WHITE PAPER

SOC 1 VS. SOC TYPE 1
CLARIFICATION ON THE DIFFERENT FORMS OF SOC REPORTING

By April Arruda, CPA and Mike Mellor, CPA, DiSanto, Priest & Co.

DiSanto Priest & Co.
Certified Public Accountants

In the modern business world, it has become common practice for organizations to outsource certain functions or business processes to third parties, rather than performing all processes “in-house.” When an organization decides to outsource a core business process to a third party, the risks of the service organization often times become the risk of the user entity. Therefore, now more than ever, it is important to understand the different forms of Service Organization Control reports and the types of risk that are addressed by each one.

For those who are not overly familiar with Service Organization Controls (SOC) reporting, a SOC report is a report on the controls at a service organization, an entity that processes information or handles business transactions on behalf of customers, relevant to the user entities or customers of that service. This report is typically prepared by a Certified Public Accountant (CPA), as it assesses internal controls. **SOC reports are designed to help service organizations evidence security and reliability in their service delivery of information and data.** Based on the type of service provided, user entities may want or have a need for a variety of internal control information. As a result, there are different kinds of SOC reports, each geared toward the purpose and expected user of that report.

©2017 DiSantoPriest

SOC 1 REPORTS

First and foremost, as the title of this posting implies, a SOC 1 report and a SOC Type I report do not refer to the same thing. Specifically, the AICPA has established three SOC reporting options, SOC 1, SOC 2, and SOC 3 reports. **Within the SOC 1 and SOC 2 options, the service organization can obtain either a Type I or Type II SOC report.** Let's elaborate.

The SOC 1 report is a report on controls at a service organization that is relevant specifically to the user entity's internal controls over financial reporting. These controls often relate to classes of transactions, procedures for processing and reporting transactions, accounting records maintained within a computer system, etc. SOC 1 reports are prepared in accordance with SSAE No. 16 (previously SAS No. 70) and are often intended for CPAs auditing the user entity, but can also be used by management and the user entity's management.

Within the SOC 1 report category, the service organization is issued either a Type I or Type II report. A Type I report provides an explanation on the appropriateness of the design of controls. In comparison, a Type II report also provides an explanation on the appropriateness of the design of controls, as well as detail on the operating effectiveness of the controls. Further, a Type I report covers a specified date (point in time), whereas a Type II report covers a specified range of dates (period).

SOC 2 REPORTS

Similarly, the SOC 2 report is also issued as either a Type I or Type II report as described above. However, a SOC 2 report is not intended for controls over financial reporting. Instead, the SOC 2 report is relevant to controls at a service organization over 5 key areas: security, availability, processing, integrity, confidentiality, and privacy. The SOC 2 report is prepared in accordance with Attestation Standard 101 and is often intended for use by management of user entities and potential customers, but can also be used by auditors of user entities when reporting on compliance with the Sarbanes-Oxley Act.

SOC 3 REPORTS

Lastly, we come to the SOC 3 report. A SOC 3 report is similar to a SOC 2 report in that it reports on controls at a service organization relevant to security, availability, processing, integrity, confidentiality, and privacy. It is also prepared in accordance with Attestation Standard 101. **However, the SOC 3 report is a general use report that provides only the auditor's opinion on whether the system achieved the trust services criteria.** There is no description of tests and results or opinions on the description of the system; and the report does not fall into the Type I or Type II categories. The SOC 3 report is the only form of SOC report that does not have a restricted use and can, therefore, be freely distributed.

In summation, there are various kinds of SOC reports, and although the similar naming convention may be confusing, service organizations should request the report that meets the needs of the intended users, i.e. management, user entities, the auditors of user entities, etc. The table below is a summary of the various SOC reports discussed.

©2017 DiSantoPriest

Topic	SOC 1 Report	SOC 2 Report	SOC 3 Report
Authoritative Guidance	SSAE No. 16	Attestation Standard 101 *AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy as well as the criteria defined in Trust Services Principles, Criteria and Illustrations.*	Attestation Standard 101 *AICPA Technical Practice Aid, Trust Services Principles, Criteria and Illustrations*
Type I or Type II Designation	Yes	Yes	No
Restricted Use Report	Yes	Yes	No
Report Users	User auditors, user management	Management, user management, Regulators	Any user or potential user
Purpose of Report	Reports on controls of financial statement audits	Reports on controls related to compliance or operations	Reports on controls related to compliance or operations

©2017 DiSantoPriest

Topic	SOC 1 Report	SOC 2 Report	SOC 3 Report
Applicability	Reports on controls at a service organization relevant to user entities internal control over financial reporting.	Reports on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy.	Similar to a SOC 2 report, but the 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 Report and Systrust for Service Organization's Seal on its website.

About Disanto, Priest & Co.
Disanto, Priest & Co. is a full service public accounting firm headquartered in Warwick, Rhode Island with expertise in assisting companies in evaluating their current and planned third party assurance needs, like those described above. Give us a call if you need assistance as we would be glad to talk with you about your needs.

Headquarters
117 Metro Center Boulevard
Suite 3000
Warwick, Rhode Island 02886
Telephone 401.921.2000
Facsimile 401.921.2010
www.disantopriest.com

©2017 DiSantoPriest