

Background:

Since 1992, Statement on Auditing Standards (SAS) no. 70, *Service Organizations*, has been the source of the requirements and guidance for CPAs reporting on controls at service organizations and for CPAs auditing the financial statements of entities that use service organizations to accomplish tasks that may affect their financial statements. SAS no. 70 has been divided and replaced by two new standards. One is a Statement on Standards for Attestation Engagements (SSAE) also known as an attestation standard; the other is a SAS (an auditing standard). The requirements for reporting on controls at service organizations has been placed in SSAE no. 16, *Reporting on Controls at a Service Organization* (see Official Releases, page 82). The requirements for auditing the financial statements of entities that use service organizations remains in the auditing standards in a new SAS, *Audit Considerations Relating to an Entity Using a Service Organization*

Moving the requirements for CPAs reporting on controls at service organizations to the attestation standards better reflects the nature of the work being performed. 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 a service organization's controls that are relevant to user entities' internal control over financial reporting.

Because an examination of a description of a system and controls is not an audit of financial statements, the Auditing Standards Board (ASB) agreed that the new standard should be moved to the attestation standards. This decision also aligns with the ASB's effort to converge its standards with

those of the International Auditing and Assurance Standards Board (IAASB). SSAE no. 16 is based on the IAASB's assurance standard (the equivalent of

an attestation standard) for service auditors, International Standard on Assurance Engagements (ISAE) no. 3402, *Assurance Reports on Controls at a Service Organization*.

HOW TO REPORT ON CONTROLS OVER MATTERS OTHER THAN FINANCIAL REPORTING

In the past, many CPAs used SAS no. 70 to report on controls at a service organization that are unrelated to user entities' internal control over financial reporting, for example, controls over the privacy of customers' information.

However, SAS no. 70 is not applicable to examinations of controls over subject matter other than financial reporting, and neither is SSAE no. 16. There is increasing demand for reports on controls over subject matter other than financial reporting. For example, many user entities are required by law or regulation to maintain the privacy of the information they collect from customers, including the privacy of that information when it is at a service organization. To address these requirements, management of the user entity may ask the service organization for a CPA's report on the effectiveness of its controls over the privacy of the information it processes for user entities.

If a CPA is engaged to examine and issue a report on controls over subject matter other than financial reporting, such an engagement should be performed under AT section 101, Attest Engagements, of the attestation standards, but not under SSAE no. 16 (nor under SAS no. 70). The increasing use of cloud computing facilities, 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 increased demand for reports by CPAs on controls over subject matter other than financial reporting at cloud computing facilities. A special task force of the AICPA Assurance Services Executive Committee is developing a new guide *Reporting on Controls at a Service Provider Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*, that will specifically address such engagements, which are performed under AT section 101. That guide is expected to be available in early 2011.

MISCONCEPTIONS ABOUT SAS 70

A popular misunderstanding about SAS no. 70 is that a service organization becomes “SAS 70 certified” after undergoing a type 1 or type 2 engagement. However, no such certification exists nor will it exist under SSAE no. 16.

An SSAE 16 report (as with a SAS 70 report) is primarily an auditor-to-auditor communication, designed to provide user auditors with detailed information about controls at a service organization that affect the information provided to user entities. All service auditors' reports include a detailed description of the service organization's system, and a type 2 report includes a detailed description of tests of controls performed by the service auditor and the results of those tests. The user auditor reads this detailed information to determine how the service organization's system generates information and how the service organization interacts with the user entity's financial reporting system, including how the information gets incorporated into the user entity's financial statements. Such information generally is lengthy and detailed and could not be communicated via a certification.

Use of an SSAE 16 report, like a SAS 70 report, is restricted by the service auditor to only the service organization client, user entities and user auditors. Therefore, an SSAE 16 report is not a general use report and, as such, should not be used by anyone other than the specified parties named in the restricted use paragraph.

REQUIREMENTS FOR CPAS EXAMINING AND ISSUING REPORTS ON CONTROLS OVER SUBJECT MATTER OTHER THAN FINANCIAL REPORTING

The basis for these examinations are housed in AT section 101, Attest Engagements, of the attestation standards, not under SSAE no. 16 (nor under SAS no. 70). The AICPA is developing a new guide that addresses reporting on a service provider's controls over subject matter other than financial reporting.

Service Organization Controls (SOC) reports are designed to help service organizations build trust and confidence in their service delivery processes and controls through a report by an independent Certified Public Accountant. Each type of SOC report is designed to help service organizations meet specific user needs:

SOC 1 Report – Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting

SOC 2 Report— Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

SOC 3 Report— Trust Services Report for Service Organizations



SOC 1 Report

REPORT ON CONTROLS AT A SERVICE ORGANIZATION RELEVANT TO USER ENTITIES' INTERNAL CONTROL OVER FINANCIAL REPORTING

These reports, prepared in accordance with *Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization*, are specifically intended to meet the needs of the managements of user entities and the user entities' auditors, as they evaluate the effect of the controls at the service organization on the user entities' financial statement assertions. These reports are important components of user entities' evaluation of their internal controls over financial reporting for purposes of comply with laws and regulations such as the Sarbanes-Oxley Act and the user entities' auditors as they plan and perform audits of the user entities' financial statements. There are two types of reports for these engagements:

- Type 2 - report on 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 to achieve the related control objectives included in the description throughout a specified period.
- Type 1 – report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design of the controls to

achieve the related control objectives included in the description as of a specified date.

The use of these reports are restricted to the management of the service organization, user entities of the service organization and user auditors.

SOC 2 Report

Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

These reports are intended to meet the needs of a broad range of users that need to understand internal control at a service organization as it relates to security, availability, processing integrity, confidentiality and privacy. These reports are performed using the *AICPA Guide: Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (currently under development) and are intended for use by stakeholders (e.g., customers, regulators, business partners, suppliers, directors) of the service organization that have a thorough understanding of the service organization and its internal controls. These reports can form an important part of stakeholders':

- Oversight of the organization
- Vendor management program
- Internal corporate governance and risk management processes
- Regulatory oversight

Similar to a SOC 1 report there are two types of report : Type 2, report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls; and Type 1, report on management's description of a service organization's system and the suitability of the

design of controls. These reports may be restricted in use.

SOC 3 Report

Trust Services Report for Service Organizations

These reports are designed to meet the needs of users who want assurance on the controls at a service organization related to security, availability, processing integrity, confidentiality, or privacy but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report. These reports are prepared using the AICPA/Canadian Institute of Chartered Accountants (CICA) *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Because they are general use reports, SOC 3 Reports can be freely distributed or posted on a website as a seal. For more information about the SysTrust for Service Organization seal program go to www.webtrust.org.

A link to the AICPA President speaking on and explaining the new standards is available at: <http://bcove.me/au9qilhv>

Reed & Associates has been performing SAS70 Type I and Type II audits for over 10 years for government contract service organizations, Oracle service providers, ISP and application hosts as well as other service and technical service providers.

Reed & Associates is a Licensed WebTrust Practitioner: <http://www.webtrust.org/index.aspx>

**Please contact us: Deirdre Reed, CPA, CISA, CGFM
Dreed@reedassociates.org
860-395-1996
703-369-5351**