IT Audit Basics

Understanding the New SOC Reports

Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CMA, CPA, is an associate professor of information systems (IS) at the University of Alabama at Birmingham (USA), a Marshall IS Scholar and a director of the Forensic Accounting Program. Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting IS using microcomputers. Singleton is also a scholar-in-residence for IT audit and forensic accounting at Carr Riggs Ingram, a large regional public accounting firm in the southeastern US. In 1999, the Alabama Society of CPAs awarded Singleton the 1998–1999 Innovative User of Technology Award. Singleton is the ISACA academic advocate at the University of Alabama at Birmingham. His articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications, including the *ISACA Journal*.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

With the transition from Statement on Auditing Standard (SAS) No. 70 reports to the new Service Organization Controls (SOC) reports, this issue's column describes these reports to provide an understanding of them, and to explain the differences among them in order to prepare CISAs for the changes ahead.

SAS 70 AND THE NEED FOR SOC

About 18 years ago, the American Institute of Certified Public Accountants (AICPA) adopted SAS 70, "Service Organizations."[1] The purpose of a SAS 70 audit was (and is) to gather evidence on internal controls of a service organization (SO) in which those controls were associated with the delivery of a service that was (and is) related to the financial reports and impacted the financial statement to a material degree. Obviously, it was put in place because the financial auditors of the user entity needed to have sufficient assurance on controls over accounts, transactions or disclosures that were material, and some of those events occurred at an SO.[2]

It was not feasible for the user auditors to be able to properly evaluate them on the site of the SO. Thus, there was a need for some assurance over the controls of the SO that are relevant to the financial audit of the service user to be provided by someone other than the user auditor. SAS 70 addressed this by creating an audit of the controls at SOs, to be performed by auditors (i.e., certified public accountants [CPAs]) who were not the user's auditors, and a report written on the results of that audit.[3] The user auditors could then rely on the opinion of the auditor's report to best fulfill their obligations—at a minimum, from an efficiency and effectiveness perspective.

Because many of these services were IT-related or involved IT (e.g., transmission of data or funds electronically), and because of the expansion of the number of controls embedded in IT, Certified Information Systems Auditors (CISAs) were often called on to be a part of the service auditor team. Over these 18 years, CISAs have become more and more involved with SAS 70 audits.

The business community began to appreciate and value a SAS 70 audit even beyond the needs of the user's auditors. For instance, service providers (especially entities such as data centers, cloud computing companies, flexible spending account vendors, banks and retirement account vendors) found that when they called on prospects, the primary concern was one of security (i.e., controls). Thus, a SAS 70 became a valuable marketing tool to show businesses that the user had sufficient controls about which the prospect could be comfortable and could gain an adequate assurance of the level of security being provided. This worked so well that companies began to use a SAS 70 for all sorts of controls assurance for an SO (e.g., a hospital outsources its pharmacy and wants assurance over privacy for US Health Insurance Portability and Accountability Act [HIPAA] purposes). However, SAS 70 specifically stated that it was for internal controls over financial reporting (ICFR) and, thus, not correctly applied to privacy or security audits.

Another issue with SAS 70 audits was that there was no standard set of controls. Instead, management of each SO determined the controls to be evaluated, and thus, there was the possibility that management might not have been able to identify one or more critical controls and, thereby, could have unintentionally tainted the SAS 70 report. Even the identification of controls was not formalized in writing.

THE NEW SERVICE ORGANIZATION CONTROLS REPORTS: SOC-1, SOC-2, SOC-3

Recently, the AICPA addressed these evolving issues about SAS 70 and provided a more effective framework for providing assurance of controls in a service organization.[4] Because of the evolving needs for a variety of the objectives of these controls, AICPA came up with Service Organization Controls (SOC) reports, identified simply as SOC-1, SOC-2 and SOC-3 (see **figure 1** for a summary of the SOC framework). These are based on technical standards of Statement on Standards for Attestation Engagements (SSAE) No. 16 and Trust Services,[5] both adopted in 2010. SOC-1 is related *only* to ICFR, SOC-2 is related to controls over security/systems and privacy, and SOC-3 is related to controls over the same.[6] In addition, AICPA has issued a "clarified SAS 70" that applies to the user auditor only.

