A COALFIRE CONTROLS PERSPECTIVE

SOC Reports – Which one is right for you?
by Jamie Kilcoyne, CPA, CIA, CISA, CITP, CAMS
Managing Director, Coalfire Controls, LLC
Which SOC is right for you?

In 2011, the American Institute of Certified Public Accountants (AICPA) introduced a new reporting framework for service organizations, Service Organization Controls (SOC) reports. The new framework provides a mechanism for service organizations to demonstrate to their customers and other constituents that they have internal controls in place to address a variety of risks. Many organizations are having a difficult time determining which of the new SOC reports is appropriate for them. The purpose of this paper is to clarify the different types of reports to help service organizations and their auditors select the correct reporting format.

SOC 1 Report: What is it?

Reports on Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting: SOC 1 engagements are performed under SSAE 16, Reporting on Controls at a Service Organization. This standard specifically disallows the reporting of nonfinancial controls. SOC 1 reports are examination engagements undertaken by a service auditor to report on controls at an organization that provides services to user entities when those controls are likely to be relevant to user entities’ internal control over financial reporting.

There are two types of SOC 1 reports

- **Type 1** – A report on management’s description of the service organization’s system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.
- **Type 2** – A report on management’s description of the service organization’s system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.

Examples of organizations that receive SOC 1 reports are payroll processing companies, insurance claims administrators, trust departments of banks, loan processors and investment custodians.

SOC 2 Report: What is it?

Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy: SOC 2 engagements use the predefined criteria in Trust Services Principles, Criteria and Illustrations, as well as the requirements and guidance in AT Section 101, Attest Engagements, of SSAEs (AICPA, Professional Standards, vol. 1). A SOC 2 report is similar to a SOC 1 report.

Either a type 1 or type 2 report may be issued and the report provides a description of the service organization’s system. For a type 2 report, it also includes a description of the tests performed by the service auditor and the results of those tests.
The primary difference between SOC 1 and SOC 2 reports is that SOC 2 reports do not include information relevant to user entities’ internal controls over financial reporting. SOC 2 reports specifically address one or more of the following five key system attributes:

- **Security** – The system is protected against unauthorized access (both physical and logical).
- **Availability** – The system is available for operation and use as committed or agreed.
- **Processing Integrity** – System processing is complete, accurate, timely and authorized.
- **Confidentiality** – Information designated as confidential is protected as committed or agreed.
- **Privacy** – Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity’s privacy notice, and with criteria set forth in Generally Accepted Privacy Principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants.

Examples of organizations that are candidates for SOC 2 reports are data centers, co-location facilities, managed service providers and organizations that provide software as a service (SaaS).

**SOC 3 Report: What is it?**

SOC 3 engagements use the predefined criteria in *Trust Services Principles, Criteria and Illustrations* that also are used in SOC 2 engagements. The key difference between a SOC 2 report and a SOC 3 report is that a SOC 2 report, which is generally a restricted-use report, contains a detailed description of the service auditor’s tests of controls and results of those tests as well as the service auditor’s opinion on the description of the service organization’s system.

A SOC 3 report is a general-use report that provides only the auditor’s report on whether the system achieved the trust services criteria (no description of tests and results or opinion on the description of the system). It also permits the service organization to use the SOC 3 seal on its website. SOC 3 reports can be issued on one or multiple Trust Services principles (security, availability, processing integrity, confidentiality and privacy).

**Summary**

Auditors of service organizations can provide valuable guidance in selecting the most appropriate SOC report, but the key consideration to keep in mind is this: if the SOC report will address financial reporting risks and cover controls relevant to user entities’ financial reporting, then SOC 1 is likely the right reporting format. If the report will cover non-financial reporting controls, then SOC 2 or 3 is likely the right format.