CBIZ Tofias
Accounting | Tax | Consulting
The Bottom Line
National Resources | Local Decision Making

Evolving Business Practices Spur Transition from SAS 70 to SOC Reports

By John Robichaud, CPA, CTIP, CIA, CISA

In response to market demand and changing business practices – particularly outsourcing and the transition to cloud computing -- the American Institute of CPAs (AICPA) in 2010 issued new auditing standards and audit guides that replaced the decades-old SAS 70 standards and audit guide. The new standards and audit guides, called Service Organization Control (SOC) reports, build on SAS 70 and focus on the misuse of SAS 70 reports for non-intended assurance purposes, align reporting with international standards, and provide more reporting options to address non-financial transaction and reporting subject matter and assurance needs. These new standards went into effect for all reports issued after June 15, 2011.

SAS 70 History

Introduced in 1992, SAS 70 arrived at a time when outsourcing was in its infancy. Companies were just beginning to outsource some key tasks, such as payroll, but for the most part still handled their primary IT processes in house. Still, outsourcing even a small fraction of tasks brought concern about how those processes were performed by a third-party organization. SAS 70 was developed to assist external auditors in planning audits of their clients' financial statements when the clients used third-party service providers for financial transaction processing and reporting services and functions.

As outsourcing became more widespread and companies were paying closer attention to corporate governance, SAS 70 was being relied upon for uses beyond the scope of its original design, which was as an external auditor-to-auditor communication on the fair presentation, design, existence and operation of financial transaction processing and reporting controls. With the introduction of Software as a Service (SaaS), cloud computing and the proliferation of data privacy laws and regulations, SAS 70's shortcomings became even more apparent. Businesses and their clients that have embraced SaaS and the cloud have demanded -- and under certain laws and regulations are legally responsible for obtaining -- greater assurance about the security, confidentiality, privacy, availability and processing integrity of their service providers.

As SAS 70 was never intended to address these concerns it became clear that. SAS 70 was not an adequate examination and reporting method for meeting the evolving variety of assurance needs, so new, more robust and appropriate standards were developed.

About SOC Reports

There are three types of SOC reports that address assurance for service organizations. According to the AICPA, "each type of report has an accepted professional standard under which the audit will be

performed to allow for a common nomenclature when referring to reports going forward while allowing for a more frequent update of the professional standards."

The new SOC reports provide a framework for CPAs to examine controls and to help management understand the related risks of outsourcing to a service provider. The new standards will eliminate the common but faulty practice of using SAS 70 to issue reports on controls related to outsourced non-financial functions and data rather than the correct attest standard. SOC reports clarify specifically which standard needs to be used and how it should be implemented.

Here's an overview of the three types of SOC reports and related professional standards.

SOC 1 reports are restricted reports intended as auditor-to-auditor communication and direct replacements for SAS 70s

These restricted-use reports address the controls at a service organization related to financial transaction processing and reporting likely to be relevant to a customer's external auditor in planning the company's financial statement audit. These reports are not designed or intended for promotional purposes, for use by prospective customers, or to address non-financial transaction and reporting controls, such as security, privacy, or regulatory compliance. The applicable professional standard is SSAE 16, *Reporting on Controls at a Service Organization*. While similar to SAS 70, SSAE 16 introduces several key differences, including:

- *Attestation Standard:* These standards are specifically designed to address guidance and requirements for examining and reporting on other subject matter than financial statements, such as controls and compliance.

- *Focuses on a Service Organization's "System of Controls":* Where the SAS 70 audit standard focused on the service organization's specified control objectives and controls and allowed service organizations to customize the scope, the revised standard focuses on the controls that a service organization implements to prevent, or detect and correct, errors, as well as omissions in the transaction processing and information that a service organization provides to its customers.

- *Management Must Provide Assertion:* Similar to SOX Section 302, management must provide an assertion report taking ownership for a description of the system of controls, design and operation of controls, and risk assessment and criteria used to establish the control objectives and controls.

- *Establishes Requirements for Subservice Providers to be Included in the Report and Tested Controls:* In order to include controls at subservice organizations (companies that provide services to the service organizations, such as a third party data center for hosting systems and a bank for lockbox and automatic clearinghouse transfer processing), the subservice organization must also provide a management assertion report and description of its system of controls, and have the auditor test its controls.

- *International Alignment:* SSAE 16 and related SOC1 reporting were aligned with the comparable international auditing and reporting standards.

- Description of Control System for the Entire Examination Period: Under SAS 70, the description needed to be a fair presentation of the controls as of the end of the examination period, such as December 31. Under SSAE 16 and SOC1, the description must fairly describe the system of controls for the entire examination period, including all changes.

SOC 2 reports address issues stemming from non-financial controls regarding information

These reports are designed to meet the needs of a broader range of users, including knowledgeable prospective customers of the service. The reports can be used to provide assurance on security, availability, processing integrity, confidentiality and privacy related to the provided services based on the AICPA's Trust Services Principles and Criteria and Generally Accepted Privacy Principles. These reports also can be used for non-financial transaction processing and reporting services, such as cloud computing, data center hosting, SaaS, email services, database and analysis services, printing and mailing services, data repositories, etc. The applicable professional standards are AT 101, *Attestation Engagements and TSP 100 Trust Services Principles, Criteria and Illustrations.*

SOC 3 reports provide for brevity

These reports are also based on the Trust Services Principles and Criteria and Generally Accepted Privacy Principles as with SOC 2. However, SOC 3 are short-form reports that can be publicly distributed and posted on a service organization's website or through the AICPA/CICA's WebTrust Seal program and site. SOC 3 reports contain a general description of the service and system of controls, management's assertion reporting, and the auditor's opinion as to whether the management-specified Trust Services Principle in the assertion report met the related Trust Services Criteria during the examination period. As with SOC 2, the applicable professional standards are AT 101, *Attestation Engagements and TSP 100 Trust Services Principles, Criteria and Illustrations.*

Because SOC 3 reports are short-form reports that exclude reporting on the detailed controls and related testing and results, service organizations that rely on controls at subservice organizations or customers to meet any applicable trust services criteria can't obtain a qualified opinion unless the report includes assertion reports and descriptions of the control systems from the subservice organizations and customers, and the auditor tests these controls. Therefore, they are only appropriate for some organizations.

Companies can choose to use SOC 2 or SOC 3 reports depending on what type of assurance they are trying to achieve. Essentially, a company looking to provide a higher level of assurance to the public would choose SOC 3 reports while a company aiming to provide deeper assurance to their clients would probably choose SOC 2 reports. In some cases, companies may elect to do both a SOC 2 and a SOC 3 audit to address the concerns of dual audiences.

For more information on how these new SOC reports may impact your organization's financial reporting, due diligence oversight of service organizations and assurance requirements, contact John Robichaud, Leader of the Internal Audit and Internal Controls Practice. He can be reached at 617.761.0546 or jrobichaud@cbiztofias.com.