SOC for Cybersecurity Overview

Banks always have to assess their risks, whether it's when sharing sensitive information with third parties or subscribing to managed security providers. SSAE SOC 2 Type 2 reports have been the standard for assessing cyber security controls, and it's very common to have over 100 of these vendor reports to review annually.

Despite being the standard, these reports can create gaps in our understanding of how third parties protect data Internet-borne threats; APIs and our understanding of how APIs are protected is particularly muddied. If a third party's controls are adequate overall, you can usually get a general measure. But the focus is seldom on cyber security itself.

Important IT general controls are almost always missing in the report's list of management controls. In our experience, we've seen SOC 2s omit anti-malware controls, change controls, and data backups.

Deer Brook's team takes our clients' SOC reports and reviews them against a list of standard IT general controls. If any controls are missing, we note them and contact the third party provider for more information.

New AICPA SOC report will help illustrate third party cybersecurity controls

SOC for Cybersecurity

A "SOC for Cybersecurity" report is what an auditor creates to examine an organization's cybersecurity risk management program. The program details the policies, processes, and controls used to protect information and systems from security events.

Through these means, SOC for Cybersecurity reports provide perspective and confidence to boards of directors, analysts, investors, business partners, industry regulators, and users.

The AICPA's primary intent for this report was to provide all organizations with a unified, consistent language in which they could report on their cybersecurity efforts. AICPA was also intending to establish a widely accepted approach for cybersecurity assessments.

SOC for Cybersecurity reports can be created for any type of organization, regardless of size or industry. These reports are for general use, specifically designed to be used by stakeholders whose decisions are directly impacted by the effectiveness of an organization's cybersecurity controls.

What's the difference between SOC for Cybersecurity reports and SOC 2 reports?

SOC for Cybersecurity reports analyze cybersecurity risk management programs, while SOC 2 reports analyze the entire system and consider the trust services criteria.

Cybersecurity risk management criteria

Nature of business and operations

The nature of the entity's business and operations, including the principal products or services the entity sells or provides, and the methods by which they are distributed.

Nature of information at risk

The principal types of sensitive information created, collected, transmitted, used, or stored by the entity.

Cybersecurity risk management program objectives

The entity's principal cybersecurity risk management program objectives (cybersecurity objectives) related to availability, confidentiality, integrity of data, and integrity of processing.

The process for establishing, maintaining, and approving cybersecurity objectives to support the achievement of the entity's objectives.

Factors that have a significant effect on inherent cybersecurity risks

Factors that have a significant effect on the entity's inherent cybersecurity risks, including:

- Characteristics of technologies, connection types, use of service providers, and delivery channels used by the entity

- Organizational and user characteristics
- Environmental, technological, organizational, and other changes during the period covered by the description at the entity and in its environment
- Also applies to security incidents that:
- Were identified during the 12-month period preceding the period end date of management's description
- Resulted in a significant impairment of the entity's achievement of its cybersecurity objectives, disclosure of the following:
    - Nature of the incident
    - Timing surrounding the incident
    - Extent (or effect) of those incidents and their disposition

Cybersecurity risk governance structure

The process for establishing, maintaining, and communicating integrity and ethical values to support the functioning of the cybersecurity risk management program.

The process for board oversight of the entity's cybersecurity risk management program. Established cybersecurity accountability and reporting lines.

The process used to hire and develop competent individuals and contractors and to hold those individuals accountable for their cybersecurity responsibilities.

Cybersecurity risk assessment process

The process for:

- Identifying cybersecurity risks and environmental, technological, organizational and other changes that could have a significant effect on the entity's cybersecurity risk management program
- Assessing the related risks to the achievement of the entity's cybersecurity objectives

Additionally, the process for identifying, assessing, and managing the risks associated with vendors and business partners.

Cybersecurity communications and quality of cybersecurity information

The process for internally communicating relevant cybersecurity information necessary to support the functioning of the entity's cybersecurity risk management program, including:

- Objectives and responsibilities for cybersecurity
- Thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents requiring a response, remediation, or both

It is also the process for communicating with external parties regarding matters affecting the functioning of the entity's cybersecurity risk management program.

Monitoring of the cybersecurity risk management program

The process for conducting ongoing and periodic evaluations of the operating effectiveness of key control activities and other components of internal control related to cybersecurity.

The process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective actions, including management and the board of directors (as appropriate).

Cybersecurity control process

The process for developing a response to assessed risks, including the design and implementation of control processes. Also included is a summary of the entity's IT infrastructure and its network architectural characteristics.

The key security policies and processes implemented and operated to address the entity's cybersecurity risks, including those addressing the following:

- Prevention of intentional and unintentional security events
- Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents
- Management of processing capacity to provide for continued operations during security, operational, and environmental events
- Detection, mitigation, and recovery from environmental events and the use of back-up procedures to support system availability

- Identification of confidential information when received or created, determination of the retention period for that information, retention of the information for the specified period, and destruction of the information at the end of the retention period

Wrapping up

As part of our vendor management augmentation services, Deer Brook provides cost-effective SSAE SOC report review services.

All our reviews follow a standardized procedure and provide vendor risk report factors for your vendor management programs.

Additionally, Deer Brook can work with your third party cyber security leads to document additional controls that aren't included in the SOC report, but are still important for your organization.

As cybersecurity SOCs evolve, our team will remain on the cutting edge and adjust our review processes accordingly.

deer-brook.com

DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS