OUTSOURCING UNDER THE SSAE 18 STANDARD: ARE YOU PREPARED?

BY PETER SCHABLIK, PARTNER

Mazars USA LLP is an independent member firm of Mazars Group.

MAZARS

Outsourcing in 1992 was primarily focused on payroll, with only one in five companies outsourcing a critical business process. The assurance of internal controls for financial reporting guidance provided by Statement on Auditing Standards No. 70 (SAS 70) was adequate.

Fast forward to 2017, when virtually all companies outsource critical business processes and the expectation for annual outsourcing industry growth is 6.7 % [1] for the next nine years. A new standard addressing this high level of reliance, existing and emerging threats, and broader stakeholder expectations is required.

The Statement on Standards for Attestation Engagements (SSAE) No. 18 *Attestation Standards: Clarification and Recoding* includes the next step in providing assurance for the continued evolution of outsourced services.

The new Standard is effective for Attestation Reports issued on or after May 1, 2017, recodifies existing standards and enhances the requirements around Service Organization attestation engagements.

SSAE 16 Attestation Standard

During the early 1990s, the accounting industry was grappling with the change from a balance sheet substantiation type of audit to a controls-based audit approach. During this time, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) standard and the Federal Deposit Corporation Improvement Act (FDICIA) requirement were issued, both focusing on a controls-based audit approach. The American Institute for of Certified Public Accountants (AICPA) SAS 70 standard established the guidance for evaluating internal controls. This remained the standard for nearly 20 years, until being replaced with the SSAE 16 standard in 2011, highlights of which included:

- **International Standards** – The SSAE 16 standard was developed in conjunction with the International Auditing and Assurance Board (IAASB) and aligned with the international ISAE 3402 standard. There were varying interpretations of the SAS 70 standard around the world. The superseded Canadian Chartered Accountant (CA)'s Section 5970 and Denmark's RS-3411 standard, both similar in scope to the US SAS 70 standard, had clear differences in the examination scope, testing approach, and report contents. The worldwide ISAE 3402 standard formed the basis for individual country standards.

- **Written Assertion** – The SSAE 16 is an attestation standard compared to the SAS 70 that was considered an auditing standard. Service organizations must provide a written assertion as part of the attestation process.

- **Non-Financial Assurance** – The previous SAS 70 standard was focused on internal controls relevant to the audit of an entity's financial statement. A service organization that was not considered an extension of the user organization's accounting information system was not deemed appropriate for a SAS 70 examination. The demand for non-financial assurance increased dramatically in the 1990s and early 2000s, often resulting in practitioners stretching the SAS 70 standard to fit specific situations. The SSAE 16 standard provided for the following versions of Service Organization Controls (SOC) reports:
  - **SOC 1 –** Most similar to the SAS 70 audit standard, this is an attest report focused on internal controls for financial reporting.
  - **SOC 2** – This is an attest report focused on the security, availability, processing integrity, confidentiality, and privacy trust principles. This report fills a previous gap in providing non-financial assurance.
  - **SOC 3** – This is a general use report that includes a certification for security, availability, and processing integrity. The SOC 3 report is for public consumption and can be displayed on the service entity's web site and marketing materials.

SSAE 18 Attestation Standard (Effective for Reports issues on or after May 1, 2017)

The SSAE 18 attestation standard builds upon and clarifies the separate SSAE 16 audit standards into a single set of requirements. The examination reports will be very similar with the exception of the following noteworthy changes:

- ***Description of the subservice organizations*** – *Subservice organization. A service organization used by another service organization to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting.*

  Subservice organizations have grown to provide increasingly large service organizations with the necessary support to meet the needs of user organizations. The new standard re-emphasizes

[1] Source: http://www.businesswire.com/news/home/20170213005510/en/Global-Network-Outsourcing-Market-Analysis-Trends-2017-2025

disclosing the relationship of the subservice organization in a fair manner, which includes evaluating the existing list of subservice organizations related to the services provided and identifying the impacted control objectives. A risk assessment should be performed to **a)** identify all subservice providers and vendors; **b)** quantify/qualify the important risks to the service organization; **c)** determine if the entity is a subservice organization or vendor; **d)** if subservice organization and carved-out method used, determine the appropriate monitoring activity.

In addition, any assumed controls at the subservice organization, or included in user control considerations, must also be disclosed.

