the practitioner or the client may misinterpret the needs or expectations of the other party. For example, it reduces the risk that the client may inappropriately rely on the practitioner to protect the entity against certain risks or to perform certain functions that are the client's responsibility. The understanding should include the objectives of the engagement, management's responsibilities, the practitioner's responsibilities, and limitations of the engagement. The practitioner should document the understanding in the working papers, preferably through a written communication with the client. If the practitioner believes an understanding with the client has not been established, he or she should decline to accept or perform the engagement.

.47 The nature, extent, and timing of planning will vary with the nature and complexity of the subject matter or the assertion and the practitioner's prior experience with management. As part of the planning process, the practitioner should consider the nature, extent, and timing of the work to be performed to accomplish the objectives of the attest engagement. Nevertheless, as the attest engagement progresses, changed conditions may make it necessary to modify planned procedures.

.48 Supervision involves directing the efforts of assistants who participate in accomplishing the objectives of the attest engagement and determining whether those objectives were accomplished. Elements of supervision include instructing assistants, staying informed of significant problems encountered, reviewing the work performed, and dealing with differences of opinion among personnel. The extent of supervision appropriate in a given instance depends on many factors, including the nature and complexity of the subject matter and the qualifications of the persons performing the work.

.49 Assistants should be informed of their responsibilities, including the objectives of the procedures that they are to perform and matters that may affect the nature, extent, and timing of such procedures. The practitioner with final responsibility for the engagement should direct assistants to bring to his or her attention significant questions raised during the attest engagement so that their significance may be assessed.

.50 The work performed by each assistant should be reviewed to determine whether it was adequately performed and to evaluate whether the results are consistent with the conclusion to be presented in the practitioner's report.

---

[9] *Attestation risk* is the risk that the practitioner may unknowingly fail to appropriately modify his or her attest report on the subject matter or an assertion that is materially misstated. It consists of (*a*) the risk (consisting of *inherent risk* and *control risk*) that the subject matter or assertion contains deviations or misstatements that could be material and (*b*) the risk that the practitioner will not detect such deviations or misstatements (*detection risk*).

[10] See SQCS No. 7 paragraph 28 (QC sec. 10A). [Footnote amended due to the issuance of SQCS No. 7, December 2008.]

Obtaining Sufficient Evidence

.51 The second standard of fieldwork is—*The practitioner must obtain sufficient evidence to provide a reasonable basis for the conclusion that is expressed in the report.* [As amended, effective when the subject matter or assertion is as of or for a period ending on or after December 15, 2006, by Statement on Standards for Attestation Engagements No. 14.]

.52 Selecting and applying procedures that will accumulate evidence that is sufficient in the circumstances to provide a reasonable basis for the level of assurance to be expressed in the attest report requires the careful exercise of professional judgment. A broad array of available procedures may be applied in an attest engagement. In establishing a proper combination of procedures to appropriately restrict attestation risk, the practitioner should consider the following presumptions, bearing in mind that they are not mutually exclusive and may be subject to important exceptions.

a. Evidence obtained from independent sources outside an entity provides greater assurance about the subject matter or the assertion than evidence secured solely from within the entity.

b. Information obtained from the independent attester's direct personal knowledge (such as through physical examination, observation, computation, operating tests, or inspection) is more persuasive than information obtained indirectly.

c. The more effective the controls over the subject matter, the more assurance they provide about the subject matter or the assertion.

.53 Thus, in the hierarchy of available attest procedures, those that involve search and verification (for example, inspection, confirmation, or observation), particularly when using independent sources outside the entity, are generally more effective in restricting attestation risk than those involving internal inquiries and comparisons of internal information (for example, analytical procedures and discussions with individuals responsible for the subject matter or the assertion). On the other hand, the latter are generally less costly to apply.

.54 In an attest engagement designed to provide a high level of assurance (referred to as an *examination*), the practitioner's objective is to accumulate sufficient evidence to restrict attestation risk to a level that is, in the practitioner's professional judgment, appropriately low for the high level of assurance that may be imparted by his or her report. In such an engagement, a practitioner should select from all available procedures—that is, procedures that assess inherent and control risk and restrict detection risk—any combination that can restrict attestation risk to such an appropriately low level.

.55 In an attest engagement designed to provide a moderate level of assurance (referred to as a *review*), the objective is to accumulate sufficient evidence to restrict attestation risk to a moderate level. To accomplish this, the types of procedures performed generally are limited to inquiries and analytical procedures (rather than also including search and verification procedures).

.56 Nevertheless, there will be circumstances in which inquiry and analytical procedures (*a*) cannot be performed, (*b*) are deemed less efficient than other procedures, or (*c*) yield evidence indicating that the subject matter or the assertion may be incomplete or inaccurate. In the first circumstance, the practitioner should perform other procedures that he or she believes can provide him or her with a level of assurance equivalent to that which inquiries and analytical procedures would have provided. In the second circumstance,

the practitioner may perform other procedures that he or she believes would be more efficient to provide him or her with a level of assurance equivalent to that which inquiries and analytical procedures would provide. In the third circumstance, the practitioner should perform additional procedures.

.57 The extent to which attestation procedures will be performed should be based on the level of assurance to be provided and the practitioner's consideration of (*a*) the nature and materiality of the information to be tested to the subject matter or the assertion taken as a whole, (*b*) the likelihood of misstatements, (*c*) knowledge obtained during current and previous engagements, (*d*) the responsible party's competence in the subject matter, (*e*) the extent to which the information is affected by the asserter's judgment, and (*f*) inadequacies in the responsible party's underlying data.

.58 As part of the attestation procedures, the practitioner considers the written assertion ordinarily provided by the responsible party. If a written assertion cannot be obtained from the responsible party, the practitioner should consider the effects on his or her ability to obtain sufficient evidence to form a conclusion about the subject matter. When the practitioner's client is the responsible party, a failure to obtain a written assertion should result in the practitioner concluding that a scope limitation exists.[11] When the practitioner's client is not the responsible party and a written assertion is not provided, the practitioner may be able to conclude that he or she has sufficient evidence to form a conclusion about the subject matter.

Representation Letter

.59 During an attest engagement, the responsible party makes many representations to the practitioner, both oral and written, in response to specific inquiries or through the presentation of subject matter or an assertion. Such representations from the responsible party are part of the evidential matter the practitioner obtains.

.60 Written representations from the responsible party ordinarily confirm representations explicitly or implicitly given to the practitioner, indicate and document the continuing appropriateness of such representations, and reduce the possibility of misunderstanding concerning the matters that are the subject of the representations. Accordingly, in an examination or a review engagement, a practitioner should consider obtaining a representation letter from the responsible party. Examples of matters that might appear in such a representation letter include the following:[12]

a. A statement acknowledging responsibility for the subject matter and, when applicable, the assertion

b. A statement acknowledging responsibility for selecting the criteria, where applicable

---

[11] When the client is the responsible party, it is presumed that the client will be capable of providing the practitioner with a written assertion regarding the subject matter. Failure to provide the written assertion in this circumstance is a client-imposed limitation on the practitioner's evidence-gathering efforts. In an examination, the practitioner should modify the report for the scope limitation. In a review engagement, such a scope limitation results in an incomplete review and the practitioner should withdraw from the engagement.

[12] Specific written representations will depend on the circumstances of the engagement (for example, whether the client is the responsible party) and the nature of the subject matter and the criteria. For example, when the client is not the responsible party but has selected the criteria, the practitioner might obtain the representation regarding responsibility for selection of the criteria from the client rather than the responsible party (see paragraph .61).

c. A statement acknowledging responsibility for determining that such criteria are appropriate for its purposes, where the responsible party is the client

d. The assertion about the subject matter based on the criteria selected

e. A statement that all known matters contradicting the assertion and any communication from regulatory agencies affecting the subject matter or the assertion have been disclosed to the practitioner

f. Availability of all records relevant to the subject matter

g. A statement that any known events subsequent to the period (or point in time) of the subject matter being reported on that would have a material effect on the subject matter (or, if applicable, the assertion) have been disclosed to the practitioner

h. Other matters as the practitioner deems appropriate

.61 When the client is not the responsible party, the practitioner should consider obtaining a letter of written representations from the client as part of the attest engagement. Examples of matters that might appear in such a representation letter include the following:

a. A statement that any known events subsequent to the period (or point in time) of the subject matter being reported on that would have a material effect on the subject matter (or, if applicable, the assertion) have been disclosed to the practitioner

b. A statement acknowledging the client's responsibility for selecting the criteria, where applicable

c. A statement acknowledging the client's responsibility for determining that such criteria are appropriate for its purposes

d. Other matters as the practitioner deems appropriate

.62 If the responsible party or the client refuses to furnish all written representations that the practitioner deems necessary, the practitioner should consider the effects of such a refusal on his or her ability to issue a conclusion about the subject matter. If the practitioner believes that the representation letter is necessary to obtain sufficient evidence to issue a report, the responsible party's or the client's refusal to furnish such evidence in the form of written representations constitutes a limitation on the scope of an examination sufficient to preclude an unqualified opinion and is ordinarily sufficient to cause the practitioner to disclaim an opinion or withdraw from an examination engagement. However, based on the nature of the representations not obtained or the circumstances of the refusal, the practitioner may conclude, in an examination engagement, that a qualified opinion is appropriate. Further, the practitioner should consider the effects of the refusal on his or her ability to rely on other representations. When a scope limitation exists in a review engagement, the practitioner should withdraw from the engagement. (See paragraph .75.)

Standards of Reporting[13]

.63 The first standard of reporting is—*The practitioner must identify the subject matter or the assertion being reported on and state the character of the engagement in the report.* [As amended, effective when the subject matter or assertion is as of or for a period ending on or after December 15, 2006, by Statement on Standards for Attestation Engagements No. 14.]

[13] The reporting standards apply only when the practitioner issues a report. [Footnote added, effective when the subject matter or assertion is as of or for a period ending on or after December 15, 2006, by Statement on Standards for Attestation Engagements No. 14.]

.64 The practitioner who accepts an attest engagement should issue a report on the subject matter or the assertion or withdraw from the attest engagement. If the practitioner is reporting on the assertion, the assertion should be bound with or accompany the practitioner's report or the assertion should be clearly stated in the practitioner's report.[14]

.65 The statement of the character of an attest engagement includes the following two elements: (*a*) a description of the nature and scope of the work performed and (*b*) a reference to the professional standards governing the engagement. The terms *examination* and *review* should be used to describe engagements to provide, respectively, a high level and a moderate level of assurance. The reference to professional standards should be accomplished by referring to "attestation standards established by the American Institute of Certified Public Accountants."

.66 The second standard of reporting is—*The practitioner must state the practitioner's conclusion about the subject matter or the assertion in relation to the criteria against which the subject matter was evaluated in the report.* However, if conditions exist that, individually or in combination, result in one or more material misstatements or deviations from the criteria, the practitioner should modify the report and, to most effectively communicate with the reader of the report, should ordinarily express his or her conclusion directly on the subject matter,[15] not on the assertion. [As amended, effective when the subject matter or assertion is as of or for a period ending on or after December 15, 2006, by Statement on Standards for Attestation Engagements No. 14.]

.67 The practitioner should consider the concept of materiality in applying this standard. In expressing a conclusion, the practitioner should consider 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. The practitioner should consider both qualitative and quantitative aspects of omissions and misstatements.

.68 The term *general use* applies to attest reports that are not restricted to specified parties. General-use attest reports should be limited to two levels of assurance: one based on a restriction of attestation risk to an appropriately low level (an *examination*) and the other based on a restriction of attestation risk to a moderate level (a *review*). In an engagement to achieve a high level of assurance (an *examination*), the practitioner's conclusion should be expressed in the form of an opinion. When attestation risk has been restricted only to a moderate level (a *review*), the conclusion should be expressed in the form of negative assurance.

.69 A practitioner may report on subject matter or an assertion at multiple dates or covering multiple periods during which criteria have changed (for example, a report on comparative information). In those circumstances, the practitioner should determine whether the criteria are clearly stated or described for each of the dates or periods, and whether the changes have been adequately disclosed.

---

[14] The use of a "hot link" within the practitioner's report to management's assertion, such as might be used in a WebTrust℠ report, would meet this requirement. [Footnote renumbered by the issuance of Statement on Standards for Attestation Engagements No. 14, November 2006.]

[15] Specific standards may require that the practitioner express his or her conclusion directly on the subject matter. For example, if management states in its assertion that a material weakness exists in the entity's internal control over financial reporting, the practitioner should state his or her opinion directly on the effectiveness of internal control, not on management's assertion related thereto. [Footnote renumbered by the issuance of Statement on Standards for Attestation Engagements No. 14, November 2006.]

.70 If the criteria used for the subject matter for the current date or period differ from those criteria used for the subject matter for a preceding date or period and the subject matter for the prior date or period is not presented, the practitioner should consider whether the changes in criteria are likely to be significant to users of the report. If so, the practitioner should determine whether the criteria are clearly stated or described and the fact that the criteria have changed is disclosed. (See paragraphs .76 and .77.)

.71 The third standard of reporting is—*The practitioner must state all of the practitioner's significant reservations about the engagement, the subject matter, and, if applicable, the assertion related thereto in the report.* [As amended, effective when the subject matter or assertion is as of or for a period ending on or after December 15, 2006, by Statement on Standards for Attestation Engagements No. 14.]

.72 *Reservations about the engagement* refers to any unresolved problem that the practitioner had in complying with these attestation standards, interpretive standards, or the specific procedures agreed to by the specified parties. The practitioner should not express an unqualified conclusion unless the engagement has been conducted in accordance with the attestation standards. Such standards will not have been complied with if the practitioner has been unable to apply all the procedures that he or she considers necessary in the circumstances.

.73 Restrictions on the scope of an engagement, whether imposed by the client or by such other circumstances as the timing of the work or the inability to obtain sufficient evidence, may require the practitioner to qualify the assurance provided, to disclaim any assurance, or to withdraw from the engagement. For example, if the practitioner's client is the responsible party, a failure to obtain a written assertion should result in the practitioner concluding that a scope limitation exists. (See paragraph .58.)

.74 The practitioner's decision to provide a qualified opinion, to disclaim an opinion, or to withdraw because of a scope limitation in an examination engagement depends on an assessment of the effect of the omitted procedure(s) on his or her ability to express assurance. This assessment will be affected by the nature and magnitude of the potential effects of the matters in question, and by their significance to the subject matter or the assertion. If the potential effects are pervasive to the subject matter or the assertion, a disclaimer or withdrawal is more likely to be appropriate. When restrictions that significantly limit the scope of the engagement are imposed by the client or the responsible party, the practitioner generally should disclaim an opinion or withdraw from the engagement. The reasons for a qualification or disclaimer should be described in the practitioner's report.

.75 In a review engagement, when the practitioner is unable to perform the inquiry and analytical or other procedures he or she considers necessary to achieve the limited assurance contemplated by a review, or when the client is the responsible party and does not provide the practitioner with a written assertion, the review will be incomplete. A review that is incomplete is not an adequate basis for issuing a review report and, accordingly, the practitioner should withdraw from the engagement.

.76 *Reservations about the subject matter or the assertion* refers to any unresolved reservation about the assertion or about the conformity of the subject matter with the criteria, including the adequacy of the disclosure of material matters. They can result in either a qualified or an adverse opinion, depending on the materiality of the departure from the criteria against which the subject

matter or the assertion was evaluated, or a modified conclusion in a review engagement.

.77 Reservations about the subject matter or the assertion may relate to the measurement, form, arrangement, content, or underlying judgments and assumptions applicable to the subject matter or the assertion and its appended notes, including, for example, the terminology used, the amount of detail given, the classification of items, and the bases of amounts set forth. The practitioner considers whether a particular reservation should affect the report given the circumstances and facts of which he or she is aware at the time.

.78 The fourth standard of reporting is—*The practitioner must state in the report that the report is intended solely for the information and use of the specified parties under the following circumstances:*

- *When the criteria used to evaluate the subject matter are determined by the practitioner to be 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*
- *When the criteria used to evaluate the subject matter are available only to specified parties*
- *When reporting on subject matter and a written assertion has not been provided by the responsible party*
- *When the report is on an attestation engagement to apply agreed-upon procedures to the subject matter*

[As amended, effective when the subject matter or assertion is as of or for a period ending on or after December 15, 2006, by Statement on Standards for Attestation Engagements No. 14.]

.79 The need for restriction on the use of a report may result from a number of circumstances, including the purpose of the report, the criteria used in preparation of the subject matter, the extent to which the procedures performed are known or understood, and the potential for the report to be misunderstood when taken out of the context in which it was intended to be used. A practitioner should consider informing his or her client that restricted-use reports are not intended for distribution to nonspecified parties, regardless of whether they are included in a document containing a separate general-use report.[16, 17] However, a practitioner is not responsible for controlling a client's distribution of restricted-use reports. Accordingly, a restricted-use report should alert readers to the restriction on the use of the report by indicating that the report is not intended to be and should not be used by anyone other than the specified parties.

.80 An attest report that is restricted as to use should contain a separate paragraph at the end of the report that includes the following elements:

a. A statement indicating that the report is intended solely for the information and use of the specified parties

---

[16] In some cases, restricted-use reports filed with regulatory agencies are required by law or regulation to be made available to the public as a matter of public record. Also, a regulatory agency as part of its oversight responsibility for an entity may require access to restricted-use reports in which they are not named as a specified party. [Footnote renumbered by the issuance of Statement on Standards for Attestation Engagements No. 14, November 2006.]

[17] This section does not preclude the practitioner, in connection with establishing the terms of the engagement, from reaching an understanding with the client that the intended use of the report will be restricted, and from obtaining the client's agreement that the client and the specified parties will not distribute the report to parties other than those identified in the report. [Footnote renumbered by the issuance of Statement on Standards for Attestation Engagements No. 14, November 2006.]

b. An identification of the specified parties to whom use is restricted

c. A statement that the report is not intended to be and should not be used by anyone other than the specified parties

An example of such a paragraph is the following.

> This report is intended solely for the information and use of [*the specified parties*] and is not intended to be and should not be used by anyone other than these specified parties.

.81 Other attestation standards may specify situations that require restricted reports such as the following:

a. A review report on management's discussion and analysis

b. A report on prospective financial information when the report is intended for use by the responsible party alone, or by the responsible party and third parties with whom the responsible party is negotiating directly, as described in section 301, *Financial Forecasts and Projections*, paragraph .10.

Furthermore, nothing in this section precludes a practitioner from restricting the use of any report.

.82 If a practitioner issues a single combined report covering both (*a*) subject matter or presentations that require a restriction on use to specified parties and (*b*) subject matter or presentations that ordinarily do not require such a restriction, the use of such a single combined report should be restricted to the specified parties.

.83 In some instances, a separate restricted-use report may be included in a document that also contains a general-use report. The inclusion of a separate restricted-use report in a document that contains a general-use report does not affect the intended use of either report. The restricted-use report remains restricted as to use, and the general-use report continues to be for general use.

Examination Reports

.84 When expressing an opinion, the practitioner should clearly state whether, in his or her opinion, (*a*) the subject matter is based on (or in conformity with) the criteria in all material respects or (*b*) the assertion is presented (or fairly stated), in all material respects, based on the criteria. Reports expressing an opinion may be qualified or modified for some aspect of the subject matter, the assertion or the engagement (see the third reporting standard). However, as stated in paragraph .66, if conditions exist that, individually or in combination, result in one or more material misstatements or deviations from the criteria, the practitioner should modify the report and, to most effectively communicate with the reader of the report, should ordinarily express his or her conclusion directly on the subject matter, not on the assertion. In addition, such reports may emphasize certain matters relating to the attest engagement, the subject matter, or the assertion. The form of the practitioner's report will depend on whether the practitioner opines on the subject matter or the assertion.

