

The 21st Century Version of SAS 70.....SSAE 16

Overview of the Standard

In April 2010, the AICPA Auditing Standards Board issued the long awaited Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. The attestation standard was chosen as a result of CPAs providing attestations on subject matter other than the fairness of the presentation of financial statements. The effective date for SSAE 16 is June 15, 2011; however, earlier implementation is permitted.

Similar to SAS 70, there remain two types of SSAE 16 audits. A Type 1 report is known as a report on management's description of a service organization's system and the suitability of the design of controls. A Type 2 report is a report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls.

Management will be called upon to describe their service organization's system in the report. The description will need to include detail such as the processes describing how transactions are processed and reported to user organizations, the specified control objectives and controls designed to achieve those objectives, along with additional aspects of internal control such as control environment, risk assessment, information and communication systems, control activities and monitoring controls. In the case of a Type 2 report, management should include relevant details of changes to the service organization's system during the period covered by the description.

Furthermore, management will need to provide the auditor with a written assertion to be included in the service auditor's report. The written assertion should state the following:

- Management's description of the service organization's system fairly presents the service organization's system that was designed and implemented as of a specified date (or for a Type 2 – throughout the specified period);
- The controls related to the control objectives stated in management's description of the service organization's system were suitably designed to achieve those control objectives as of the specified date (or for a Type 2 – throughout the specified period);
- The controls related to the control objectives stated in management's description of the service organization's system operated effectively throughout the specified period to achieve those control objectives (Type 2 only).

With the new SSAE 16, the service auditor will now make an attestation on these management assertions. The service auditor will assess whether management has used suitable criteria:

- In preparing its description of the service organization's system;
- In evaluating whether controls were suitably designed to achieve the control objectives stated in the description; and
- In the case of a Type 2 report, in evaluating whether controls operated effectively throughout the specified period to achieve the control objectives stated in the description of the service organization's system.

Key Differences from the SAS 70 Audit Standard

While at first look the new SSAE 16 standard and the old SAS 70 standard may appear to be very similar, there are significant differences. The first of which is the auditor's opinion letter. The SAS 70 auditor's opinion was a direct reporting opinion where the auditor directly reported on the fairness of the description of controls, design of the control activities to meet the objectives, and whether the controls were placed in operation and their operating effectiveness. In the SSAE 16 standard, auditors are attesting to management's assertion as noted above.

The service auditor now has responsibility for determining whether management has used suitable criteria in preparing its description of the service organization's system. The service auditor will need to understand the criteria and process management has performed to develop their assertion.

In the case of a Type 2 report, the SAS 70 audit standard did not notate the portion of testing that was performed by internal audit and that which was performed by the service auditor. The SSAE 16 standard has reversed that stance and now the service auditor will disclose in a Type 2 report those tests that were performed by the client's internal audit department and the description of the procedures the service auditor performed with respect to that work.

How do I prepare for SSAE 16?

Service organizations need to perform an analysis of their current SAS 70 audit description of controls to identify gaps in the description needed to satisfy SSAE 16 requirements. SSAE 16 requires the service organization to develop a description of the service organization's system. The service auditor will examine the description of the service organization's system to ensure it is fairly presented and ask questions regarding the description such as:

- Does management's description address all major aspects of the service provided and includes in the scope of the engagement?
- Is the description prepared at a level of detail that could reasonably be expected to provide a broad range of user auditors with sufficient information to obtain an understanding of the internal control structure?

After the description of systems has been drafted, the service organization needs to identify the control objectives and the risks that threaten the achievement of the control objectives stated in the description. The service organization also needs to design suitable controls that are operating effectively and provide reasonable assurance that the control objectives will be achieved.

Service organizations should begin to develop their assertions which will be included in the service auditor's report. In addition, management should consider if any sub-service organizations need to develop assertions. Vendors who may not be sub-service organizations but have an impact on the service organization's internal control structure should also be examined to determine if current contractual requirements to provide the service organization with a SAS 70 report should be updated for SSAE 16.

SSAE 16 is not for Cloud Computing

The AICPA is fully aware of the increased use of cloud computing companies and the need for assurance in the cloud computing arena. Neither SSAE 16 nor SAS 70 should be used to assess controls of cloud computing companies. The AICPA has created a special task force of the Assurance Services Executive Committee to write a new guide which will address such engagements which are performed under AT section 101. AT Section 101 allows for CPAs to perform attestation engagements under this standard when another applicable standard does not apply.

Service organizations should have discussions with their auditors or obtain consultation regarding the new SSAE 16 standard to ensure their compliance efforts are brought into the 21st century.

Scott G. Price, CPA, CFF, CISA, CIA, Director – A-align CPAs

About the Author

Scott Price is a director at A-align with over 12 years of experience providing risk advisory services including SAS 70 and internal audits, business process reviews, and regulatory compliance assessments. Scott is a Certified Public Accountant, Certified in Financial Forensics, Certified Information Systems Auditor and Certified Internal Auditor.

References:

SSAE 16: Reporting on Controls at a Service Organization

AICPA FAQs – New Service Organization Standards and Implementation Guidance.