IT Audit Basics

Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CPA, is an associate professor of information systems (IS) at Columbus State University (Columbus, Georgia, USA). 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 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. His articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications.

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:

How to Properly Audit a Client Who Uses a Service Organization—SOC Report or No SOC Report

The new standards from the American Institute of Certified Public Accountants (AICPA) on service organization controls[1] have created a situation in which IT auditors, especially Certified Information Systems Auditors (CISAs), are particularly needed and useful. Usually, the controls of interest associated with the service organization (SO) are embedded in IT, about IT or are IT (e.g., automated controls). In the case of Service Organization Control (SOC) 2 and 3 report engagements, there is an even greater need for a subject matter expert, such as a CISA®, to identify and evaluate the controls associated with the five Trust Services Principles, which are the benchmarks of those engagements and associated controls.

However, this article focuses on SOC 1/Statement on Standards for Attestation Engagements (SSAE) No. 16 engagements because of the unique situation regarding the user auditors who are evaluating internal controls over financial reporting (ICFR), usually IT auditors, and their need to have a SOC 1[2] Type II[3] report to cover the controls of interest at the SO. This is complicated by the fact that sometimes the SOC 1 report is somewhat ineffective and may not exist at all. The latter is sometimes accompanied by the presence of another independent controls report, such as an International Organization for Standardization (ISO) report.

What should user auditors do under these circumstances and what is their responsibility to be compliant with the risk-based standards of the AICPA?

WHERE TO START?

The fundamental thought process is to remember what the standards require of the user auditor and to keep that as the driver of the audit plans, procedures and processes, rather than becoming engrossed in what is right, wrong, bad or strange.

Gain an Understanding of the Relevant Process

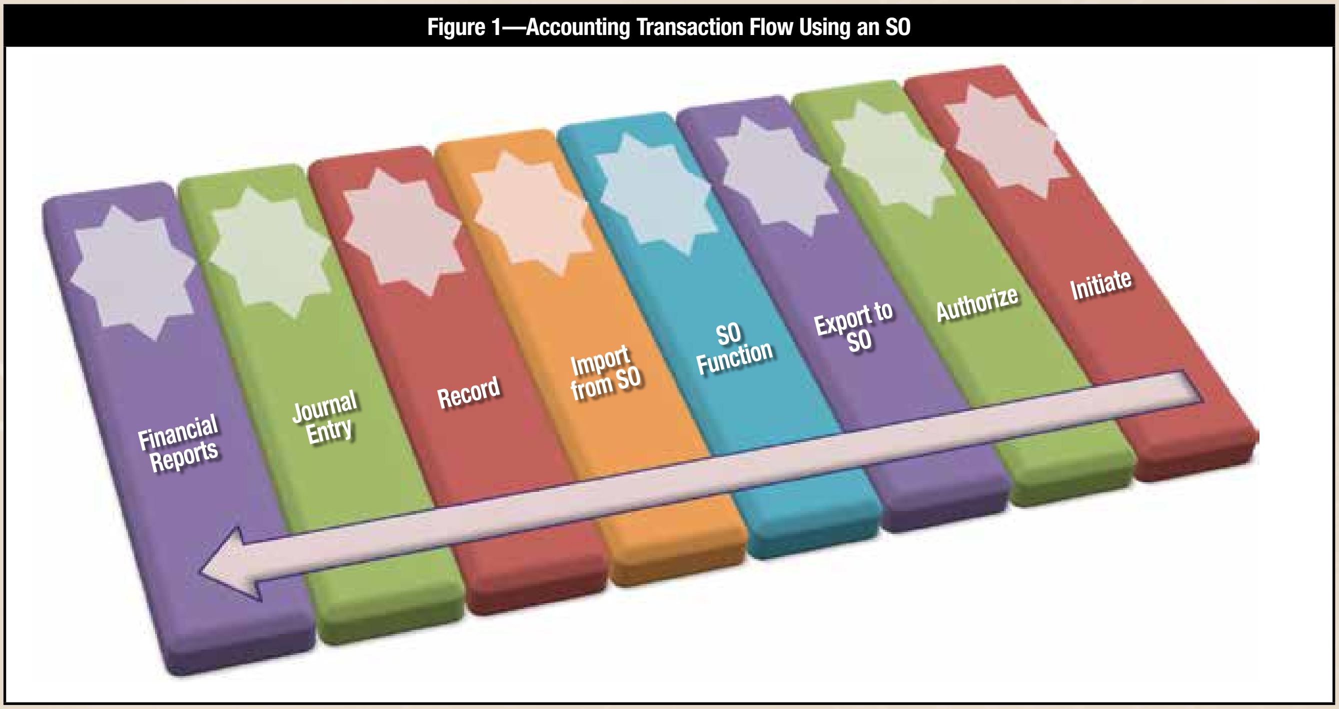
The risk-based standards[4] of the AICPA require the auditor to gain an adequate understanding of the processes involved—in this case, an understanding of the processes existing between the SO and user entity. A map or diagram is usually helpful in gaining an understanding of processes. The traditional accounting process flow is helpful to remember in developing a map or diagram: Initialize → Authorize → Record/Journalize → Report.

