SOC FOR CYBER

schellman

Quality, above all.

1. What is SOC for Cybersecurity?

In April 2017, the AICPA introduced a cybersecurity risk management reporting framework called System and Organization Controls (SOC) for Cybersecurity to help organizations communicate the effectiveness of their cybersecurity risk management program. SOC for Cybersecurity is an examination engagement performed in accordance with the AICPA's clarified attestation standards on an entity's cybersecurity risk management program. The cybersecurity risk management examination report includes management's description of the entity's cybersecurity risk management program, management assertion, and the practitioner's report (opinion letter).

2. Is SOC for Cybersecurity for me?

Unlike the SOC attestations before, the SOC for Cybersecurity is for ANY type of entity. While the traditional SOC reports are only intended for businesses defined as "service organizations," the new SOC for Cybersecurity is applicable to all entities.

3. What If I already have a SOC 2?

If you already have completed a SOC 2 examination then you are likely in a good place. While the report types are not interchangeable, the SOC 2 examination and reporting process provides a good start towards the SOC for cybersecurity preparedness. Adding a SOC for cybersecurity would allow for additional assurance on your risk management processes. Additionally, since the SOC 2 and the SOC for Cybersecurity examinations are conducted using the same standard (SSAE No. 18), adding a SOC for Cybersecurity in conjunction with your SOC 2 could come at a reduced cost, due to potential synergies. Finally, unlike the SOC 2, the SOC for Cybersecurity is not a restricted use report, so organizations are able to utilize a SOC for Cybersecurity report to communicate their security and cybersecurity risk management efforts to a larger audience – including the board of directors, regulators, investors, and prospective customers.

4. What are the key differences in a SOC 2 and SOC for Cybersecurity?

The four key differences in a SOC 2 examination and a SOC for Cybersecurity include: the purpose and use of the report, the audience, report types, and how subservice organizations are treated.

→ Purpose and Use

A SOC for Cybersecurity report communicates information regarding an organization's cybersecurity risk management efforts, which gives the report users added assurance over an organization's risk management process. A SOC 2 is used by service organizations only, that want to validate their work product to their customers related to information and security processes. A SOC 2 report communicates information about their internal controls relevant to information security.

→ Audience

SOC for Cybersecurity is a general user report and is designed to be used by anyone whose decisions are directly impacted by the effectiveness of an organization's cybersecurity controls. A SOC 2 is more restrictive as its intended for an audience with a prior understanding of the system, and the Trust Services Criteria, such as the user entity of the services.

→ Report Types

There are two types of SOC 2 reports, a Type 1 and a Type 2 report. A Type 1 report is an attestation of the fairness of the presentation of the description of the system, and the design of a service organization's controls. The Type 1 report provides assurance as of a point in time (review date). A type 2 report is an attestation that includes the components of the Type 1 report, but also includes the auditor's tests of the design and operating effectiveness of controls over a specified period of time (review period). The SOC for Cybersecurity has a similar report choice but they are designated differently. The 'Type 1' version of the SOC for Cybersecurity is named the design-only examination, while the standard SOC for Cybersecurity tests both the design and operating effective of controls, by default (similar to a SOC 2 Type 2).

→ Treatment of Subservice Organizations (SSO)

In a SOC 2 report, an entity can choose to include or carve out certain third parties, known as subservice organization, from the scope of the report. In a SOC for Cybersecurity engagement, organizations are not able to offshore control responsibilities to third parties. Instead organzations are responsible for all controls within the risk management program. This means that if an entity is using third parties for controls within its program, the entity must include the third party and their associated controls within the scope of the audit. Additionally, when evaluating the effectiveness of the controls within the entity's risk management program, the practitioner must conclude on whether the entity's monitoring controls over the processes and controls performed by third parties are effective to achieve the entity's cybersecurity objectives. Therefore, the entity being accessed should have clear and formal monitoring controls over third parties.

Note, this does not mean that in order to attain a SOC for Cybersecurity report, the auditor has to go visit AWS, or wherever you are hosted. The examination is of the entity's program and assumes that it factors in the review and risk management of its third parties. This is identical to the way an ISO 27001 Information Security Management System treats third parties. The auditor confirms through clause A.15 (Supplier Relationship) that the entity has processes to manage its third party relationships.

5. What Criteria must we follow?

As part of SOC for Cybersecurity, the AICPA has developed two complementary sets of criteria for use during an examination. Management uses the description criteria when preparing the narrative description of the entity's cybersecurity risk management program. These are not controls but criteria for what must be included in the description.

In addition, management uses the control criteria when evaluating the effectiveness of the controls within the program. For the control criteria, an entity can opt to use the Trust Services Criteria for Security, Availability, Confidentiality (trust services criteria) or other control criteria such as the NIST Critical Infrastructure Cybersecurity Framework, ISO 27001/27002, and others.

→ What is meant by description criteria?

The AICPA has developed a set of benchmarks know as description criteria, that are used by management, when preparing a description of an entity's cybersecurity risk management program, and used by the practitioners when evaluating that description, in connection with services performed on an entity's cybersecurity risk management program. For a SOC for Cybersecurity attestation, the practiconer expresses their opinion on whether the description presented is in accordance with the description criteria.

The description criteria for a SOC Cybersecurity examination are categorized into the nine sections below:

1. Nature of business and operations
2. Nature of information at risk
3. Cybersecurity risk Management Program objectives
4. Factors that have a significant effect on inherent cybersecurity risks
5. Cybersecurity risk governance structure
6. Cybersecurity risk assessment process
7. Cybersecurity communications and the quality of cybersecurity information
8. Monitoring of the Cybersecurity risk Management Program
9. Cybersecurity control processes

Discover how Schellman can help you.

TALK WITH A SPECIALIST

Our Schellman teams have experience performing thousands of attestation examinations. **We're here to answer your questions on SOC for Cybersecurity.**

CLICK HERE TO TALK WITH A SPECIALIST

schellman

www.schellman.com

4010 W Boy Scout Blvd, Suite 600
Tampa, FL 33607
1.866.254.0000

Outside of the United States,
please dial: +1.973.854.4684