TECH INSIGHTS

weaver Assurance • Tax • Advisory IT advisory services

TRUST AND TRANSPARENCY IN A CLOUDY WORLD

Service Organization Controls (SOC) Reporting for Financial and Data Security

In a world of cloud computing and business process outsourcing, how can companies know that their most sensitive data is secure? How can vendors ("service organizations") demonstrate their trustworthiness?

In 1992, the American Institute of CPAs (AICPA) created an auditing standard called "SAS 70" to guide audits of internal control at service organizations (companies that provide outsourced services). With these audits, customers receive some assurance that a service organization was properly processing and safeguarding the integrity of the financial data they process on behalf of their customers. However, SAS 70 audits were intended only to address processes performed by the service organization that are "likely to be relevant to users' internal control over financial reporting" (ICFR). In the post-Enron Sarbanes-Oxley compliance world, SAS 70 became a requirement for many service organizations providing services to publicly traded companies. Ultimately, SAS 70 became the de facto standard for service organizations to provide third-party assurance to their clients.

Business trends resulted in the rapid expansion of outsourcing beyond the traditional data processing services to include a variety of more IT-based services such as data center colocation, Software as a Service (SaaS), online backups, data hosting, cloud computing, etc. All of this resulted in SAS 70 being used to provide third-party assurance over a variety of subjects (nonfinancial) that it was not intended for including data security, privacy, disaster recovery, etc.

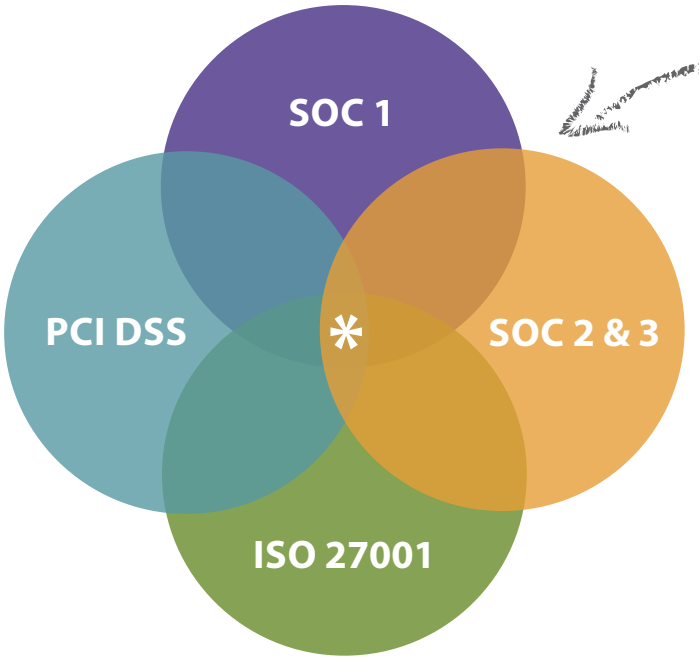
To address this issue, the AICPA developed a new standard that could keep up with new technologies and effectively address nonfinancial data. With the new Service Organization Controls (SOC ^{SM}) standards, published in 2011, the AICPA opened its umbrella to cover other information services that companies might purchase or outsource.

But What Are Service Organization Controls?

Let's begin with the term "Service Organization" (SO), which is used by the AICPA to describe outsourced service providers. The key element is that a SO performs services that directly or indirectly have an impact on customers' data, whether processing payment transactions, handling insurance claims, managing customer contact information, or just hosting software or hardware systems. If you provide services like these, you are a SO. If you purchase them, you are the client or user of a SO.

Controls are activities performed within a business process to ensure the quality and integrity of the information produced in that process. Controls may be built into computer systems themselves (e.g., a calculation or system setting), or they may

Third Party Assurance



SOs often have to provide ***multiple forms of assurance.*** Each one is intended for a different purpose, however, there is some ***overlap among the forms.*** It's important for SOs to identify ***points of synergy.***

be manual—requiring a human to perform them each time (e.g., an approval or a review).

A single, outsourced service may involve hundreds of separate controls, which are performed by the SO to ensure the integrity of the outsourced function. If these controls are inadequate, inappropriate or malfunctioning, it may cause transactional errors or allow data to become corrupted or compromised.

The point of examining service organization controls is to ensure that the proper controls have been implemented and designed correctly, as well as operating effectively to manage the risks associated with the outsourced services.

How Do SOC Reports Fit In?

Some SOs are asked to provide multiple forms of third-party assurance to their clients against various standards such as ISO 27001, PCI DSS, HITRUST (HIPAA), FISMA and more. SOC reports are a piece of the picture, but certainly not the only form of third-party assurance that a SO may be requested to provide. That said, as depicted in the diagram, each of these reports of assurance has some relation to the other. SOs faced with multiple forms of third-party assurance should discuss these requirements with their auditors, as there should be some synergy that can be gained by the SO in pursuing multiple third-party assurance paths.