.85 The practitioner's examination report on subject matter should include the following:

a. A title that includes the word *independent*

b. An identification of the subject matter and the responsible party

c. A statement that the subject matter is the responsibility of the responsible party

d. A statement that the practitioner's responsibility is to express an opinion on the subject matter based on his or her examination

e. A statement that the examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and, accordingly, included procedures that the practitioner considered necessary in the circumstances

f. A statement that the practitioner believes the examination provides a reasonable basis for his or her opinion

g. The practitioner's opinion on whether the subject matter is based on (or in conformity with) the criteria in all material respects

h. A statement restricting the use of the report to specified parties under the following circumstances (see paragraphs .78 to .83):

(1) When the criteria used to evaluate the subject matter are determined by the practitioner to be 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

(2) When the criteria used to evaluate the subject matter are available only to the specified parties

(3) When a written assertion has not been provided by the responsible party (The practitioner should also include a statement to that effect in the introductory paragraph of the report.)

i. The manual or printed signature of the practitioner's firm

j. The date of the examination report

Appendix A [paragraph .114], *Examination Reports*, includes a standard examination report on subject matter. (See Example 1.)

.86 The practitioner's examination report on an assertion should include the following:

a. A title that includes the word *independent*

b. An identification of the assertion and the responsible party (When the assertion does not accompany the practitioner's report, the first paragraph of the report should also contain a statement of the assertion.)

c. A statement that the assertion is the responsibility of the responsible party

d. A statement that the practitioner's responsibility is to express an opinion on the assertion based on his or her examination

e. A statement that the examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and, accordingly, included procedures that the practitioner considered necessary in the circumstances

f. A statement that the practitioner believes the examination provides a reasonable basis for his or her opinion

g. The practitioner's opinion on whether the assertion is presented (or fairly stated), in all material respects, based on the criteria (However, see paragraph .66.)

h. A statement restricting the use of the report to specified parties under the following circumstances (see paragraphs .78 to .83):

(1) When the criteria used to evaluate the subject matter are determined by the practitioner to be 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

(2) When the criteria used to evaluate the subject matter are available only to the specified parties

i. The manual or printed signature of the practitioner's firm

j. The date of the examination report

Appendix A [paragraph .114] includes a standard examination report on an assertion. (See Example 2.)

.87 Nothing precludes the practitioner from examining an assertion but opining directly on the subject matter. (See Appendix A [paragraph .114], Example 3.)

Review Reports

.88 In a review report, the practitioner's conclusion should state whether any information came to the practitioner's attention on the basis of the work performed that indicates that (*a*) the subject matter is not based on (or in conformity with) the criteria or (*b*) the assertion is not presented (or fairly stated) in all material respects based on the criteria. (As discussed more fully in the commentary to the third reporting standard, if the subject matter or the assertion is not modified to correct for any such information that comes to the practitioner's attention, such information should be described in the practitioner's report.)

.89 The practitioner's review report on subject matter should include the following:

a. A title that includes the word *independent*

b. An identification of the subject matter and the responsible party

c. A statement that the subject matter is the responsibility of the responsible party

d. A statement that the review was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants

e. A statement that a review is substantially less in scope than an examination, the objective of which is an expression of opinion on the subject matter, and accordingly, no such opinion is expressed

f. A statement about whether the practitioner is aware of any material modifications that should be made to the subject matter in order for it to be based on (or in conformity with), in all material respects, the criteria, other than those modifications, if any, indicated in his or her report

g. A statement restricting the use of the report to specified parties under the following circumstances (see paragraphs .78 to .83):

(1) When the criteria used to evaluate the subject matter are determined by the practitioner to be 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

(2) When the criteria used to evaluate the subject matter are available only to the specified parties

(3) When a written assertion has not been provided by the responsible party and the responsible party is not the client (The practitioner should also include a statement to that effect in the introductory paragraph of the report.)

h. The manual or printed signature of the practitioner's firm

i. The date of the review report

Appendix B [paragraph .115] *Review Reports*, includes a standard review report on subject matter. (See Example 1.) Appendix B [paragraph .115] also includes a review report on subject matter that is the responsibility of a party other than client; the report is restricted as to use because a written assertion has not been provided by the responsible party. (See Example 2.)

.90 The practitioner's review report on an assertion should include the following:

a. A title that includes the word *independent*

b. An identification of the assertion and the responsible party (When the assertion does not accompany the practitioner's report, the first paragraph of the report should also contain a statement of the assertion.)

c. A statement that the assertion is the responsibility of the responsible party

d. A statement that the review was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants

e. A statement that a review is substantially less in scope than an examination, the objective of which is an expression of opinion on the assertion, and accordingly, no such opinion is expressed

f. A statement about whether the practitioner is aware of any material modifications that should be made to the assertion in order for it to be presented (or fairly stated), in all material respects, based on (or in conformity with) the criteria, other than those modifications, if any, indicated in his or her report (However, see paragraph .66.)

g. A statement restricting the use of the report to specified parties under the following circumstances (see paragraphs .78 to .83):

(1) When the criteria used to evaluate the subject matter are determined by the practitioner to be 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

(2) When the criteria used to evaluate the subject matter are available only to the specified parties

h. The manual or printed signature of the practitioner's firm

i. The date of the review report

Appendix B [paragraph .115] includes a review report on an assertion that is restricted as to use because the criteria are available only to the specified parties. (See Example 3.)

Other Information in a Client-Prepared Document Containing the Practitioner's Attest Report[18]

.91 A client may publish various documents that contain information (hereinafter referred to as *other information*) in addition to the practitioner's attest report on subject matter (or on an assertion related thereto). Paragraphs .92 to .94 provide guidance to the practitioner when the other information is contained in (*a*) annual reports to holders of securities or beneficial interests, annual reports of organizations for charitable or philanthropic purposes distributed to the public, and annual reports filed with regulatory authorities under the Securities Exchange Act of 1934 or (*b*) other documents to which the practitioner, at the client's request, devotes attention. These paragraphs are not applicable when an attest report appears in a registration statement filed under the Securities Act of 1933. (See AU section 634, *Letters for Underwriters and Certain Other Requesting Parties*, and AU section 711, *Filings Under Federal Securities Statutes*.) Also, these paragraphs are not applicable to other information on which the practitioner or another practitioner is engaged to issue an opinion.

.92 The practitioner's responsibility with respect to other information in such a document does not extend beyond the information identified in his or her report, and the practitioner has no obligation to perform any procedures to corroborate any other information contained in the document. However, the practitioner should read the other information not covered by the practitioner's report or by the report of the other practitioner and consider whether it, or the manner of its presentation, is materially inconsistent with the information appearing in the practitioner's report. If the practitioner believes that the other information is inconsistent with the information appearing in the practitioner's report, he or she should consider whether the practitioner's report requires revision. If the practitioner concludes that the report does not require revision, he or she should request the client to revise the other information. If the other information is not revised to eliminate the material inconsistency, the practitioner should consider other actions, such as revising his or her report to include an explanatory paragraph describing the material inconsistency, withholding the use of his or her report in the document, or withdrawing from the engagement.

.93 If, while reading the other information for the reasons set forth in paragraph .92, the practitioner becomes aware of information that he or she believes is a material misstatement of fact that is not a material inconsistency as described in paragraph .92, he or she should discuss the matter with the client. In connection with this discussion, the practitioner should consider that he or she may not have the expertise to assess the validity of the statement, that there may be no standards by which to assess its presentation, and that there may be valid differences of judgment or opinion. If the practitioner concludes he or she has a valid basis for concern, the practitioner should propose that the client consult with some other party whose advice may be useful, such as the entity's legal counsel.

---

[18] Such guidance pertains only to other information in a client-prepared document. The practitioner has no responsibility to read information contained in documents of nonclients. Further, the practitioner is not required to read information contained in electronic sites, or to consider the consistency of other information in electronic sites with the original documents since electronic sites are a means of distributing information and are not "documents" as that term is used in this section. Practitioners may be asked by their clients to render attest services with respect to information in electronic sites, in which case, other attest standards may apply to those services. [Footnote renumbered by the issuance of Statement on Standards for Attestation Engagements No. 14, November 2006.]

.94 If, after discussing the matter, the practitioner concludes that a material misstatement of fact remains, the action taken will depend on his or her judgment in the circumstances. The practitioner should consider steps such as notifying the client's management and audit committee in writing of his or her views concerning the information and consulting his or her legal counsel about further action appropriate in the circumstances.[19]

Consideration of Subsequent Events in an Attest Engagement

.95 Events or transactions sometimes occur subsequent to the point in time or period of time of the subject matter being tested but prior to the date of the practitioner's report that have a material effect on the subject matter and therefore require adjustment or disclosure in the presentation of the subject matter or assertion. These occurrences are referred to as *subsequent events*. In performing an attest engagement, a practitioner should consider information about subsequent events that comes to his or her attention. Two types of subsequent events require consideration by the practitioner.

.96 The first type consists of events that provide additional information with respect to conditions that existed at the point in time or during the period of time of the subject matter being tested. This information should be used by the practitioner in considering whether the subject matter is presented in conformity with the criteria and may affect the presentation of the subject matter, the assertion, or the practitioner's report.

.97 The second type consists of those events that provide information with respect to conditions that arose subsequent to the point in time or period of time of the subject matter being tested that are of such a nature and significance that their disclosure is necessary to keep the subject matter from being misleading. This type of information will not normally affect the practitioner's report if the information is appropriately disclosed.

.98 While the practitioner has no responsibility to detect subsequent events, the practitioner should inquire of the responsible party (and his or her client if the client is not the responsible party) as to whether they are aware of any subsequent events, through the date of the practitioner's report, that would have a material effect on the subject matter or assertion.[20] If the practitioner has decided to obtain a representation letter, the letter ordinarily would include a representation concerning subsequent events. (See paragraphs .60 and .61.)

.99 The practitioner has no responsibility to keep informed of events subsequent to the date of his or her report; however, the practitioner may later become aware of conditions that existed at that date that might have affected

---

[19] If the client does not have an audit committee, the practitioner should communicate with individuals whose authority and responsibility are equivalent to those of an audit committee, such as the board of directors, the board of trustees, an owner in a owner-managed entity, or those who engaged the practitioner. [Footnote renumbered by the issuance of Statement on Standards for Attestation Engagements No. 14, November 2006.]

[20] For certain subject matter, specific subsequent event standards have been developed to provide additional requirements for engagement performance and reporting. Additionally, a practitioner engaged to examine the design or effectiveness of internal control over items not covered by section 501, *An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements*, or section 601, *Compliance Attestation*, should consider the subsequent events guidance set forth in sections 501.129–.134 and 601.50–.52. [Footnote renumbered by the issuance of Statement on Standards for Attestation Engagements No. 14, November 2006.]

the practitioner's report had he or she been aware of them. In such circumstances, the practitioner may wish to consider the guidance in AU section 561, *Subsequent Discovery of Facts Existing at the Date of the Auditor's Report*.

Attest Documentation[21]

.100 The practitioner should prepare and maintain attest documentation, the form and content of which should be designed to meet the circumstances of the particular attest engagement.[22] Attest documentation is the principal record of attest procedures applied, information obtained, and conclusions or findings reached by the practitioner in the engagement. The quantity, type, and content of attest documentation are matters of the practitioner's professional judgment. [As amended, effective for attest engagements when the subject matter or assertion is as of or for a period ending on or after December 15, 2002, by Statement on Standards for Attestation Engagements No. 11.]

.101 Attest documentation serves mainly to:

a. Provide the principal support for the practitioner's report, including the representation regarding observance of the standards of fieldwork, which is implicit in the reference in the report to attestation standards.[23]

b. Aid the practitioner in the conduct and supervision of the attest engagement.

For examinations of prospective financial statements, attest documentation ordinarily should indicate that the process by which the entity develops its prospective financial statements was considered in determining the scope of the examination. [Paragraph added, effective for attest engagements when the subject matter or assertion is as of or for a period ending on or after December 15, 2002, by Statement on Standards for Attestation Engagements No. 11.]

.102 Examples of attest documentation are work programs, analyses, memoranda, letters of confirmation and representation, abstracts or copies of entity documents, and schedules or commentaries prepared or obtained by the practitioner. Attest documentation may be in paper form, electronic form, or other media. [Paragraph renumbered and amended, effective for attest engagements when the subject matter or assertion is as of or for a period ending on or after December 15, 2002, by Statement on Standards for Attestation Engagements No. 11.]

.103 Attest documentation should be sufficient to (*a*) enable members of the engagement team with supervision and review responsibilities to understand the nature, timing, extent, and results of attest procedures performed,

---

[21] *Attest documentation* also may be referred to as *working papers*. [Footnote added, effective for attest engagements when the subject matter or assertion is as of or for a period ending on or after December 15, 2002, by Statement on Standards for Attestation Engagements No. 11. Footnote renumbered by the issuance of Statement on Standards for Attestation Engagements No. 14, November 2006.]

[22] [Footnote renumbered and deleted by the issuance of Statement on Standards for Attestation Engagements No. 11, January 2002. Footnote subsequently renumbered by the issuance of Statement on Standards for Attestation Engagements No. 14, November 2006.]

[23] However, there is no intention to imply that the practitioner would be precluded from supporting his or her report by other means in addition to attest documentation. [Footnote added, effective for attest engagements when the subject matter or assertion is as of or for a period ending on or after December 15, 2002, by Statement on Standards for Attestation Engagements No. 11. Footnote renumbered by the issuance of Statement on Standards for Attestation Engagements No. 14, November 2006.]

and the information obtained[24] and (*b*) indicate the engagement team member(s) who performed and reviewed the work. [Paragraph added, effective for attest engagements when the subject matter or assertion is as of or for a period ending on or after December 15, 2002, by Statement on Standards for Attestation Engagements No. 11.]

.104 Attest documentation is the property of the practitioner, and some states recognize this right of ownership in their statutes. The practitioner should adopt reasonable procedures to retain attest documentation for a period of time sufficient to meet the needs of his or her practice and to satisfy any applicable legal or regulatory requirements for records retention.[25, [26]] [Paragraph renumbered and amended, effective for attest engagements when the subject matter or assertion is as of or for a period ending on or after December 15, 2002, by Statement on Standards for Attestation Engagements No. 11.]

.105 The practitioner has an ethical, and in some situations a legal, obligation to maintain the confidentiality of client information or information of the responsible party.[27] Because attest documentation often contains confidential information, the practitioner should adopt reasonable procedures to maintain the confidentiality of that information.† [Paragraph added, effective for attest engagements when the subject matter or assertion is as of or for a period ending on or after December 15, 2002, by Statement on Standards for Attestation Engagements No. 11.]

.106 The practitioner also should adopt reasonable procedures to prevent unauthorized access to attest documentation. [Paragraph added, effective for attest engagements when the subject matter or assertion is as of or for a period ending on or after December 15, 2002, by Statement on Standards for Attestation Engagements No. 11.]

.107 Certain attest documentation may sometimes serve as a useful reference source for the client, but it should not be regarded as a part of, or a substitute for, the client's records. [Paragraph renumbered and amended, effective for attest engagements when the subject matter or assertion is as of or for a period ending on or after December 15, 2002, by Statement on Standards for Attestation Engagements No. 11.]

---

[24] A firm of practitioners has a responsibility to adopt a system of quality control policies and procedures to provide the firm with reasonable assurance that its personnel comply with applicable professional standards, including attestation standards, and the firm's standards of quality in conducting individual attest engagements. Review of attest documentation and discussions with engagement team members are among the procedures a firm performs when monitoring compliance with the quality control policies and procedures that it has established. (Also, see paragraphs .17 and .18.) [Footnote added, effective for attest engagements when the subject matter or assertion is as of or for a period ending on or after December 15, 2002, by Statement on Standards for Attestation Engagements No. 11. Footnote renumbered by the issuance of Statement on Standards for Attestation Engagements No. 14, November 2006.]

[25] The procedures should enable the practitioner to access electronic attest documentation throughout the retention period. [Footnote added, effective for attest engagements when the subject matter or assertion is as of or for a period ending on or after December 15, 2002, by Statement on Standards for Attestation Engagements No. 11. Footnote renumbered by the issuance of Statement on Standards for Attestation Engagements No. 14, November 2006.]

[26] [Footnote renumbered and deleted by the issuance of Statement on Standards for Attestation Engagements No. 11, January 2002. Footnote subsequently renumbered by the issuance of Statement on Standards for Attestation Engagements No. 14, November 2006.]

[27] Also, see Rule 301, *Confidential Client Information*, of the AICPA's Code of Professional Conduct [ET section 301.01]. [Footnote added, effective for attest engagements when the subject matter or assertion is as of or for a period ending on or after December 15, 2002, by Statement on Standards for Attestation Engagements No. 11. Footnote renumbered by the issuance of Statement on Standards for Attestation Engagements No. 14, November 2006.]

† ***Note:*** See the Attest Interpretation, "Providing Access to or Copies of Attest Documentation to a Regulator" (section 9101.43–.46).

[.108] [Paragraph renumbered and deleted by the issuance of Statement on Standards for Attestation Engagements No. 11, January 2002.]

Attest Services Related to Consulting Service Engagements

Attest Services as Part of a Consulting Service Engagement

.109 When a practitioner provides an attest service (as defined in this section) as part of a consulting service engagement, this SSAE applies only to the attest service. The SSCS applies to the balance of the consulting service engagement. [Paragraph renumbered by the issuance of Statement on Standards for Attestation Engagements No. 11, January 2002.]

.110 When the practitioner determines that an attest service is to be provided as part of a consulting service engagement, the practitioner should inform the client of the relevant differences between the two types of services and obtain concurrence that the attest service is to be performed in accordance with the appropriate professional requirements. The practitioner should take such actions because the professional requirements for an attest service differ from those for a consulting service engagement. [Paragraph renumbered by the issuance of Statement on Standards for Attestation Engagements No. 11, January 2002.]

.111 The practitioner should issue separate reports on the attest engagement and the consulting service engagement and, if presented in a common binder, the report on the attest engagement or service should be clearly identified and segregated from the report on the consulting service engagement. [Paragraph renumbered by the issuance of Statement on Standards for Attestation Engagements No. 11, January 2002.]

Subject Matter, Assertions, Criteria, and Evidence

.112 An attest service may involve subject matter, an assertion, criteria, or evidential matter developed during a concurrent or prior consulting service engagement. Subject matter or an assertion developed with the practitioner's advice and assistance as the result of such consulting services engagement may be the subject of an attest engagement, provided the responsible party accepts and acknowledges responsibility for the subject matter or assertion. (See paragraph .12.) Criteria developed with the practitioner's assistance may be used to evaluate subject matter in an attest engagement, provided such criteria meet the requirements of this section. Relevant information obtained in the course of a concurrent or prior consulting service engagement may be used as evidential matter in an attest engagement, provided the information satisfies the requirements of this section. [Paragraph renumbered by the issuance of Statement on Standards for Attestation Engagements No. 11, January 2002.]

Effective Date

.113 This section is effective when the subject matter or assertion is as of or for a period ending on or after June 1, 2001. Early application is permitted. [Paragraph renumbered by the issuance of Statement on Standards for Attestation Engagements No. 11, January 2002.]

.114

Appendix A

Examination Reports

Example 1

This is a standard examination report on subject matter for general use. This report pertains to subject matter for which suitable criteria exist and are available to all users through inclusion in a clear manner in the presentation of the subject matter. (See paragraphs .78 to .83 for guidance on restricting the use of the report when criteria are available only to specified parties; see Example 4 for an illustration of such a report.) A written assertion has been obtained from the responsible party.

Independent Accountant's Report

We have examined the [*identify the subject matter—for example, the accompanying schedule of investment returns of XYZ Company for the year ended December 31, 20XX*]. XYZ Company's management is responsible for the schedule of investment returns. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting [*identify the subject matter—for example, XYZ Company's schedule of investment returns*] and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

[*Additional paragraph(s) may be added to emphasize certain matters relating to the attest engagement or the subject matter.*]

In our opinion, the schedule referred to above presents, in all material respects, [*identify the subject matter—for example, the investment returns of XYZ Company for the year ended December 31, 20XX*] based on [*identify criteria—for example, the ABC criteria set forth in Note 1*].

[*Signature*]

[*Date*]

Example 2

This report is a standard examination report on an assertion for general use. The report pertains to subject matter for which suitable criteria exist and are available to all users through inclusion in a clear manner in the presentation of the subject matter. (See paragraphs .78 to .83 for guidance on restricting the use of the report when criteria are available only to specified parties.) A written assertion has been obtained from the responsible party.