A more applicable flowchart would be one that incorporates the SO and its impact (see **figure 1**). The additional steps are key focal points. These three intermediate steps—export to SO, SO process/service and import from SO—help the IT auditor to identify where and what controls should be in place. They also represent the impact and effect of the SO on the accounting process flow and the underlying financial data. The user auditor must answer questions about exactly what processes are taking place, where they are taking place, how the SO processes interact and interface with user entity systems and data files, and what controls should be in place throughout all of those processes.

Gain an Understanding of the Export/Import Controls and Processes

The key to evaluating controls at the SO by the user auditor is to understand the process. An important element of these tasks is that data are usually being exported to the SO for it to process and provide its service, and then the resulting transactional data are imported by the user back into its accounting records. The user entity almost always has some controls and/or processes associated with the export and import steps that end up being complementary controls to the SO controls and its processes.

Figure 1—Accounting Transaction Flow Using an SO



The user auditor needs to gain an understanding of the three steps (**figure 1**) related to the SO. For example, if the SO is a payroll provider, the user might have some manual review of the pay data that are being sent to the SO to make sure they are complete and accurate (similar to assertions about this class of transactions or resulting account balances). That review process is a key complementary control to whatever controls the SO has in place to process the incoming data to generate payroll checks and to properly process all of the financial factors associated with payroll, such as taxes. Of course, the user entity might also have either an automated reconciliation or IT-dependent control[5] that serves the same purpose as manual review.

Later, when the checks and payroll data are imported back to the user, the incoming data might be subject to some reconciliation by the user. That control is complementary to those used by the SO in performing its service and can be manual, automated or IT-dependent.

Part of this analysis is not only evaluating what controls are in place, but also thinking through what controls *should* be in place, which will be referred to herein as the “anticipated controls.” The IT auditor needs to go through that thought process to determine if any key controls are missing.

The end goal is to have some comfort and assurance that the SO controls, the complementary user controls or a combination of the two provide adequate assurance about the underlying financial data.

SOC 1 REPORT EVALUATION

The next step would be to see if the SO has a SOC 1 report. If it does, the IT auditor would probably be asked to evaluate the SOC report to see if it adequately describes assurance over the anticipated controls. If the key relevant controls are addressed, the user auditor can proceed with the audit program. That evaluation process would include gathering evidence that those key relevant controls are designed effectively, placed into operation and operating effectively (i.e., a SOC 1 Type II report).

The key steps in fulfilling the user auditor’s responsibility are as follows:

- Make sure the controls identified in the SOC report (or alternative report) are the key relevant controls (clarified SAS No. 70).
  – If there is no SOC 1 report:
    - Consider an alternative applicable report, if present, and whether it can be used.

    - If no alternative is present or usable, focus on complementary controls.
    - If complementary controls provide an inadequate level of assurance, consider changing the nature, timing and extent of procedures to obtain the appropriate level of assurance (skip rest of steps).
- Obtain evidence that those controls (the anticipated controls) are designed effectively, were placed into operation and operated effectively during the period (something many alternative reports will not be able to provide, including even SOC 2 and SOC 3 reports).
- Document evidence. Standards do expect the documentation to map the controls at the SO to the complementary controls at the user and the applicable management assertions and account balance or class of transactions.
- Determine what tests of controls should be conducted, i.e., where risk of material misstatement (RMM) can be reduced, and allow the user auditor to reduce substantive procedures (change nature, timing and extent of procedures), e.g., reduce the sample size of a procedure.

If the IT auditor (user) relies on a SOC 1 report, the evaluation needs to be documented. The mapping mentioned previously is a key aspect of documentation as it relates to specific user management assertions and user complementary controls. The point is to connect specific SO controls to specific management assertions and account balances. That mapping could be accomplished by a sophisticated system, a spreadsheet or even some manual documentation.

The presence of a SOC 1 report is *not* justification to "check a box" marking the audit step as done with no further work. Such a reaction would result in a failure to comply with the risk-based auditing standards. Secondly, the presence of a SOC 1 report does *not* automatically lead to a reduction in sample size. Any reduction in sample size should be based on evidence obtained by applicable tests of controls.

