FAQs — New Service Organization Standards and Implementation Guidance

In April 2010 the AICPA's Auditing Standards Board (ASB) issued Statement on Standards for Attestation Engagements (SSAE) No. 16, *Reporting on Controls at a Service Organization.* The SSAEs are also known as the attestation standards; in an attestation report a CPA attests to subject matter or an assertion about something other than the fairness of the presentation of financial statements.

SSAE 16 is applicable when an entity outsources a business task or function to another entity (usually one that specializes in that task or function) and the data resulting from that task or function is incorporated in the outsourcer's financial statements. In SSAE 16 an entity that performs a specialized task or function for other entities is known as a *service organization* and an entity that outsources the task or function to a service organization is known as a *user entity*.

One example of a service organization is an entity 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 based on rules established by the insurers, for example, rules related to eligibility and the amount to be paid for each service. 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 that information is generated by the claims processor, management of the health insurers is still responsible for the accuracy of that information because it is included in their 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 has for auditing other financial statement information.

One way a user auditor may obtain evidence about the quality and accuracy of the data provided to a user entity by a service organization is to obtain a CPA's report (a service auditor's report) on controls at the service organization that affect data provided to the user entities and incorporated in the user entities' financial statements. The rationale for this approach is that controls are designed to prevent, or detect and correct, errors or misstatements. If controls at a service organization are operating effectively, errors in data provided to the user entities will be prevented, or detected and corrected, and misstatements in the user entities' financial statements will be avoided.

Prior to the issuance of SSAE 16, the guidance for service auditors reporting on controls at a service organization and for user auditors auditing the financial statements of a user entity was contained in a section of Statements on Auditing Standards (SAS) entitled "Service Organizations." 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 codification of the SASs is divided into sections and the section of the SASs in which SAS 70 was inserted is AU section 324, so sometimes the terms SAS 70 and AU section 324 are used interchangeably. SSAE 16 will be located in section 801 of the attestation standards (AT sec. 801).

SSAE 16 (and also SAS 70) enables CPAs to provide two types of service auditor's reports. In both reports the service organization must prepare a description of its system that includes, among other things, the nature of the service provided, how the service is performed, and the service organization's controls over the service and related control objectives. A service auditor may provide two types of reports. In a *type 1 report*, the service auditor expresses an opinion on

whether the description is fairly presented (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 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 operate effectively *do* achieve the control objectives they were intended to achieve. Both types of reports are examination reports which means the CPA obtains a high level of assurance.

The following are some questions and answers to help explain the changes resulting from the issuance of SSAE 16:

Q. — Why was the guidance for service auditors moved from the SASs (auditing standards) to the SSAEs (attestation standards)?

A. —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, a CPA reports on a service organization's description of its system and on the service organization's controls that are relevant to user entities' financial statements. Because an examination of a description of a system and controls is not an audit of financial statements, the ASB concluded that the new standard should be placed in the attestation standards along with SSAE 15, *An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements,* in which a CPA reports on an entity's controls over financial reporting. SSAE 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 is included in its assurance standards (the equivalent of the attestation standards). Accordingly, the guidance for service auditors was moved to the attestation standards.

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

A. — The guidance for user auditors, currently in AU section 324 of the SASs, will be unchanged until the new SAS for user auditors, already 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.

Q. — When will the new standards become effective?

A. — SSAE 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.

Q. — During the period after SSAE 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?

A. — 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 16. The guidance for user auditors can be gleaned without deleting the guidance for service auditors.

Q. — Should service organizations use an SSAE 16 service auditor's report to market their services to potential customers?

A. — 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 only addresses controls that the service organization believes would be relevant to clients of the service organization and their user auditors. Therefore, a service auditor's report provides useful information only to a user organization that actually uses those services and needs that information to make decisions about its own internal control over financial reporting. As a result, use of an SSAE 16 report (as with a SAS 70 report) is restricted to user entities that are customers of the service organization and user auditors. An SSAE 16 report is not intended to be used as a marketing or sales tool by the client.

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

A. — No! A popular misconception about SAS 70 is that a service organization becomes "certified" as SAS 70 compliant after undergoing a type 1 or type 2 service auditor's engagement. There is no such thing as being SAS 70 certified and there will be no such thing as being SSAE 16 certified. An SSAE 16 report (as with a SAS 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' financial statements.

Q. — Is the existing AICPA guide *Service Organizations* (commonly known as the SAS 70 guide), being rewritten?

A. — Yes. The existing guide is being overhauled and rewritten to reflect the requirements and guidance in SSAE 16. The revised guide is expected to be available for sale in early 2011.

Q. — May SSAE 16 be used for reporting on controls over subject matter other than financial reporting?

A. — No. SSAE 16 (as well as SAS 70) does not apply to examinations of controls over subject matter other than financial reporting. Such engagements would be performed under AT Section 101, *Attest Engagements*, of the attestation standards. For example, an entity may be required by law or regulation to maintain the privacy of the information it collects. That information may be passed on to a service provider that performs certain tasks for the user entity. Even though certain controls over privacy are implemented at a service provider, management of the user entity is not relieved of its responsibility for effective internal control over the privacy of the information the service provider processes for the user entity. In this situation, management of the service provider may engage a CPA to report on the effectiveness of its controls over privacy that are relevant to the user entities, and may provide that report to the user entities. Such an examination would be performed under AT Section 101, not SSAE 16.

Q. — Does the AICPA have any guidance on examining such nonfinancial reporting controls?

A. — In addition to revising the service organizations guide to help CPAs implement SSAE 16, the AICPA is also developing a new guide *Reporting on Controls at a Service Provider Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* that addresses reporting on a service provider's controls over subject matter other than financial reporting.

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. A special task force of the Assurance Services Executive Committee is writing a new guide that will specifically address such engagements, which are performed under AT section 101.

Q. — When will this guide be issued?

A. —It is anticipated that this guide will also be issued in early 2011. This will be an authoritative guide and therefore will be cleared by the Auditing Standards Board.

Q. — Have significant changes been made to SSAE 16 that would affect a service auditor's engagement?

A. —The two major changes are that (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 the description of the system, and about the suitability of the design and, in a type 2 engagement, the operating effectiveness of the controls. That assertion will either accompany the service auditor's report or be included in the service organization's description, and (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 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