

February 2011

No More SAS 70s?

Who Does This impact?

Anyone who uses a third-party (service organization) and needs or wants to understand the controls at the service organization.

What Does it do?

CPAs have always had the need to understand the risks related to an entity's use of service organizations for an audit. Historically, CPAs have assessed the risk of an entity using a third-party to perform processing or provide services to the entity by relying on an auditor's report that was based upon Statement of Auditing Standard No. 70 (SAS 70). The SAS 70 included an auditor's opinion of the controls, the third-party's description of the systems and the relevant controls, the implementation of those controls (referred to as Type I report), and in the case of a Type II report, testing of those controls for effectiveness in relationship to the entity's financial reporting process.

This reporting process created at least three hurdles. First, many times the entity expected the SAS 70 report to include controls that were related to the service organization's ability to protect the accuracy, confidentiality, integrity and reliability of the information the service organization processed. These controls were frequently out of scope of a SAS 70 engagement. Second, the service organization wanted the SAS 70 to include representations of their ability to process information as they have indicated to the entity and to use the SAS 70 report as a sales or marketing tool to attract new customers. And third, under SAS 70, the service auditor's report was restricted to the service organization, current users of the service organization and the auditor's of the user entity. Both the service organization and prospective users of the service organization wanted to use the report as part of the sales and marketing process. As a result, SAS 70 reports sometimes included controls outside of the financial reporting process and were provided to entities not permitted to use the report.

Since the auditing standards relate specifically to

financial statement audits, moving SAS 70 for service organization auditors to the Attestation Engagement Standards (SSAE), permits changes to both the content and the audience of the reports. The new requirements for reporting on controls at a service organization are now in SSAE No. 16, Reporting on Controls at a Service Organization. The standards for financial statement auditor of the user entity are still located in the Auditing Standards (AU324).

Within SSAE No. 16, the AICPA has now established three Service Organization Control (SOC) reporting options. They are SOC 1, SOC 2 and SOC 3 reports. SOC 1 reports focus solely on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements only. SOC 1 is a restricted use report for use by the service organization client, existing user entities, and user auditors and its purpose is to report on controls relevant to the financial statement audits.

SOC 2 and SOC 3 engagements address controls at the service organization based upon principles and criteria at a service organization other than those relevant to user entities' internal control over financial reporting. Both SOC 2 and SOC 3 are based upon the Trust Service Principles, Criteria, and Illustrations such as those controls related to security, availability, processing integrity, confidentiality, or privacy.

SOC 2 includes a description of the controls as well as the tests of controls (if a Type II) similar to a SOC 1 report. SOC 2 is also generally a restricted use report – this time for use by the service organizations stakeholders (for example, customers, regulators, business partners, suppliers, and management) of the service organization that have a thorough understanding of the service organization and its controls.

(Continued on back)



DOEREN MAYHEW
Certified Public Accountants and Consultants

SOC 3 is a general use report to provide assurance on controls at a service organization related to security, availability, processing integrity, confidentiality, or privacy but the detailed description of the controls nor the tests performed on controls is included in the report. The SOC 3 report may be used by current and prospective customers of the service organization.

When Is This Effective?

SSAE No. 16 will take effect for periods ending on or after June 15, 2011. Doeren Mayhew will provide additional information on SSAE No. 16 over the next several months.