The New Standards

The intent of the new standards, which went into effect in June 2011, was to provide options that would fix some of the abuses of SAS 70 in the past, and to bring the standard more in line with newly developed international standards (ISAE 3402). The AICPA released a new set of options for reporting on internal controls at service organizations:

- **SOC 1℠ — The direct successor to the old SAS 70 report** for examining financial controls, SOC 1 is delivered under SSAE 16 ("Statements on Standards for Attestation Engagements No. 16"). SOC 1 is a restricted use auditor-to-auditor report, in which scope is focused on financial reporting and is intended for use in customers' financial audits.

  There are two types of SOC 1 engagements:

  - Type 1, in which the auditor examines the company's controls to be sure they are in *place and designed appropriately.*
  - Type 2, in which the auditor also tests those controls to make sure they are *effective.*

- **SOC 2℠** — Also an auditor-to-auditor report, SOC 2 scope focuses on the Trust Services Principles as described in the AICPA document TSP 100.

SOC 2 engagements include any combination of the five principles:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

Companies **do not** have to include all five principles to meet the standard; they can select only the principles relevant to their business. Like SOC 1, SOC 2 examinations can be performed as Type 1 or Type 2. This examination is executed in accordance with the AICPA's AT 101 standard, "Attest Engagements."

- **SOC 3**℠ (SysTrust or WebTrust) – This examination is focused on the same scope as SOC 2, however the primary difference is that the resulting report is meant for broad distribution and therefore contains significantly less information. SOC 3's primary use for the SO is to convey to its clients that it has undergone an examination against the relevant principles and is often used as a marketing tool in conjunction with a SOC 2.

More than one of these standards may be relevant to some SOs. For example, a health insurance claims processor needs to assure clients about the accuracy of their financial data and the privacy of their patients' protected health information (PHI).

Contrary to common belief, **there is no "certification" under any of the SOC standards.** The auditor is providing an independent report to the SO based on the agreed scope. Although it's not the same as being certified, companies who have been issued a SOC 3 report are allowed to place a seal on their website and other marketing materials signifying this achievement. In addition, for no cost, the AICPA allows SOs who have undergone an SOC examination within the past year to utilize its SOC logo on their website.

Why Pursue a SOC Examination?

Any SOC engagement involves a significant commitment from the service organization. Beyond the cost of hiring an independent auditor, a SOC examination requires the company to compile detailed descriptions of its systems, to provide a written assertion that its controls were designed appropriately and are adequate to protect its clients, and to assist the service auditor throughout the project. There is no direct regulatory requirement to undertake these audits. *So why do it?*

When your clients, the users of your service, entrust their most sensitive financial or confidential data—or their customers' information—to a third party, they want to know that their information is safe. They want to know that results are reliable. They need assurances that their vendors are safeguarding their information against errors or intrusion.

The obligation to obtain a SOC report is typically passed to a SO contractually by their current or prospective clients. Larger (more sophisticated) organizations in regulated industries that may be planning to process sensitive information through a SO will normally want assurances over the services they acquire. The procurement function of such clients often translates the requirement for assurances to a SOC report. Therefore, SOs without SOC reports are often precluded from bidding on these opportunities. **Service organizations that have obtained a SOC report will have a competitive advantage.**

The Details – SOC 1: SSAE No. 16 Replaced SAS 70

Financial Assurance

Companies seeking assurance on **internal controls over financial reporting** should plan for a SOC 1 engagement. The AICPA developed the examination standard SSAE 16 along the lines of an international standard known as ISAE 3402. There are minor differences between the two standards, so companies serving international customers should consult with their auditor to identify the report that will meet the appropriate requirements.

How is SSAE 16 Different from SAS 70?

Although there are many technical differences between SAS 70 and SSAE 16, the two most significant changes to the SO include:

- **System of Internal Control**
- **Managegment's Assertion**

First, the description of the internal control systems must be much more detailed. "Systems" means "the services provided, along with all supporting processes, policies, procedures, personnel and operational activities that aid and facilitate the daily functioning of the service organization's core activities that are relevant to user entities" (i.e., your clients).

Organizations cannot merely list these services and processes. They must describe how the system captures and reports data; control objectives and related controls; and elements of internal control, including the control environment, activities, communication, risk assessment and monitoring.

Second, SSAE 16 requires a "written assertion" from management that confirms:

1. The system description is accurate and complete.
2. Control objectives and controls themselves were suitably designed and (for a Type 2 report) are operating effectively.

Design or Design and Operation? Type 1 and Type 2 Reports

A Type 1 report is focused on "a point-in-time." It examines the design of the system, the control objectives (i.e., identified risks) and the controls designed to reduce those risks. It answers the question, "Are the control systems designed properly to protect these systems and data?"

A Type 2 report asks, "Do those controls work?" Such an examination requires the auditor to actually test the controls and determine whether the controls accomplished what they were intended to over a specified period of time.

