AuditOne LLP SOC Program

Program Summary

- Globally recognized security assurance reports for your customers or investors
- Streamlined process based on over a decade of experience with SOC audits
- A 72-item security control set which satisfies the industry recognized SOC 2 security compliance framework
- Ability to reduce the number of security controls to 40 or 50 and perform a less stringent SOC 1 audit
- AuditOne LLP can facilitate the required annual risk assessment review, and annual third-party penetration testing
- Sample policies, procedures, and forms can be provided if necessary
- Time period from contract signing to report issuance can be as little as 90 days

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, which saves time and money.

SOC 1 or SOC 2

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 and 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.

The AuditOne LLP SOC Program Process

- Risk assessment and penetration test performed prior to audit
- Audit kick off meeting – 2 to 4 weeks before audit start
- Daily or weekly scheduled meetings when audit begins
- ♦ Audit and evidence gathering phase – 2 weeks
- Report issued in as little as 90 days

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

https://www.AuditOneLLP.com