SSAE 16 & SAS 70

A Primer on Changes to Service Organization Audit Standards

Author: Jack Fletcher, Risk Control Technology Specialist

Published: November 2014

Executive Summary

The review and analysis of a company's internal financial and management controls by outside auditors dates back to 1939 when the first Statement on Auditing Procedures (SAP) was developed.[1] Beginning in 1982, SAPs were replaced by Statement on Auditing Standards (SAS). In 1992, SAS 70 – titled Service Organizations – was developed by the American Institute of Certified Public Accountants (AICPA) to provide a framework for a very detailed examination of a service organization's financial and operational controls, often including the IT control procedures.[2]

In 2011, SAS 70 was superseded by the Statement on Standards for Attestation Engagements No. 16 or SSAE 16, which has become the gold standard for reporting on the effectiveness of controls utilized by service organizations. SSAE 16 was developed due in part by the implementation of the Sarbanes-Oxley Act of 2002 and the creation of International Standards on Assurance Engagements (ISAE) 3402.

So why should technology insurance professionals understand these reporting standards? Besides remaining abreast of current compliance trends, as risk managers, it is important to appreciate industry expectations regarding operational controls. SAS 70, which was an in-house report, only verified that a company's controls and processes were being followed. SSAE 16 not only verifies controls, but additionally documents the procedures so the service organization (such as a colocation facility, data center or cloud hosting service) can provide evidence to their customers and auditors evaluating the effectiveness of the service organization's controls. From a risk management perspective, SAS 70 and now SSAE 16 assessments allow technology insurance professionals to better assess the exposures and controls for those organizations servicing our clients, thereby enabling us to underwrite and price the risk more effectively.

As government and regulatory agencies place increased importance on accountability, it behooves companies to ensure their corporate culture supports an effective infrastructure that reinforces good management practices. The consequences of non-compliance with Sarbanes Oxley, OSHA, 10K and other financial reporting requirements can have negative consequences both financial and criminal in nature.

This whitepaper will discuss:

- Defining a service organization.
- Differences between SAS 70 and SSAE 16
- Compliance requirements for SSAE 16
- Service organization controls
- Importance of compliance to SSAE 16

What is a Service Organization?

A service organization provides services to a client user organization that may impact that customer's financial or information technology framework. In this whitepaper, the terms service organization, organization and company are used interchangeably.

- SSAE 16 defines a service organization as "The entity that provides services to a user organization that are part of the user organization's information system."[3]
- ISAE 3402 defines a service organization as "A third-party organization that provides services to user entities that are likely to be relevant to user entities' internal controls as it relates to financial reporting."[4]

Examples of service organizations used by firms in the information and medical technology segments include: hosted data centers, colocation providers, application service providers (ASPs), managed security providers, web hosting, credit processing organizations and clearinghouses, Software as a Service (SaaS) providers, cloud computing services, internet service providers (ISP), web design and social media firms.

SAS 70 vs. SSAE 16: What's the Difference?

In 2011, SAS 70 was replaced by SSAE 16. The purpose of SAS 70 was to certify that the service organization's financial and operational controls had been examined by an outside auditing firm. A final report was prepared, which included the auditor's opinion of the various controls in effect. However, SAS 70 reports were often misinterpreted as a means to obtain assurance regarding the entity's controls over compliance and operations.[5] They were never designed to evaluate the effectiveness of the controls just whether they were being done. The audit did not verify that the controls were good, best practices or terrible just whether the corporation was doing what they said they were going to do. SAS 70 is, in fact, identified as an "audit" standard.[6] An audit evaluates the company's financial controls intended to prevent accounting inconsistencies, errors and misrepresentation, and determines whether these controls are effective. Importantly, the auditor would only evaluate the criteria requested by the service organization.

SSAE 16 was designed to address changes in both accounting standards and company workflows, especially the increasing reliance on IT infrastructure. SSAE 16 is identified as an "attestation" standard.[7] An attestation provides a user organization with some level of assurance regarding the accuracy of the information used to evaluate a service organization. This attestation is based upon well-defined criteria.[8]

SSAE 16 requires a description of management systems while SAS 70 only required a description of management controls. SSAE 16 also requires the company's management to document its affirmation regarding the report's accuracy, which SAS 70 never required.

- AICPA defines management system as: "the services provided, along with the supporting processes, policies, procedures, personnel and operational activities that constitute the service organization's core activities that are relevant to user entities."
- A management control is any internal function designed to manage any process that could impact the client's financial reporting objectives, such as payroll reporting.

The focus of SSAE 16 is with the integrity of the data through the internal processing chain to ensure that the data wasn't tampered with or modified.

What Does SSAE 16 Require?

Description of "Controls" vs. a "System"
SAS 70 only requires a description of internal controls which include control environment, risk assessment, control activities, information/communication and monitoring.[9]

SSAE 16 requires a description of the "system." An organization's system describes the services provided by the company including operational and supporting activities that affect the service's customers. Systems are generally viewed as more detailed than pure control functions.

