FAQs — New Service Organization Standards and Implementation Guidance

During the past two years several significant changes have occurred in audit and attest standards for reporting on controls at service organizations. In April 2010, the Auditing Standards Board (ASB) issued Statement on Standards for Attestation Engagements (SSAE) No. 16, *Reporting on Controls at a Service Organization* (AT sec. 801), which replaces the guidance for service auditors reporting on a service organization's controls relevant to user entities' internal control over financial reporting (ICFR) in Statement on Auditing Standards (SAS) No. 70, *Service Organizations* (AU sec 324),. SSAE 16 is effective for service auditors' reports for periods ending on or after June 15, 2011. Reports issued under SSAE No 16 provide audit evidence to CPAs auditing the financial statements of entities that use a service organization. In SSAE No. 16, an entity that performs a specialized task or function for other entities is known as a *service organization* and an entity that outsources a task or function to a service organization is known as a *user entity*.

Prior to the issuance of SSAE No. 16, the guidance for service auditors reporting on controls at a service organization and for user auditors auditing the financial statements of user entities was contained in a section of the auditing standards titled, "Service Organizations" (AU sec. 324). That guidance originated in a SAS issued in April 1992 that was numbered 70. Since then, reports on controls at a service organization have colloquially been called "SAS 70 reports."

The SSAEs (which are commonly called the attest standards) enable a practitioner to report on subject matter other than financial statements, for example, the design and operating effectiveness of a service organization's controls relevant to user entities' ICFR. AT section 101, *Attest Engagements*, provides a framework that enables practitioners to develop engagements and report on subject matter other than financial statements.

A CPA may be engaged to examine and report on controls at a service organization relevant to subject matter other than user entities' ICFR. An example of such an engagement is a report on controls over the privacy of information processed by a service organization for user entities. The appropriate attestation standard for reporting on controls at a service organization depends on the subject matter of the controls that the service auditor is reporting on.

In the past some CPAs have used SAS No. 70 to report on controls at a service organization relevant to subject matter other than user entities' ICFR. SAS No. 70 was never intended for such reporting and neither is SSAE No. 16. Paragraph 2 of SSAE No. 16 clarifies that SSAE No. 16 should not be used for that purpose and also states that SSAE No. 16 may be helpful to practitioners in developing and performing such engagements under AT section 101. The AICPA has developed a guide to assist practitioners in performing and reporting on an examination of controls at a service organization relevant to subject matter other than user entities' ICFR, specifically, an examination of a service organization's controls relevant to the security, availability, or processing integrity of a system or the confidentiality, or privacy of the information processed by the system. To make practitioners aware of the various professional standards and guides available to them for examining and reporting on controls at a service organization and to help practitioners select the appropriate standard or guide for a particular engagement, the AICPA has introduced the term *SERVICE ORGANIZATION CONTROL REPORTS*^SM which is abbreviated as SOC reports. The following are the designations for the three engagements included in the SOC report series and the source of the guidance for performing and reporting on them:

- SOC 1: SSAE No. 16, *Reporting on Controls at a Service Organization* (product no. 023035),**^New** and the AICPA Guide *Service Organizations*: *Applying SSAE No. 16*, Reporting on Controls at a Service Organization (product no.0127910) **^New**
- SOC 2: AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (product no.0128210) **^New** and AT section 101, *Attest Engagements*
- SOC 3: TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) and AT section 101, *Attest Engagements*

An example of a SOC 1^SM engagement is an examination of controls at a service organization that processes medical claims for health insurance companies. Participants in health insurance plans submit their claims to the claims processor which processes the claims for the health insurers. The claims processor provides the health insurers with claims data such as the total cost of claims paid during a period. The insurers use that data to record their claims expense and the related liability. That information flows through to the insurers' financial statements. Even though the information is generated by the claims processor, the health insurer is still responsible for the accuracy of that information because it is included in its financial statements. The auditor of a user entity's financial statements (user auditor) has the same responsibility for auditing that information as he or she does for auditing other financial statement information.

The same claims processing service organization may also be the subject of a SOC 2^SM engagement, for example, an examination of its controls over the privacy of the information it processes for user entities. Participants in health insurance plans whose claims are being processed by a claims processor expect the information in their medical claims to remain private. Regulatory requirements such the Health Insurance Portability and Accountability Act of 1996 may require health insurers to maintain the privacy of the information included in such claims, including the privacy of that information while it is at the claims processor. To address these requirements, management of the health insurer may ask the claims processor for a CPA's report on the effectiveness of its controls over the privacy of the information it processes for user entities (a SOC 2^SM report).