Independent Accountant's Report

We have examined management's assertion that [*identify the assertion—for example, the accompanying schedule of investment returns of XYZ Company for the year ended December 31, 20XX is presented in accordance with ABC criteria set forth in Note 1*]. XYZ Company's management is responsible for the assertion. Our responsibility is to express an opinion on the assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting management's assertion and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

[*Additional paragraph(s) may be added to emphasize certain matters relating to the attest engagement or the assertion.*]

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on [*identify established or stated criteria—for example, the ABC criteria set forth in Note 1*].

[*Signature*]

[*Date*]

Example 3

This is an examination report for general use; the introductory paragraph states the practitioner has examined management's assertion but the practitioner opines directly on the subject matter (see paragraph .87). The report pertains to subject matter for which suitable criteria exist and are available to all users through inclusion in a clear manner in the presentation of the subject matter. (See paragraphs .78 to .83 for guidance on restricting the use of the report when criteria are available only to specified parties.) A written assertion has been obtained from the responsible party.

Independent Accountant's Report

We have examined management's assertion that [*identify the assertion—for example, the accompanying schedule of investment returns of XYZ Company for the year ended December 31, 20XX is presented in accordance with the ABC criteria set forth in Note 1*]. XYZ Company's management is responsible for the assertion. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting [*identify the subject matter—for example, XYZ Company's schedule of investment returns*] and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

[*Additional paragraph(s) may be added to emphasize certain matters relating to the attest engagement or the assertion.*]

In our opinion, the schedule referred to above, presents, in all material respects, [*identify the subject matter—for example, the investment returns of XYZ Company for the year ended December 31, 20XX*] based on [*identify criteria—for example, the ABC criteria set forth in Note 1*].

[*Signature*]

[*Date*]

Example 4

This is an examination report on subject matter. Although suitable criteria exist, use of the report is restricted because the criteria are available only to specified parties. (See paragraph .34.) A written assertion has been obtained from the responsible party.

Independent Accountant's Report

We have examined the accompanying schedule of investment returns of XYZ Company for the year ended December 31, 20XX. XYZ Company's management is responsible for the schedule of investment returns. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting [*identify the subject matter—for example, XYZ Company's schedule of investment returns*] and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

[*Additional paragraph(s) may be added to emphasize certain matters relating to the attest engagement or the assertion.*]

In our opinion, the schedule referred to above, presents, in all material respects, [*identify the subject matter—for example, the investment returns of XYZ Company for the year ended December 31, 20XX*] based on the ABC criteria referred to in the investment management agreement between XYZ Company and DEF Investment Managers, Ltd., dated November 15, 20X1.

This report is intended solely for the information and use of XYZ Company and [*identify other specified parties—for example, DEF Investment Managers, Ltd.*] and is not intended to be and should not be used by anyone other than these specified parties.

[*Signature*]

[*Date*]

Example 5

This is an examination report with a qualified opinion because conditions exist that, individually or in combination, result in one or more material misstatements or deviations from the criteria; the report is for general use. The report pertains to subject matter for which suitable criteria exist and are available to all users through inclusion in a clear manner in the presentation of the subject matter. (See paragraphs .78 to .83 for guidance on restricting the use of the report when criteria are available only to specified parties.) A written assertion has been obtained from the responsible party.

Independent Accountant's Report

We have examined the accompanying schedule of investment returns of XYZ Company for the year ended December 31, 20XX. XYZ Company's management is responsible for the schedule of investment returns. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting [*identify the subject matter—for example, XYZ Company's schedule of investment returns*] and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Our examination disclosed the following [*describe condition(s) that, individually or in the aggregate, resulted in a material misstatement or deviation from the criteria*].

In our opinion, except for the material misstatement [*or deviation from the criteria*] described in the preceding paragraph, the schedule referred to above, presents, in all material respects, [*identify the subject matter—for example, the investment returns of XYZ Company for the year ended December 31, 20XX*] based on [*identify criteria—for example, the ABC criteria set forth in Note 1*].

[*Signature*]

[*Date*]

Example 6

This is an examination report that contains a disclaimer of opinion because of a scope restriction. (See paragraph .74 for reporting guidance when there is a scope restriction.) The report pertains to subject matter for which suitable criteria exist and are available to all users through inclusion in a clear manner in the presentation of the subject matter.

Independent Accountant's Report

We were engaged to examine the accompanying schedule of investment returns of XYZ Company for the year ended December 31, 20XX. XYZ Company's management is responsible for the schedule of investment returns.

[*Scope paragraph should be omitted.*]

[*Include paragraph to describe scope restrictions.*]

Because of the restriction on the scope of our examination discussed in the preceding paragraph, the scope of our work was not sufficient to enable us to express, and we do not express, an opinion on whether the schedule referred to above presents, in all material respects, [*identify the subject matter—for example, the investment returns of XYZ Company for the year ended December 31, 20XX*] based on [*identify criteria—for example, the ABC criteria set forth in Note 1*].

[*Signature*]

[*Date*]

Example 7

This is an examination report on subject matter that is the responsibility of a party other than the client. The report is restricted as to use since a written assertion has not been provided by the responsible party. (See paragraph .78.) The subject matter pertains to criteria that are suitable and are available to the client.

Independent Accountant's Report

To the Board of Directors

DEF Company:

We have examined the [*identify the subject matter—for example, the accompanying schedule of investment returns of XYZ Company for the year ended December 31, 20XX*]. XYZ Company's management is responsible for the schedule of investment returns. XYZ management did not provide us a written assertion about their schedule of investment returns for the year ended December 31, 20XX. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting [*identify the subject matter—for example, XYZ Company's schedule of investment returns*] and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

[*Additional paragraph(s) may be added to emphasize certain matters relating to the attest engagement or the subject matter.*]

In our opinion, the schedule referred to above presents, in all material respects, [*identify the subject matter—for example, the investment returns of XYZ Company for the year ended December 31, 20XX*] based on [*identify criteria—for example, the ABC criteria set forth in Note 1*].

This report is intended solely for the information and use of the management and board of directors of DEF Company and is not intended to be and should not be used by anyone other than these specified parties.

[*Signature*]

[*Date*]

[Paragraph renumbered by the issuance of Statement on Standards for Attestation Engagements No. 11, January 2002.]

.115

Appendix B

Review Reports

Example 1

This is a standard review report on subject matter for general use. The report pertains to subject matter for which suitable criteria exist and are available to all users through inclusion in a clear manner in the presentation of the subject matter. (See paragraphs .78 to .83 for guidance on restricting the use of the report when criteria are available only to specified parties.) A written assertion has been obtained from the responsible party.

Independent Accountant's Report

We have reviewed the [*identify the subject matter—for example, the accompanying schedule of investment returns of XYZ Company for the year ended December 31, 20XX*]. XYZ Company's management is responsible for the schedule of investment returns.

Our review was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. A review is substantially less in scope than an examination, the objective of which is the expression of an opinion on [*identify the subject matter—for example, XYZ Company's schedule of investment returns*]. Accordingly, we do not express such an opinion.

[*Additional paragraph(s) may be added to emphasize certain matters relating to the attest engagement or the subject matter.*]

Based on our review, nothing came to our attention that caused us to believe that the [*identify the subject matter—for example, schedule of investment returns of XYZ Company for the year ended December 31, 20XX*] is not presented, in all material respects, in conformity with [*identify the criteria—for example, the ABC criteria set forth in Note 1*].

[*Signature*]

[*Date*]

Example 2

This is a review report on subject matter that is the responsibility of a party other than the client. This review report is restricted as to use since a written assertion has not been provided by the responsible party. (See paragraph .78.) The subject matter pertains to criteria that are suitable and are available to the client.

Independent Accountant's Report

To the Board of Directors

DEF Company:

We have reviewed [*identify the subject matter—for example, the accompanying schedule of investment returns of XYZ Company for the year ended December 31, 20XX*]. XYZ Company's management is responsible for the schedule of investment returns. XYZ Company's management did not provide us a written assertion about their schedule of investment returns for the year ended December 31, 20XX.

Our review was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. A review is substantially less in scope than an examination, the objective of which is the expression of an opinion on [*identify the subject matter—for example, XYZ Company's schedule of investment returns*]. Accordingly, we do not express such an opinion.

[*Additional paragraph(s) may be added to emphasize certain matters relating to the attest engagement or the subject matter.*]

Based on our review, nothing came to our attention that caused us to believe that [*identify the subject matter—for example, the schedule of investment returns of XYZ Company for the year ended December 31, 20XX*] is not presented, in all material respects, in conformity with [*identify the criteria—for example, the ABC criteria set forth in Note 1*].

This report is intended solely for the information and use of the management and board of directors of DEF Company and is not intended to be and should not be used by anyone other than these specified parties.

[*Signature*]

[*Date*]

Example 3

This is a review report on an assertion. Although suitable criteria exist for the subject matter, the report is restricted as to use since the criteria are available only to specified parties; if the criteria are available as described in paragraph .33 (*a*) to (*d*), the paragraph restricting the use of the report would be omitted. A written assertion has been obtained from the responsible party.

Independent Accountant's Report

We have reviewed management's assertion that [*identify the assertion—for example, the accompanying schedule of investment returns of XYZ Company for the year ended December 31, 20XX is presented in accordance with the ABC criteria referred to in Note 1*]. XYZ Company's management is responsible for the assertion.

Our review was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. A review is substantially less in scope than an examination, the objective of which is the expression of an opinion on management's assertion. Accordingly, we do not express such an opinion.

[*Additional paragraph(s) may be added to emphasize certain matters relating to the attest engagement or the assertion.*]

Based on our review, nothing came to our attention that caused us to believe that management's assertion referred to above is not fairly stated, in all material respects, based on [*identify the criteria—for example, the ABC criteria referred to in the investment management agreement between XYZ Company and DEF Investment Managers, Ltd., dated November 15, 20X1*].

This report is intended solely for the information and use of XYZ Company and [*identify other specified parties—for example, DEF Investment Managers, Ltd.*] and is not intended to be and should not be used by anyone other than these specified parties.

[*Signature*]

[*Date*]

[Paragraph renumbered by the issuance of Statement on Standards for Attestation Engagements No. 11, January 2002.]

AT Section 601

Compliance Attestation

Source: SSAE No. 10.

Effective when the subject matter or assertion is as of or for a period ending on or after June 1, 2001. Earlier application is permitted.

Introduction and Applicability

.01 This section provides guidance for engagements related to either (*a*) an entity's compliance with requirements of specified laws, regulations, rules, contracts, or grants or (*b*) the effectiveness of an entity's internal control over compliance with specified requirements.[1] Compliance requirements may be either financial or nonfinancial in nature. An attest engagement conducted in accordance with this section should comply with the general, fieldwork, and reporting standards established in section 50, *SSAE Hierarchy*, and the specific standards set forth in this section. [Revised, November 2006, to reflect conforming changes necessary due to the issuance of Statement on Standards for Attestation Engagements No. 14.]

.02 This section does not—

a. Affect the auditor's responsibility in an audit of financial statements performed in accordance with generally accepted auditing standards (GAAS).

b. Apply to situations in which an auditor reports on specified compliance requirements based solely on an audit of financial statements, as addressed in AU section 623, *Special Reports*, paragraphs .19 through .21.

c. Apply to engagements for which the objective is to report in accordance with AU section 801, *Compliance Audits*, unless the terms of the engagement specify an attest report under this section.

d. Apply to engagements covered by AU section 634, *Letters for Underwriters and Certain Other Requesting Parties*.

e. Apply to the report that encompasses internal control over compliance for a broker or dealer in securities as required by rule 17a-5 of the Securities Exchange Act of 1934 (the 1934 Act).[2]

[Revised, December 2010, to reflect conforming changes necessary due to the issuance of SAS No. 117.]

---

[1] Throughout this section—
a. An entity's compliance with requirements of specified laws, regulations, rules, contracts, or grants is referred to as *compliance with specified requirements*.
b. An entity's internal control over compliance with specified requirements is referred to as its *internal control over compliance*. The internal control addressed in this section may include parts of but is not the same as internal control over financial reporting.

[2] An example of this report is contained in AICPA Audit and Accounting Guide *Brokers and Dealers in Securities*.

.03 A report issued in accordance with the provisions of this section does not provide a legal determination of an entity's compliance with specified requirements. However, such a report may be useful to legal counsel or others in making such determinations.

Scope of Services

.04 The practitioner may be engaged to perform agreed-upon procedures to assist users in evaluating the following subject matter (or assertions related thereto)—

a. The entity's compliance with specified requirements

b. The effectiveness of the entity's internal control over compliance[3]

c. Both the entity's compliance with specified requirements and the effectiveness of the entity's internal control over compliance

The practitioner also may be engaged to examine the entity's compliance with specified requirements or a written assertion thereon.

.05 An important consideration in determining the type of engagement to be performed is expectations by users of the practitioner's report. Since the users decide the procedures to be performed in an agreed-upon procedures engagement, it often will be in the best interests of the practitioner and users (including the client) to have an agreed-upon procedures engagement rather than an examination engagement. When deciding whether to accept an examination engagement, the practitioner should consider the risks discussed in paragraphs .31 through .35.

.06 A practitioner may be engaged to examine the effectiveness of the entity's internal control over compliance or an assertion thereon. However, in accordance with section 50, the practitioner cannot accept an engagement unless he or she has reason to believe that the subject matter is capable of reasonably consistent evaluation against criteria that are suitable and available to users.[4] If a practitioner determines that such criteria do exist for internal control over compliance, he or she should perform the engagement in accordance with

---

[3] An entity's internal control over compliance is the process by which management obtains reasonable assurance of compliance with specified requirements. Although the comprehensive internal control may include a wide variety of objectives and related policies and procedures, only some of these may be relevant to an entity's compliance with specified requirements. (See footnote 1b.) The components of internal control over compliance vary based on the nature of the compliance requirements. For example, internal control over compliance with a capital requirement would generally include accounting procedures, whereas internal control over compliance with a requirement to practice nondiscriminatory hiring may not include accounting procedures.

[4] Criteria issued by regulatory agencies and other groups composed of experts that follow due-process procedures, including exposure of the proposed criteria for public comment, ordinarily should be considered suitable criteria for this purpose. For example, the Committee of Sponsoring Organizations (COSO) of the Treadway Commission's Report, *Internal Control—Integrated Framework*, provides suitable criteria against which management may evaluate and report on the effectiveness of the entity's internal control. However, more detailed criteria relative to specific compliance requirements may have to be developed and an appropriate threshold for measuring the severity of control deficiencies needs to be developed in order to apply the concepts of the COSO report to internal control over compliance.

Criteria established by a regulatory agency that does not follow such due-process procedures also may be considered suitable criteria for use by the regulatory agency. The practitioner should determine whether such criteria are suitable for general use reporting by evaluating them against the attributes in section 101.24. If the practitioner determines that such criteria are suitable for general use reporting, those criteria should also be available to users as discussed in section 101.33.

If the practitioner concludes that the criteria are appropriate only for a limited number of parties or are available only to specified parties, the practitioner's report shall state that the use of the report is restricted to those parties specified in the report. (See section 101.30, .34, and .78–.83.)

section 101, *Attest Engagements*. Additionally, section 501, *An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements*, may be helpful to a practitioner in such an engagement. [Revised, November 2006, to reflect conforming changes necessary due to the issuance of Statement on Standards for Attestation Engagements No. 14.]

.07 A practitioner should not accept an engagement to perform a review, as defined in section 101.55, of an entity's compliance with specified requirements or about the effectiveness of an entity's internal control over compliance or an assertion thereon.

.08 The practitioner may be engaged to provide other types of services in connection with the entity's compliance with specified requirements or the entity's internal control over compliance. For example, management may engage the practitioner to provide recommendations on how to improve the entity's compliance or related internal control. A practitioner engaged to provide such nonattest services should refer to the guidance in CS section 100, *Consulting Services: Definitions and Standards*.

Conditions for Engagement Performance

.09 A practitioner may perform an agreed-upon procedures engagement related to an entity's compliance with specified requirements or the effectiveness of internal control over compliance if the following conditions are met.

a. The responsible party accepts responsibility for the entity's compliance with specified requirements and the effectiveness of the entity's internal control over compliance.

b. The responsible party evaluates the entity's compliance with specified requirements or the effectiveness of the entity's internal control over compliance.

See also section 201, *Agreed-Upon Procedures Engagements*.

.10 A practitioner may perform an examination engagement related to an entity's compliance with specified requirements if the following conditions are met.

a. The responsible party accepts responsibility for the entity's compliance with specified requirements and the effectiveness of the entity's internal control over compliance.

b. The responsible party evaluates the entity's compliance with specified requirements.

c. Sufficient evidential matter exists or could be developed to support management's evaluation.

.11 As part of engagement performance, the practitioner should obtain from the responsible party a written assertion about compliance with specified requirements or internal control over compliance. The responsible party may present its written assertion in either of the following:

a. A separate report that will accompany the practitioner's report

b. A representation letter to the practitioner

.12 The responsible party's written assertion about compliance with specified requirements or internal control over compliance may take many forms. Throughout this section, for example, the phrase "responsible party's assertion that W Company complied with [*specify compliance requirement*] as of [*date*]," illustrates such an assertion. Other phrases may also be used. However, a practitioner should not accept an assertion that is so subjective (for example, "very effective" internal control over compliance) that people having competence in and using the same or similar criteria would not ordinarily be able to arrive at similar conclusions.

.13 Regardless of whether the practitioner's client is the responsible party, the responsible party's refusal to furnish a written assertion as part of an examination engagement should cause the practitioner to withdraw from the engagement. However, an exception is provided if an examination of an entity's compliance with specified requirements is required by law or regulation. In that instance, the practitioner should disclaim an opinion on compliance unless he or she obtains evidential matter that warrants expressing an adverse opinion. If the practitioner expresses an adverse opinion and the responsible party does not provide an assertion, the practitioner's report should be restricted as to use. (See section 101.78–.81.) If, as part of an agreed-upon procedures engagement, the practitioner's client is the responsible party, a refusal by that party to provide an assertion requires the practitioner to withdraw from the engagement. However, withdrawal is not required if the engagement is required by law or regulation. If, in an agreed-upon procedures engagement, the practitioner's client is not the responsible party, the practitioner is not required to withdraw but should consider the effects of the responsible party's refusal on the engagement and his or her report.

.14 Additionally, at the beginning of the engagement, the practitioner may want to consider discussing with the client and the responsible party the need for the responsible party to provide the practitioner with a written representation letter at the conclusion of the examination engagement or an agreed-upon procedures engagement in which the client is the responsible party. In that letter, the responsible party will be asked to provide, among other possible items, an acknowledgment of their responsibility for establishing and maintaining effective internal control over compliance and their assertion stating their evaluation of the entity's compliance with specified requirements. The responsible party's refusal to furnish these representations (see paragraphs .68 through .70) will constitute a limitation on the scope of the engagement.

Responsible Party

.15 The responsible party is responsible for ensuring that the entity complies with the requirements applicable to its activities. That responsibility encompasses the following.

a. Identify applicable compliance requirements.

b. Establish and maintain internal control to provide reasonable assurance that the entity complies with those requirements.

c. Evaluate and monitor the entity's compliance.

d. Specify reports that satisfy legal, regulatory, or contractual requirements.

The responsible party's evaluation may include documentation such as accounting or statistical data, entity policy manuals, accounting manuals, narrative memoranda, procedural write-ups, flowcharts, completed questionnaires, or internal auditors' reports. The form and extent of documentation will vary depending on the nature of the compliance requirements and the size and complexity of the entity. The responsible party may engage the practitioner to gather information to assist it in evaluating the entity's compliance. Regardless of the procedures performed by the practitioner, the responsible party must accept responsibility for its assertion and must not base such assertion solely on the practitioner's procedures.

Agreed-Upon Procedures Engagement

.16 The objective of the practitioner's agreed-upon procedures is to present specific findings to assist users in evaluating an entity's compliance with specified requirements or the effectiveness of an entity's internal control over compliance based on procedures agreed upon by the users of the report. A practitioner engaged to perform agreed-upon procedures on an entity's compliance with specified requirements or about the effectiveness of an entity's internal control over compliance should follow the guidance set forth herein and in section 201.

