September 5, 2017

SOC for Cybersecurity Reports: Overview and Comparison to SOC 2 Reports

CYBERSECURITY, HEALTH CARE, SOC
BY SCHNEIDER DOWNS PROFESSIONAL

The AICPA recently updated the System and Organization Controls (SOC) reporting suite of services with the releases of Statement on Standards for Attestation Engagements (SSAE) No. 18; the 2017 Trust Services Criteria for Security, Availability, Processing Integrity (2017 TSC); and the cybersecurity risk-management program and controls reporting framework (SOC for Cybersecurity). This blog post provides an overview of the SOC for Cybersecurity reporting framework, and highlights some of the key differences between SOC for Cybersecurity and SOC 2 reports.

SOC for Cybersecurity Reporting Framework

A SOC for Cybersecurity Report is an examination that provides stakeholders with information regarding an organization's cybersecurity risk-management program. The main objectives of the SOC for Cybersecurity Report are to provide transparency to stakeholders regarding the entity's cybersecurity risk-management program and a means of independently assessing the effectiveness of cybersecurity controls.

The AICPA is in the process of creating three reporting levels for the SOC for Cybersecurity Report: entity, service provider, and supply chain. Each reporting level will provide different benefits as follows:

- **Entity**: Provides transparency to key elements of an organization's entitywide cybersecurity risk-management program.
- **Service provider**: In addition to entity-level benefits, provides sufficient, detailed information to address user entities' vendor risk-management needs.
- **Supply chain**: In addition to entity-level benefits, provides sufficient, detailed information to address the user entities' supply chain risk-management needs.

The AICPA determined that the entity-level reporting framework should be developed first. Both the service provider and supply chain level reports are still in the planning stages. The following components only pertain to the entity-level report:

- **Management's description**: A management-prepared narrative description of the entity's cybersecurity risk-management program.
- **Management's assertion**: An assertion that the description was prepared in accordance with the description criteria and that the controls implemented as part of the program

were effective in achieving the entity's cybersecurity objectives.

- **Practitioner's opinion**: A CPA's opinion on the description of the entity's cybersecurity risk-management program and the effectiveness of controls within that program to achieve the entity's cybersecurity objectives.

Differences between SOC 2 Reports and SOC for Cybersecurity Reports

A SOC 2 engagement is an examination on the fairness of the presentation of management's description of the service organization's system, the suitability of the design of the controls included in the description, and, in a type 2 engagement, the operating effectiveness of those controls. This engagement is performed in accordance with the attestation standards and the AICPA guide, *Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)*. Though there are many similarities between a SOC for Cybersecurity Report and a SOC 2 Report, there are distinct differences. Here are a few of note:

- **Purpose**
  - SOC for Cybersecurity – To provide intended users with useful information about an entity's cybersecurity risk-management program for making informed decisions.
  - SOC 2 – To provide a broad range of system users with information about controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy to support users' evaluations of their own systems of internal control.
- **General or Restricted Use**
  - SOC for Cybersecurity – Appropriate for general use; however, practitioners can decide to restrict the use of their report to specified parties.
  - SOC 2 – Restricted to user entity personnel and specified parties, such as independent auditors and practitioners of user entities, prospective user entities, and regulators, who have sufficient knowledge and understanding of the system.
- **Description Criteria**
  - SOC for Cybersecurity – Specific description criteria were developed and can be found in the AICPA guide, *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*.
  - SOC 2 – Paragraphs 1.26–1.27 of the AICPA guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)*, contain the criteria for the description of the service organization's system.
- **Control Criteria**
  - SOC for Cybersecurity – The 2017 TSC or other control frameworks, such as ISO 27001 and NIST SP 800-53, are considered suitable criteria for evaluating the design and operating effectiveness of controls.
  - SOC 2 – The 2017 TSC are the criteria for evaluating the design and operating effectiveness of controls.
- **Contents of the Report**
  - SOC for Cybersecurity – The report contains management's description, a written assertion by management, and a practitioner's opinion about whether the description

was presented in accordance with the description criteria, and whether the controls within that cybersecurity risk-management program were effective in achieving the entity's cybersecurity objectives based on the control criteria. The report does not contain a description of the practitioner's tests of controls and the results of those tests.

- SOC 2 – The report contains management's description, a written assertion by management, and a service auditor's opinion on the fairness of the presentation of the description of the service organization's system and the suitability of the design and operating effectiveness of the controls (Type 2) to meet the criteria. A Type 2 report will also include a description of the service auditor's tests of controls and the results of those tests.

With all the changes in the SOC suite of services, now is a good time to educate your clients on the benefits of engaging a CPA firm to perform a SOC for Cybersecurity examination and how SOC for Cybersecurity Reports and SOC 2 Reports are similar and different. For more information, contact Schneider Downs or visit the Our Thoughts On blog.

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.