Figure 1—SOC Framework			
Applicable…	**SOC-1**	**SOC-2**	**SOC-3**
Standard	SSAE 16: AICPA Guide (2011)	AT 101: AICPA Guide (2011)	AT 101: Technical Practice Aid
Controls	ICFR	Security/ Systems, Privacy	Security/ Systems, Privacy
Controls reference	Undefined	Trust Services Principles[7]/ GAPP[8]	Trust Services Principles/ GAPP
Usage of report	User auditor, management of SO, management of user	Knowledgeable parties (see AT 101)	Anyone

SOC-1: REPORTING ON CONTROLS AT A SERVICE ORGANIZATION

SOC-1 is the report of the service auditor over ICFR and is associated with a new standard that partially replaces the service auditor side of SAS 70. SSAE 16,[9] virtually identical to its international complement, the International Accounting Standards Board (IASB)'s International Standard on Assurance Engagements (ISAE) 3402, provides new guidance for assurance over ICFR in an SO. Both standards become effective for reports on or after 15 June 2011. It is important that CISAs and IT auditors in general understand the differences between SAS 70 and SSAE 16.

SAS 70 vs. SSAE 16

There are a number of differences between SAS 70 and the new SSAE 16, some of which are rather significant—at least to the process of conducting the attest service (see **figure 2**).

Figure 2—SAS 70 vs. SSAE 16[10]		
Issue	**SAS 70**	**SSAE 16**
Focus	ICFR	ICFR (not technically different)
Basis	Management's choice	Risk basis for controls implemented/chosen
Period	Specific point in time: close	System description covers entire period of testing
Assertion	Audit	Attest
Management	Not applicable	Management's written assertion
Use	Basically, the public	User auditor, management of SO, management of user

The focus of both SAS 70 and SSAE 16 is on the ICFR of the user where some controls located at the SO are key controls. That said, some past SAS 70 audits addressed examinations of controls over subject matter other than financial reporting. SSAE 16 cannot be used legitimately to address these other controls, but they can be addressed in SOC-2 and SOC-3 (AT 101). Therefore, there is no difference between the two regarding focus, but in practicality, it may be better to restrict the use of SSAE 16 to ICFR.

Under the old SAS 70, the basis of controls evaluated was the prerogative of the SO's management. Management simply decided which controls to test and, as mentioned previously, sometimes was unable to properly identify key controls. There was no accountability or feedback to management about its choice because the auditors were forbidden from choosing them. In the new standard, management has to identify the risks associated with the service and financial reporting by the user and then identify controls that can mitigate those risks. The clarified SAS 70 provides for the user auditor to evaluate the proper choice of controls.

The period of the controls included in the report was simply a point in time in the old SAS 70. Under SSAE 16, the report covers the entire period of testing used in the report. This fact changes the service auditor's service/process considerably, in planning, testing and gathering evidence.

An obvious difference for the service auditor is the change from audit to attest. AICPA states that audit services are reserved for financial audit, and thus, what the service auditor does is attest. As such, the new standard was issued as an SSAE, applied under AT 101. Attest services are very definitive; management identifies specific procedures and the auditor then performs exactly those procedures (agreed-upon procedures [AUPs]). This approach fits the evaluation of controls for an SO.

A new requirement, among others, is that management must provide a written assertion about the fairness of the presentation of the description of the system and the suitability of the design (type I) and effectiveness (type II) of the controls. The written assertion is part of the final report by the service auditor.

One other noteworthy difference is the users of the report. SAS 70 was designed for multiple users and basically went into the public domain. For instance, many large companies would post their SAS 70 on their web site as a "seal of approval." SOC-1/SSAE 16 restricts use of the report to service/user management and user auditors; that is, it *cannot* be used as a marketing tool to prospects.