.17 The practitioner's procedures generally may be as limited or as extensive as the specified users desire, as long as the specified users (*a*) agree upon the procedures performed or to be performed and (*b*) take responsibility for the sufficiency of the agreed-upon procedures for their purposes. (See section 201.15.)

.18 To satisfy the requirements that the practitioner and the specified users agree upon the procedures performed or to be performed and that the specified users take responsibility for the sufficiency of the agreed-upon procedures for their purposes, ordinarily the practitioner should communicate directly with and obtain affirmative acknowledgment from each of the specified users. For example, this may be accomplished by meeting with the specified users or by distributing a draft of the anticipated report or a copy of an engagement letter to the specified users and obtaining their agreement. If the practitioner is not able to communicate directly with all of the specified users, the practitioner may satisfy these requirements by applying any one or more of the following or similar procedures.

- Compare the procedures to be applied to written requirements of the specified users.
- Discuss the procedures to be applied with appropriate representatives of the specified users involved.
- Review relevant contracts with or correspondence from the specified users.

The practitioner should not report on an engagement when specified users do not agree upon the procedures performed or to be performed and do not take responsibility for the sufficiency of the procedures for their purposes. See section 201.36 for guidance on satisfying these requirements when the practitioner is requested to add other parties as specified parties after the date of completion of the agreed-upon procedures.

.19 In an engagement to perform agreed-upon procedures on an entity's compliance with specified requirements or about the effectiveness of an entity's

internal control over compliance, the practitioner is required to perform only the procedures that have been agreed to by users.[5] However, prior to performing such procedures, the practitioner should obtain an understanding of the specified compliance requirements, as discussed in paragraph .20. (See section 201.)

.20 To obtain an understanding of the specified compliance requirements, a practitioner should consider the following:

a. Laws, regulations, rules, contracts, and grants that pertain to the specified compliance requirements, including published requirements

b. Knowledge about the specified compliance requirements obtained through prior engagements and regulatory reports

c. Knowledge about the specified compliance requirements obtained through discussions with appropriate individuals within the entity (for example, the chief financial officer, internal auditors, legal counsel, compliance officer, or grant or contract administrators)

d. Knowledge about the specified compliance requirements obtained through discussions with appropriate individuals outside the entity (for example, a regulator or a third-party specialist)

.21 When circumstances impose restrictions on the scope of an agreed-upon procedures engagement, the practitioner should attempt to obtain agreement from the users for modification of the agreed-upon procedures. When such agreement cannot be obtained (for example, when the agreed-upon procedures are published by a regulatory agency that will not modify the procedures), the practitioner should describe such restrictions in his or her report or withdraw from the engagement.

.22 The practitioner has no obligation to perform procedures beyond the agreed-upon procedures. However, if noncompliance comes to the practitioner's attention by other means, such information ordinarily should be included in his or her report.

.23 The practitioner may become aware of noncompliance that occurs subsequent to the period addressed by the practitioner's report but before the date of the practitioner's report. The practitioner should consider including information regarding such noncompliance in his or her report. However, the practitioner has no responsibility to perform procedures to detect such noncompliance other than obtaining the responsible party's representation about noncompliance in the subsequent period, as described in paragraph .68.

.24 The practitioner's report on agreed-upon procedures on an entity's compliance with specified requirements (or the effectiveness of an entity's internal control over compliance) should be in the form of procedures and findings. The practitioner's report should contain the following elements:

a. A title that includes the word *independent*

b. Identification of the specified parties

c. Identification of the subject matter of the engagement (or management's assertion thereon), including the period or point in time addressed and a reference to the character of the engagement[6]

---

[5] AU section 322, *The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements*, does not apply to agreed-upon procedures engagements.

[6] Generally, management's assertion about compliance with specified requirements will address a *period* of time, whereas an assertion about internal control over compliance will address a *point* in time.

d. An identification of the responsible party

e. A statement that the subject matter is the responsibility of the responsible party

f. A statement that the procedures, which were agreed to by the specified parties identified in the report, were performed to assist the specified parties in evaluating the entity's compliance with specified requirements or the effectiveness of its internal control over compliance

g. A statement that the agreed-upon procedures engagement was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants

h. A statement that the sufficiency of the procedures is solely the responsibility of the specified parties and a disclaimer of responsibility for the sufficiency of those procedures

i. A list of the procedures performed (or reference thereto) and related findings (The practitioner should not provide negative assurance. See section 201.24.)

j. Where applicable, a description of any agreed-upon materiality limits (See section 201.25.)

k. A statement that the practitioner was not engaged to and did not conduct an examination of the entity's compliance with specified requirements (or the effectiveness of an entity's internal control over compliance), a disclaimer of opinion thereon, and a statement that if the practitioner had performed additional procedures, other matters might have come to his or her attention that would have been reported

l. A statement restricting the use of the report to the specified parties

m. Where applicable, reservations or restrictions concerning procedures or findings as discussed in section 201.33, .35, .39, and .40

n. Where applicable, a description of the nature of the assistance provided by the specialist as discussed in section 201.19–.21

o. The manual or printed signature of the practitioner's firm

p. The date of the report

.25 The following is an illustration of an agreed-upon procedures report on an entity's compliance with specified requirements in which the procedures and findings are enumerated rather than referenced.

Independent Accountant's Report on Applying Agreed-Upon Procedures

We have performed the procedures enumerated below, which were agreed to by [*list specified parties*], solely to assist the specified parties in evaluating [*name of entity*]'s compliance with [*list specified requirements*] during the [*period*] ended [*date*].[7] Management is responsible for [*name of entity*]'s compliance with those requirements. This agreed-upon procedures engagement

[7] If the agreed-upon procedures have been published by a third-party user (for example, a regulator in regulatory policies or a lender in a debt agreement), this sentence might begin, "We have performed the procedures included in [*title of publication or other document*] and enumerated below, which were agreed to by [*list specified parties*], solely to assist the specified parties in evaluating ...."

was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. The sufficiency of these procedures is solely the responsibility of those parties specified in this report. Consequently, we make no representation regarding the sufficiency of the procedures described below either for the purpose for which this report has been requested or for any other purpose.

[*Include paragraphs to enumerate procedures and findings.*]

We were not engaged to and did not conduct an examination, the objective of which would be the expression of an opinion on compliance. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

This report is intended solely for the information and use of [*list or refer to specified parties*] and is not intended to be and should not be used by anyone other than these specified parties.

[*Signature*]

[*Date*]

.26 Evaluating compliance with certain requirements may require interpretation of the laws, regulations, rules, contracts, or grants that establish those requirements. In such situations, the practitioner should consider whether he or she is provided with the suitable criteria required to evaluate an assertion under the third general attestation standard. If these interpretations are significant, the practitioner may include a paragraph stating the description and the source of interpretations made by the entity's management. An example of such a paragraph, which should precede the procedures and findings paragraph(s), follows.

We have been informed that, under [*name of entity*]'s interpretation of [*identify the compliance requirement*], [*explain the nature and source of the relevant interpretation*].

.27 The following is an illustration of an agreed-upon procedures report on the effectiveness of an entity's internal control over compliance in which the procedures and findings are enumerated rather than referenced.

Independent Accountant's Report on Applying Agreed-Upon Procedures

We have performed the procedures enumerated below, which were agreed to by [*list specified parties*], solely to assist the specified parties in evaluating the effectiveness of [*name of entity*]'s internal control over compliance with [*list specified requirements*] as of [*date*].[8] Management is responsible for [*name of entity*]'s internal control over compliance with those requirements. This agreed-upon procedures engagement was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. The sufficiency of these procedures is solely the responsibility of those parties specified in this report. Consequently, we make no representation regarding the sufficiency of the procedures described below either for the purpose for which this report has been requested or for any other purpose.

[8] If the agreed-upon procedures have been published by a third-party user (for example, a regulator in regulatory policies or a lender in a debt agreement), this sentence might begin, "We have performed the procedures included in [*title of publication or other document*] and enumerated below, which were agreed to by [*list specified parties*], solely to assist the specified parties in evaluating the effectiveness of [*name of entity*]'s internal control over compliance ...."

[*Include paragraphs to enumerate procedures and findings.*]

We were not engaged to and did not conduct an examination, the objective of which would be the expression of an opinion on the effectiveness of internal control over compliance. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

This report is intended solely for the information and use of [*list or refer to specified parties*] and is not intended to be and should not be used by anyone other than these specified parties.

[*Signature*]

[*Date*]

.28 In some agreed-upon procedures engagements, procedures may relate to both compliance with specified requirements and the effectiveness of internal control over compliance. In these engagements, the practitioner may issue one report that addresses both. For example, the first sentence of the introductory paragraph would state the following.

We have performed the procedures enumerated below, which were agreed to by [*list users of report*], solely to assist the users in evaluating [*name of entity*]'s compliance with [*list specified requirements*] during the [*period*] ended [*date*] and the effectiveness of [*name of entity*]'s internal control over compliance with the aforementioned compliance requirements as of [*date*].

.29 The date of completion of the agreed-upon procedures should be used as the date of the practitioner's report.

Examination Engagement

.30 The objective of the practitioner's examination procedures applied to an entity's compliance with specified requirements is to express an opinion on an entity's compliance (or assertion related thereto), based on the specified criteria. To express such an opinion, the practitioner accumulates sufficient evidence about the entity's compliance with specified requirements, thereby restricting attestation risk to an appropriately low level.

Attestation Risk

.31 In an engagement to examine compliance with specified requirements, the practitioner seeks to obtain reasonable assurance that the entity complied, in all material respects, based on the specified criteria. This includes designing the examination to detect both intentional and unintentional material noncompliance. Absolute assurance is not attainable because of factors such as the need for judgment, the use of sampling, and the inherent limitations of internal control over compliance and because much of the evidence available to the practitioner is persuasive rather than conclusive in nature. Also, procedures that are effective for detecting noncompliance that is unintentional may be ineffective for detecting noncompliance that is intentional and concealed through collusion between personnel of the entity and a third party or among management or employees of the entity. Therefore, the subsequent discovery that material noncompliance exists does not, in and of itself, evidence inadequate planning, performance, or judgment on the part of the practitioner.

.32 Attestation risk is the risk that the practitioner may unknowingly fail to modify appropriately his or her opinion. It is composed of inherent risk,

control risk, and detection risk. For purposes of a compliance examination, these components are defined as follows:

a. *Inherent risk*—The risk that material noncompliance with specified requirements could occur, assuming there are no related controls

b. *Control risk*—The risk that material noncompliance that could occur will not be prevented or detected on a timely basis by the entity's controls

c. *Detection risk*—The risk that the practitioner's procedures will lead him or her to conclude that material noncompliance does not exist when, in fact, such noncompliance does exist

Inherent Risk

.33 In assessing inherent risk, the practitioner should consider factors affecting risk similar to those an auditor would consider when planning an audit of financial statements. Such factors are discussed in AU section 316, *Consideration of Fraud in a Financial Statement Audit*, paragraph .85 (Appendix). In addition, the practitioner should consider factors relevant to compliance engagements, such as the following:

- The complexity of the specified compliance requirements
- The length of time the entity has been subject to the specified compliance requirements
- Prior experience with the entity's compliance
- The potential impact of noncompliance

[Revised, January 2004, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 99.]

Control Risk

.34 The practitioner should assess control risk as discussed in paragraphs .45 and .46. Assessing control risk contributes to the practitioner's evaluation of the risk that material noncompliance exists. The process of assessing control risk (together with assessing inherent risk) provides evidential matter about the risk that such noncompliance may exist. The practitioner uses this evidential matter as part of the reasonable basis for his or her opinion.

Detection Risk

.35 In determining an acceptable level of detection risk, the practitioner assesses inherent risk and control risk and considers the extent to which he or she seeks to restrict attestation risk. As assessed inherent risk or control risk decreases, the acceptable level of detection risk increases. Accordingly, the practitioner may alter the nature, timing, and extent of compliance tests performed based on the assessments of inherent risk and control risk.

Materiality

.36 In an examination of an entity's compliance with specified requirements, the practitioner's consideration of materiality differs from that of an audit of financial statements in accordance with GAAS. In an examination of an entity's compliance with specified requirements, the practitioner's consideration of materiality is affected by (*a*) the nature of the compliance requirements, which may or may not be quantifiable in monetary terms, (*b*) the nature

and frequency of noncompliance identified with appropriate consideration of sampling risk, and (*c*) qualitative considerations, including the needs and expectations of the report's users.

.37 In a number of situations, the terms of the engagement may provide for a supplemental report of all or certain noncompliance discovered. Such terms should not change the practitioner's judgments about materiality in planning and performing the engagement or in forming an opinion on an entity's compliance with specified requirements or on the responsible party's assertion about such compliance.

Performing an Examination Engagement

.38 The practitioner should exercise (*a*) due care in planning, performing, and evaluating the results of his or her examination procedures and (*b*) the proper degree of professional skepticism to achieve reasonable assurance that material noncompliance will be detected.

.39 In an examination of the entity's compliance with specified requirements, the practitioner should—

a. Obtain an understanding of the specified compliance requirements. (See paragraph .40.)

b. Plan the engagement. (See paragraphs .41 through .44.)

c. Consider relevant portions of the entity's internal control over compliance. (See paragraphs .45 through .47.)

d. Obtain sufficient evidence including testing compliance with specified requirements. (See paragraphs .48 and .49.)

e. Consider subsequent events. (See paragraphs .50 through .52.)

f. Form an opinion about whether the entity complied, in all material respects, with specified requirements (or whether the responsible party's assertion about such compliance is fairly stated in all material respects), based on the specified criteria. (See paragraph .53.)

Obtaining an Understanding of the Specified Compliance Requirements

.40 A practitioner should obtain an understanding of the specified compliance requirements. To obtain such an understanding, a practitioner should consider the following:

a. Laws, regulations, rules, contracts, and grants that pertain to the specified compliance requirements, including published requirements

b. Knowledge about the specified compliance requirements obtained through prior engagements and regulatory reports

c. Knowledge about the specified compliance requirements obtained through discussions with appropriate individuals within the entity (for example, the chief financial officer, internal auditors, legal counsel, compliance officer, or grant or contract administrators)

d. Knowledge about the specified compliance requirements obtained through discussions with appropriate individuals outside the entity (for example, a regulator or third-party specialist)

Planning the Engagement

General Considerations

.41 Planning an engagement to examine an entity's compliance with specified requirements involves developing an overall strategy for the expected conduct and scope of the engagement. The practitioner should consider the planning matters discussed in section 101.42–.47.

Multiple Components

.42 In an engagement to examine an entity's compliance with specified requirements when the entity has operations in several components (for example, locations, branches, subsidiaries, or programs), the practitioner may determine that it is not necessary to test compliance with requirements at every component. In making such a determination and in selecting the components to be tested, the practitioner should consider factors such as the following:

a. The degree to which the specified compliance requirements apply at the component level

b. Judgments about materiality

c. The degree of centralization of records

d. The effectiveness of the control environment, particularly management's direct control over the exercise of authority delegated to others and its ability to supervise activities at various locations effectively

e. The nature and extent of operations conducted at the various components

f. The similarity of operations over compliance for different components

Using the Work of a Specialist

.43 In some compliance engagements, the nature of the specified compliance requirements may require specialized skill or knowledge in a particular field other than accounting or auditing. In such cases, the practitioner may use the work of a specialist and should follow the relevant performance and reporting guidance in AU section 336, *Using the Work of a Specialist*.

Internal Audit Function

.44 Another factor the practitioner should consider when planning the engagement is whether the entity has an internal audit function and the extent to which internal auditors are involved in monitoring compliance with the specified requirements. A practitioner should consider the guidance in AU section 322, *The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements*, when addressing the competence and objectivity of internal auditors, the nature, timing, and extent of work to be performed, and other related matters.

Consideration of Internal Control Over Compliance

.45 The practitioner should obtain an understanding of relevant portions of internal control over compliance sufficient to plan the engagement and to assess control risk for compliance with specified requirements. In planning the

examination, such knowledge should be used to identify types of potential noncompliance, to consider factors that affect the risk of material noncompliance, and to design appropriate tests of compliance.

.46 A practitioner generally obtains an understanding of the design of specific controls by performing the following:

a. Inquiries of appropriate management, supervisory, and staff personnel

b. Inspection of the entity's documents

c. Observation of the entity's activities and operations

The nature and extent of procedures a practitioner performs vary from entity to entity and are influenced by factors such as the following:

- The newness and complexity of the specified requirements
- The practitioner's knowledge of internal control over compliance obtained in previous professional engagements
- The nature of the specified compliance requirements
- An understanding of the industry in which the entity operates
- Judgments about materiality

When seeking to assess control risk below the maximum, the practitioner should perform tests of controls to obtain evidence to support the assessed level of control risk.

.47 During the course of an examination engagement, the practitioner may become aware of significant deficiencies or material weaknesses in the design or operation of internal control over compliance that could adversely affect the entity's ability to comply with specified requirements. A practitioner's responsibility to communicate these deficiencies in an examination of an entity's compliance with specified requirements is similar to the auditor's responsibility described in AU section 325, *Communicating Internal Control Related Matters Identified in an Audit*. If, in a multiple-party arrangement, the practitioner's client is not the responsible party, the practitioner has no responsibility to communicate significant deficiencies or material weaknesses to the responsible party. For example, if the practitioner is engaged by his or her client to examine the compliance of another entity, the practitioner has no obligation to communicate any significant deficiencies or material weaknesses that he or she becomes aware of to the other entity. However, the practitioner is not precluded from making such a communication. [Revised, May 2006, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 112. Revised, January 2010, to reflect conforming changes necessary due to the issuance of SAS No. 115.]

Obtaining Sufficient Evidence

.48 The practitioner should apply procedures to provide reasonable assurance of detecting material noncompliance. Determining these procedures and evaluating the sufficiency of the evidence obtained are matters of professional judgment. When exercising such judgment, practitioners should consider the guidance contained in section 101.51–.54 and AU section 350, *Audit Sampling*.

.49 For engagements involving compliance with regulatory requirements, the practitioner's procedures should include reviewing reports of significant examinations and related communications between regulatory agencies and the entity and, when appropriate, making inquiries of the regulatory agencies, including inquiries about examinations in progress.

Consideration of Subsequent Events

.50 The practitioner's consideration of subsequent events in an examination of an entity's compliance with specified requirements is similar to the auditor's consideration of subsequent events in a financial statement audit, as outlined in AU section 560, *Subsequent Events*. The practitioner should consider information about such events that comes to his or her attention after the end of the period addressed by the practitioner's report and prior to the issuance of his or her report.

.51 Two types of subsequent events require consideration by the responsible party and evaluation by the practitioner. The first consists of events that provide additional information about the entity's compliance during the period addressed by the practitioner's report and may affect the practitioner's report. For the period from the end of the reporting period (or point in time) to the date of the practitioner's report, the practitioner should perform procedures to identify such events that provide additional information about compliance during the reporting period. Such procedures should include but may not be limited to inquiring about and considering the following information:

- Relevant internal auditors' reports issued during the subsequent period
- Other practitioners' reports identifying noncompliance, issued during the subsequent period
- Regulatory agencies' reports on the entity's noncompliance, issued during the subsequent period
- Information about the entity's noncompliance, obtained through other professional engagements for that entity

.52 The second type consists of noncompliance that occurs subsequent to the period being reported on but before the date of the practitioner's report. The practitioner has no responsibility to detect such noncompliance. However, should the practitioner become aware of such noncompliance, it may be of such a nature and significance that disclosure of it is required to keep users from being misled. In such cases, the practitioner should include in his or her report an explanatory paragraph describing the nature of the noncompliance.

Forming an Opinion

.53 In evaluating whether the entity has complied in all material respects (or whether the responsible party's assertion about such compliance is stated fairly in all material respects), the practitioner should consider (*a*) the nature and frequency of the noncompliance identified and (*b*) whether such noncompliance is material relative to the nature of the compliance requirements, as discussed in paragraph .36.