In both a SOC 1^SM and a SOC 2^SM engagement, the practitioner has the option of providing either a *type 1* or a *type 2 report*. In both reports the service organization prepares a description of its system. In a type 1 report, the service auditor expresses an opinion on whether the description is fairly presented (that is, does it describe what actually exists) and whether the controls included in the description are suitability designed. Controls that are suitably designed *are able* to achieve the related control objectives or criteria if they operate effectively. In a type 2 report, the service auditor's report contains the same opinions that are included in a type 1 report but also includes an opinion on whether the controls were operating effectively. Controls that are operating effectively *do* achieve the control objectives they were intended to achieve. SOC 1^{SM} and SOC 2^{SM} reports are both examination reports, which means the practitioner obtains a high level of assurance.

In April 2010, the AICPA developed an initial version of "FAQs--New Service Organization Standards and Implementation Guidance" to assist CPAs in implementing SSAE No. 16. In response to additional practice questions received, the AICPA has revised the FAQs to respond to these questions and to reflect the issuance of the SOC 1^{SM} and SOC 2^{SM} guides.

Q1. — Why was the guidance for service auditors reporting on a service organization's controls relevant to user entities' ICFR moved from the SASs (auditing standards) to the SSAEs (attestation standards)?

A1. —The SASs primarily provide guidance on reporting on an audit of financial statements, whereas the SSAEs primarily provide guidance on reporting on other subject matter. In a service auditor's engagement under SSAE No. 16, and also under SAS No. 70, the practitioner reports on a service organization's description of its system and on the service organization's controls relevant to user entities' ICFR. Because an examination of a description of a system and controls is not an audit of financial statements, the Auditing Standards Board (ASB) concluded that the new standard should be placed in the attestation standards, along with SSAE No. 15, *An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements* (AICPA, *Professional Standards*, AT sec. 501)*,* in which a CPA reports on an entity's own controls over financial reporting. SSAE No. 16 is a product of the ASB's project to clarify its standards and to converge with standards of the International Auditing and Assurance Standards Board (IAASB). The IAASB's standard for service auditors, International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization,* is included in its assurance standards (the equivalent of the attestation standards). Accordingly, the guidance for service auditors was moved to the attestation standards.

Q2. — Have significant changes been made to SSAE No. 16 that will affect service auditors' engagements?

A2. —The following are the three major changes introduced by SSAE No. 16.

1. Management of the service organization will now be required to provide the service auditor with a written assertion about the fairness of the presentation of management's description of the service organization's system, the suitability of the design of the controls included in the description and, in a type 2 engagement, the operating effectiveness of those controls. That assertion will either be attached to or included in the service organization's description of its system;

2. In a type 2 engagement, the description of the service organization's system and the service auditor's opinion on the description will cover a period (the same period as the period covered by the service auditor's tests of the operating effectiveness of controls). In SAS No. 70, the description of the service organization's system in a type 2 report was as of a specified date, rather than for a period.

3. The service auditor is required to identify, in the description of tests of controls, any tests of controls performed by the internal audit function (other than those performed in a direct assistance capacity) and the service auditor's procedures with respect to that work. Tests of controls are procedures designed to evaluate the operating effectiveness of controls in achieving the control objectives stated in management's description of the service organization's system.

Q3. — Will the guidance for user auditors change, and will it remain in the auditing standards?

A3. — The guidance for user auditors, currently in AU section 324 of the SASs, will be unchanged until the new SAS for user auditors, which has been approved by the ASB, becomes effective. The new SAS does not contain any significant changes for user auditors. However, the ASB believes that because the new SAS is written in clarity format, it will be easier for user auditors to use and, thereby, meet their responsibilities. The new guidance for user auditors will remain in the SASs.

Q4. — When will SSAE No. 16 and the new SAS for user auditors become effective?

A4. — SSAE No. 16 is effective for service auditor's reports for periods ending on or after June 15, 2011, with earlier implementation permitted. This is the same effective date as the effective date of the IAASB's standard for service auditors. The new clarified SAS for user auditors, *Audit Considerations Relating to an Entity Using a Service Organization*, will have the same effective date as the other ASB clarified SASs.

Q5. —After SSAE No. 16 becomes effective and before the new clarified SAS for user auditors becomes effective, will the guidance for service auditors that is currently in AU section 324 be deleted?

A5. — No. The guidance for service auditors and user auditors currently in AU section 324 is so intertwined that if the guidance for service auditors were deleted, the guidance for user auditors would not be meaningful. During the interim period before the new SAS for user auditors becomes effective, a notation will be placed at the beginning of AU section 324 informing readers that the guidance for service auditors has been superseded by SSAE No. 16. The guidance for user auditors can be gleaned without deleting the guidance for service auditors.

