

## ***Time's up SAS 70.... SSAE 16 and ISAE 3402 are moving in.***

### *Lifecycle of the SAS 70 audit standard*

The SAS 70 audit standard first came on the scene in 1992. It was a result of the new outsourcing craze taking off and how to comply with the requirements of SAS 55 which outlined requirements for auditors to understand their client's internal control structure. The SAS 70 report was the only form of auditor to auditor communication. During the Dot.Com boom, the SAS 70 audit report evolved into a necessary validation of a start up company's controls and processes.

As the regulatory landscape changed in the early 2000s with HIPAA regulations in the healthcare arena and Gramm-Leach-Bliley in banking, companies required their vendors to undergo a SAS 70 audit as a form of due diligence and risk mitigation related to the outsourced service. Sarbanes-Oxley legislation in 2002 resulted in a significant increase in the number of companies subjected to SAS 70 audits requirements. This was due to the requirements for publicly traded companies to document and test their internal controls over financial reporting. Many companies realized that service organizations impacted the companies' financial reporting and must be considered for Sarbanes-Oxley purposes.

### *Why was a change in the SAS 70 audit standard needed?*

The change was needed for a multitude of reasons but one of the major ones was to bring the SAS 70 audit standard more in line with Sarbanes-Oxley. Sarbanes-Oxley compliance called for management to provide assertions on their internal controls over financial reporting while the SAS 70 audit standard was not an assertion based report.

Additionally, as the economic landscape became more global, the SAS 70 audit standard was applied on an international basis. The International Auditing and Assurance Standards Board (IAASB) took notice of the international application of SAS 70 and during their revision of their standards an international standard regarding service organizations, a new ISAE, was drafted. ISAE 3402 was issued in December of 2009 to cover service auditor's reports ending on or after June 15, 2011. As the IAASB began their project to develop ISAE 3402, the American Institute of CPAs began a convergence project to ensure AICPA audit standards more closely mirrored the IAASB standards. This was a result of the impending move to International Financial Reporting Standards (IFRS) in the coming years. With the move to IFRS a change to the audit standards to align with the IAASB standards was needed.

### *What is included in ISAE 3402?*

ISAE 3402 adopts an assertion based model with a risk-based approach. Assertions are made by the service organization regarding their process to identify risk and design control activities to place in operation to mitigate the risk. The service auditor opines on the assertion made by the service organization rather than directly reporting on the control activities as is the case in the current SAS 70 audit standard. ISAE 3402 provides for more detail in the disclosure of the performance of the testing of control activities. Many organizations utilize their internal audit department to perform testing of the control activities which then in turn the service auditor relies on to form the basis for their opinion. Under current standards, disclosure of which entity, service organization internal audit or service auditor, performed the testing is not made. ISAE 3402 requires disclosure of the entity performing the testing.

Additionally, ISAE 3402 requires the service auditor to take action if they become aware of compliance with laws and regulations, fraud, or uncorrected errors attributable to a service organization that are not clearly trivial and may affect one or more user entities.

*What does the future hold for SAS 70?*

There is no doubt that the existing SAS 70 audit standard will be replaced with Statement on Standards for Attestation Engagements (SSAE) No. 16. SSAE 16 has taken the long road to issuance. The comment letter period ended February 17, 2009. Many thought that issuance would happen by December 2009. The final vote on the new standard was to take place in January 2010 with issuance expected by March 2010. March has passed and many believe we will see final issuance in June 2010 with an effective date of June 15, 2011 which mirrors the ISAE 3402 implementation date. We don't know yet of the treatment of some of the key items in SSAE 16 and ISAE 3402.

During the comment period, it was noted that service auditors were not keen on the disclosure of whether internal audit or the service auditor performed the testing. This may be due to the potential confusion of the reader on division of responsibility or the fact that disclosure of the amount of testing performed by internal audit on an engagement may question the significance of involvement of the service auditor. Additionally, the AICPA has taken a pro-CPA approach with regards to the responsibility to detect and report on fraud. In the AICPA's eyes, the ISAE 3402 standard may place too heavy of a burden on the auditor for fraud detection and disclosure.

*What do companies do now to prepare for the change?*

CPA firms are already gearing up their clients for the change and trying to get ahead of the game. SSAE 16 provides for companies to examine the control objectives and related control activities in their report to examine the significance of each control using a risk based approach. This may result in companies improving their assessment of risk to identify controls that are lacking and need to be implemented. On the other hand, companies may uncover control activities that are tested in the SAS 70 audit report that have little to no value in reducing risk to their user organization. Due to independence reasons, the service auditor cannot play a significant role in the assertion development but other firms without independence conflicts can help the company develop their process for assessing risk and their assertion. Notwithstanding the direction of the count of control activities, companies need to work on their process for the assertion development and reasoning along with the system description.

Also, service organizations that use the inclusive method for reporting (the company includes a sub-service organization's controls in their report) need to assess whether or not to continue that practice. If so, the sub-service organization will need to develop their own assertions and system description for the service organization's auditors to opine on the assertion of the sub-service organization.

For a standard that has typically been seen as a stagnant audit standard for many years, the last year has seen much activity in the industry. A-align CPAs will continue to keep you informed of the developments and impacts of SSAE 16 and other related standards when they are finalized.



*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.