Reporting

.54 The practitioner may examine and report directly on an entity's compliance (see paragraphs .55 and .56) or he or she may examine and report on the responsible party's written assertion (see paragraphs .57, .58, and .61), except as described in paragraph .64.

.55 The practitioner's examination report on compliance, which is ordinarily addressed to the entity, should include the following:

a. A title that includes the word *independent*

b. Identification of the specified compliance requirements, including the period covered, and of the responsible party[9]

c. A statement that compliance with the specified requirements is the responsibility of the entity's management

d. A statement that the practitioner's responsibility is to express an opinion on the entity's compliance with those requirements based on his or her examination

e. A statement that the examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence about the entity's compliance with those requirements and performing such other procedures as the practitioner considered necessary in the circumstances

f. A statement that the practitioner believes the examination provides a reasonable basis for his or her opinion

g. A statement that the examination does not provide a legal determination on the entity's compliance

h. The practitioner's opinion on whether the entity complied, in all material respects, with specified requirements based on the specified criteria[10] (See paragraph .64 for reporting on material noncompliance.)

i. A statement restricting the use of the report to the specified parties (see the fourth reporting standard)[11] under the following circumstances (See also paragraph .13.):

- When the criteria used to evaluate compliance are determined by the practitioner to be 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.
- When the criteria used to evaluate compliance are available only to the specified parties

j. The manual or printed signature of the practitioner's firm

k. The date of the examination report

.56 The following is the form of report a practitioner should use when he or she is expressing an opinion on an entity's compliance with specified requirements during a period of time.

---

[9] A practitioner also may be engaged to report on an entity's compliance with specified requirements as of point in time. In this case, the illustrative reports in this section should be adapted as appropriate.

[10] Frequently, criteria will be contained in the compliance requirements, in which case it is not necessary to repeat the criteria in the practitioner's report; however, if the criteria are not included in the compliance requirement, the practitioner's report should identify the criteria. For example, if a compliance requirement is to "maintain $25,000 in capital," it would not be necessary to identify the $25,000 in the report; however, if the requirement is to "maintain adequate capital," the practitioner should identify the criteria used to define *adequate.*

[11] In certain situations, however, criteria that have been specified by management and other report users may be suitable for general use.

Independent Accountant's Report

[*Introductory paragraph*]

We have examined [*name of entity*]'s compliance with [*list specified compliance requirements*] during the [*period*] ended [*date*]. Management is responsible for [*name of entity*]'s compliance with those requirements. Our responsibility is to express an opinion on [*name of entity*]'s compliance based on our examination.

[*Scope paragraph*]

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence about [*name of entity*]'s compliance with those requirements and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion. Our examination does not provide a legal determination on [*name of entity*]'s compliance with specified requirements.

[*Opinion paragraph*]

In our opinion, [*name of entity*] complied, in all material respects, with the aforementioned requirements for the year ended December 31, 20XX.[12]

[*Signature*]

[*Date*]

.57 The practitioner's examination report on an entity's assertion about compliance with specified requirements, which is ordinarily addressed to the entity, should include the following:

a. A title that includes the word *independent*

b. Identification of the responsible party's assertion about the entity's compliance with specified requirements, including the period covered by the responsible party's assertion, and of the responsible party (When the responsible party's assertion does not accompany the practitioner's report, the first paragraph of the report should also contain a statement of the responsible party's assertion.)[13]

c. A statement that compliance with the requirements is the responsibility of the entity's management

d. A statement that the practitioner's responsibility is to express an opinion on the responsible party's assertion on the entity's compliance with those requirements based on his or her examination

e. A statement that the examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence about the entity's compliance with those requirements and performing such other procedures as the practitioner considered necessary in the circumstances

---

[12] If it is necessary to identify criteria (see footnote 10), the criteria should be identified in the opinion paragraph (for example, "... in all material respects, based on the criteria set forth in Attachment 1").

[13] A practitioner also may be engaged to report on the responsible party's assertion about an entity's compliance with specified requirements as of a point in time. In this case, the illustrative reports in this section should be adapted as appropriate.

f. A statement that the practitioner believes the examination provides a reasonable basis for his or her opinion

g. A statement that the examination does not provide a legal determination on the entity's compliance

h. The practitioner's opinion on whether the responsible party's assertion about compliance with specified requirements is fairly stated in all material respects based on the specified criteria[14] (See paragraph .64 for reporting on material noncompliance.)

i. A statement restricting the use of the report to the specified parties (see the fourth reporting standard)[15, 16] under the following circumstances:

- When the criteria used to evaluate compliance are determined by the practitioner to be 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
- When the criteria used to evaluate compliance are available only to the specified parties

j. The manual or printed signature of the practitioner's firm

k. The date of the examination report

.58 The following is the form of report that a practitioner should use when expressing an opinion on management's assertion about compliance with specified requirements.

Independent Accountant's Report

[*Introductory paragraph*]

We have examined management's assertion, included in the accompanying [*title of management report*], that [*name of entity*] complied with [*list specified compliance requirements*] during the [*period*] ended [*date*].[17, 18] Management is responsible for [*name of entity*]'s compliance with those requirements. Our responsibility is to express an opinion on management's assertion about [*name of entity*]'s compliance based on our examination.

[*Standard scope paragraph*]

[*Opinion paragraph*]

---

[14] Frequently, criteria will be contained in the compliance requirements, in which case it is not necessary to repeat the criteria in the practitioner's report; however, if the criteria are not included in the compliance requirement, the practitioner's report should identify the criteria. For example, if a compliance requirement is to "maintain $25,000 in capital," it would not be necessary to identify the $25,000 in the report; however, if the requirement is to "maintain adequate capital," the practitioner should identify the criteria used to define *adequate.*

[15] Although a practitioner's report may be appropriate for general use, the practitioner is not precluded from restricting the use of the report.

[16] In certain situations, however, criteria that have been specified by management and other report users may be suitable for general use.

[17] The practitioner should identify the management report examined by reference to the report title used by management in its report. Further, he or she should use the same description of compliance requirements as management uses in its report.

[18] If management's assertion is stated in the practitioner's report and does not accompany the practitioner's report, the phrase "included in the accompanying [*title of management report*]" would be omitted.

> In our opinion, management's assertion that [*name of entity*] complied with the aforementioned requirements during the [*period*] ended [*date*] is fairly stated, in all material respects.[19]
>
> [*Signature*]
>
> [*Date*]

.59 Evaluating compliance with certain requirements may require interpretation of the laws, regulations, rules, contracts, or grants that establish those requirements. In such situations, the practitioner should consider whether he or she is provided with the suitable criteria required to evaluate compliance under the third general attestation standard. If these interpretations are significant, the practitioner may include a paragraph stating the description and the source of interpretations made by the entity's management. The following is an example of such a paragraph, which should directly follow the scope paragraph:

> We have been informed that, under [*name of entity*]'s interpretation of [*identify the compliance requirement*], [*explain the source and nature of the relevant interpretation*].

.60 The date of completion of the examination procedures should be used as the date of the practitioner's report.

.61 Nothing precludes the practitioner from examining an assertion but opining directly on compliance.

.62 Section 101.78–.83 provide guidance on restricting the use of an attest report. Nothing in this section precludes the practitioner from restricting the use of the report. For example, if the practitioner is asked by a client to examine another entity's compliance with certain regulations, he or she may want to restrict the use of the report to the client since the practitioner has no control over how the report may be used by the other entity.

Report Modifications

.63 The practitioner should modify the standard report described in paragraphs .55 and .57, if any of the following conditions exist.

- There is material noncompliance with specified requirements (paragraphs .64 through .67).
- There is a restriction on the scope of the engagement.[20]
- The practitioner decides to refer to the report of another practitioner as the basis, in part, for the practitioner's report.[21]

Material Noncompliance

.64 When an examination of an entity's compliance with specified requirements discloses noncompliance with the applicable requirements that the practitioner believes have a material effect on the entity's compliance, the practitioner should modify the report and, to most effectively communicate with the reader of the report, should state his or her opinion on the entity's specified compliance requirements, not on the responsible party's assertion.

---

[19] If it is necessary to identify criteria (see footnote 10), the criteria should be identified in the opinion paragraph (for example, "...in all material respects, based on the criteria set forth in Attachment 1").

[20] The practitioner should refer to section 101.73 and .74 for guidance on scope restrictions.

[21] The practitioner should refer to section 501.122–.125 for guidance on an opinion based in part on the report of another practitioner and adapt such guidance to the standard reports in this section.

.65 The following is the form of report, modified with explanatory language, that a practitioner should use when he or she has concluded that a qualified opinion is appropriate under the circumstances. It has been assumed that the practitioner has determined that the specified compliance requirements are both suitable for general use and available to users as discussed in section 101.23–.33, and, therefore, that a restricted use paragraph is not required.

Independent Accountant's Report

[*Introductory paragraph*]

We have examined [*name of entity*]'s compliance with [*list specified compliance requirements*] for the [*period*] ended [*date*]. Management is responsible for compliance with those requirements. Our responsibility is to express an opinion on [*name of entity*]'s compliance based on our examination.

[*Standard scope paragraph*]

[*Explanatory paragraph*]

Our examination disclosed the following material noncompliance with [*type of compliance requirement*] applicable to [*name of entity*] during the [*period*] ended [*date*]. [*Describe noncompliance.*]

[*Opinion paragraph*]

In our opinion, except for the material noncompliance described in the third paragraph, [*name of entity*] complied, in all material respects, with the aforementioned requirements for the [*period*] ended [*date*].

[*Signature*]

[*Date*]

.66 The following is the form of report, modified with explanatory language, that a practitioner should use when he or she concludes that an adverse opinion is appropriate in the circumstances. The practitioner has determined that the specified compliance requirements are both suitable for general use and available to users as discussed in section 101.23–.33.

Independent Accountant's Report

[*Introductory paragraph*]

We have examined [*name of entity*]'s compliance with [*list specified compliance requirements*] for the [*period*] ended [*date*]. Management is responsible for compliance with those requirements. Our responsibility is to express an opinion on [*name of entity*]'s compliance based on our examination.

[*Standard scope paragraph*]

[*Explanatory paragraph*]

Our examination disclosed the following material noncompliance with [*type of compliance requirement*] applicable to [*name of entity*] during the [*period*] ended [*date*]. [*Describe noncompliance.*]

[*Opinion paragraph*]

In our opinion, because of the effect of the noncompliance described in the third paragraph, [*name of entity*] has not complied with the aforementioned requirements for the [*period*] ended [*date*].

[*Signature*]

[*Date*]

.67 If the practitioner's report on his or her examination of the entity's compliance with specified requirements is included in a document that also includes his or her audit report on the entity's financial statements, the following sentence should be included in the paragraph of an examination report that describes material noncompliance.

> These conditions were considered in determining the nature, timing, and extent of audit tests applied in our audit of the 20XX financial statements, and this report does not affect our report dated [*date of report*] on those financial statements.

The practitioner also may include the preceding sentence when the two reports are not included within the same document.

Representation Letter

.68 In an examination engagement or an agreed-upon procedures engagement, the practitioner should obtain written representations from the responsible party—[22]

a. Acknowledging the responsible party's responsibility for complying with the specified requirements.

b. Acknowledging the responsible party's responsibility for establishing and maintaining effective internal control over compliance.

c. Stating that the responsible party has performed an evaluation of (1) the entity's compliance with specified requirements or (2) the entity's controls for ensuring compliance and detecting noncompliance with requirements, as applicable.

d. Stating the responsible party's assertion about the entity's compliance with the specified requirements or about the effectiveness of internal control over compliance, as applicable, based on the stated or established criteria.

e. Stating that the responsible party has disclosed to the practitioner all known noncompliance.

f. State that the responsible party has made available all documentation related to compliance with the specified requirements.

g. Stating the responsible party's interpretation of any compliance requirements that have varying interpretations.

h. State that the responsible party has disclosed any communications from regulatory agencies, internal auditors, and other practitioners concerning possible noncompliance with the specified requirements, including communications received between the end of the period addressed in the written assertion and the date of the practitioner's report.

i. Stating that the responsible party has disclosed any known noncompliance occurring subsequent to the period for which, or date as of which, the responsible party selects to make its assertion.

---

[22] AU section 333, *Management Representations*, paragraph .09, provides guidance on the date as of which the representation letter should be signed and who should sign it.

.69 The responsible party's refusal to furnish all appropriate written representations in an examination engagement constitutes a limitation on the scope of the engagement sufficient to preclude an unqualified opinion and is ordinarily sufficient to cause the practitioner to disclaim an opinion or withdraw from the engagement. However, based on the nature of the representations not obtained or the circumstances of the refusal, the practitioner may conclude in an examination engagement that a qualified opinion is appropriate. When the practitioner is performing agreed-upon procedures and the practitioner's client is the responsible party, the responsible party's refusal to furnish all appropriate written representations constitutes a limitation on the scope of the engagement sufficient to cause the practitioner to withdraw. When the practitioner's client is not the responsible party, the practitioner is not required to withdraw but should consider the effects of the responsible party's refusal on his or her report. Further, the practitioner should consider the effects of the responsible party's refusal on his or her ability to rely on other representations of the responsible party.

.70 When the practitioner's client is not the responsible party, the practitioner may also want to obtain written representations from the client. For example, when a practitioner's client has entered into a contract with a third party (responsible party) and the practitioner is engaged to examine the responsible party's compliance with that contract, the practitioner may want to obtain written representations from his or her client as to their knowledge of any noncompliance.

Other Information in a Client-Prepared Document Containing Management's Assertion About the Entity's Compliance With Specified Requirements or the Effectiveness of the Internal Control Over Compliance

.71 An entity may publish various documents that contain information (referred to as *other information*) in addition to the practitioner's attest report on either (*a*) the entity's compliance with specified requirements or (*b*) the effectiveness of the entity's internal control over compliance or written assertion thereon. Section 101.91–.94 provide guidance to the practitioner if the other information is contained in either of the following:

a. Annual reports to holders of securities or beneficial interests, annual reports of organizations for charitable or philanthropic purposes distributed to the public, and annual reports filed with regulatory authorities under the 1934 Act

b. Other documents to which the practitioner, at the client's request, devotes attention

Effective Date

.72 This section is effective when the subject matter or assertion is as of or for a period ending on or after June 1, 2001. Early application is permitted.

AT Section 801

Reporting on Controls at a Service Organization

(Supersedes the guidance for service auditors in AU section 324, *Service Organizations*.)

Source: SSAE No. 16.

Effective for service auditors' reports for periods ending on or after June 15, 2011. Earlier implementation is permitted.

Introduction

Scope of This Section

.01 This section 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 relevant to user entities' internal control over financial reporting. It complements AU section 324, *Service Organizations*, in that reports prepared in accordance with this section may provide appropriate evidence under AU section 324. (Ref: par. .A1)

.02 The focus of this section is on controls at service organizations likely to be relevant to user entities' internal control over financial reporting. The guidance herein also may be helpful to a practitioner performing an engagement under section 101, *Attest Engagements*, to report on controls at a service organization

a. other than those that are likely to be relevant to user entities' internal control over financial reporting (for example, controls that affect user entities' compliance with specified requirements of laws, regulations, rules, contracts, or grants, or controls that affect user entities' production or quality control). Section 601, *Compliance Attestation*, is applicable if a practitioner is reporting on an entity's own compliance with specified requirements or on its controls over compliance with specified requirements. (Ref: par. .A2–.A3)

b. when management of the service organization is not responsible for the design of the system (for example, when the system has been designed by the user entity or the design is stipulated in a contract between the user entity and the service organization). (Ref: par. .A4)

.03 In addition to performing an examination of a service organization's controls, a service auditor may be engaged to (*a*) examine and report on a user entity's transactions or balances maintained by a service organization, or (*b*) perform and report the results of agreed upon procedures 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 addressed in this section.

.04 The requirements and application material in this section are based on the premise that management of the service organization (also referred to as management) will provide the service auditor with a written assertion that is included in or attached to management's description of the service organization's system. Paragraph .10 of this section addresses the circumstance in which management refuses to provide such a written assertion. Section 101 indicates that when performing an attestation engagement, a practitioner may report directly on the subject matter or on management's assertion. For engagements conducted under this section, the service auditor is required to report directly on the subject matter.

Effective Date

.05 This section is effective for service auditors' reports for periods ending on or after June 15, 2011. Earlier implementation is permitted.

Objectives

.06 The objectives of the service auditor are to

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

i. management's description of the service organization's system fairly presents the system that was designed and implemented throughout the specified period (or in the case of a type 1 report, as of a specified date).

ii. the controls related to the control objectives stated in management's description of the service organization's system were suitably designed throughout the specified period (or in the case of a type 1 report, as of a specified date).

iii. when included in the scope of the engagement, the controls operated effectively to provide reasonable assurance that the control objectives stated in management's description of the service organization's system were achieved throughout the specified period.

b. report on the matters in 6(a) in accordance with the service auditor's findings.

Definitions

.07 For purposes of this section, the following terms have the meanings attributed in the subsequent text:

Carve-out method. Method of addressing the services provided by a subservice organization whereby management's 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. Management's description of the service organization's system and the scope of the service auditor's engagement include controls at the service organization that monitor the effectiveness of controls at the subservice organization, which may include management of the service organization's review of a service auditor's report on controls at the subservice organization.

Complementary user entity controls. Controls that management of the service organization assumes, in the design of the service provided by the service organization, will be implemented by user entities, and which, if necessary to achieve the control objectives stated in management's 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 address the risks that controls are intended to mitigate.

Controls at a service organization. The policies and procedures at a service organization likely to be relevant to user entities' internal control over financial reporting. These policies and procedures are designed, implemented, and documented 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. .A5)

Controls at a subservice organization. The policies and procedures at a subservice organization likely to be relevant to internal control over financial reporting of user entities of the service organization. These policies and procedures are designed, implemented, and documented 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. (Ref: par. .A6)

Inclusive method. Method of addressing the services provided by a subservice organization whereby management's description of the service organization's 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. (Ref: par. .A7–.A9)

Internal audit function. The service organization's internal auditors and others, for example, members of a compliance or risk department, who perform activities similar to those performed by internal auditors. (Ref: par. .A10)

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

a. Management's description of the service organization's system.

b. A written assertion by management of the service organization about whether, in all material respects, and based on suitable criteria,

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

ii. the controls related to the control objectives stated in management's description of the service organization's system 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)(i)–(b)(ii).

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

a. Management's description of the service organization's system.

b. A written assertion by management of the service organization about whether in all material respects, and based on suitable criteria,

i. management's description of the service organization's system fairly presents the service organization's system that was designed and implemented throughout the specified period.

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

iii. the controls related to the control objectives stated in management's 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

i. expresses an opinion on the matters in (b)(i)–(b)(iii).

ii. includes a description of the 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, which are likely to be relevant to those user entities' internal control over financial reporting.

Service organization's assertion. A written assertion about the matters referred to in part (b) of the definition of *Report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls*, for a type 2 report; and, for a type 1 report, the matters referred to in part (b) of the definition of *Report on management's description of a service organization's system and the suitability of the design of controls*.

Service organization's system. The policies and procedures designed, implemented, and documented, by management of the service organization to provide user entities with the services covered by the service auditor's report. Management's description of the service organization's system identifies the services covered, the period to which the description relates (or in the case of a type 1 report, the date 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. (Ref: par. .A11)

Subservice organization. A service organization used by another service organization to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting.