Q6. — Should service organizations use SOC 1^{SM} reports to market their services to potential customers?

A6. — No. The nature of the services performed at a service organization, how they are performed, and the controls over those services differ for each service organization. A service auditor's report provides useful information only to an entity that actually uses those services and needs that information to make decisions about its own ICFR. As a result, use of a SOC 1 ^{SM} report (as with a SAS No. 70 report) is restricted to management of the service organization, user entities that are customers of the service organization, and user auditors. A SOC 1^{SM} report is not intended to be used as a marketing or sales tool by the client.

Q7. — Will entities now become "SSAE 16 certified"?

A7. —No. A popular misconception about SAS No. 70 is that a service organization becomes "certified" as SAS No. 70 compliant after undergoing a type 1 or type 2 service auditor's engagement. No such certification exists under SAS No. 70 nor does it exist under SSAE No. 16. An SSAE 16 report (as with a SAS No. 70 report) is primarily an auditor-to-auditor communication, the purpose of which is to provide user auditors with information about controls at a service organization that are relevant to the user entities' ICFR.

Q8. — *What does SOC stand for and how will the term be used? Are SOC 1^{SM} and SOC 2^{SM} professional standards?*

A8. — SOC stands for "service organization controls," as in *service organization controls report* or *service organization controls engagement*. The term *SOC* is part of the AICPA's branding efforts to better communicate the engagement and reporting options available to CPAs when reporting on controls at a service organization. SSAE No. 16 is the official standard that establishes the requirements and guidance for performing a SOC 1^{SM} engagement. AT section 101, *Attest Engagements*, is the official standard for SOC 2^{SM} and SOC 3^{SM} engagements. The SOC 1^{SM} and SOC 2^{SM} guides are authoritative guides that have been cleared by the AICPA's ASB. AT section 50, *SSAE Hierarchy*, classifies attestation guidance included in an AICPA guide as an interpretive publication and indicates that a practitioner should be aware of and consider interpretive publications applicable to his or her examination. If a practitioner does not apply the attestation guidance included in an applicable interpretive publication, the practitioner should be prepared to explain how he or she complied with the SSAE provisions addressed by such attestation guidance.

Q9. — *Now that SSAE No.16 has been issued, what is the appropriate manner to refer to reports previously issued under SAS No. 70,* Service Organizations*? Should they be referred to as SOC 1* ^{SM} *reports?*

A9. — They will most likely be referred to as SSAE 16 reports or SOC 1 ^{SM} reports. One of the advantages of using the term SOC is that it is a one syllable word that is easy to say; whereas, the term SSAE is a 4 syllable word that may be more difficult to remember and say.

Q10. — Has the existing AICPA Guide *Service Organizations: Applying SAS No. 70, as Amended* (commonly known as the SAS 70 guide) been rewritten to reflect SSAE No. 16?

A10. — Yes. The existing guide has been overhauled and rewritten to reflect the requirements and guidance in SSAE No. 16. Both the electronic and print versions of the revised guide are available at the AICPA store http://www.cpa2biz.com/

Q11. — May SSAE No. 16 be used for reporting on controls over subject matter other than user entities' ICFR? If not, what standard should be used for such engagements?

A11. — No. SSAE No. 16 does not apply to examinations of controls over subject matter other than user entities' ICFR, and neither does SAS No. 70. Such engagements would be performed under AT section 101 of the attestation standards. The new AICPA guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (SOC 2 ^{SM} guide) uses AT section 101 as a framework for reporting on the effectiveness of controls relevant to security, availability, processing integrity, confidentiality, or privacy.

The increasing use of *cloud computing* companies (which provide user entities with on-demand network access to a shared pool of computing resources, such as networks, servers, storage, applications, and services) has created an increasing demand for CPAs to report on nonfinancial reporting controls implemented by cloud computing service providers.

Q12. — *How can I purchase the SOC 2 ^{SM} guide?*

A12. — Both the electronic and print versions of the SOC 2 ^{SM} guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* can be purchased online at the AICPA store http://www.cpa2biz.com/

Q13. — *Does SSAE No. 16 require that a type 2 report cover a minimum period? If so, does that period differ from the minimum period in SAS No. 70?*

A13. — Both SSAE No. 16 and SAS No. 70 discourage the service auditor from performing a type 2 engagement that covers a period of less than six months. Paragraph A42 of SSAE No. 16 indicates that a type 2 report that covers a period of less than six months is unlikely to be useful to user entities and their auditors. However, there are certain limited circumstances, such as the following, in which a type 2 report covering less than six months may be considered.

- The service auditor was engaged close to the date by which the report on controls is to be issued, precluding the service auditor from testing the operating effectiveness of controls 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.

