SOC Reports Explained

SOC 1 or SOC 2

A SOC 1 report focuses on a service provider's controls that are relevant to financial statement oversight. This report is the successor to the SAS70 and SSAE16 report formats. Security controls related to both business process and information technology are normally included in a SOC 1 report. This report format is still widely accepted for service provider security assurance purposes.

A SOC 2 report addresses a service providers controls related to security, confidentiality, availability, processing integrity, and privacy. The AICPA defines the audit process and report structure. The AICPA recently integrated their SOC 2 format with the widely-used COSO compliance framework.

The decision to obtain a SOC 1 report vs. a SOC 2 report depends on what the client's customers and/or investors are requiring. The SOC 2 report is currently the standard for security assurance testing, and most clients or investors will ask for this report by name. The AuditOne LLP SOC Program provides the flexibility for clients to start with a SOC 1 report, and then migrate to a SOC 2 report.

SOC 3

A SOC 2 report contains a detailed description of the client's operation and all the security controls in place. This report should only be provided to existing customers and investors with signed NDAs.

A SOC 3 report is a public version of a SOC 2 report. A SOC 3 does not contain a listing of the client's controls, and the system description section is scaled down for public disclosure. Organizations can provide a SOC 3 report to any potential customer without the requirement of a signed non-disclosure agreement (NDA). Many client's place a SOC 3 report on their website for customers to download.

Type I or Type II

A type I report is a point in time report (example: as of December 31, 2019) where AuditOne LLP assesses the client's security controls in place, and then determines if the controls are sufficiently designed. No collection of evidence is performed.

A type II report is a time period-based report (example: January 1, 2019 to December 31, 2019). AuditOne LLP will be assessing the client's security control effectiveness during a specific time period. Evidence collection, and audit steps are performed.

The minimum time period for a type II report is six months. A client's stated security controls need to be in place during this period. Customers, and/or investors, may not accept a type I report due to the lack of audit review.

About AuditOne LLP

AuditOne LLP provides a cost-effective program to deliver globally recognized third-party security audit reports. Our SOC audit reports establish confidence in your organization, can be used as a sales tool, and are often required by larger companies for due diligence purposes. The AuditOne LLP audit process is simpler, and a far less time consuming compared to other third-party security audits.

Robert Kluba CISM CISSP
Managing Director
Phone: 408.656.9300
Robert.Kluba@AuditOneLLP.com

https://www.AuditOneLLP.com