SOC-2: REPORT ON CONTROLS AT A SERVICE ORGANIZATION RELEVANT TO SECURITY, AVAILABILITY, PROCESSING INTEGRITY, CONFIDENTIALITY OR PRIVACY

This report type is intended to meet the need to understand an SO's internal controls related to such criteria as confidentiality, availability, processing integrity (the conventional information security triangle), security and privacy. The process of performing the attest follows the AICPA guide *Reports on Controls at a Service Organization Over Security, Availability, Processing Integrity, Confidentiality or Privacy* (to be issued in 2011). It is intended for use by stakeholders such as customers, regulators, business partners, suppliers and directors. Similar to SOC-1, there are two types: type I, report on management's description of a service organization's system and the suitability of the design of controls, and type II, report on management's description of an SO's system and the suitability of the design and effectiveness of controls. The reports are restricted in use (see **figure 1**).

SOC-2 should be of great interest to many SOs, including data centers and cloud computing companies. It also applies to any entity subject to HIPAA or the US Gramm-Leach-Bliley Act (GLBA), if nothing else to give owner-managers or board members assurance that they are in compliance with regulations. Banks could also use SOC-2 reports.

SOC-3: TRUST SERVICES REPORT FOR SERVICE ORGANIZATION

Trust Services was revised by AICPA in 2010 to incorporate the former SysTrust (security, etc., of a system) and Privacy (especially personal data) principle documents that were in place for years. This report type is intended to meet the needs of users who want assurance on the controls at an SO such as confidentiality, availability, processing integrity (again, the conventional information security triangle), security and privacy, but who do not have the need for or the knowledge necessary to make effective use of a SOC-2 report. The report is prepared using the AICPA/Canadian Institute of Chartered Accountants (CICA) Trust Services principles.[11] The reports are for general use and, therefore, can be freely distributed or posted on a web site. In fact, it is the only SOC report available to the public. Thus, if an SO wants to have an assurance service and use the subsequent report as a marketing tool, then, by default, the proper report is a SOC-3.

CONCLUSION

These new standards and SOC reports will provide the opportunity for IT auditors, especially CISAs, to perform needed services. IT auditors need to understand these reports, the standards and guidelines behind them, and the differences among them to provide the right service in the proper manner.

Because the controls of these SOC reports are so often embedded in IT, IT auditors, especially CISAs, will be needed to perform the attest services.

ENDNOTES

[1] See AU324 of the American Institute of Certified Public Accountants (AICPA) auditing standards for details of SAS 70.

[2] The user auditors had the option of changing the nature, timing or extent (most likely the latter) in place of examination of controls at the SO. However, there would be a need to do a lot of substantive procedures, and all would likely be manual procedures, which would be an expensive option.

[3] There are two types of SAS 70 reports: Type I (focused on fairness of controls put into place and suitability of the design of the controls) and Type II (same as Type I plus operating effectiveness of the controls). This article focuses on Type II.

[4] For more on SOC reports, visit the AICPA SOC site at *www.aicpa.org/soc*.

[5] Trust Services was changed in 2010 to include the previous SysTrust and Privacy services that have been around for years. The AICPA intends to release a new guide on Trust Services (SOC-2 and SOC-3) in 2011.

[6] SOC-2 differs from SOC-3 primarily in its distribution and the fact that no description of the SO system is required in a SOC-3 report.

[7] AICPA, Trust Services Principles, *www.aicpa.org/trustservices*

[8] AICPA, Generally Accepted Privacy Principles, *www.aicpa.org/privacy*.

[9] AICPA, *Reporting on Controls at a Service Organization*, SSAE 16, 2010

[10] There are a number of other differences between the clarified SAS 70/SSAE and the old SAS 70, which the author believes to be of a more minor nature for CISAs/IT auditors.

[11] AICPA, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, 2009