October 30, 2018

SOC Report Refresher: What Are the Different Types of SOC Reports?

CYBERSECURITY, SOC
BY ANDREW JACKSON

The rise of cloud computing has played a key role with businesses that outsource certain functions to service organizations. Since such organizations are now being held accountable for computing, processing, storage and the protection of customer data, entities are requiring them to complete a System and Organization Control (SOC) report prior to engagement.

Additionally, the constant threat of cybersecurity breaches has resulted in assurance needs for management of all organizations, so the AICPA has introduced a new type of SOC report that any organization can engage a CPA to perform to evaluate its cybersecurity risk management program.

Below is a refresher on all the current types of SOC reports and the differences between them.

Overview of Different SOC Examinations

- **SOC 1** engagements are examinations of the internal control over financial reporting at a service organization. These engagements are performed under SSAE 18 (Statement on Standards for Attestation Engagements No. 18). The SOC 1 guide provides guidance to practitioners in examining and reporting on a service organization's controls over the services it provides to user entities when those controls are likely to be relevant to user entities' internal control over financial reporting. SOC 1 examinations are warranted if a service organization processes financial transactions on behalf of its customers that affect its client's financial reporting. Examples of SOC 1 clients would be payroll providers, claims processor and third-party benefit administrator organizations.
- **SOC 2** examinations are mainly used for service organizations that host or process other types of data for clients that do not impact financial reporting. Service organization clients require assurance over how vendors handle their data securely and want to ensure that their data is available when needed. SOC 2 examinations include reporting on a combination of one or more of the following Trust Service Categories: security, availability, confidentiality, processing integrity and privacy. Service organizations like datacenters and Software-as-a-service (SaaS) organizations are prime candidates for SOC 2 examinations.
- **SOC 3** examinations result in general-use reports that can be distributed to any party and made available publicly on a service organization's website. SOC 3 reports do not include a description of the service auditor's tests of controls and the results thereof. The procedures performed in a SOC 3 are substantially the same as the procedures performed in a SOC 2; therefore, service organizations may choose to have

the service auditor issue two reports as a result of a SOC 2 examination – a SOC 2 and a SOC 3.

- **SOC for Cybersecurity** engagements can be performed for any organization. This type of SOC report involves practitioners examining and reporting on an entity's cybersecurity risk management program. In the examination, the subject matter is (a) the description of the entity's cybersecurity risk management program in accordance with the description criteria and (b) the effectiveness of controls within that program to achieve the entity's cybersecurity objectives based on the control criteria. The AICPA's guide "Reporting on an Entity's Cybersecurity Risk Management Program and Controls" presents description criteria that may be used when preparing and evaluating the description of the entity's cybersecurity risk management program and applicable trust services criteria (which can be used as control criteria).

For additional information on SOC examinations, visit Schneider Downs' "Frequently Asked Questions about SOC Reports" here: https://www.schneiderdowns.com/soc-report-faq.

Please contact us if you are interested in learning about our experience performing SOC examinations and how we can help you with your SOC reporting needs.

You've heard our thoughts... We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.