WHAT SSAE №18 MEANS FOR THE SOC 1 REPORTING WORLD

A BRIEF HISTORY

SSAE NO. 18

For as long as organizations have relied on other third party providers for the delivery of their outsourced services, those organizations have had a need for information about the third parties they use for those outsourced services. Whether the information was specific to how the third party ensured quality in its services provided to the organization, the accuracy and completeness of transactions processed, the security of their information, or the overall health of its control environment, many of the basic drivers for reliable and timely information have not changed much over the last few decades.

SSAE NO. 18

Since the early 1990's

Service organizations have been using public accountants' service auditor reports to communicate this information to interested parties. The American Institute of Certified Public Accounts (AICPA) has been and remains the industry leader in providing organizations with a reporting framework for obtaining this information, as well as providing the service providers and auditors with guidance for producing and interpreting this information.

The AICPA's auditing standards board (ASB) is the entity that promulgates the standards upon which service auditors' reports are produced and relied on, and the underlying auditing procedures that produce these reports. In the summer of 2004, the AICPA's ASB embarked on a plan to improve the readability and understandability of its standards (including the service auditor reporting standards) as well as increase the alignment of the U.S. standards with similar standards managed by its international counterpart, the International Auditing and Assurance Standards Board (IAASB).

This clarity and convergence project would mean dramatic and significant changes for the service auditor reporting world, including the elimination of SAS 70 reports that were used for almost 20 years, and the establishment of SOC branded reports SOC 1, SOC 2, and SOC 3. Perhaps more noteworthy though, is the purposeful identification, separation, and codification of the various auditing and attestation standards themselves. Very clear standards and guidance could now be developed to govern the performance of SOC examinations, and separately, the use of those reports. Now with the Clarity Project complete, the standards which govern how practitioner's audit service providers, report on the controls at service providers, and how those reports are ultimately shared and used have materially changed since the earlier SAS 70 days.

A summary of the AICPA's Clarity and Convergence project can be found here: www.aicpa.org

SSAE NO. 18

What SSAE No. 18 Means to You

Simply put, SSAE No 18 is the standard which recodifies all the previous attestation standards. It is the culmination of the efforts to clarify the various standards for performing attestation engagements, which includes among many others, SOC 1 (commonly referred to as SSAE No. 16) and SOC 2 and SOC 3 (AT Section 101), into a single set of standards for the auditors.

No doubt, there will be report users, service providers, and auditors that will refer to SSAE No. 18 in much the same way that 'SAS 70', 'SSAE 16', 'AT 101' were and are currently being used; however, for many interested parties these acronyms alone may be nothing more than esoteric references to concepts or ideas about audits or reports.

For the SOC reporting space, the recodification of attestation standards (SSAE No. 18) is largely a simplified version of the existing standards. The net effect is that an 'SSAE 16' SOC 1 will look nearly identical to an 'SSAE 18' SOC 1.fn 1. The practitioners performing the attestation engagements for SOC reports will not notice very many material changes in the standards; however, there are a few key areas of emphasis worth noting for SOC 1 reports:

- Modification to assertion criteria
- Evaluating the reliability of evidence provided by the service organization
- Monitoring of subservice organizations
- Obtaining an understanding of the service organization's system and assessing the risk of material misstatement

SSAE NO. 18

Modification to assertion criteria

An additional description criterion related to subservice organizations (relevant third party organizations used by the service organization) is included within the re-codified attestation standard. The services performed by subservice organizations and whether the subservice organization's controls have been included or carved-out of the scope of the examination have always been part of the SOC 1 examination and resulting report. This change, however, does re-emphasize the importance of describing this specific relationship and disclosing it in a fair manner.

Fair presentation of subservice organizations also includes a description of any controls (complementary subservice organization controls) that the service organization assumed in the design of its controls. A common example is when a service organization outsources data center operations to a colocation facility or its platform hosting services to a cloud services provider. In both instances, the service organization normally assumes that the colocation provider or cloud services provider has implemented controls regarding the physical and/or logical safeguarding of their operating environment.