Q14. — *Does the SOC 2 ^{SM} guide require that a type 2 report cover a specified minimum period?*

A14. — The SOC 2 ^{SM} guide does not prescribe a minimum period of coverage for a SOC 2 ^{SM} report. However paragraph 2.09 of the SOC 2 ^{SM} guide states that one of the relevant factors to consider when determining whether to accept or continue a SOC 2 ^{SM} engagement is the period covered by the report. The guide presents an example of a service organization that wishes to engage a service auditor to perform a type 2 engagement for a period of less than two months. It further states that in those circumstances, the service auditor should consider whether a report covering that period will be useful to users of the report, particularly if many of the controls related to the applicable trust services criteria are performed on a monthly or quarterly basis. The practitioner would need to use professional judgment in determining whether the report covers a sufficient period.

Q15. — *Does SSAE No. 16 require that management's assertion accompany the service organization's description of its system?*

A15. — Yes. Paragraph 9c vii of SSAE No. 16 states that one of the conditions for engagement acceptance or continuance is that management provide a written assertion that will be included in or attached to management's description of the service organization's system.

Q16. — *In a SOC 2^{SM} engagement, does management's assertion need to accompany the service organization's description of its system?*

A16. — Paragraph 2.13 (b) of the SOC 2^{SM} guide states, in part, that a service auditor ordinarily should accept or continue an engagement to report on controls at a service organization only if management of the service organization acknowledges and accepts responsibility for ….”providing a written assertion that will be attached to management's description of the service organization's system and provided to users.” The recommendation in the SOC 2^{SM} guide is that the assertion be attached to the description, rather than included in the description to avoid the impression that the practitioner is reporting on the assertion rather than on the subject matter.

Q17. — *Does SSAE No. 16 require that management's description of the service organization's system include a description of the service organization's IT control objectives and related controls? If so, does the SOC 1^{SM} guide address which IT control objectives and controls would usually be relevant to a user entity's* ICFR*?*

A17. — The definition of *service organization's system* in paragraph 7 of SSAE No. 16 indicates that the description of the service organization's system includes 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. Paragraph A11 of SSAE No.16 further clarifies that sentence by stating that “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.” Paragraph 3.65 of the SOC 1^{SM} guide indicates that if the control objectives in a service organization's description of its system only address application controls, and the proper functioning of general computer controls is necessary for the application controls to operate effectively, the service organization would be expected to include the relevant general computer controls in its description of the system as they relate to the specified control objectives. “”Appendix D “Illustrative Control Objectives for Various Types of Service *Organizations*” of the SOC 1 guide includes illustrative control objectives related to general computer controls.

Q18. — *Are there a prescribed set of control objectives for SOC 2^{SM} and SOC 3^{SM} engagements?*

.

A18. — In SOC 2^{SM} and SOC 3^{SM} engagements, the service auditor uses the criteria in TSP section 100 *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*), for evaluating and reporting on controls relevant to security, availability, processing integrity, confidentiality, or privacy. In TSP section 100, these five attributes of a system are known as *principles.* A service auditor may be engaged to report on a description of a service organization's system and the suitability of the design and operating effectiveness of controls relevant to one or more of the trust services principles The criteria in TSP section 100 that are applicable to the principle(s) being reported on are known as the *applicable trust services criteria*. Accordingly, in every SOC 2^{SM} and SOC 3^{SM} engagement that addresses the same principle(s), the criteria will be the same (the applicable trust services criteria).

Q19. — *Does the service organization's description of its system need to identify the risks that could prevent the service organization's controls relevant to user entities* ICFR *from achieving the related control objectives?*

A19. — There is no requirement in SSAE No. 16 for management to identify in its description of the service organization's system the risks related to each control objective included in the description. However, the service auditor would probably expect management to be able to discuss its consideration of risks in designing the controls to achieve the related control objectives.

Q20. — *Paragraph 14 of SSAE No. 16 indicates that management's description of a service organization's system should include aspects of the service organization's risk assessment process. What information should be included in describing the risk assessment process?*

A20. — The content of the description of the risk assessment process will vary depending on the complexity of the service organization's process. Paragraph A18 of SSAE No. 16 indicates that 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. In those circumstances nothing precludes management from including the details of its process in the description. However, because control objectives relate to the risks that controls seek to mitigate, paragraph A18 of SSAE No. 16 indicates that management's thoughtful identification of the control objectives when designing, implementing, and documenting the service organization's system may itself comprise an informal process for identifying relevant risks.

