Understanding a SOC 3 Report

Overview

Over the last decade, companies have started to see outsourcing as a way of reducing costs and improving inefficiencies which lead to a rapid growth in outsourcing of software as service and other cloud-based technologies. The change led to an increased demand of SOC reports and has also increased the necessity for auditor reporting at service organizations to make sure that these service providers have appropriate internal controls in place to manage their information systems. As these requests from customers for these reports become more frequent, it can often become confusing on which report you ought to be providing also as which report are going to be more useful for the Service Organization.

Introduction

AICPA has 5 main Trust Services Criteria namely security, availability, processing integrity, confidentiality and privacy. A Service Organization Control 3 (SOC 3) report provides information related to a service organization's internal controls around these TSCs.

A SOC 3 is intended for a public audience. These reports are short and include lesser details as compared to a Soc 2 report, which is distributed to a focused audience of stakeholders. Due to generic nature, Soc 3 reports can be shared openly and posted on a company's website to portray their compliance. However, the report may still be invaluable for an organization looking for insights on their current security and control landscape.

Difference Between a SOC 2 and SOC 3 Report

Basically, both SOC 2 and SOC 3 reports revolve around same AICPA standards and the work performed by the service auditor for the two reports is very similar. Both reports are based on the AICPA's TSCs and the controls identified and tested are usually same for both the reports. Following are some key differences between both the reports:

- SOC 2 reports can be either Type I or a Type II while a SOC 3 report is always a Type II report

- SOC 3 report has a less detailed description of controls related to compliance and operations. Also, it does not include detailed testing procedures or results of testing.
- SOC 2 reports are meant for restricted use reports of the service organization's management, customers, and customers' auditors. On contrary, SOC 3 reports are general use reports that can be distributed freely as they contain significantly less detail.
- SOC 3 report are more used as tool for attracting prospective customers but it may not satisfy the needs of current customers and their auditors.
- A SOC 2 report is larger in size as it includes an auditor's opinion, management's assertion, a detailed description of the system. It also includes description of service organization's internal controls and their test results performed by the service auditors. However, a SOC 3 report is much smaller in size and consists of a brief auditor's opinion, management assertion, and a brief narrative providing background on the service organization. It contains very less detail on the specific controls operating within the service organization

Benefits of a SOC 3 Report

Following are some key benefits of obtaining a SOC 3 report:

- It evidences that your organization invests in security measures and portrays customers that you're transparent about your practices
- SOC 3 report can help enhance your company's credibility and gain the trust of new clients.
- Provides you an edge over competitors who do not have any third-party certification
- A positive report demonstrates you have a professional team and your organization cares about clients to ensure that their data is safe from cyber threats.

Summary

To conclude, it is relatively easier for an organization to decide if they need a SOC 1 or a SOC 2 because the key difference between being that SOC 1 is more inclined towards impact of service organization's controls on the customer's internal control over financial reporting. The decision becomes a little more difficult when deciding between a SOC 2 and SOC 3 report.

Important thing to remember is that a SOC 2 is a restricted use report that contains detailed information on the system, the controls in place, the service auditor's test procedures and the results of their test procedures. SOC 2 reports are useful for corporate oversight, vendor management programs, internal corporate governance and risk management processes.

A SOC 3 is a general use report that does not include much detail and is a great marketing tool. They can be used to attract new client and induce confidence and trust in both upcoming and existing clients.

We believe this the article would have enhanced your understanding about SOC 3 reports. Please feel free to reach out if you have any queries related to SOC reports or need to get a SOC/ISO/GDPR certification done for your organization.

You can also visit our website https://accorppartners.com/soc/index.php to read more articles related to SOC reporting.