As a result, those safeguards and controls would complement the additional controls to be performed by the service organization itself. In these instances, a description of such assumed complementary controls should be included in the service organization's system description. This change impacts the assertion letter to be included in the SOC 1 reports.

Monitoring the effectiveness of controls at a subservice organization

In keeping with the aforementioned additional criterion specific to subservice organizations, the revised attestation standard does promote the requirement for the auditor to determine and report on the controls the service organization has implemented to monitor the relevant controls at subservice organizations.

SSAE NO. 18

The revised standard also formally includes monitoring of subservice organizations, if any, into the scope of a service organization's SOC 1. The revised standard provides for examples of monitoring activities which include the following:

- **Reviewing and reconciling output reports –** Service organizations may implement procedures to verify the accuracy and completeness of output reports (or files) received from their subservice organizations. Management of the service organization should be prepared to describe the review and/or reconciliation procedures performed (including the nature, timing, and extent of the review procedures), the source of the data or information used for reconciling against the subservice organization's output reports, and the process for remediation or corrective action if deviations are determined.

- **Periodic discussion with the subservice organization personnel –** An effective way for the service organization's management to determine the sufficiency of the subservice organization's controls and their operation, may also include periodic discussions with the relevant subservice organization personnel. Due to the limitations on the reliability of inquiry-based assurance methods, however, service organizations may consider 1) the use of comprehensive and structured written questionnaires with requests for corroborative documented evidence, and 2) that the questionnaires (or discussions) be completed by members of the subservice organization with the requisite knowledge, skills, and familiarity with the applicable controls and the service organization's system. Management of the service organization should be prepared to describe the process for these discussions in its system description.

- **Regular site visits –** In many instances, the service organization may determine an on-site walkthrough and tour of the relevant portions of the subservice organization's operations is warranted. This may include an on-site discussion during the site visit as well. Management of the service organization should be prepared to describe the frequency and extent of the site visit processes, including the process for handling nonconformities or deviations that may affect the services organization's services.

SSAE NO. 18

- **Testing controls at the subservice organization –** Perhaps the most effective method service organizations may use to monitor the performance of the controls at their relevant subservice organizations is to use the service organization's internal audit personnel to conduct tests of controls at the subservice organization. Several factors can be considered with this approach, including a risk assessment of key or critical controls when developing the audit plan(s), the rotation or frequency of the audits if multiple subservice organizations are used for the services, the skills and knowledge of the service organization's internal audit personnel that would perform the audits, and whether the audits would be efficient and provide the relevant control performance information in a timely manner.

It remains, however, that controls testing can provide very effective information on the controls performance of subservice organizations, particularly when combined with the other monitoring methods described in this article. Management of the service organization should be prepared to describe the process for conducting testing of controls at subservice organizations, including the process for determining which controls to test, the frequency of the controls testing, the method of documenting and reporting the results of those tests, and the process for ensuring identified deficiencies and deviations are resolved by the subservice organization in a timely manner.

- **Monitoring external communications –** Service organizations may decide, alone or in combination with other monitoring methods, that monitoring external communications such as customer complaints, regulatory agency reports, or other communications on the effectiveness of the control operations at subservice organizations is an appropriate method for determining the sufficiency of controls at those organizations. Management should be prepared to describe these monitoring processes within its description of its system.

- **Reviewing SOC Reports of the subservice organization's system –** An increasingly popular trend for service organizations to get the information they need regarding the control performance at subservice organizations is to receive and read the SOC reports from those subservice organizations. Typically, Type 2 SOC 1 or Type 2 SOC 2 reports are likely to provide the necessary information regarding the control performance over their Type 1 counterparts or SOC 3 reports, but service organizations may also consider other types of properly prepared attestations that are relevant to their services.

SSAE NO. 18

Many organizations use this monitoring method for its comprehensiveness, stability, and efficiency, particularly if the service organizations use multiple subservice organizations and performing the audits of those subservice organizations would be too time consuming or expensive.