Q21. — *Paragraph 9 (c) (ii) of SSAE No. 16 states that one of the requirements for a service auditor to accept or continue a type 1 or type 2 engagement is that management acknowledge and accept responsibility for having a reasonable basis for its assertion. Paragraph A17 of SSAE No. 16 indicates that a service auditor's report on controls is not a substitute for the service organization's own processes that provide a reasonable basis for its* assertion. *How does the service auditor determine whether management has a reasonable basis for its assertion?*

A21. — SSAE No. 16 indirectly describes how the service auditor makes this determination. First, paragraph14 (a) (vii) of SSAE No. 16 indicates, in part, that the service organization's description of its system should include the service organization's monitoring activities. Because a service auditor is required to determine whether the description is fairly stated, in doing so the service auditor would determine whether the section of the description that describes monitoring controls is fairly stated. Second, paragraph A17 of SSAE No. 16 defines the term *monitoring of controls* and indicates that management's monitoring activities may provide evidence of the design and operating effectiveness of controls in support of management's assertion.

Note: Similar guidance for SOC 2 ^{SM} engagements is included in Appendix A, "Information for Management of a Subservice Organization," of the SOC 2^{SM} guide, under the subheading "Providing a Written Assertion."

Q22. — *Where can I find an example of management's assertion for an SSAE 16 engagement?*

A22. — Exhibit A of SSAE No. 16 contains illustrative management assertions for type 1 and type 2 engagements. Appendix B of the SOC 1 ^{SM} guide provides illustrative assertions for type 2 engagements.

Note: Appendix C of the SOC 2 ^{SM} guide contains illustrative assertions by management of a service organization for type 2 SOC 2 ^{SM} engagements.

Q23. *— May a service auditor provide a service organization with a bridge letter under SSAE No. 16 (a letter from a service auditor stating that nothing has changed since the last type 1 or type 2 report)?*

A23. — Neither SAS No. 70 nor SSAE No. 16 address such communications. A service organization may choose to issue a letter that describes updates or changes in its controls since the previous type 1 or type 2 report. However, there are no provisions in SSAE No. 16 for service auditors to report on such a letter. Service auditors and user auditors are cautioned against providing assurance on or inferring assurance from such letters, respectively.

Q24. — *Other than the addition of management's assertion and the changes to the auditor's report, will the format of the SSAE No. 16 report package look the same as it did under SAS No. 70?*

A24. — Except for the addition of management's assertion, SSAE No. 16 continues to have the same report package as it did under SAS No. 70. That package consists of the following components:

- Section 1: The service auditor's report, that is, the letter from the service auditor
- Section 2: Management of the service organization's written assertion
- Section 3: Management's description of the service organization's system
- Section 4: The service auditor's description of' tests of the operating effectiveness of controls and results of those tests (type 2 reports only)
- Section 5: Optional other information provided by management of the service organization

Q25. — *If an auditor performs a SOC 1 ^{SM} engagement for a service organization and also audits that service organization's financial statements, in auditing the service organization's financial statements, will the auditor still need to obtain a sufficient understanding of the service organization and its environment, including its internal control, sufficient to assess the risks of material misstatement and design audit procedures?*

A25 — In an SSAE No. 16 engagement the service auditor focuses on *controls* at the service organization that are relevant to the ***user entities'*** ICFR, rather than controls at the service organization relevant to the ***service organization's*** ICFR. Some of the controls included in the service organization's description of its system may be relevant to the service organization's own ICFR, but because the controls evaluated and tested for the purposes of a SOC 1 ^{SM} engagement are not necessarily controls that affect the service organization's financial reporting, the auditor of the service organization's financial statements would still need to obtain an understanding of the service organization's internal control for the purpose of the audit.

Q26. — Who *determines whether a SOC 1^{SM}, SOC2^{SM}, or SOC 3^{SM} engagement should be performed—the service auditor or management of the service organization?*

A26. SOC 1^{SM} engagements address a service organization's controls relevant to user entities' ICFR, whereas SOC 2^{SM} and SOC 3^{SM} engagements address a service organization's controls relevant to the security, availability, or processing integrity of a system or the confidentiality or privacy of the information the system processes. In SOC 2^{SM} and SOC 3^{SM} engagements, the service auditor uses the criteria in TSP section 100 for evaluating and reporting on controls relevant to the security, availability, or processing integrity of a system, or the confidentiality or privacy of the information processed by the system. In TSP section 100, these five attributes of a system are known as *principles.* A service auditor may be engaged to report on a description of a service organization's system and the suitability of the design and operating effectiveness of controls relevant to one or more of the trust services principles The criteria in TSP section 100 that are applicable to the principle(s) being reported on are known as the *applicable trust services criteria*.

If management of the service organization is not knowledgeable about the differences among these three engagements, the service auditor may assist management in obtaining that understanding and selecting the appropriate engagement. Determining which engagement is appropriate depends on the subject matter addressed by the controls and the risk management and governance needs of the user entities, and often involves discussion with the user entities regarding their needs.

