Feature

Common Myths of Service Organization Controls (SOC) Reports

Deepa Seshadri, CISA, CISM, is a senior manager in a Big Four firm with 15 years of experience as an internal control specialist. She has been involved in SAS 70/SSAE 16/ISAE 3402 reviews, third-party assessments, security review, infrastructure review, general computer controls review and application review engagements in various technical environments. Seshadri has been involved in a number of offshore development reviews, with engagements in the manufacturing, software, and banking and financial services sectors.

In today's dynamic environment, organizations face multiple challenges in terms of various standards and compliance requirements. They are required to provide certificates, opinions and reports to their customers for various purposes. While organizations need to provide assurance to their customers, often there is ambiguity on the certificate/opinion that will be relevant to an organization.

This article provides an overview of the Service Organization Controls (SOC) reports available. The article also aims to highlight the key mistakes or misnomers of usage of SOC reports and key pointers that organizations need to keep in mind to ensure their investments in such activities are fruitful and provide a real benefit to their customers.

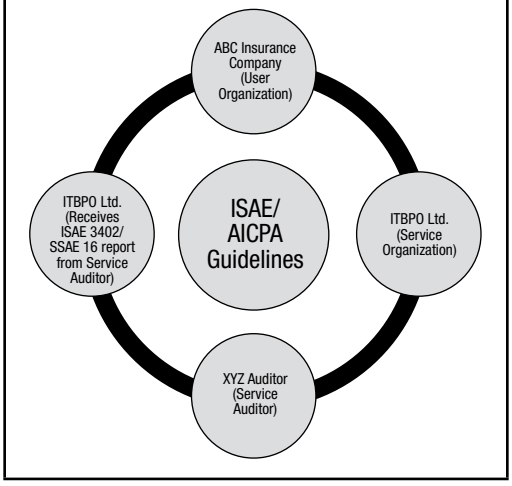
SOC 1 REPORTING PROCESS

In December 2009, the International Auditing and Assurance Standards Board (IAASB) issued a new International Standard on Assurance Engagements: ISAE 3402 *Assurance Reports on Controls at a Service Organization*. Shortly thereafter, the American Institute of Certified Public Accountants (AICPA) revised the Statement on Auditing Standards (SAS) No. 70 guidance around the execution of third-party service organization reports, releasing Statement on Standards for Attestation Engagements (SSAE) 16 *Reporting on Controls in a Service Organization*.

The following fictional example explains how the ISAE 3402/SSAE 16 process works. ABC Insurance Company outsources certain claims processing functions to service provider ITBPO Ltd. In ISAE 3402/SSAE 16 terminology, ABC Insurance Company is the user organization and ITBPO Ltd. is the service organization. To ensure that the claims are processed properly and adequate internal controls are in place at the service organization, the user organization appoints an independent Certified Public Accountant (CPA) or service auditor (XYZ Auditor) to examine and report on the service organization's controls. The service organization must respond to meet the needs of the user organization and obtain an objective evaluation of the effectiveness of controls that address operations, compliance and financial reporting at ABC Insurance Company. The CPA uses the ISAE 3402 or SSAE 16 SOC reporting options—SOC 1, SOC 2 and SOC 3—as the framework to examine controls and to help management understand the related risk factors. The service auditor, based on the IAASB/AICPA guidelines, performs the engagement and provides the report to ITBPO Ltd., which, in turn, shares the report with ABC Insurance Company.

The overall approach is depicted in **figure 1**.

Figure 1—Service Organization Reporting Approach



The service organizations can provide these reports to various user organizations to provide reassurance on the functioning of internal controls. A service organization can obtain this report by appointing an independent service auditor to perform the audit and provide a SOC 1 report. A SOC 1 report provides assurance on the controls that support internal controls over financial reporting This report can then be shared with user organizations and their auditors on request or as deemed necessary.

