Attinkom
We verify your trust

SOC for Cyber Security

Attinkom

We verify your trust

This publication contains general information only and Attinkom is not, by means of this publication, rendering any professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Attinkom shall not be responsible for any loss sustained by any person who relies on this publication. As used in this document, “Attinkom" means Attinkom LLC. Please see https://attinkom.com and email us at info@attinkom.com for any specific services that you may be looking for.

Attinkom

We verify your trust

Table of Contents

Introduction

To address this market need, the AICPA has developed a cybersecurity risk management reporting framework that assists organizations as they communicate relevant and useful information about the effectiveness of their cybersecurity risk management programs.

The framework is a key component of a new System and Organization Controls (SOC) for Cybersecurity engagement, through which a CPA reports on an organizations' enterprise-wide cybersecurity risk management program. This information can help senior management, boards of directors, analysts, investors, and business partners gain a better understanding of organizations' efforts.

SOC for Cyber security Evaluation

SOC for Cybersecurity is an evaluation engagement performed by CPAs (practitioners) on an entity's cybersecurity risk management program. In a cybersecurity risk management evaluation, there are two distinct but complementary subject matters: (i) the description of the entity's cybersecurity risk management program and (ii) the effectiveness of controls within that program to achieve the entity's cybersecurity objectives. A cybersecurity risk management evaluation results in the issuance of a cybersecurity risk management evaluation report that is for general use. The cybersecurity risk management examination report includes the following three key components a) Management's description, b) Management's Assertion, c) Practitioner's opinion

What's SOC for Cybersecurity Risk Management Report

The SOC for Cybersecurity Report includes the following three key components:

Management's description
The description of the entity's cybersecurity risk management program. This description is designed to provide information about how the entity identifies its information assets, the ways in which the entity manages the cybersecurity risks that threaten it, and the key security policies and processes implemented and operated to protect the entity's information assets against those risks.

Management's assertion
Management provides the assertion regarding the presentation and effectiveness of the controls in place to achieve the cybersecurity criteria. Specifically, the assertion addresses whether (a) the description is presented in accordance with the description criteria and (b) the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

Practitioner's opinion
A CPA firm's opinion on the description and effectiveness of controls in place to achieve the cybersecurity criteria. Specifically, the opinion addresses whether (a) the description is presented in accordance with the description criteria and (b) the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

Benefits of the SOC for Cybersecurity Assessment

SOC for Cybersecurity includes the auditor’s examinations of the organization’s design and operating effectiveness of controls within the organization’s cybersecurity risk management program. The report will grow the confidence of those charged with governance of the organization that the processes, policies, and controls in place are designed and operating effectively to prevent a cybersecurity attack, or on the other hand, it will give the organization an opportunity to see the gaps in their cybersecurity risk management program and recommendations on how to improve it. The report also indicates the results of the auditor’s tests of such controls to provide a level of comfort over their effectiveness. A SOC for Cybersecurity renders this useful information on how the organization is mitigating the ever-growing cybersecurity risk in a crystalline manner for the use of management.

Is SOC for Cybersecurity a SOC 2 report?

There are distinct differences between SOC for Cybersecurity and SOC 2, from their purpose and uses to their audience.

Scope

A SOC 2 report assesses data management by third-party service providers and focuses on information security processes for specific business units or services. The SOC for Cybersecurity, on the other hand, evaluates the entire organization's cybersecurity risk management program.

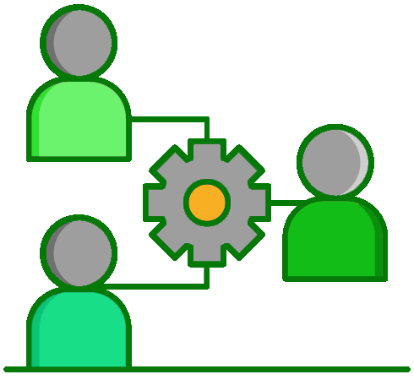
Control Criteria

SOC for Cybersecurity doesn't have a specific baseline for evaluation and can use any cybersecurity framework already applied by the organization (such as ISO 27001 or the NIST Cybersecurity Framework). SOC 2 is limited to the AICPA's Trust Service Criteria, which adhere to the COSO frameworks.

Audience

The SOC for Cybersecurity is for general use. It has a broad audience, so it is suitable for stakeholders interested in knowing that the entity's cybersecurity objectives and programs are well-designed. On the other hand, SOC 2 is aimed at active service organization users, with detailed information on information security processes, so its audience is limited and specialized.

Third-Party Risks



Within a SOC for Cybersecurity report, all third-party risks must be considered and evaluated at a high level.

SOC 2 reports are more nuanced. First, determine which third parties are considered "subservice organizations" per the SOC 2 definition. These are third parties whose services help meet your SOC 2 trust services criteria. Typical examples of subservice organizations include cloud hosting services and data centers — you are relying on their internal controls to meet your SOC 2 requirements.

In SOC 2 reports, you must have documentation of due diligence and vendor management processes for all subservice organizations. In some cases, you may also include the actual controls performed by specific sub-service organizations.

Sensitive Information

A SOC 2 report contains the Trust Services Criteria and the results from the auditor's tests of controls, so it may collect sensitive information that should only be shared with a specific audience. On the other hand, the SOC for Cybersecurity is more general in scope and intended for a broader audience, so it does not include sensitive data. It could, for example, be posted on your corporate website for all to see.

The Importance of Your Auditor’s Role in SOC for Cybersecurity

Cybersecurity is not just about IT security it is about Information and Data security. Any misguided assurances from the internal team or a cybersecurity company are the major reasons why hackers are succeeding in their attempts. They target your processes, people, procedures, and poor links. Cybersecurity audits ensure a 360-degree in-depth audit of your organization’s security postures. It detects any vulnerabilities, risks, and threats that organizations face and the influence of such risks causing across these areas.

Does Attinkom perform SOC for Cybersecurity examinations?

We perform SOC for Cybersecurity examinations. The firm delivers Service Organization Controls reports to various entities and will leverage this background, as well as our IT audit and cybersecurity expertise in delivering these services.

Disclaimer:

This whitepaper contains common information only and we Attinkom is not, by means of this whitepaper, providing any or other professional advice or services.