Q27. — *Does SSAE No. 16 define or suggest specific control objectives for service organizations that provide services that are likely to be relevant to user entities' ICFR or does the service organization continue to define its own control objectives and controls, as is the case in SAS No. 70?*.

A27. — SSAE No. 16 does not define or suggest specific control objectives for service organizations that provide services that are likely to be relevant to user entities' ICFR. In a SOC 1^{SM} engagement, the service auditor evaluates whether the service organization's controls were suitably designed or operating effectively by determining whether the control objectives specified by management of the service organization were achieved. SSAE No. 16 requires that the control objectives be reasonable in the circumstances. Although most service organizations that provide similar services will have similar control objectives, in order for control objectives to be reasonable in the circumstances, they should reflect features of the particular service organization such as the nature of the services provided, the industry in which the user entities operate, and the needs of the user entities. Accordingly, in SOC 1^{SM} engagements, not all service organizations will have the same control objectives. However, certain control objectives are typical for certain types of service organizations. To assist service auditors, Appendix D of the AICPA Guide *Service Organizations: Applying SSAE No 16*, Reporting on Controls at a Service Organization, contains illustrative control objectives for various types of service organizations, including application service providers, claims processors, credit card payment processors investment managers, payroll processors and transfer agents. The appendix also includes illustrative general control objectives which may be applicable to any service organization.

Q28. — *In an inclusive SOC 1^{SM} engagement, is the service auditor required to determine whether management of the subservice organization has a reasonable basis for its assertion?*

A28. — As stated in question 21 of these FAQs, paragraph 9 (c) (ii) of SSAE No. 16 states that one of the requirements for a service auditor to accept or continue a type 1 or type 2 engagement is that management acknowledge and accept responsibility for having a reasonable basis for its assertion. Paragraph A7 of SSAE No. 16 states that when the inclusive method is used, the requirements of SSAE No. 16 also apply to the services provided by the subservice organization, including the requirement to acknowledge and accept responsibility for the matters in paragraph 9(c)(i)–(vii) of SSAE No. 16, as they relate to the subservice organization. Paragraph 9(c)(vii) requires a service organization to provide a written assertion; therefore; a subservice organization also would be required to provide a written assertion and have a reasonable basis for its assertion.

Note: Similar guidance on this topic for a SOC 2 ^{SM} engagement is included in paragraphs 2.13 (b-c) and 2.15 of the SOC 2 ^{SM} guide.

Q29. — *At what point in a SOC 1 ^{SM} or SOC 2 ^{SM} engagement should management provide the service auditor with its written assertion?*

A29. — Management may provide its written assertion to the service auditor at any time after the end of the period covered by the service auditor's type 2 report, and for a type 1 report, at any time after the as of date of the type 1 report. The date of the service auditor's report should be no earlier than the date on which management provides its written assertion.

Q30. — *In a SOC 1 ^{SM} engagement, if the service auditor identifies deviations in the subject matter (that is, the fairness of the presentation of the description, the suitability of the design of the controls, and the operating effectiveness of the controls) and qualifies the report because of these deviations, does management need to revise its assertion to reflect these deviations?*

A30. — If management of the service organization agrees with the service auditor's findings regarding the deviations, management would be expected to revise its assertion to reflect the deviations identified in the service auditor's report. If management does not revise its assertion, the service auditor should add an explanatory paragraph to the report indicating that the deficiencies identified in the service auditor's report have not been identified in management's assertion.

Note: Similar guidance for a SOC 2 ^{SM} engagement is included in paragraph 3.105 of the SOC 2 ^{SM} guide.

Q31. — *How is the general market being educated about SOC reporting?*

A31. — The AICPA has employed a broad strategy to promote and provide information about SOC reporting. The AICPA recognizes that there are diverse perspectives and needs in the marketplace across the spectrum of user entities, user auditors, service organizations, and service auditors. In early 2010, the AICPA developed a set of frequently asked questions related to service organization control reporting entitled "FAQs — New Service Organization Standards and Implementation Guidance." This set of FAQs updates and revises the original set of FAQs to reflect the issuance of the SOC 2 ^{SM} guide. The AICPA has conducted several webcasts on the topic of service organization control reporting and additional webcasts are anticipated. The *Service Organization Control Reports* page on the AICPA website is also a good source of information about SOC reporting. An introductory SOC brochure can be downloaded from that site.

