



# New Reporting Options For Service Organizations

*New reporting standards are allowing service organizations greater flexibility to address the risk and governance concerns of their user organizations.*

The long standing SAS 70 audit standard for reporting on controls at a service organization is now superseded by the SSAE 16 attestation standard.

Statement on Standards for Attestation Engagements (SSAE) No. 16, "Reporting on Controls at a Service Organization," does not significantly overhaul the reporting process but does include the following changes:

- An increased focus on the proper application of the standard and use of the report
- Modifications to the form and content of the previous SAS 70 reporting format
- Written management assertion accompanying the report

The AICPA recently introduced a **Service Organization Controls (SOC)** reporting structure consisting of three types of reports, including SSAE 16. These SOC reports are designed to meet a specific user need and are comprised of the following:

## ▶ New Reporting Standards

SOC 1	SOC 2	SOC 3
<ul style="list-style-type: none"> <li>- SSAE No. 16</li> <li>- Restricted use report</li> <li>- Type I or II</li> <li>- Reports on controls for <u>financial statement audits</u></li> </ul>	<ul style="list-style-type: none"> <li>- Attest Standards, AT 101</li> <li>- Trust services principles and criteria</li> <li>- Restricted use report</li> <li>- Type I or II</li> <li>- Reports on controls to <u>compliance or operations</u></li> </ul>	<ul style="list-style-type: none"> <li>- Attest Standards, AT 101</li> <li>- Trust services principles and criteria</li> <li>- General use report</li> <li>- Public seal</li> <li>- Reports on controls to <u>compliance or operations</u></li> </ul>

## ▶ Service Organization Control Reports

Many types of service organizations may benefit from a one time or annual Service Organization Control report. The type of report your organization would



require depends upon the clientele that you service and the regulatory laws with which either you or they must comply. Service organizations that may benefit from these types of reports include:

- Regulated Industries (Financial Services, Healthcare Providers) and organizations that process personal information such as credit card numbers, social security numbers, HIPPA compliant information, bank account numbers, third party benefit administrators and more.
- Organizations that provide key service operations such as payroll processing, accounting services, inventory management, logistics, electronic records retention and more.
- IT Service Organizations including Software-as-a Service (SaaS), Cloud Service Organizations, Data Center, Call Centers and more.

## ▶ Types and Content of Reports

The SOC 1 and SOC 2 may be issued in either a Type I or Type II format.

- A **Type I report** describes the service organization's description of controls as of a specific date.
- A **Type II report** includes detailed testing of the service organization's stated controls over the review period, in addition to the description of controls. Type II reports contain 4-5 sections, including the Auditor's Report (Section I), the service organization's management assertion (Section II), description of controls (Section III), description of the auditor's operational effectiveness and the results of the tests (Section IV) and an optional "other information" provided by the service organization (Section V).

# New Reporting Options For Service Organizations

Here are brief descriptions of the three new SOC reports:

A **SOC 1 report** results from an engagement performed under the new standard, *Statement on Standards for Attestation Engagements, SSAE 16 – Reporting on Controls at a Service Organization*. This report requires the same level of evidence and assurance expected under the former SAS 70 service auditor engagement. It essentially fills the role of a SAS 70 report as it was originally intended.

**SOC 2 reports** provide detail on controls at a service organization covering *security, availability, processing integrity, confidentiality or privacy*. Its use is generally restricted to certain identified users who, among other things, have some knowledge of the nature of the services that the service organization provides. The SOC 2 report can offer greater assurance to customers and stakeholders about internal controls that are related to operations and compliance at the service organization.

**SOC 3 reports** are Trust Service examination reports. They address the same subject areas as a SOC 2 report, but in a shortened version that can be used in a service organization's promotional efforts and on its website.

## ▶ Difference Between SOC 2 and SOC 3 Reports

- SOC 3 is a general-use report
- SOC 3 provides only the auditor's report on whether the system achieved the trust services criteria (no description of testing or results of tests performed is included)
- Permits the service organization to use the SOC 3 seal on its website



## ▶ Who Benefits?

When it comes to the various reporting options, there are several parties who may directly benefit from a SOC report.

**1. Consumers.** Many organizations process personal information that is sensitive and must be kept strictly confidential. By obtaining a SOC 1 or 2 report, organizations are proving they have effective controls in place to safeguard such information from any internal and external risk that may breach security measures.

**2. End Users.** Many companies that outsource payroll, accounting, and other services require that contracted service organizations obtain a SOC report because it allows internal and external auditors to gain a level of confidence regarding the controls surrounding these processes and saves time that may be otherwise wasted on unnecessary testing.

**3. Service Organizations.** Service organizations will benefit by undergoing a SOC report. During the audit, management will be notified of both areas that need improvement and areas that are designed and operating effectively.

## ▶ Additional Services

- Payment Card Industry (PCI) data security standards assessments
- Network vulnerability assessments
- Network penetration testing
- HIPAA compliance assessments

## ▶ Alpern Rosenthal Service Team



**Brian Kirkpatrick, MBA, CIA**  
*Co-Director and Senior Manager,  
Business Advisory and Risk Services*

[e] [bkirkpatrick@alpern.com](mailto:bkirkpatrick@alpern.com)  
[p] 412.281.7692 x497