SOC Progress Report

Four Things Learned in the Field

Brian Vazzana, CISA, CITP, CPA, is an information systems (IS) and assurance services senior manager with BDO USA, LLP, an independent member firm of BDO International Limited, the fifth largest accounting services firm in the world. He manages the Chicago, Illinois, USA, and Milwaukee, Wisconsin, USA, IS assurance practices at BDO USA.

The new Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organizations Controls (SOC) reports became effective on 15 June 2011. Where user entities outsource certain business functions to third-party service organizations, the SOC reports examine the controls present at the service organizations and consider how those controls are designed and operate. These reports (as well as the corresponding controls) are examined by independent service auditors and, thus, provide user entities with a level of comfort with respect to those outsourced functions.

As the first year of reporting under these new standards has completed, now seems like a good time to reflect on a few things learned while performing these examinations.[1]

"I WANT YOUR SOCS"

"To SOC 1 or not to SOC 1?" That is the question. Perhaps the question should be: "To SOC 1 or SOC 2… or possibly, SOC 3?" Ultimately, the service organization determines which report best fits its needs, but service auditors also need to make sure that they have an appropriate handle on what their potential clients need and expect.

A SOC 1 (SSAE 16) examination and report focuses on the controls established by a service organization that are pertinent to the financial statements of its user entities (customers).[2]

SOC 2 and SOC 3 examinations and reports consider specific trust principles, namely security, availability, processing integrity, confidentiality and/or privacy of data and systems.[3, 4]

Is the service organization looking to provide comfort to a customer base where the financial statements of those customers are impacted by the service organization's controls, or is that customer base more concerned with the security, availability and integrity of the data processed by the service organization? Depending on the service organization's purpose and use of the report, and depending on the information specifically processed by that service organization, a different SOC may apply (see **figure 1**).

IT IS ALL IN THE DESIGN

It is important to remember that both the old SAS 70 guidance and the recent SOC 1 and SOC 2 guidance provide two types of report options (Type I and Type II). Among these various service organization reports, the basic difference between a Type I report and a Type II report is that a Type I report considers the design of controls at a single point in time, while a Type II report further considers the operating effectiveness of those controls over a specified period of time.[5, 6]

There are a number of subtle differences between the testing performed in conjunction with a Type II SAS 70 examination and report and that performed in conjunction with a SOC 1 examination and report. One nuance that is easier to miss is the consideration of the design of the service organization's controls.

Auditing under the old SAS 70 guidance, service auditors concerned themselves with the design of such controls *as of a point in time* and, then, tested operating effectiveness throughout the period under audit. SOC 1 forces auditors to expand their thought processes. Because design concerns are no longer considered as of a point in time, auditors need to understand the design of those key controls *throughout* the reporting period,[7] just as they need to test the operating effectiveness of those controls where a Type II report is concerned.

Service auditors are undoubtedly considering this nuance and taking extra effort to document and understand control design at the service organizations. As a forewarning, however, auditors need to be consciously aware that inquiry alone is not enough. Their initial walk-throughs with respect to control design

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.

Go directly to the article:

Figure 1—SOC Reports Comparison

REPORT	GUIDANCE	SUBJECT MATTER (SERVICE ORGANIZATIONS)	USERS
SOC 1	SSAE 16, *Reporting on Controls at a Service Organization* *AICPA Guide: Service Organizations—Applying SSEA No. 16, Reporting on Controls at a Service Organization (SOC 1)*	Controls relevant to user entities' internal controls over financial reporting	User entities' auditors; user entities' management; service organizations' management
SOC 2	AT 101, *Attestation Engagements* *AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2)*	Controls relevant to security, availability, processing integrity, confidentiality or privacy (if privacy, also compliance with the service organization's statement of privacy practices)	User entities' management and parties understanding: 1) The nature of the service provided 2) The interaction of systems among the service organization, user entities, subservice organizations and other parties 3) Internal control and its limitations 4) The applicable trust service criteria and risks/controls that address such criteria
SOC 3	AT 101, *Attestation Engagements* AICPA Technical Practice Aid, *Trust Services Principles, Criteria, and Illustrations*	Controls relevant to security, availability, processing integrity, confidentiality or privacy (if privacy, also compliance with the service organization's statement of privacy practices)	Anyone

allow service auditors to corroborate with various service organization personnel regarding the level or lack of control changes in a given reporting period. That said, auditors will need to add audit steps to ensure that they have considered control design beyond inquiry and a walk-through at a point in time.

SOC guidance does not allow service auditors to rely on prior-year controls as a means of assessing controls in the current reporting period.[8] Perhaps service auditors can use their understanding of previous control design to corroborate the level or lack of design change in the current year—to a greater extent than via inquiry alone or via inquiry and a walk-through at a point in time. As an example, a service organization has represented that operating system password parameters require complexity in the current reporting period, and the service auditor identifies that the control is designed as such via walk-through procedures and observation of the operating system's password policies. If the service auditor has corroborated the service organization's assertion that complexity enforcement is consistent with prior years by looking at prior-year examination documents, the auditor is probably more comfortable with the design of that control throughout the current period than via inquiry and observation at a single point in time.

Not every service organization retains the same service auditor indefinitely, so those prior-year work papers may not exist. Whether or not this is the case, the service auditor may want to consider the design of controls at multiple points in time rather than during one field visit. Auditors visiting their clients well in advance of the end of the reporting period should be cognizant of the need to refresh their testing. This roll-forward or refresh testing of controls serves to update the understanding of the design of key controls throughout the period and ensures that those controls are tested for operating effectiveness throughout the appropriate reporting period.