Q32. — *Will there be a SOC seal that can be displayed on a service organization's website indicating that the service organization has undergone a SOC1, SOC 2, or SOC 3 engagement?*

A32. — A seal is available only for SOC 3 ^{SM} engagements. A SOC 3 SysTrust for Service Organization Seal (seal) can be issued and displayed on a service organization's website. All practitioners who wish to provide this registered seal must be licensed by the CICA. Typically the seal is linked to the report issued by the practitioner. For more information on licensure, go to www.webtrust.org. It is important to note that a practitioner can perform a SOC 3 engagement and issue a SOC 3 report without issuing a SOC 3 seal. In such cases the practitioner does not need to be licensed by the CICA. The license is only for the issuance of a seal.

In addition, SOC logos are available for (a) CPAs to market and promote SOC services and (b) service organizations that have undergone a SOC 1 ^{SM}, SOC 2 ^{SM} or SOC 3 ^{SM} engagement within the prior 12 months. These logos are designed to make the public aware of these SOC services and do not offer or represent assurance that an organization obtained an unqualified (or clean) opinion. Click here for more information about SOC logos*.*

Q33. — *Is SOC 2 a professional standard?*

A33. — No. The term *SOC 2* merely refers to the subject matter of the engagement the service auditor performs (reporting on a service organization's controls relevant to security, availability, processing integrity, confidentiality, or privacy), using the performance and reporting requirements in AT section 101 and the criteria in TSP section 100. To help practitioners better understand how to apply AT section 101 in this engagement, the AICPA has developed the SOC 2 ^{SM} guide. The SOC 2 ^{SM} guide is an interpretation and application of AT section 101 which is the official standard for a SOC 2 ^{SM} engagement. Paragraph 6 of AT section 50, *Defining Professional Requirements in Statements on Standards for Attestation Engagements,* states, in part, "If a practitioner does not apply the attestation guidance included in an applicable attestation interpretation, the practitioner should be prepared to explain how he or she complied with the SSAE provisions addressed by such attestation guidance. The SOC 2 ^{SM} guide is an authoritative guide and, therefore, was cleared by the AICPA's ASB.

Q34. — *SSAE No. 16 requires management of a subservice organization to provide a written assertion when the inclusive method is used. SSAE No. 16 contains illustrative management assertions for management of a service organization. Is an illustrative assertion for management of a subservice organization available?*

A34. — Yes. Example 2 of Appendix B in the SOC 1 ^{SM} guide contains an illustrative assertion for an inclusive engagement.

Q35. — *The SOC 2 ^{SM} guide contains illustrative management assertions for management of a service organization. Is an illustrative assertion for management of a subservice organization available in the SOC 2 ^{SM} guide?*

A35. — No. However, the illustrative assertions in Appendix C of the SOC 2 ^{SM} guide can be used to construct the subservice organization's assertion. The requirement for an assertion by management of a subservice organization when the inclusive method is used is covered in paragraphs 2.13 - 2.15 of the SOC 2^{SM} guide.

Q36. — *When using the inclusive method, if management of a subservice organization will not provide a written assertion, what should the service auditor do?*

A36. — Paragraph A8 of SSAE No. 16 indicates that the subservice organization's refusal to provide the service auditor with a written assertion precludes the service auditor from using the inclusive method. However, the service auditor may instead use the carve-out method.

Note: For SOC 2^{SM} engagements, refer to similar guidance in paragraph 2.15 of the SOC 2^{SM} Guide.

Q37. — *SSAE No. 16 is based on the International Auditing and Assurance Standards Board's (IAASB) International Standard on Assurance Engagements (ISAE) 3402,* Assurance Reports on Controls at a Service Organization*. May a U.S. CPA perform and report under ISAE 3402?*

A37. — Unless they also meet the international requirements, a U.S. CPA could not issue a standalone ISAE 3402 report. However, a U.S. CPA could issue a report indicating that the examination was performed in accordance with AICPA and the IAASB standards, assuming that the requirements of both standards have been met.

Q38. — *Under what circumstances would a service organization request that a service auditor report under both AICPA and IAASB standards?*

A38. — Engagements performed under SSAE No. 16 and ISAE 3402 are very similar. (Exhibit B of SSAE No. 16 identifies the differences between SSAE No. 16 and ISAE 3402.) For service organizations with international operations or international clients, there may be a benefit to obtaining a report indicating that the examination was performed in accordance with AICPA and IAASB standards. An engagement that is performed in accordance with both sets of standards would not be expected to involve a substantially different examination scope or approach than an individual SSAE No. 16 engagement would.

Q39. — *If a service organization in the U.S. provides services to a user entity in Europe, may the practitioner perform the examination under SSAE No. 16 or should it be performed under ISAE 3402?*

A39. — The applicability of SSAE No. 16 is not limited to user entities located in the U.S. Accordingly, a user entity in Europe could be a recipient of an SSAE No. 16 report.