Test of controls. A procedure designed to evaluate the operating effectiveness of controls in achieving the control objectives stated in management's 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

Management and Those Charged With Governance

.08 When this section requires the service auditor to inquire of, request representations from, communicate with, or otherwise interact with management of the service organization, the service auditor should determine the appropriate person(s) within the service organization's management or governance structure with whom to interact. This should include consideration of which person(s) have the appropriate responsibilities for and knowledge of the matters concerned. (Ref: par. .A12)

Acceptance and Continuance

.09 A service auditor should accept or continue an engagement to report on controls at a service organization only if (Ref: par. .A13)

a. the service auditor has the capabilities and competence to perform the engagement. (Ref: par. .A14–.A15)

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

i. the criteria to be used will be suitable and available to the intended user entities and their auditors;

ii. the service auditor will have access to sufficient appropriate evidence to the extent necessary; and

iii. the scope of the engagement and management's 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.

c. management agrees to the terms of the engagement by acknowledging and accepting its responsibility for the following:

i. Preparing its description of the service organization's system and its assertion, including the completeness, accuracy, and method of presentation of the description and assertion. (Ref: par. .A16)

ii. Having a reasonable basis for its assertion. (Ref: par. .A17)

iii. Selecting the criteria to be used and stating them in the assertion.

iv. 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.

v. Identifying the risks that threaten the achievement of the control objectives stated in the description and designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that the control objectives stated in the description of the service organization's system will be achieved. (Ref: par. .A18)

vi. Providing the service auditor with

(1) access to all information, such as records and documentation, including service level agreements, of which management is aware that is relevant to the description of the service organization's system and the assertion;

(2) additional information that the service auditor may request from management for the purpose of the examination engagement;

(3) 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; and

(4) written representations at the conclusion of the engagement.

vii. Providing a written assertion that will be included in, or attached to management's description of the service organization's system, and provided to user entities.

.10 If management will not provide the service auditor with a written assertion, the service auditor should not circumvent the requirement to obtain an assertion by performing a service auditor's engagement under section 101. (Ref: par. .A19)

.11 Management's subsequent refusal to provide a written assertion represents a scope limitation and consequently, 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.

Request to Change the Scope of the Engagement

.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 a reasonable justification for the change exists. (Ref: par. .A20–.A21)

Assessing the Suitability of the Criteria (Ref: par. .A6 and .A22–.A23)

.13 As required by paragraph .23 of section 101, the service auditor should assess whether management has used suitable criteria

a. in preparing its description of the service organization's system;

b. in evaluating whether controls were suitably designed to achieve the control objectives stated in the description; and

c. in the case of a type 2 report, in evaluating whether controls operated effectively throughout the specified period to achieve the control objectives stated in the description of the service organization's system.

.14 In assessing the suitability of the criteria to evaluate whether management's description of the service organization's system is fairly presented, the service auditor should determine if the criteria include, at a minimum,

a. whether management's description of the service organization's system presents how the service organization's system was designed and implemented, including the following information about the service organization's system, if applicable:

i. The types of services provided including, as appropriate, the classes of transactions processed.

ii. The procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities.

iii. 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 and other information prepared for user entities.

iv. How the service organization's system captures and addresses significant events and conditions other than transactions.

v. The process used to prepare reports and other information for user entities.

vi. The specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of the service organization's controls.

vii. 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 the services provided. (Ref: par. A17 and .A24)

b. in the case of a type 2 report, whether management's description of the service organization's system includes relevant details of changes to the service organization's system during the period covered by the description. (Ref: par. .A44)

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

.15 In assessing the suitability of the criteria to evaluate whether the controls are suitably designed, the service auditor should determine if the criteria include, at a minimum, whether

a. the risks that threaten the achievement of the control objectives stated in management's description of the service organization's system have been identified by management.

b. the controls identified in management's description of the service organization's system would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

.16 In assessing the suitability of the criteria to evaluate whether controls operated effectively to provide reasonable assurance that the control objectives stated in management's description of the service organization's system were achieved, the service auditor should determine if the criteria include, at a minimum, whether the controls were consistently applied as designed throughout the specified period, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Materiality

.17 When planning and performing the engagement, the service auditor should evaluate materiality with respect to the fair presentation of management's 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. (Ref: par. .A25–.A27)

Obtaining an Understanding of the Service Organization's System (Ref: par. .A28–.A30)

.18 The service auditor should obtain an understanding of the service organization's system, including controls that are included in the scope of the engagement.

Obtaining Evidence Regarding Management's Description of the Service Organization's System (Ref: par. .A26 and .A31–.A35)

.19 The service auditor should obtain and read management's 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 management's description of the service organization's system are reasonable in the circumstances. (Ref: par. .A34)

b. controls identified in management's description of the service organization's system were implemented. (Ref: par. .A35)

c. complementary user entity controls, if any, are adequately described. (Ref: par. .A32)

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 in relation to them.

.20 The service auditor should determine through inquiries made in combination with other procedures whether the service organization's system has been implemented. Such other procedures should include observation and

inspection of records and other documentation of the manner in which the service organization's system operates and controls are applied. (Ref: par. .A35)

Obtaining Evidence Regarding the Design of Controls (Ref: par .A26 and .A36–.A39)

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

a. identifying the risks that threaten the achievement of the control objectives stated in management's description of the service organization's system, and (Ref: par. .A36)

b. evaluating the linkage of the controls identified in management's description of the service organization's system with those risks.

Obtaining Evidence Regarding the Operating Effectiveness of Controls (Ref: par. .A26 and .A40–.A45)

Assessing Operating Effectiveness

.22 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 management's 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. (Ref: par. .A40–.A44)

.23 When performing a type 2 engagement, 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, the service auditor should determine whether those changes are included in management's description of the service organization's system. If such changes are not included in the description, the service auditor should describe the changes in the service auditor's report and determine the effect on the service auditor's report. If the superseded controls are relevant to the achievement of the control objectives stated in the description, the service auditor should, if possible, test the superseded controls before the change. If the service auditor cannot test superseded controls relevant to the achievement of the control objectives stated in the description, the service auditor should determine the effect on the service auditor's report. (Ref: par. .A42(c) and .A45)

.24 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:

i. How the control was applied.

ii. The consistency with which the control was applied.

iii. 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.

.25 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. AU section 350, *Audit Sampling*, addresses planning, performing, and evaluating audit samples. If the service auditor determines that sampling is appropriate, the service auditor should apply the requirements in paragraphs .31–.43 of AU section 350, which address sampling in tests of controls. Paragraphs .01–.14 and .45–.46 of AU section 350 provide additional guidance regarding the principles underlying those paragraphs.

Nature and Cause of Deviations

.26 The service auditor should investigate the nature and cause of any deviations identified, 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 other controls is necessary to reach a conclusion about whether the controls related to the control objectives stated in management's description of the service organization's system operated effectively throughout the specified period.

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

.27 If, as a result of performing the procedures in paragraph .26, the service auditor becomes aware that any identified deviations have resulted from intentional acts by service organization personnel, the service auditor should assess the risk that management's description of the service organization's system is not fairly presented, the controls are not suitably designed, and in a type 2 engagement, the controls are not operating effectively. (Ref: par. .A31)

Using the Work of the Internal Audit Function

Obtaining an Understanding of the Internal Audit Function (Ref: par. .A46–.A47)

.28 If the service organization has an internal audit function, the service auditor should obtain an understanding of the nature of the responsibilities of the internal audit function and of the activities performed in order to determine whether the internal audit function is likely to be relevant to the engagement.

Planning to Use the Work of the Internal Audit Function

.29 When the service auditor intends to use the work of the internal audit function, the service auditor should determine whether the work of the internal

audit function is likely to be adequate for the purposes of the engagement by evaluating the following:

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

b. Whether the work of the internal audit function is likely to be carried out with due professional care

c. Whether it is likely that effective communication will occur between the internal audit function and the service auditor, including consideration of the effect of any constraints or restrictions placed on the internal audit function by the service organization

.30 If the service auditor determines that the work of the internal audit function is likely to be adequate for the purposes of the engagement, in determining the planned effect of the work of the internal audit function on the nature, timing, or extent of the service auditor's procedures, the service auditor should evaluate the following:

a. The nature and scope of specific work performed, or to be performed, by the internal audit function

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

c. 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 (Ref: par. .A48)

.31 In order for the service auditor to use specific work of the internal audit function, the service auditor should evaluate and perform procedures on that work to determine its adequacy for the service auditor's purposes.

.32 To determine the adequacy of specific work performed by the internal audit function for the service auditor's purposes, the service auditor should evaluate whether

a. the work was performed by members of the internal audit function having adequate technical training and proficiency;

b. the work was properly supervised, reviewed, and documented;

c. sufficient appropriate evidence was obtained to enable the internal audit function to draw reasonable conclusions;

d. conclusions reached are appropriate in the circumstances and any reports prepared by the internal audit function are consistent with the results of the work performed; and

e. exceptions relevant to the engagement or unusual matters disclosed by the internal audit function are properly resolved.

Effect on the Service Auditor's Report

.33 If the work of the internal audit function has been used, the service auditor should not make 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. (Ref: par. .A49)

.34 In the case of a type 2 report, if the work of the internal audit function has been used in performing tests of controls, that part of the service auditor's report that describes the service auditor's 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. (Ref: par. .A50)

Direct Assistance

.35 When the service auditor uses members of the service organization's internal audit function to provide direct assistance, the service auditor should adapt and apply the requirements in paragraph .27 of AU section 322, *The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements*.

Written Representations (Ref: par. .A51–.A55)

.36 The service auditor should request management to provide written representations that

a. reaffirm its assertion included in or attached to the description of the service organization's system;

b. it has provided the service auditor with all relevant information and access agreed to; and [1]

c. it has disclosed to the service auditor any of the following of which it is aware:

i. Instances of noncompliance with laws and regulations or uncorrected errors attributable to the service organization that may affect one or more user entities.

ii. Knowledge of any actual, suspected, or alleged intentional acts by management or the service organization's employees, that could adversely affect the fairness of the presentation of management's description of the service organization's system or the completeness or achievement of the control objectives stated in the description.

iii. Design deficiencies in controls.

iv. Instances when controls have not operated as described.

v. Any events subsequent to the period covered by management's description of the service organization's system up to the date of the service auditor's report that could have a significant effect on management's assertion.

.37 If a service organization uses a subservice organization and management's description of the service organization's system uses the inclusive method, the service auditor also should obtain the written representations identified in paragraph .36 from management of the subservice organization.

.38 The 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.

.39 If management does not provide one or more of the written representations requested by the service auditor, the service auditor should do the following:

a. Discuss the matter with management

b. Evaluate the effect of such refusal on the service auditor's assessment of the integrity of management and evaluate the effect that

---

[1] See paragraph .09(c)(vi)(1).

this may have on the reliability of management's representations and evidence in general

c. Take appropriate actions, which may include disclaiming an opinion or withdrawing from the engagement

If management refuses to provide the representations in paragraphs .36(a)–.36(b) of this section, the service auditor should disclaim an opinion or withdraw from the engagement.

Other Information (Ref: par. .A56–.A57)

.40 The service auditor should read other information, if any, included in a document containing management's 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.

.41 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.[2]

Subsequent Events

.42 The service auditor should inquire whether management is aware of any events subsequent to the period covered by management's description of the service organization's system up to the date of the service auditor's report that could have a significant effect on management's assertion. If the service auditor becomes aware, through inquiry or otherwise, of such an event, or any other event that is of such a nature and significance that its disclosure is necessary to prevent users of a type 1 or type 2 report from being misled, and information about that event is not disclosed by management in its description, the service auditor should disclose such event in the service auditor's report.

.43 The service auditor has no responsibility to keep informed of events subsequent to the date of the service auditor's report; however, after the release of the service auditor's report, the service auditor may become aware of conditions that existed at the report date that might have affected management's assertion and the service auditor's report had the service auditor been aware of them. The evaluation of such subsequent information is similar to the evaluation of information discovered subsequent to the date of the report on an audit of financial statements, as described in AU section 561, *Subsequent Discovery of Facts Existing at the Date of the Auditor's Report*, and therefore, the service auditor should adapt and apply the guidance in AU section 561.

Documentation (Ref: par. .A58)

.44 The service auditor should prepare documentation that is sufficient to enable an experienced service auditor, having no previous connection with the engagement, to understand the following:

---

[2] See paragraphs .91–.94 of section 101, *Attest Engagements*.

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

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

c. Significant findings or issues arising during the engagement, the conclusions reached thereon, and significant professional judgments made in reaching those conclusions

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

a. Identifying characteristics of the specific items or matters being tested

b. Who performed the work and the date such work was completed

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

.46 If the service auditor uses specific work of the internal audit function, the service auditor should document the conclusions reached regarding the evaluation of the adequacy of the work of the internal audit function and the procedures performed by the service auditor on that work.

.47 The service auditor should document discussions of significant findings or issues with management and others, including the nature of the significant findings or issues, when the discussions took place, and with whom.

.48 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.

.49 The service auditor should assemble the engagement documentation in an engagement file and complete the administrative process of assembling the final engagement file on a timely basis, no later than 60 days following the service auditor's report release date.

.50 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.

.51 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. The specific reasons for making them

b. When and by whom they were made and reviewed

Preparing the Service Auditor's Report

Content of the Service Auditor's Report (Ref: par. .A59)

.52 A service auditor's type 2 report should include the following elements:

a. A title that includes the word *independent*.

b. An addressee.

c. Identification of

i. management's description of the service organization's system and the function performed by the system.

ii. any parts of management's description of the service organization's system that are not covered by the service auditor's report. (Ref: par. .A56)

iii. any information included in a document containing the service auditor's report that is not covered by the service auditor's report. (Ref: par. .A56)

iv. the criteria.

v. any services performed by a subservice organization and whether the carve-out method or the inclusive method was used in relation to them. Depending on which method is used, the following should be included:

(1) If the carve-out method was used, a statement that management's 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.

(2) If the inclusive method was used, a statement that management's 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 related to the subservice organization.

d. If management's 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.

e. A reference to management's assertion and a statement that management is responsible for (Ref: par. .A60)

i. preparing the description of the service organization's system and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion;

ii. providing the services covered by the description of the service organization's system;

iii. specifying the control objectives unless the control objectives are specified by law, regulation, or another party, and stating them in the description of the service organization's system;

iv. identifying the risks that threaten the achievement of the control objectives;

v. selecting the criteria; and

vi. designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description of the service organization's system.

f. A statement that the service auditor's responsibility is to express an opinion on the fairness of the presentation of management's description of the service organization's system 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 the service auditor's examination.

g. A statement that the examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and that those standards require the service auditor to plan and perform the examination to obtain reasonable assurance about whether management's description of the service organization's system is fairly presented and the controls are suitably designed and operating effectively throughout the specified period to achieve the related control objectives.

h. A statement that an examination of management's description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description.

i. A statement that the examination included assessing the risks that management's description of the service organization's system is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives.

j. A statement that the examination also included testing the operating effectiveness of those controls that the service auditor considers necessary to provide reasonable assurance that the related control objectives stated in management's description of the service organization's system were achieved.

k. A statement that an examination engagement of this type also includes evaluating the overall presentation of management's description of the service organization's system and suitability of the control objectives stated in the description.

l. A statement that the service auditor believes the examination provides a reasonable basis for his or her opinion.

m. A statement about the inherent limitations of controls, including the risk of projecting to future periods any evaluation of the fairness of the presentation of management's description of the service organization's system or conclusions about the suitability of the design or operating effectiveness of controls.

n. The service auditor's opinion on whether, in all material respects, based on the criteria described in management's assertion,

i. management's description of the service organization's system fairly presents the service organization's system that was designed and implemented throughout the specified period.

ii. the controls related to the control objectives stated in management's 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.

iii. the controls the service auditor tested, which were those necessary to provide reasonable assurance that the control objectives stated in management's description of the service organization's system were achieved, operated effectively throughout the specified period.

iv. if the application of complementary user entity controls is necessary to achieve the related control objectives stated in management's description of the service organization's system, a reference to this condition.

o. A reference to a description of the service auditor's tests of controls and the results thereof, that includes

i. identification of the controls that were tested, 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. (Ref: par. .A50)

ii. if deviations have been identified in the operation of controls included in the description, the extent of testing performed by the service auditor that led to the identification of the deviations (including the number of items tested), and the number and nature of the deviations noted (even if, on the basis of tests performed, the service auditor concludes that the related control objective was achieved). (Ref: par. .A65)

p. A statement restricting the use of the service auditor's report to management of the service organization, user entities of the service organization's system during some or all of the period covered by the service auditor's report, and the independent auditors of such user entities. (Ref: par. .A61–.A64)

q. The date of the service auditor's report.

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

.53 A service auditor's type 1 report should include the following elements:

a. A title that includes the word *independent*.

b. An addressee.

c. Identification of

i. management's description of the service organization's system and the function performed by the system.

ii. any parts of management's description of the service organization's system that are not covered by the service auditor's report. (Ref: par. .A56)

iii. any information included in a document containing the service auditor report that is not covered by the service auditor's report. (Ref: par. .A56)

iv. the criteria.

v. any services performed by a subservice organization and whether the carve-out method or the inclusive method was

used in relation to them. Depending on which method is used, the following should be included:

(1) If the carve-out method was used, a statement that management's 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.

(2) If the inclusive method was used, a statement that management's 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 related to the subservice organization.

d. If management's 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.

e. A reference to management's assertion and a statement that management is responsible for (Ref: par. .A60)

i. preparing the description of the service organization's system and assertion, including the completeness, accuracy, and method of presentation of the description and assertion;

ii. providing the services covered by the description of the service organization's system;

iii. specifying the control objectives, unless the control objectives are specified by law, regulation, or another party, and stating them in the description of the service organization's system;

iv. identifying the risks that threaten the achievement of the control objectives,

v. selecting the criteria; and

vi. designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description of the service organization's system.

f. A statement that the service auditor's responsibility is to express an opinion on the fairness of the presentation of management's description of the service organization's system and on the suitability of the design of the controls to achieve the related control objectives stated in the description, based on the service auditor's examination.

g. A statement that the examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and that those standards require the service auditor to plan and perform the examination to obtain

reasonable assurance about whether management's description of the service organization's system is fairly presented and the controls are suitably designed as of the specified date to achieve the related control objectives.

h. A statement that the service auditor has not performed any procedures regarding the operating effectiveness of controls and, therefore, expresses no opinion thereon.

i A statement that an examination of management's description of a service organization's system and the suitability of the design of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design of those controls to achieve the related control objectives stated in the description.

j. A statement that the examination included assessing the risks that management's description of the service organization's system is not fairly presented and that the controls were not suitably designed to achieve the related control objectives.

k. A statement that an examination engagement of this type also includes evaluating the overall presentation of management's description of the service organization's system and suitability of the control objectives stated in the description.

l. A statement that the service auditor believes the examination provides a reasonable basis for his or her opinion.

m. A statement about the inherent limitations of controls, including the risk of projecting to future periods any evaluation of the fairness of the presentation of management's description of the service organization's system or conclusions about the suitability of the design of the controls to achieve the related control objectives.

n. The service auditor's opinion on whether, in all material respects, based on the criteria described in management's assertion,

i. management's description of the service organization's system fairly presents the service organization's system that was designed and implemented as of the specified date.

ii. the controls related to the control objectives stated in management's 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.

ii. if the application of complementary user entity controls is necessary to achieve the related control objectives stated in management's description of the service organization's system, a reference to this condition.

o. A statement restricting the use of the service auditor's report to management of the service organization, user entities of the service organization's system as of the end of the period covered by the service auditor's report, and the independent auditors of such user entities. (Ref: par. .A61–.A64)

p. The date of the service auditor's report.

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

Report Date

.54 The service auditor should date the service auditor's report no earlier than the date on which the service auditor has obtained sufficient appropriate evidence to support the service auditor's opinion.

Modified Opinions (Ref: par. .A66)

.55 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, if the service auditor concludes that

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 management's 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 management's description of the service organization's system; or

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

.56 If the service auditor plans to disclaim an opinion because of the inability to obtain sufficient appropriate evidence, and, based on the limited procedures performed, has concluded that,

a. certain aspects of management's description of the service organization's system are not fairly presented, in all material respects;

b. certain controls were not suitably designed to provide reasonable assurance that the control objectives stated in management's description of the service organization's system would be achieved if the controls operated as described; or

c. in the case of a type 2 report, certain controls did not operate effectively throughout the specified period to achieve the related control objectives stated in management's description of the service organization's system,

the service auditor should identify these findings in his or her report.

.57 If the service auditor plans to disclaim an opinion, the service auditor should not identify the procedures that were performed nor include statements describing the characteristics of a service auditor's engagement in the service auditor's report; to do so might overshadow the disclaimer.