The SOC 1 report, however, may not cover the anticipated controls to a level of sufficiency. For example, there could be one or more key anticipated controls that are not in place, or there could be one or more key controls that are not operating effectively as described in the SOC report. A Type I report does not provide for testing of controls and operating effectiveness and, thus, limits the ability to use the report to gain audit efficiencies. A SOC 3 report is of little to no value because it does not describe the tests and results. In either case, the user auditor needs to examine ways to change the nature, timing and extent of audit procedures to gain adequate assurance. For instance, extent could be changed by pulling a larger sample size to test transactions that were affected by the SO's processes. The user auditor also has the option of relying on complementary controls—if they sufficiently provide assurance over the SO's process and resulting transactions and, thus, provide compensating controls.

A REPORT, BUT NOT A SOC 1 REPORT

The preferred report is a SOC 1 report that gets the controls right—that is, a SOC 1 report that includes anticipated controls. However, there are occasions where no SOC 1 report exists. For instance, Paypal has a large presence in e-commerce payment systems, yet it has no SOC 1 report. Such entities do sometimes have an alternative report.

The key thing to remember in this situation is what was discussed in the "Where to Start?" section and in the basic steps list. That is, the process using a different type of report is basically the same process. Care should be taken in exercising judgment to consider comfort and assurance that the alternative report provides.

That is, it is possible that an alternative report could include the relevant, anticipated controls and some assurance about these controls. While it may not be as substantive or reliable as a SOC 1 report, that does not mean it cannot be used or relied upon. The process described previously should assist the IT auditor in reaching a sound conclusion about the SO and controls when using an alternative report.

Some examples of potential alternative reports are listed in **figure 2**. When an alternative report is used, it is particularly important to include an IT auditor because the average financial auditor may not have heard of these reports nor know how to interpret them.

Figure 2—Some Alternative Assurance Providers

ISO 9001	A set of eight principles designed to ensure that the quality of management systems meets the needs of customers and other stakeholders, while meeting statutory and regulatory requirements
ISO 22000	Considered a derivative of ISO 9000; a procedures-based vs. principles-based approach that focuses on industry-specific risk management systems (originally for food industry)
ISO 27001	An information security standard that reports on information security controls
AT601/AUP	Compliance attestation
TRUSTe	Specifically addresses online e-commerce sites; a seal of approval
PCI DSS	For credit card transactions and processors; a standard for security of using credit cards
FFIEC	Required for the banking industry; resulting report addresses many of the same controls in which the IT auditor would be interested.

NO REPORT

The user auditor is left with two choices if there is no SOC 1 report and no suitable alternative report. The first is to focus on complementary controls at the user and indicated in the steps listed previously. That is, the user auditor should evaluate complementary user controls and see if export/import controls reduce RMM to an acceptable level. The second is to examine the need to adjust the nature, timing and extent of audit procedures to obtain the necessary assurance.

CONCLUSION

The presence of an effective SOC 1 report is a great tool for the IT auditor who is involved in a financial audit for a user who has an SO that is in scope. However, it is not uncommon for an SO in scope to not have an effective SOC 1 report. Sometimes the report is present, but not effective. Sometimes there is no SOC 1 report at all. However, the IT auditor may be able to rely on either complementary user controls or an alternative controls report (e.g., an applicable ISO report). One key thing to remember is that the steps and auditor process are essentially the same in all cases because the goal or purpose is the same.

ENDNOTES

[1] Those standards include: (1) the replacement of the service side of SAS 70, Statement on Standards for Attestation Engagements (SSAE) No. 16, "Reporting on Controls at a Service Organization" and the concomitant Service Organization Control (SOC) 1 report, an engagement that is formulated as an agreed-upon procedure (AUP) and follows the applicable attest standard, AT 801, and which is specifically for evaluating internal controls over financial reporting (ICFR) related to the SO; (2) SOC 2 report, again is an AUP engagement that follows AT 801, but is about controls as described in the Trust Services Principles of the AICPA; and (3) SOC 3 report, again an AUP engagement following AT801, and is the only SOC report with unlimited distribution, and addresses the Trust Services Principles.

[2] While the SOC 2 report may provide adequate ICFR coverage on some entities, for the most part, a SOC 2 will not be an effective report to use for reviewing SO in terms of ICFR. A SOC 3 is even less effective because it has such limited information in it (e.g., it eliminates tests and results details).

[3] A Type I report provides for no operating effectiveness tests of the controls in place. Therefore, since the full scope of this process includes effects of the further audit procedures, especially opportunities for reducing substantive tests, the Type II report is the focus of this article. Any time SOC 1 is mentioned, it is by default referring to a Type II report.

[4] The risk-based standards include Statements on Auditing Standards Nos. 104–111. SAS No. 109 "Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement" is of particular interest. SAS No. 103 has some applicability as it relates to proper documentation.

[5] IT-dependent controls are those that are partly manual and partly automated.