AICPA also provides for two other reports: SOC 2 and SOC 3. The SOC 2 and SOC 3 reports are used for reporting on controls other than the internal controls over financial reporting. One of the key differences between SOC 2 and SOC 3 reports is that a SOC 3 is a general-use report that can be provided to anyone while SOC 2 reports are for users as specified in the report.

SOC 1 MYTHS VS. FACTS

Service organizations frequently adopt the SOC 1 (ISAE 3402/SSAE 16 Type I and Type II) reports (SSAE 16 reports were formerly known as SAS 70 reports) for the wrong purposes. Some of the common errors surrounding of adoption are:

1. **These reports are certifications.** After completion of the work, organizations publish externally (to customers and stakeholders) that they are SOC 1- or SSAE 16-certified organizations.

   Fact: IAASB/AICPA guidelines clarify that ISAE 3402/SSAE 16 reports are not certifications. The guideline specifies that the reports are limited distribution reports and can be used by the service organization, user organization and user auditors only.
2. **These reports can be generally distributed to potential customers and used as a marketing tool.** Organizations distribute or plan to distribute Type I and Type II reports to potential customers, not considering the restriction in use of the report as part of the opinion.

   Fact: The SOC reports are issued by the service organization for a specific purpose. The audiences for the reports are clearly defined. The reports are generally limited-distribution reports and have specific restrictions on use.
3. **All operational areas can be included in SOC 1 reports.** Organizations blindly scope in operational, marketing and regulatory areas that do not have a direct/indirect impact on financial reporting.

   Fact: IAASB/AICPA guidelines specify that the SOC 1 report is applicable only to internal controls over financial reporting. In cases where organizations want to include other areas such as privacy or confidentiality, for example, they should adopt SOC 2/SOC 3 reports. The key difference is that SOC 1 reports are used for internal controls over financial reporting exclusively, while SOC 2/SOC 3 reports cover areas with respect to security, confidentiality, availability and privacy.
4. **Once the report is obtained, no controls need to be verified by the user organization.** Very often, stakeholders rely on SOC reports, see the controls defined in report on a stand-alone basis and do not consider the controls at the user-entity level while reading the report.

   Fact: While evaluating controls at the service organization, the controls at the user organization should also be considered.
5. **Application software can be made to comply with SSAE 16 requirements.** When software vendors develop particular application software that is used for financial reporting, they generally would like the software to be compliant to SSAE 16 requirements.

   Fact: Usually SOC 1 reports are assurance provided on the internal controls over financial reporting and not product evaluations.
6. **Work done by an internal auditor cannot be used for the purposes of SSAE 16 engagements.** The work of the internal auditor is not being used for purposes related to SSAE 16.

   Fact: The work of the internal auditor can be used for work related to SSAE 16, and whether to do so is the judgment of the service auditor.
7. **The service auditor needs to verify accuracy of the section related to "other information provided by service organization."** Service organizations provide considerable information (e.g., the business continuity plan) in this section. Organizations are under the assumption that accuracy of such information may not be verified by the service auditor.

Fact: The service organization has an obligation to verify accuracy of the other information provided by them; however, the service auditor will not opine on this section.

8. **The service auditor does not test the effectiveness of the entity-level controls.** The entity-level controls described by the service organization are used by the service auditor and no testing is performed on them.

   Fact: Service auditors do opine on entity-level controls, such as the control environment, risk assessment, information and communication, and monitoring.

9. **The period for testing of controls should be six months.** Organizations avoid performing SOC 1 reports if controls are newly designed, thinking SOC 1 reports are not applicable.

   Fact: There are specific circumstances when reports can be issued for a period of less than six months and the service auditor puts in the necessary restrictions in section 1 of the report.

CONCLUSION

AICPA's SSAE 16 and IAASB's ISAE 3402 standards define the purpose of SOC 1 reports as reports that provide assurance on the processes that support internal controls over financial reporting. Organizations should, therefore, take due care to understand the purpose of a SOC 1 report and also accurately define the scope of the processes to be covered. This report can be extremely useful to user organizations to understand the controls that impact financial operations and related IT controls at the service organization, especially in multiple-service-provider scenarios.