Other Communication Responsibilities

.58 If the service auditor becomes aware of incidents of noncompliance with laws and regulations, fraud, or uncorrected errors attributable to management or other service organization personnel that are not clearly trivial and that may affect one or more user entities, the service auditor should determine the effect of such incidents on management's 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. (Ref: par. .A67)

Application and Other Explanatory Material

Scope of This Section

.A1 *Internal control* is a process designed to provide reasonable assurance regarding the achievement of objectives related to the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. Controls related to a service organization's operations and compliance objectives may be relevant to a user entity's internal control over financial reporting. Such controls may pertain to assertions about presentation and disclosure relating to account balances, classes of transactions or disclosures, or may pertain to evidence that the user auditor evaluates or uses in applying auditing procedures. For example, a payroll processing service organization's controls related to the timely remittance of payroll deductions to government authorities may be relevant to a user entity because late remittances could incur interest and penalties that would result in a liability for the user entity. Similarly, a service organization's controls over the acceptability of investment transactions from a regulatory perspective may be considered relevant to a user entity's presentation and disclosure of transactions and account balances in its financial statements. (Ref: par. .01)

.A2 Paragraph .02 of this section refers to other engagements that the practitioner may perform and report on under section 101 to report on controls at a service organization. Paragraph .02 is not, however, intended to

- provide for the alteration of the definitions of *service organization* and *service organization's system* in paragraph .07 to permit reports issued under this section to include in the description of the service organization's system aspects of their services (including relevant control objectives and related controls) not likely to be relevant to user entities' internal control over financial reporting, or
- permit a report to be issued that combines reporting under this section on a service organization's controls that are likely to be relevant to user entities' internal control over financial reporting, with reporting under section 101 on controls that are not likely to be relevant to user entities' internal control over financial reporting. (Ref: par. .02(a))

.A3 When a service auditor conducts an engagement under section 101 to report on controls at a service organization other than those controls likely to be relevant to user entities' internal control over financial reporting, and the service auditor intends to use the guidance in this section in planning and performing that engagement, the service auditor may encounter issues that differ significantly from those associated with engagements to report on a service organization's controls likely to be relevant to user entities' internal control over financial reporting. For example,

- identification of suitable and available criteria, as prescribed in paragraphs .23–.34 of section 101, for evaluating the fairness of presentation of management's description of the service organization's system and the suitability of the design and the operating effectiveness of the controls.
- identification of appropriate control objectives, and the basis for evaluating the reasonableness of the control objectives in the circumstances of the particular engagement.

- identification of the intended users of the report and the manner in which they intend to use the report.
- relevance and appropriateness of the definitions in paragraph .07 of this section, many of which specifically relate to internal control over financial reporting.
- application of references to auditing standards (AU sections) that are intended to provide the service auditor with guidance relevant to internal control over financial reporting.
- application of the concept of materiality in the circumstances of the particular engagement.
- developing the language to be used in the practitioner's report, including addressing paragraphs .84–.87 of section 101, which identify the elements to be included in an examination report. (Ref: par. .02(a))

.A4 When management of the service organization is not responsible for the design of the system, it is unlikely that management of the service organization will be in a position to assert that the system is suitably designed. Controls cannot operate effectively unless they are suitably designed. Because of the inextricable link between the suitability of the design of controls and their operating effectiveness, the absence of an assertion with respect to the suitability of design will likely preclude the service auditor from opining on the operating effectiveness of controls. As an alternative, the practitioner may perform tests of controls in either an agreed-upon procedures engagement under section 201, *Agreed Upon Procedures Engagements*, or an examination of the operating effectiveness of the controls under section 101. (Ref: par. .02(b))

Definitions

Controls at a Service Organization (Ref: par. .07)

.A5 The policies and procedures referred to in the definition of *controls at a service organization* in paragraph .07 include aspects of user entities' information systems maintained by the service organization and may also include aspects of one or more of the other components of internal control at a service organization. For example, the definition of *controls at a service organization* may include aspects of the service organization's control environment, monitoring, and control activities when they relate to the services provided. Such definition does not, however, include controls at a service organization that are not related to the achievement of the control objectives stated in management's description of the service organization's system; for example, controls related to the preparation of the service organization's own financial statements.

Criteria (Ref: par. .07 and .14–.16)

.A6 For the purposes of engagements performed in accordance with this section, criteria need to be available to user entities and their auditors to enable them to understand the basis for the service organization's assertion about the fair presentation of management's description of the service organization's system, the suitability of the design of controls that address control objectives stated in the description of the system and, in the case of a type 2 report, the operating effectiveness of such controls. Information about suitable criteria is provided in paragraphs .23–.34 of section 101. Paragraphs .14–.16 of this section

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 (Ref: par. .07)

.A7 As indicated in the definition of *inclusive method* in paragraph .07, a service organization that uses a subservice organization presents management's description of the service organization's system to include a description of the services provided by the subservice organization as well as the subservice organization's relevant control objectives and related controls. When the inclusive method is used, the requirements of this section also apply to the services provided by the subservice organization, including the requirement to obtain management's acknowledgement and acceptance of responsibility for the matters in paragraph .09(c)(i)–(vii) as they relate to the subservice organization.

.A8 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, for example, 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 a service auditor's report. If the service auditor is unable to obtain an assertion from the subservice organization regarding management's description of the service organization's system provided, including the relevant control objectives and related controls at the subservice organization, the service auditor is unable to use the inclusive method but may instead use the carve-out method.

.A9 There may be instances when the service organization's controls, such as monitoring controls, permit the service organization to include in its assertion the relevant aspects of the subservice organization's system, including the relevant control objectives and related controls of the subservice organization. In such instances, the service auditor is basing his or her opinion solely on the controls at the service organization, and hence, the inclusive method is not applicable.

Internal Audit Function (Ref: par. .07)

.A10 The "others" referenced in the definition of *internal audit function* may be individuals who perform activities similar to those performed by internal auditors and include service organization personnel (in addition to internal auditors), and third parties working under the direction of management or those charged with governance.

Service Organization's System (Ref: par. .07)

.A11 The policies and procedures referred to in the definition of *service organization's system* refer to the guidelines and activities for providing transaction processing and other services to user entities and include the infrastructure, software, people, and data that support the policies and procedures.

Management and Those Charged With Governance (Ref: par. .08)

.A12 Management and governance structures vary by entity, reflecting influences such as size and ownership characteristics. Such diversity means that it is not possible for this section to specify for all engagements the person(s) with whom the service auditor is to interact regarding particular matters. For

example, the service organization may be a segment of an organization and not a separate legal entity. In such cases, identifying the appropriate management personnel or those charged with governance from whom to request written representations may require the exercise of professional judgment.

Acceptance and Continuance

.A13 If one or more of the conditions in paragraph .09 are not met and the service auditor is nevertheless required by law or regulation to accept or continue an engagement to report on controls at a service organization, the service auditor is required, in accordance with the requirements in paragraphs .55–.56, to determine the effect on the service auditor's report of one or more of such conditions not being met. (Ref: par. .09)

Capabilities and Competence to Perform the Engagement (Ref: par. .09a)

.A14 Relevant capabilities and competence to perform the engagement include matters such as the following:

- Knowledge of the relevant industry
- An understanding of information technology and systems
- Experience in evaluating risks as they relate to the suitable design of controls
- Experience in the design and execution of tests of controls and the evaluation of the results

.A15 In performing a service auditor's engagement, the service auditor need not be independent of each user entity. (Ref: par. .09a)

Management's Responsibility for Documenting the Service Organization's System (Ref: par. .09(c)(i))

.A16 Management of the service organization is responsible for documenting the service organization's system. No one particular form of documentation is prescribed and the extent of documentation may vary depending on the size and complexity of the service organization and its monitoring activities.

Reasonable Basis for Management's Assertion (Ref: par. .07, definition of service organization's system; par. .09(c)(ii) and .14(a)(vii))

.A17 Management's monitoring activities may provide evidence of the design and operating effectiveness of controls in support of management's assertion. *Monitoring of controls* is a process to assess the effectiveness of internal control performance over time. It involves assessing the effectiveness of controls on a timely basis, identifying and reporting deficiencies to appropriate individuals within the service organization, and taking necessary corrective actions. Management accomplishes monitoring of controls through ongoing activities, separate evaluations, or a combination of the two. Ongoing monitoring activities are often built into the normal recurring activities of an entity 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 may also include using information communicated by external parties, such as customer complaints and regulator comments, which may indicate problems or highlight areas in need of improvement. The greater the degree and effectiveness of ongoing monitoring, the less need for separate evaluations. Usually, some combination of

ongoing monitoring and separate evaluations will ensure that internal control maintains its effectiveness over time. The service auditor's report on controls is not a substitute for the service organization's own processes to provide a reasonable basis for its assertion.

Identification of Risks (Ref: par. .09(c)(v))

.A18 Control objectives relate to risks that controls seek to mitigate. For example, the risk that a transaction is recorded at the wrong amount or in the wrong period can be expressed as a control objective that transactions are recorded at the correct amount and in the correct period. Management is responsible for identifying the risks that threaten achievement of the control objectives stated in management's description of the service organization's system. Management may have a formal or informal process for identifying relevant risks. A formal process may include estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about actions to address them. However, because control objectives relate to risks that controls seek to mitigate, thoughtful identification by management of control objectives when designing, implementing, and documenting the service organization's system may itself comprise an informal process for identifying relevant risks.

Management's Refusal to Provide a Written Assertion

.A19 A recent change in service organization management or the appointment of the service auditor by a party other than management are examples of situations that may cause management to be unwilling to provide the service auditor with a written assertion. However, other members of management may be in a position to, and will agree to, sign the assertion so that the service auditor can meet the requirement of paragraph .09(c)(vii). (Ref: par. .10)

Request to Change the Scope of the Engagement (Ref: par. .12)

.A20 A request to change the scope of the engagement may not have a reasonable justification if, for example, the request is made

- to exclude certain control objectives 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 control objectives.
- to prevent the disclosure of deviations identified at a subservice organization by requesting a change from the inclusive method to the carve-out method.

.A21 A request to change the scope of the engagement may have a reasonable justification when, for example, the request is made to exclude from the engagement a subservice organization because the service organization cannot arrange for access by the service auditor, and the method used for addressing the services provided by that subservice organization is changed from the inclusive method to the carve-out method.

Assessing the Suitability of the Criteria (Ref: par. .13–.16)

.A22 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 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 management's description of the service organization's system (type 1 and type 2 reports).	Management's description of the service organization's system that is likely to be relevant to user entities' internal control over financial reporting and is covered by the service auditor's report, and management's assertion about whether the description is fairly presented.	Management's description of the service organization's system is fairly presented if it *a*. presents how the service organization's system was designed and implemented including, as appropriate, the matters identified in paragraph .14(a) and, in the case of a type 2 report, includes relevant details of changes to the service organization's system during the period covered by the description. *b*. does not omit or distort information relevant to the service organization's system, while acknowledging that management's description of the service organization's system is prepared 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 management's description of the service organization's system are provided in paragraph .14. Paragraphs .19–.20 and .A31–.A33 offer further guidance on determining whether these criteria are met.

(continued)

	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 management's description of the service organization's system.	The controls are suitably designed and operating effectively to achieve the control objectives stated in management's description of the service organization's system if *a*. management has identified the risks that threaten the achievement of the control objectives stated in management's description of the service organization's system. *b*. the controls identified in management's description of the service organization's system would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved. *c*. the controls were consistently applied as designed throughout the specified period. This includes whether manual controls were applied by individuals who have the appropriate competence and authority.	When the criteria for this opinion are met, controls will have provided reasonable assurance that the related control objectives stated in management's description of the service organization's system were achieved throughout the specified period.	The control objectives stated in management's 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, 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.

	Subject Matter	*Criteria*	*Comment*
Opinion on suitability of design (type 1 reports).	The suitability of the design of the controls necessary to achieve the control objectives stated in management's 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 management's description of the service organization's system if *a.* management has identified the risks that threaten the achievement of the control objectives stated in its description of the service organization's system. *b.* the controls identified in management's description of the service organization's system 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 these criteria does not, of itself, provide any assurance that the control objectives stated in management's description of the service organization's system were achieved because no evidence has been obtained about the operating effectiveness of the controls.

.A23 Paragraph .14(a) identifies a number of elements that are included in management's description of the service organization's system as appropriate. These elements may not be appropriate if the system being described is not a system that processes transactions; for example, if the system relates to general controls over the hosting of an IT application but not the controls embedded in the application itself. (Ref: par. .14)

.A24 The requirement to include in management's 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 the services provided" is also applicable to the internal control components of subservice organizations used by the service organization when the inclusive method is used. See AU section 314, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, for a discussion of these components. (Ref: par. .14(a)(vii))

Materiality (Ref: par. .17)

.A25 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 management's 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. The concept of materiality takes into account 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.

.A26 Materiality with respect to the fair presentation of management's description of the service organization's system and with respect to the design of controls primarily includes the consideration of qualitative factors; for example, whether

- management's description of the service organization's system includes the significant aspects of the processing of significant transactions.
- management's description of the service organization's system omits or distorts relevant information.
- the controls have the ability, as designed, to provide reasonable assurance that the control objectives stated in management's description of the service organization's system 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 (a quantitative matter) and the nature and cause of any observed deviations (a qualitative matter).

.A27 The concept of materiality is not applied when disclosing, in the description of the tests of controls, the results of those tests when deviations have been identified. This is because, in the particular circumstances of a specific user entity or user auditor, a deviation may have significance beyond whether or not, in the opinion of the service auditor, it prevents a control from operating effectively. For example, the control to which the deviation relates may be particularly significant in preventing a certain type of error that may be material in the particular circumstances of a user entity's financial statements.

Obtaining an Understanding of the Service Organization's System (Ref: par. .18)

.A28 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 management's 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 management's description of the service organization's system, 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

.A29 Management's description of the service organization's system includes "aspects of the service organization's control environment, risk assessment process, information and communication systems (including relevant

business processes), control activities and monitoring activities that are relevant to the services provided." Although aspects of the service organization's control environment, risk assessment process, and monitoring activities may not be presented in the description in the context of control objectives, they may nevertheless be necessary to achieve the specified control objectives stated in the description. Likewise, deficiencies in these controls may have an effect on the service auditor's assessment of whether the controls, taken as a whole, were suitably designed or operating effectively to achieve the specified control objectives. See AU section 314 for a discussion of these components of internal control.

.A30 The service auditor's procedures to obtain the understanding referred to in paragraph .A28 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

One or more of the preceding procedures may be accomplished through the performance of a walkthrough.

Obtaining Evidence Regarding Management's Description of the Service Organization's System (Ref: par. .19–.20)

.A31 In a service auditor's examination engagement, the service auditor plans and performs the engagement to obtain reasonable assurance of detecting errors or omissions in management's description of the service organization's system and instances in which control objectives were not achieved. Absolute assurance is not attainable because of factors such as the need for judgment, the use of sampling, and the inherent limitations of controls at the service organization that affect whether the description is fairly presented and the controls are suitably designed and operating effectively to achieve the control objectives, and because much of the evidence available to the service auditor is persuasive rather than conclusive in nature. Also, procedures that are effective for detecting unintentional errors or omissions in the description, and instances in which control objectives were not achieved, may be ineffective for detecting intentional errors or omissions in the description and instances in which the control objectives were not achieved that are concealed through collusion between service organization personnel and a third party or among management or employees of the service organization. Therefore, the subsequent discovery of the existence of material omissions or errors in the description or instances in which control objectives were not achieved does not, in and of itself, evidence inadequate planning, performance, or judgment on the part of the service auditor. (Ref: par. .27)

.A32 Considering the following questions may assist the service auditor in determining whether management's description of the service organization's system is fairly presented, in all material respects:

- Does management's 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 prepared 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? 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 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?
- Does the description include relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time?
- 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 does include complementary user entity controls, the description separately identifies those controls along with the specific control objectives that cannot be achieved by the service organization alone. (Ref: par. .19(c))
- If the inclusive method has been used, does the description separately identify controls at the service organization and controls at the subservice organization? If the carve-out method is used, does the description identify the functions that are performed by the subservice organization? When the carve-out method is used, the description need not describe the detailed processing or controls at the subservice organization.

.A33 The service auditor's procedures to evaluate the fair presentation of management's 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 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

.A34 Paragraph .19(a) requires the service auditor to evaluate whether the control objectives stated in management's 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 specified by 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 specified by the service organization 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 (for example, assertions about existence and accuracy that are affected by access controls that prevent or detect unauthorized access to the system)? 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 specified by the service organization complete? Although a complete set of control objectives can provide a broad range of user auditors with a framework to assess the effect of controls at the service organization on assertions commonly embodied in user entities' financial statements, 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 and cannot, therefore, determine whether control objectives are complete from the viewpoint of individual user entities or user auditors. It is the responsibility of individual user entities or user auditors to assess whether the service organization's description addresses the particular control objectives that are relevant to their needs. 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. (Ref: par. .19(a))

.A35 The service auditor's procedures to determine whether the system described by the service organization has been implemented may be similar to, and performed in conjunction with, procedures to obtain an understanding of that system. Other procedures that the service auditor may use in combination with inquiry of management and other service organization personnel 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. (Ref: par. .19(b) and .20)

Obtaining Evidence Regarding the Design of Controls (Ref: par. .21)

.A36 The risks and control objectives identified in paragraph .21(a) encompass intentional and unintentional acts that threaten the achievement of the control objectives. (Ref: par. .21(a))

.A37 From the viewpoint of a user auditor, a control is suitably designed to achieve the control objectives stated in management's 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 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(s) stated in the description of the service organization's system are achieved.

.A38 A service auditor may consider using flowcharts, questionnaires, or decision tables to facilitate understanding the design of the controls.

.A39 Controls may consist of a number of 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 may allow the service auditor to conclude that controls related to the control objective are suitably designed to achieve the control objective.

Obtaining Evidence Regarding the Operating Effectiveness of Controls (Ref: par. .22–.27)

.A40 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 affect whether or not a misstatement resulting from a control deviation is material to those user entities. 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 management's description of the service organization's system are achieved. Similarly, a service auditor is not in a position to determine whether any observed control deviation would result in a material misstatement from the viewpoint of an individual user entity. (Ref: par. .22)

.A41 Obtaining an understanding of controls sufficient to opine on the suitability of their design is not sufficient evidence regarding their operating effectiveness unless some automation 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. (Ref: par. .22)

.A42 A type 2 report that covers a period that is less than six months is unlikely to be useful to user entities and their auditors. If management's description of the service organization's system covers a period that is less than six months, the description 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:

- 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.
- The service organization or a particular system or application has been in operation for less than six months.
- 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. (Ref: par. .23)

.A43 Evidence about the satisfactory operation of controls in prior periods does not provide evidence of the operating effectiveness of controls during the current period. 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 for the current period. Knowledge of deviations observed in prior engagements may, however, lead the service auditor to increase the extent of testing during the current period. (Ref: par. .22)

.A44 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. (Ref: par. .14(b) and .23)

.A45 Certain controls 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 controls at various times throughout the reporting period. (Ref: par. .22)

Using the Work of an Internal Audit Function

Obtaining an Understanding of the Internal Audit Function (Ref: par. .28)

.A46 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.

.A47 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.

Using the Work of the Internal Audit Function (Ref: par .31–.32)

.A48 The nature, timing, and extent of the service auditor's procedures on specific work of the internal auditors will depend on the service auditor's assessment of the significance of that work to the service auditor's conclusions (for example, the significance of the risks that the controls tend to mitigate), the evaluation of the internal audit function, and the evaluation of the specific work of the internal auditors. Such procedures may include the following:

- Examination of items already examined by the internal auditors
- Examination of other similar items
- Observation of procedures performed by the internal auditors

Effect on the Service Auditor's Report (Ref: par. .33–.34)

.A49 The responsibility to report on management's description of the service organization's system and the suitability of the design and operating effectiveness of controls rests solely with the service auditor and cannot be shared with the internal audit function. Therefore, the judgments about the significance of deviations in the design or operating effectiveness of controls, the sufficiency of tests performed, the evaluation of identified deficiencies, and other matters affecting the service auditor's report are those of the service auditor. In making judgments about the extent of the effect of the work of the internal audit function on the service auditor's procedures, the service auditor may determine, based on risk associated with the controls and the significance of the judgments relating to them, that the service auditor will perform the work relating to some or all of the controls rather than using the work performed by the internal audit function.