Typically speaking the Type 1 report is normally obtained only as a stepping stone to obtaining a Type 2 report in the future. **Clients or users generally want a Type 2 report.**

Neither report is intended for distribution to prospective customers or for use as a marketing tool. The reports contain detailed information that make them **inappropriate for public distribution.**

The Details – SOC 2 and 3: The Trust Service Principles

Data Integrity and Security

The other two SOC reports are performed under a different AICPA standard known as AT Section 101. Where SOC 1 assessments focus exclusively on ICFR, SOC 2 and 3 involve any combination of the following Trust Services Principles:

1. **Security**
2. **Availability**
3. **Processing Integrity**
4. **Confidentiality**
5. **Privacy**

Business trends resulted in the rapid expansion of outsourcing beyond the traditional data processing services to include a variety of more IT-based services such as data center colocation, Software as a Services (SaaS), online backups, data hosting, cloud computing, etc.

SOs can define the scope of a project to include any or all of these principles, depending on what applies to their operations. Auditors are not required to perform evaluations on irrelevant criteria, and this **flexibility helps control costs.**

Auditor to Auditor: SOC 2

Like a SOC 1 report, a SOC 2 report contains detailed information about internal controls, the appropriateness of their design and their operating effectiveness. A SOC 2 report would be appropriate, for example, for a backup service provider where data confidentiality is paramount. Clients of an online contact-management system or project tracking solution might also find such a report useful.

Similar to a SOC 1, SOC 2 assessments can be performed as Type 1 (design) or Type 2 (design and operation). SOC 2 also contains similar restrictions on report usage, although it is permitted for SOs to send their SOC 2 reports to prospective users as well as existing users.

Intended for Public Consumption: SOC 3

A SOC 3 engagement does not result in a detailed report, but a general report analogous to an auditor's opinion and a seal that **can be displayed on the service organization's website**. This report can be used for **marketing purposes**; it merely summarizes the findings of whether the service organization achieved the appropriate trust services criteria.

Although the SOC 3 report is a high-level summary, the examination itself is a Type 2 engagement including tests of controls. Therefore, a SOC 3 assessment can be thought of as a SOC 2, Type 2 engagement with a different reporting output.

Requirements of the Service Organization

Getting Ready

Only CPA firms can perform SOC assessments, and not all CPAs are qualified. Service organizations should look for a CPA firm with experience performing these engagements, preferably for other clients in the same industry.

The service organization should work with the firm to define the scope of the exam, the control objectives, or relevant principles and criteria, as well as the scope of testing for a Type 2 report. Setting these parameters early on will help prevent delays and cost overruns.

It may be wise to perform a **"readiness assessment"** before beginning the actual SOC examination itself in order to ensure a good final report. Organizations can do this internally if they have the skills and capacity; they can also request help from the firm performing the actual assessment or from a firm that specializes in helping companies prepare for SOC examinations.

During the Assessment

The first step of a SOC engagement is for the service organization's management to prepare a **system description** and a **written assertion** from management to the auditor. The firm performing the assessment will offer guidance, however these are requirements of the service organization itself.

The **system description** must be thorough and detailed. SOs that previously performed SAS 70 examinations will discover that the SSAE 16 standard requires a much deeper dive into their processes. This is how SOC reports define a "system":

> *The services provided, along with all supporting processes (technological or manual), policies, procedures, personnel, and operational activities that aid and facilitate the daily functioning of the service organization's core activities that are relevant to user entities.*

In other words, it's defined as any activity or process relevant to the defined control objectives or principles and criteria.

The **written assertion** is a positive statement that the controls are appropriately designed to accomplish their objectives, and in the case of a Type 2 examination, that the controls are operated effectively throughout the reporting period. The firm will help guide the writing, but management itself must produce the statement.

A Report or a Seal? Choosing the Right SOC

The choice of SOC 1, 2 or 3 comes down to what kind of information is being handled and the SO's goals:

- Protecting financial transactions and data? **SOC 1**
- Protecting online security, privacy, confidentiality, availability and integrity? **SOC 2 or 3** (depending on the report distribution needs)

SOs should work with the auditor to define their goals and concerns before beginning the project. Any of these engagements require significant time, effort and dollar investment. At the end, though, a successful SOC engagement will assure SOs and their customers that their sensitive information is being handled appropriately.

FOR MORE INFORMATION:

AICPA Standards
www.aicpa.org/SOC

Canadian Institute of Chartered Accountants
WebTrust and SysTrust licensing
www.webtrust.org

Weaver
www.weaverllp.com

CONTACT US

BRIAN THOMAS, CISA, CISSP
Partner, IT Advisory Services
Brian.Thomas@weaverllp.com
713.800.1050

NEHA PATEL, CPA, CISA
Senior Manager, IT Advisory Services
Neha.Patel@weaverllp.com
972.448.9804

Weaver has offices throughout Texas.