Q40. — *In the past, many IT service organizations provided their user entities with SAS No. 70 reports covering these services. If a service organization plans to undergo a SOC 2^{SM} or SOC 3^{SM} examination for the first time and has a fully defined set of controls and control objectives related to the IT services, does the service organization need to adopt a new set of controls to meet the applicable trust services criteria?*

A40. — The SOC 2 guide and Appendix C of TSP section 100 require the service organization to establish controls that meet all of the applicable trust services criteria. A service organization planning to undergo a SOC 2^{SM} or SOC 3^{SM} engagement for the first time may have controls in place that address all of the applicable trust services criteria. However, the service organization will need to determine whether its existing control objectives align with the applicable trust services criteria and whether its controls address all of the applicable trust services criteria. If not, it will need to implement or revise certain controls to meet all of the applicable trust services criteria.

Q41. — *In a type 1 report for a SOC 1 ^{SM} or SOC 2 ^{SM} engagement, do the controls included in management's description of the service organization's system need to be implemented?*

A41. — Yes. In order for the description of the service organization's system to be fairly presented, the controls would have to be placed in operation (implemented). (See paragraph 4.01(b) of the SOC 1 ^{SM} guide and paragraph 3.13 of the SOC 2 ^{SM} guide.)

Q42. — *Could a SOC 2 ^{SM} or SOC 3 ^{SM} engagement be used to report on compliance with other standards or authoritative requirements that are substantially similar to the applicable trust services criteria, for example, requirements in Special Publication 800-53,* Recommended Security Controls for Federal Information Systems, *issued by the National Institute of Standards and Technology (NIST) or in* Payment Card Industry (PCI) Security Standards *issued by the PCI Security Counsel?*

A42. — Yes. A service organization may request that a service auditor's report address additional subject matter that is not specifically covered by the applicable trust services criteria. An example of such subject matter is the service organization's compliance with certain criteria established by a regulator, for example, security requirements under the Health Insurance Portability and Accountability Act of 1996 or compliance with performance criteria established in a service-level agreement. Paragraph 1.38 of the SOC 2 ^{SM} guide states that in order for a service auditor to report on such additional subject matter, the service organization provides the following:

- An appropriate supplemental description of the subject matter
- A description of the criteria used to measure and present the subject matter
- If the criteria are related to controls, a description of the controls intended to meet the control-related criteria
- An assertion by management regarding the additional subject matter

Paragraph 1.39 of the SOC 2 ^{SM} guide states,

> The service auditor should perform appropriate procedures related to the additional subject matter, in accordance with AT section 101 and the relevant guidance in this guide. The service auditor's description of the scope of the work and related opinion on the subject matter should be presented in separate paragraphs of the service auditor's report. In addition, based on the agreement with the service organization, the service auditor may include additional tests performed and detailed results of those tests in a separate attachment to the report.

Q43. — *SAS No. 70 provides for type 1 and type 2 engagements. Do SSAE No. 16 and the SOC 2 guide also provide for type 1 and type 2 engagements?*

A43. — Yes.

Q44. — *Going forward, will service organizations that include control objectives relevant to user entities ICFR along with control objectives that are not relevant to user entities' ICFR in their descriptions need to request two separate reports – SOC 1 and SOC 2?*

A44. — Yes, Service organizations will now need to request separate SOC reports if the service organization would like to address control objectives relevant to user entities' ICFR and control objectives that are not relevant to user entities' ICFR. See paragraph 1.23 of the SOC 2 ^{SM} guide.

The following are other sources of information about reporting on controls at a service organization currently offered on the SOC website.

- "Service Organization Controls - Managing Risks by Obtaining a Service Auditor's Report" (SOC brochure)
- "Replacing SAS 70 - New standards for engagements involving outsourcing" *Journal of Accountancy* (August 2010)
- "Expanding Service Organization Controls Reporting" *Journal of Accountancy* (July 2011)

The AICPA gratefully appreciates the contribution and involvement of the Service Organization Control Reporting Task Force of the AICPA IT Executive Committee.

Service Organization Control Reporting Task Force
of the Information Technology Executive Committee

Dan Schroeder, *Chair*
Joseph (Jody) R. Allred
Angela Appleby
Catherine Bruder
Audrey Katcher
Curtis Stewart
Brian J.Thomas
Steve Ursillo Jr.
David C. Wood

AICPA Staff

Erin Mackler
Sr. Technical Manager, Business Reporting Assurance & Advisory Services

Janis Parthun
Sr. Technical Manager, IT Division of Specialized Communities

Judith Sherinsky
Sr. Technical Manager, Audit and Attest Standards