.A50 In the case of a type 2 report, when the work of the internal audit function has been used in performing tests of controls, the service auditor's description of that work and of the service auditor's procedures with respect to that work may be presented in a number of ways, for example, (Ref: par. .34 and .52(o)(i))

- by including introductory material to the description of tests of controls indicating that certain work of the internal audit function was used in performing tests of controls.

- attribution of individual tests to internal audit.

Written Representations (Ref: par. .36–.39)

.A51 Written representations reaffirming the service organization's assertion about the effective operation of controls may be based on ongoing monitoring activities, separate evaluations, or a combination of the two. (Ref: par. .A12)

.A52 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.

.A53 The written representations required by paragraph .36 are separate from and in addition to the assertion included in or attached to management's description of the service organization's system required by paragraph .09(c)(vii).

.A54 If the service auditor is unable to obtain written representations regarding relevant control objectives and related controls at the subservice organization, management of the service organization would be unable to use the inclusive method but could use the carve-out method.

.A55 In addition to the written representations required by paragraph .36, the service auditor may consider it necessary to request other written representations.

Other Information

.A56 The "other information" referred to in paragraphs .40–.41 may be the following:

- Information provided by the service organization and included in a section of the service auditor's type 1 or type 2 report, or
- Information outside the service auditor's type 1 or type 2 report included in a document that contains the service auditor's report. This other information may be provided by the service organization or by another party. (Ref: par. .40, .52(c)(ii)–(iii), and .53(c)(ii)–(iii))

.A57 If other information included in a document containing management's description of the service organization's system and the service auditor's report contains future-oriented information that cannot be reasonably substantiated, the service auditor may request that the information be removed or revised. (Ref: par. .41)

Documentation

.A58 Paragraph 57 of Statement on Quality Control Standards No. 7, *A Firm's System of Quality Control* (QC sec. 10A), requires the firm to establish policies and procedures that address engagement performance, supervision responsibilities, and review responsibilities. The requirement to document who reviewed the work performed and the extent of the review, in accordance with the firm's policies and procedures addressing review responsibilities, does not imply a need for each specific working paper to include evidence of review. The requirement, however, means documenting what work was reviewed, who reviewed such work, and when it was reviewed. (Ref: par. .44)

Preparing the Service Auditor's Report

Content of the Service Auditor's Report (Ref: par. .52–.53)

.A59 Examples of service auditors' reports are presented in appendixes A–C and illustrative assertions by management of the service organization are presented in exhibit A.

.A60 The service organization's assertion may be presented in management's description of the service organization's system or may be attached to the description. (Ref: par. .52(e) and .53(e))

Use of the Service Auditor's Report (Ref: par. .52(p) and .53(o))

.A61 Paragraph .79 of section 101 requires that the 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, user entities of the service organization ("during some or all of the period covered by the report" for a type 2 report, and "as of the ending date of the period covered by the report" for a type 1 report), and their user auditors. (The illustrative service auditor's reports in appendix A illustrate language for a paragraph restricting the use of a service auditor's report.)

.A62 Paragraph .79 of section 101 indicates that the need for restriction on the use of a report may result from a number of circumstances, including the potential for the report to be misunderstood when taken out of the context in which it was intended to be used, and the extent to which the procedures performed are known or understood.

.A63 Although a service auditor is not responsible for controlling a service organization's distribution of a service auditor's report, a service auditor may inform the service organization of the following:

- A service auditor's type 1 report is not intended for distribution to parties other than the service organization, user entities of the service organization's system as of the end of the period covered by the service auditor's report, and their user auditors.
- A service auditor's type 2 report is not intended for distribution to parties other than the service organization, user entities of the service organization's system during some or all of the period covered by the service auditor's report, and their user auditors.

.A64 A user entity is also considered a user entity of the service organization's subservice organizations if controls at subservice organizations are relevant to internal control over financial reporting of the user entity. In such case, the user entity is referred to as an indirect or downstream user entity of the subservice organization. Consequently, an indirect or downstream user entity may be included in the group to whom use of the service auditor's report is restricted if controls at the service organization are relevant to internal control over financial reporting of such indirect or downstream user entity.

Description of the Service Auditor's Tests of Controls and the Results Thereof (Ref: par. .52(o)(ii))

.A65 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. .55–.57)

.A66 Examples of elements of modified service auditor's reports are presented in appendix B.

Other Communication Responsibilities (Ref: par. .58)

.A67 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 (after giving additional consideration to instances in which the service organization has not appropriately communicated this information to affected user entities, and the service organization is unwilling to do so) include the following:

- Obtaining legal advice about the consequences of different courses of action
- Communicating with those charged with governance of the service organization
- Disclaiming an opinion, modifying the service auditor's opinion, or adding an emphasis paragraph
- Communicating with third parties, for example, a regulator, when required to do so
- Withdrawing from the engagement

.A68

Appendix A: 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 of its [*type or name of*] system for processing user entities' transactions [*or identification of the function performed by the system*] throughout the period [*date*] to [*date*] (description) and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description.

Service organization's responsibilities

On page XX of the description, XYZ Service Organization has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. XYZ Service Organization is responsible for preparing the description and for the assertion, 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, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting 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 and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period [*date*] to [*date*].

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 to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and 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. Our procedures also 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 therein, and the suitability of the criteria specified by the service organization and described at page *[aa]*. 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 [*or identification of the function performed by the system*]. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

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

a. the description 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 were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period [*date*] to [*date*].

c. the controls 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*].

Description of tests of controls

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

Restricted use

This report, including the description of tests of controls and results thereof on pages [*yy–zz*], is intended solely for the information and use of XYZ Service Organization, user entities of XYZ Service Organization's [*type or name of*] system during some or all of the period [*date*] to [*date*], and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. 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 and state*]

Following is a modification of the scope paragraph in a type 2 service auditor's report if the description refers to the need for complementary user entity controls. (New language is shown in boldface italics):

> We have examined XYZ Service Organization's description of its [*type or name of*] system for processing user entities' transactions [*or identification of the function performed by the system*] throughout the period [*date*] to [*date*] (description) and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. ***The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of XYZ Service Organization's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.***

Following is a modification of the applicable subparagraphs of the opinion paragraph of a type 2 service auditor's report if the application of complementary user entity controls is necessary to achieve the related 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 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 user entities 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 tested, which ***together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively,*** 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*].

Following is a modification of the paragraph that describes the responsibilities of management of the service organization for use in a type 2 service auditor's report when the control objectives have been specified by an outside party. (New language is shown in boldface italics):

> On page XX of the description, XYZ Service Organization has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. XYZ Service Organization is responsible for preparing the description and for its assertion], 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 documenting controls to achieve the related 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 of its [*type or name of*] system for processing user entities' transactions [*or identification of the function performed by the system*] as of [*date*], and the suitability of the design of controls to achieve the related control objectives stated in the description.

Service organization's responsibilities

On page XX of the description, XYZ Service Organization has provided an assertion about the fairness of the presentation of the description and suitability of the design of the controls to achieve the related controls objectives stated in the description. XYZ Service Organization is responsible for preparing the description and for its assertion, 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, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting 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 the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance, in all material respects, about whether the description is fairly presented and the controls were suitably designed to achieve the related control objectives stated in the description as of [*date*].

An examination of a description of a service organization's system and the suitability of the design of the service organization's controls to achieve 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. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed 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 therein, and the suitability of the criteria specified by the service organization and described at page *[aa]*.

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 [*or identification of the function performed by the system*]. The projection

to the future of any evaluation of the fairness of the presentation of the description, or any conclusions about the suitability of the design of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become ineffective or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in XYZ Service Organization's assertion,

a. the description 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 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 XYZ Service Organization, user entities of XYZ Service Organization's [*type or name of*] system as of [*date*], and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when obtaining an understanding of user entities 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 and state*]

Following is a modification of the scope paragraph in a type 1 report if the description of the service organization's system refers to the need for complementary user entity controls. (New language is shown in boldface italics)

> We have examined XYZ Service Organization's description of its [type or name of] system (description) made available to user entities of the system for processing their transactions [or identification of the function performed by the system] as of [date], and the suitability of the design of controls to achieve the related control objectives stated in the description. ***The description indicates that certain complementary user entity controls must be suitably designed and implemented at user entities for related controls at the service organization to be considered suitably designed to achieve the related control objectives. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.***

Following is a modification of the applicable subparagraph in the opinion paragraph of a type 1 report if the application of complementary user entity controls is necessary to achieve the related control objectives stated in management's 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 were suitably designed to provide reasonable assurance that those control objectives would be achieved if the controls operated effectively as of [*date*] ***and user entities applied the complementary user entity controls contemplated in the design of XYZ Service Organization's controls as of [date].***

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

> On page XX of the description, XYZ Service Organization has provided an assertion about the fairness of the presentation of the description and suitability of the design of the controls to achieve the related control objectives stated in the description. XYZ Service Organization is responsible for preparing the description and assertion, 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 documenting controls to achieve the related 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***.

.A69

Appendix B: Illustrative Modified Service Auditor's Reports

The following examples of modified service auditor's 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 appendix A.

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

The following is an illustrative paragraph describing the basis for the qualified opinion. The paragraph would be inserted before the modified opinion paragraph. All other report paragraphs are unchanged.

Basis for qualified opinion

The accompanying description 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 XYZ Service Organization'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

The following is an illustrative paragraph describing the basis for the qualified opinion. The paragraph would be inserted before the modified opinion paragraph. All other report paragraphs are unchanged.

Basis for qualified opinion

As discussed on 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 also are no specified requirements to test such changes or provide test results to an authorized reviewer prior to implementing the changes. As a result the controls are not suitably designed to achieve the control objective, "Controls provide reasonable assurance that changes to existing applications are authorized, tested, approved, properly implemented, and documented."

Opinion

In our opinion, except for the matter described in the preceding paragraph, and based on the criteria described in XYZ Service Organization'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

The following is an illustrative paragraph describing the basis for the qualified opinion. The paragraph would be inserted before the modified opinion paragraph. All other report paragraphs are unchanged.

Basis for qualified opinion

XYZ Service Organization states in its description that it has automated controls in place to reconcile loan payments received with the various output reports. However, as noted on 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. XYZ Service Organization 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 XYZ Service Organization's assertion on page [*aa*], in all material respects. . . .

Example 4: Qualified Opinion—The Service Auditor is Unable to Obtain Sufficient Appropriate Evidence

The following is an illustrative paragraph describing the basis for the qualified opinion. The paragraph would be inserted before the modified opinion paragraph. All other report paragraphs are unchanged.

Basis for qualified opinion

XYZ Service Organization states in its description 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 XYZ Service Organization's assertion on page [*aa*], in all material respects. . .

.A70

Appendix C: Illustrative Report Paragraphs for Service Organizations That Use a Subservice Organization

Following are modifications of the illustrative type 2 report in example 1 of appendix A 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 of its system for processing user entities' transactions [*or identification of the function performed by the system*] throughout the period [*date*] to [*date*] (description) 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 of ~~its~~ ***their*** [*type or name of*] system for processing user entities' transactions [*or identification of the function performed by the system*] throughout the period [*date*] to [*date*] (description) 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 user entities, as well as relevant control objectives and controls of ABC Subservice Organization.***

XYZ Service Organization's responsibilities

On page XX of the description, XYZ Service Organization ***and ABC Subservice Organization*** ~~has~~ ***have*** provided ~~an~~ ***their*** assertion***s*** about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. XYZ Service Organization ***and ABC Subservice Organization are*** ~~is~~ responsible for preparing the description and assertion***s***, including the completeness, accuracy, and method of presentation of the description and assertion***s***, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria,

and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Inherent limitations

Because of their nature, controls at a service organization ***or subservice organization*** may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or any conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization ***or subservice organization*** may become ineffective or fail.

Opinion

In our opinion, in all material respects, based on the criteria specified in XYZ Service Organization**'s and ABC Subservice Organization's** assertions on page [*aa*],

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 user entities [or identification of the function performed by the service organization's system]*** that ***were*** ~~was~~ designed and implemented throughout the period [*date*] to [*date*].

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 the control objectives would be achieved if the controls operated effectively throughout the period [*date*] to [*date*].

c. the controls ***of XYZ Service Organization and ABC Subservice 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.

.A71

Exhibit A: Illustrative Assertions by Management of a Service Organization

The assertion by management of the service organization may be included in management's description of the service organization's system or may be attached to the description. The following illustrative assertions are intended for assertions that are included in the description.

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

Example 1: Assertion by Management of a Service Organization for a Type 2 Report

XYZ Service Organization's Assertion

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

a. the description fairly presents the [*type or name of*] system made available to user entities of the system during some or all of the period [*date*] to [*date*] for processing their transactions [*or identification of the function performed by the system*]. The criteria we used in making this assertion were that the description

i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including

(1) the classes of transactions processed.

(2) 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 user entities of the system.

(3) 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 presented to user entities of the system.

(4) how the system captures and addresses significant events and conditions, other than transactions.

(5) the process used to prepare reports or other information provided to user entities' of the system.

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

(7) 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 user entities of the system.

ii. does not omit or distort information relevant to the scope of the [*type or name of*] system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the [*type or name of*] system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.

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

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;

ii. the controls identified in the description 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

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

Example 2: Assertion by Management of a Service Organization for a Type 1 Report

XYZ Service Organization's Assertion

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

a. the description fairly presents the [*type or name of*] system made available to user entities of the system as of [*date*] for processing their transactions [*or identification of the function performed by the system*]. The criteria we used in making this assertion were that the description

i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including

(1) the classes of transactions processed.

(2) 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 user entities of the system.

(3) 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 user entities of the system.

(4) how the system captures and addresses significant events and conditions, other than transactions.

(5) the process used to prepare reports or other information provided to user entities of the system.

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

(7) 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 user entities of the system.

ii. does not omit or distort information relevant to the scope of the [*type or name of*] system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the [*type or name of*] system that each individual user entity 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 description were suitably designed as of [*date*] to achieve those control objectives. The criteria we used in making this assertion were that

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization.

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

.A72

Exhibit B: Comparison of Requirements of Section 801, *Reporting On Controls at a Service Organization*, With Requirements of International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organization*

This analysis was prepared by the AICPA Audit and Attest Standards staff to highlight substantive differences between section 801, *Reporting on Controls at a Service Organization*, and International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*, and to explain the rationale for those differences. This analysis is not authoritative and is prepared for informational purposes only.

1. Intentional Acts by Service Organization Personnel

Paragraph .26 of this section requires the service auditor to investigate the nature and cause of any deviations identified, as does paragraph 28 of ISAE 3402. Paragraph .27 of this section indicates that if the service auditor becomes aware that the deviations resulted from intentional acts by service organization personnel, the service auditor should assess the risk that the description of the service organization's system is not fairly presented and that the controls are not suitably designed or operating effectively. The ISAE does not contain the requirement included in paragraph .27 of this section. The Auditing Standards Board (ASB) believes that information about intentional acts affects the nature, timing, and extent of the service auditor's procedures. Therefore, paragraph .27 provides follow-up action for the service auditor when he or she obtains information about intentional acts as a result of performing the procedures in paragraph .26 of this section.

Paragraph .36(c)(ii) of this section, which is not included in ISAE 3402, also requires the service auditor to request written representations from management that it has disclosed to the service auditor knowledge of any actual, suspected, or alleged intentional acts by management or the service organization's employees, of which it is aware, that could adversely affect the fairness of the presentation of management's description of the service organization's system or the completeness or achievement of the control objectives stated in the description.

2. Anomalies

Paragraph 29 of ISAE 3402 contains a requirement that enables a service auditor to conclude that a deviation identified in tests of controls involving sampling is not representative of the population from which the sample was drawn. This section does not include this requirement because of concerns about use of terms such as, "in the extremely rare circumstances" and "a high degree of certainty." These terms are not used in U.S professional standards and the ASB believes their introduction in this section could have unintended consequences. The ASB also believes that the deletion of this requirement will enhance examination quality because deviations identified by the service auditor in tests of controls involving sampling will be treated in the same manner as any other deviation identified by the practitioner, rather than as an anomaly.

3. Direct Assistance

Paragraph .35 of this section requires the service auditor to adapt and apply the requirements in paragraph .27 of AU section 322, *The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements*, when the service auditor uses members of the service organization's internal audit function to provide direct assistance. Because AU section 322 provides for an auditor to use the work of the internal audit function in a direct assistance capacity, paragraph .35 of this section also provides for this. The International Standards on Auditing and the ISAEs do not provide for use of the internal audit function for direct assistance.

4. Subsequent Events

With respect to events that occur subsequent to the period covered by the description of the service organization's system up to the date of the service auditor's report, paragraph .42 of this section requires the service auditor to disclose in the service auditor's report, if not disclosed by management in its description, any event that is of such a nature and significance that its disclosure is necessary to prevent users of a type 1 or type 2 report from being misled. The ASB believes that information about such events could be important to user entities and their auditors. ISAE 3402 limits the types of subsequent events that would need to be disclosed in the service auditor's report to those that could have a significant effect on the service auditor's report.

Paragraph .43 of this section requires the service auditor to adapt and apply the guidance in AU section 561, *Subsequent Discovery of Facts Existing at the Date of the Auditor's Report*, if, after the release of the service auditor's report, the service auditor becomes aware of conditions that existed at the report date that might have affected management's assertion and the service auditor's report had the service auditor been aware of them. The ISAE does not include a similar requirement. The ASB believes that, by analogy, AU section 561 provides needed guidance to a service auditor by presenting the various circumstances that could occur during the subsequent events period and the actions a service auditor should take.

5. Statement Restricting Use of the Service Auditor's Report

This section requires the service auditor's report to include a statement restricting the use of the report to management of the service organization, user entities of the service organization's system, and user auditors. The ASB believes that the unambiguous language in the restricted use statement prevents misunderstanding regarding who the report is intended for. Paragraphs .A61–.A62 of this section explain the reasons for restricting the use of the report. ISAE 3402 requires the service auditor's report to include a statement indicating that the report is intended only for user entities and their auditors, However, the ISAE does not require the inclusion of a statement restricting the use of the report to specified parties, although it does not prohibit the inclusion of restricted use language in the report.

6. Documentation Completion

Paragraph 50 of the ISAE requires the service auditor to assemble the documentation in an engagement file and complete the administrative process of assembling the final engagement file on a timely basis after the date of the service auditor's assurance report. Paragraph .49 of this section also requires the service auditor to assemble the engagement documentation in an engagement

file and complete the administrative process of assembling the final engagement file on a timely basis, but also indicates that a timely basis is no later than 60 days following the service auditor's report release date. The ASB made this change to parallel the definition of *documentation completion date* in paragraph .27 of AU section 339, *Audit Documentation*.

7. Engagement Acceptance and Continuance

Paragraph .09 of this section establishes conditions for the acceptance and continuance of an engagement to report on controls at a service organization. One of the conditions is that management acknowledge and accept responsibility for providing the service auditor with written representations at the conclusion of the engagement. ISAE 3402 does not include this requirement as a condition of engagement acceptance and continuance.

8. Disclaimer of Opinion

If management does not provide the service auditor with certain written representations, paragraph 40 of ISAE 3402 requires the service auditor, after discussing the matter with management, to disclaim an opinion. In the same circumstances, paragraph .39 of this section requires the service auditor to take appropriate action, which may include disclaiming an opinion or withdrawing from the engagement.

Paragraphs .56–.57 of this section contain certain incremental requirements when the service auditor plans to disclaim an opinion.

9. Elements of the Section 801 Report That Are Not Required in the ISAE 3402 Report

Paragraphs .52–.53 of this section contain certain requirements regarding the content of the service auditor's report, which are incremental to those in ISAE 3402. These incremental requirements are included in paragraphs .52(c)(iii); .52(e)(iv); .52(i); and .52(k) for type 2 reports, and in paragraphs .53(c)(iii); .53(e)(iv); .53(j); and .53(k) for type 1 reports.