IT IS MANAGEMENT'S BABY

The new SOC standards have incorporated an additional requirement to the respective reports whereby management of the service organization is responsible for making certain assertions. The service auditor, meanwhile, must perform due diligence to ensure the reasonableness of the subject matter of the engagement (to which management is asserting) in conjunction with the results of the examination.

What assertions must management make? Considering SOC 1 reporting specifically, management must attest to the following:

- The description of its systems must fairly present those systems designed and implemented as of a specific date or period of time, depending on whether a Type I or Type II examination and report is performed.
- The controls related to the control objectives provided in management's description must be appropriately designed as of a specific point or period of time to achieve those control objectives (and those control objectives and related controls must be operating effectively in a Type II report).
- Management must select the criteria used in making the previous assertions.[9]

Furthermore, if the service organization relies on a second organization (a subservice organization) to perform some services, the service organization must provide a description of such outsourced services in its report. If the service organization describes the outsourced controls in its report, it must then provide a similar assertion from the subservice organization's management. Then, the service auditors must examine this assertion in conjunction with the audit, as well as examine the subservice organization's entity-level controls. Carving out the subservice organization's controls and simply acknowledging the services performed may prove the more efficient manner by which service organizations complete these reports, given possible confidentiality concerns by subservice organizations.

While the text of the overall assertion is given robust coverage within the guidance provided by the American Institute of Certified Public Accountants (AICPA), the manner in which the assertion is presented in the report is subject to interpretation. Some service organizations provide a formally executed document, signed and printed on company letterhead; others may simply provide the text of the assertion with an electronic signature and keep a formal copy on file. Ultimately, the manner of presentation should be discussed and agreed upon by the service organization and service auditor; it should be evident that management made its assertion in conjunction with the audit standards, and the assertion should be clearly segregated from the rest of the text in the document.

When must management make these assertions? Given that these SOC reports cover a defined period, service organizations cannot simply write the assertion on day one and ignore it for the remainder of the period. While it is a best practice for the service organization to actively monitor its controls and draft its assertion over the course of the examination period, management should not consider its assertion finalized until that period is completed. Otherwise, management does not assert to the operating effectiveness of the controls over the course of the entire examination period.

TO SOC 3 OR NOT TO SOC 3?

I started this article musing over preparing a SOC 1 examination vs. a SOC 2 examination, but when might a SOC 3 examination come into play?

A SOC 3 examination operates in a manner similar to that of a SOC 2; however, the report is written for a broader audience and, thus, provides a more limited discussion of the service organization's systems. Effectively, a service organization can freely distribute the report, including via a publicly displayed SOC 3 seal linked on its web site. Current and prospective customers can then access the report via this SOC 3 Report: SysTrust for Service Organizations seal.

It is interesting to note that there are certain limitations to SOC 3 reporting, of which service auditors and service organizations need to be aware. First and foremost, the SOC 3 report must consider the design and operating effectiveness of controls over a period; unlike SOC 1 and SOC 2, a Type I report option, in which controls may be attested to on a particular date, does not exist. Service organizations must take care to ensure that controls are operating over a reasonable period before considering a SOC 3 report.

Furthermore, the audit guidance expressly forbids carve-outs of controls within a SOC 3 report;[10] service organizations must either operate all of the key controls relevant to the report or they must include any key controls that have been outsourced to subservice organizations. With this in mind, the ability of service organizations to publish a SOC 3 report may be limited, particularly if such organizations rely on a third party for data processing or network hosting services. Ultimately, a company must operate its controls independently and effectively over an established period in order for a SOC 3 report option to be viable or to convince a subservice organization to provide an assertion with respect to any outsourced controls and allow the service auditor to test those controls at the subservice organization.

An unqualified SOC 3 audit opinion merits the SOC 3 seal; thus, if service organizations are finding that the above issues are present, a SOC 3 report may not be the preferred route.

CONCLUSION

The new SOC standards provide service organizations with expanded opportunities to provide comfort to their customers with respect to data security, availability and the like. The onus, however, is on those organizations to monitor and ensure the operating effectiveness of the key controls they design as well as to attest to such effectiveness. Meanwhile, service auditors need to remain diligent in ensuring that they are not simply adhering to the old SAS 70 approach to auditing these controls, but considering those subtle nuances that the new guidance provides. By doing this, both service auditors and service organizations provide greater value to these respective reports and greater comfort to their recipients.

ENDNOTES

[1] This article is based on the experiences of the author.

[2] American Institute of Certified Public Accountants, *AICPA Guide: Service Organizations—Applying SSAE No. 16, Reporting on Controls at a Service Organization (SOC 1)*, April 2011, paragraphs 1.03 and 1.10

[3] American Institute of Certified Public Accountants, *AICPA Guide: Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)*, May 2011, paragraph 1.06

[4] Katcher, Audrey; Suzanne Nersessian; David Palmer; John F. Hudson; *Service Organization Control Reports: A Closer Look at SOC 2 & SOC 3 Engagements*, AICPA Learning Center, American Institute of Certified Public Accountants, 2011

[5] *Op cit*, American Institute of Certified Public Accountants, May 2011, paragraphs 1.16 (a) & 1.16 (b)

[6] AICPA Auditing Standards Board, *Statement on Standards for Attestation Engagements No. 16: Reporting on Controls at a Service Organization*, American Institute of Certified Public Accountants, March 2010, paragraph 7

[7] *Ibid.*, paragraph 16

[8] *Ibid.*, paragraph A43

[9] *Op cit*, American Institute of Certified Public Accountants, April 2011, preface

[10] *Op cit*, Katcher *et al*