Written Assertion by Management
A management assertion must be provided in writing and confirm the following:

- The description fairly represents the service organization's "system."
- The control objectives were suitably designed.
- The criteria used for making these assertions are in place and are consistently applied.[10]

This written assertion was prompted by the adoption of the Sarbanes Oxley Act, which increased the level of management accountability that is now required as concerns the company's operations.

Subservice Organization Reporting Requirements
Subservice organizations also have SSAE 16 reporting requirements. A subservice organization is defined as a service organization used by the primary service organization to conduct its operations. An example would be subcontracted IT service that deals with financial data.

Service Organization Controls

The AICPA has also established Service Organization Control (SOC) reporting options including SOC 1, SOC 2 and SOC 3 reports.[11]

- SOC 1 reports pertain to examinations related to the internal controls over financial reporting.
- SOC 2 reports provide a comprehensive overview of a company's controls and specifically address one or more of the following five key systems attributes.
    - Security
    - Availability
    - Processing integrity
    - Confidentiality
    - Privacy pertaining to personal information
- SOC 3 reports are general-use reports that provide only the auditor's report on whether the system achieved trust services criteria (no description of the tests and results or opinion on the description of the system is necessary).

SOC 2 HIPAA is also used for HIPAA reporting (Health Insurance Portability and Accountability Act) compliance. The HIPAA Security Rule requires companies to protect individuals' electronic personal health information that is created, received, used or

maintained by a covered entity. There are three specific provisions within HIPAA that need to be covered by a SOC 2 assessment:

- Administrative Safeguards: Implement policies and procedures to prevent, detect, contain and correct security violations.
- Physical Safeguards: Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
- Technical Safeguards: Implement technical policies and procedures for electronic information systems that maintain electronic, protected health information and allow access only to those persons or software programs that have been granted access rights.

Why is Compliance with SSAE 16 Important?

Completion of an SSAE 16 report should be viewed as an opportunistic resource by service companies. This report provides a consistent framework for a potential customer to evaluate the service entity's financial and operational control capabilities, thereby minimizing one-off, custom requests within requests for proposals (RFPs). Furthermore, in the case of an SOC 2 report, it also provides an assessment of security and confidentiality capabilities. Without this report in place, a company may receive requests from many different user organizations (clients) or their auditors, who may be requesting an audit. SSAE 16 ensures that all companies maintain consistent and reliable information to facilitate the evaluation of their management and system controls. What's more, the review process often results in operational improvements.[12] SSAE also provides a framework for compliance with international standards, namely ISAE 3402.

Summary

Over the past 20 years, the AICPA rules governing the practice of management and system controls by service organizations has expanded. The broader scope levels the playing field as user organizations consider their service provider options. As well, insurance professionals have greater confidence in their ability to understand the degree of risk within a given service provider's operating environment, as well as the controls in place to monitor, report and improve upon these procedures.

Contact Us

To learn more about how OneBeacon Technology Insurance can help you manage online and other technology risks, please contact Dan Bauman, Vice President of Risk Control for OneBeacon Technology Insurance at dbauman@onebeacontech.com or 262.966.2739.

References

[1] SAS 70 History and Timeline. Accessed July 2014. http://sas70.com/sas70_history.html
[2] SAS Overview. Accessed July 2014. http://sas70.com/sas70_overview.html
[3] AICPA.org AU-00324-Service Organizations, page 1, Accessed July 2014.http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00324.pdf
[4] International Standard on Assurance Engagements (ISAE) 3402 Assurance Reports on Controls at a Service Organization, page 327. Accessed July 2014. http://www.ifac.org/sites/default/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf
[5] "Service Organization Controls - Managing Risks by Obtaining a Service Auditor's Report." AICPA. Accessed July 2014 http://www.aicpa.org/interestareas/informationtechnology/resources/trustservices/downloadabledocuments/10957-378%20soc%20whitepaper.pdf

[6] SSAE 16 vs. SAS 70 | What you Need to Know and Why. Accessed July 2014. http://www.ssae16.org/white-papers/ssae-16-vs-sas-70-what-you-need-to-know-and-why.html

[7] Ibid 6

[8] (2009). "Chapter 1: Introduction to Attestation Engagements From the Attestation Guide." Accessed July 2014. http://tax.cchgroup.com/landingpages/pfx/aasolutions-micro/pdf/Attest-CH1.pdf

[9] SAS 70 Audit Report Contents. NDB LLP Accountants and Consultants. Accessed July 2014.http://www.sas70.us.com/what-is/whats-in-a-sas70-report.php

[10] Ibid 6

[11] Ibid 5

[12] SSAE 16 Benefits To Service Organizations. Accessed July 2014 http://ssae16.com/SSAE16_service.html