Organizations that use SOC or other attestation reports to monitor those subservice organizations should pay additional attention to any complementary user entity controls (CUECs) described in those reports, as those CUECs represent the control assumptions their subservice organization assumed the service organization would implement when the subservice organization designed its controls.

Management of the service organization should be prepared to describe the process for reviewing the SOC 1 reports, including any procedures performed to determine the sufficiency of the scope and timing of the SOC report, the individuals at the service organization responsible for reviewing the report, communicating with the subservice organization for any identified deviations, as necessary, the process for identifying any CUECs in the report and determining if those CUECs apply to the service organizations system, and the related action items for ensuring the CUECs are addressed, as necessary.

Service organizations can expect these or similar monitoring controls to be a more prominent subject within their SOC 1 reports going forward.

Evaluating the reliability of evidence produced by the service organization

This has long been a tenant of effective auditing and included in prior and existing auditing and attestation standards, and, for most auditors and service organizations, is unlikely to present major changes in the performance of the SOC 1 examination. However, in the previous standards governing SOC 1 reporting, it had not been described in such clear and definitive terms.

SSAE NO. 18

Although this writing is focused on SOC 1, auditors of SOC 2 and SOC 3 examinations alike are required to ensure the evidence provided by the service organizations is sufficiently accurate, complete, and detailed for their audit purposes. SSAE No. 18 provides the following listing of examples of information a service auditor receives, which may likely require additional evaluation going forward:

- Population lists used for sample tests
- Exception reports
- Lists of data with specific characteristics
- Transaction reconciliations
- System-generated reports
- Other system-generated data (e.g. configurations, parameters, etc.)
- Documentation that provides evidence of the operating effectiveness of controls, such as user access listing

For SOC auditors, this may require more detailed and documented qualitative procedures to determine the sufficiency of the evidence provided by the service organization. For service organizations, this may require more detailed or corroborative artifacts supporting the evidence provided to auditors.

Obtaining an understanding of the service organization's system and assessing the risk of material misstatement

Consistent with extant SSAE No. 16, service auditors are required to gain an understanding of the service organization's system, including controls that are included in the scope of the engagement. The recodification under SSAE No. 18, builds on this requirement, with additional guidance on assessing the risk of material misstatement. Again, the requirements for both understanding the service organization's system and the assessment of risk were previous requirements under SSAE No. 16; however, the revised standard speaks to these areas in a more prominent way. Service organizations are unlikely to notice any difference regarding this area.

SSAE NO. 18

What service organizations should do next

Service organizations are encouraged to consult with a competent professional regarding their SOC 1 reports and the impact of the SSAE No. 18 recodification to their SOC 1 examinations and reports. While the above summary is not intended to be an exhaustive review of all of the differences from SSAE No. 16 as provided by SSAE No. 18, it should provide most service organizations with a starting point for a discussion with their SOC 1 audit teams. SSAE No. 18 becomes effective as of May 2017.

[fn 1] = 'SSAE 16' SOC 1 AND 'SSAE 18' SOC 1 ARE NOT AUTHORITATIVE TERMS USED TO DESCRIBED SOC 1 REPORTS. THE AUTHOR MENTIONS THESE TERMS FOR ILLUSTRATIVE PURPOSES ONLY.

Ryan Buckner
Principal

Ryan Buckner is a Principal at Schellman. Ryan currently leads Schellman's SOC 1 practice and has been a leading advocate for the adoption of SOC 1 and SOC 2 solutions by cloud service providers. Ryan also is an AICPA-approved and nationally listed SOC Peer Review Specialist for SOC 1 and SOC 2 examinations. Having completed over 800 service audits, Ryan is one of the most experienced service auditors in the United States.

CLICK HERE TO TALK WITH A SPECIALIST

schellman
formerly BrightLine

www.schellmanco.com

4010 Boy Scout Blvd., Suite 600
Tampa, Florida 33607
1.866.254.0000

Outside of the United States, please dial: +1.973.854.4684