- ***Monitoring the effectiveness of controls at subservice organizations*** – The discussion around the role of monitoring controls culminated in the AICPA release in 2014 of the "Evolving the CPA Profession's Peer Review Program for the Future: A provocative vision of what practice monitoring could become." The view was that many internal control environments overly focused on control activities instead of monitoring that would provide for effective feedback about the operation of internal controls. This focus on monitoring, combined with an increased reliance upon subservice providers, resulted in new guidance regarding monitoring. The standard identifies the following as potential monitoring controls:

    - Reviewing and reconciling output reports
    - Periodic discussion with the subservice organization personnel
    - Regular site visits
    - Testing controls at the subservice organization
    - Monitoring external communications
    - Reviewing SOC reports of the subservice organization's system

- ***Evaluating the Reliability of Information Produced by the Service Organization*** – During the past few years, reviews of audit quality conducted by peer review teams, the PCAOB and other organizations have focused on the reliability of information provided during an attestation engagement. Similar to the results of these audit reviews, the AICPA has established guidance for third party attestations conducted under SSAE 18. The AICPA has provided the following list of examples that can be used to evaluate the reliability of evidence:

    - 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 access listings

- ***Identifying Risks of Material Misstatement*** – The need to gain an understanding of the risk of material misstatement in a service organization's controls is not new. However, the standard highlights the need for focus on the risk of material misstatement. A service provider is now required to provide the auditor a detailed risk assessment, based around key internal risks, where there is potential for material misstatement (i.e., what could go wrong) and supporting controls.

Best Practices

Our experience of performing hundreds of third party assurance examinations during the past 25 years has highlighted the following best practices:

- ***Perform a readiness engagement*** – We strongly encourage service entities planning for an initial third party examination to consider a readiness engagement to document controls, identify potential gaps and prepare a remediation plan. The initial readiness engagement is typically a learning experience that sets expectations, minimizes surprises during the examination phases and universally has a positive return on investment.

- ***Communicate with user organizations and auditors*** – We have often found that the term "SOC 1" is used by procurement personnel as part of an RFP process. A discussion with the current or potential user organizations and their auditors is critical to determine whether the most appropriate solution is a SOC 1, SOC 2, SOC 3, or other type of engagement.

- ***Encourage a controls culture*** – We strongly encourage adopting a culture of controls, with employees having the ability to recommend or report concerns. We have found that control exceptions or weaknesses are known by individuals within organizations well in advance of conducting third party examinations. Encouraging an environment of control conscientiousness and communication can have a dramatic impact on both the effectiveness and efficiencies of performing third party assurance engagements.

- ***Implement forms automation and workflow*** – Forms automation with rules for completion can provide for a complete population of a control occurrence and minimize misplaced or incomplete documents. We have found that incomplete documents are the most common control exception.

- ***Reliance upon vendor supported software tools*** – The new SSAE 18 standard emphasizes the need for accurate and complete information in the examination process. Although there are many highly flexible freeware tools, there are concerns related to access to the underlying data files and integrity of log files. Vendor supported tools for administering support tickets, monitoring application changes, and other functions are more reliable since the data is typically encrypted and less prone to unauthorized alteration.

Recodification

SSAE 18 recodifies and replaces certain existing requirements. Section numbers now include AT-C titles replacing previous AT titles. For example AT Section 601 *Compliance Attestation* has been superseded by AT-C Section 315 *Compliance Attestation* and AT Section 801 *Reporting on Controls at a Service Organization* has been superseded by AT-C Section 320 *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting.*

Conclusion

The SSAE 18 standard represents the culmination of the previous standards, with a heightened focus on subservice organizations, reliability of evidence produced, and a re-emphasis on the risk of material misstatement. Early planning and consideration of best practices for conducting an SSAE 18 examination would reduce any potential rework or exceptions that would negatively impact the budget or schedule.

FOR MORE INFORMATION CONTACT:

PETER SCHABLIK, PARTNER
GOVERNANCE RISK AND COMPLIANCE
617.501.4195
Peter.Schablik@MazarsUSA.com

VISIT US AT www.mazarsusa.com

Disclaimer of Liability
Our firm provides the information in this e-newsletter for general guidance only, and does not constitute the provision of legal advice, tax advice, accounting services, investment advice, or professional consulting of any kind. The information provided herein should not be used as a substitute for consultation with professional tax, accounting, legal, or other competent advisers. Before making any decision or taking any action, you should consult a professional adviser who has been provided with all pertinent facts relevant to your particular situation.

***Mazars USA LLP** is an independent member firm of Mazars Group.*

***CONFIDENTIALITY NOTICE:** The information contained in this communication may be privileged, confidential and protected from use and disclosure. If you are not the intended recipient, or responsible for delivering this message to the intended recipient, you are hereby notified that any review, disclosure, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the sender immediately by replying to the message and deleting it from your computer. Thank you for your cooperation. Mazars USA LLP*