AuditOne LLP SOC Program

Program Summary

- Globally recognized security assurance reports
- Streamlined process based on a decade of experience performing SOC audits
- Sample control set based on the SOC 2 framework
- Ability to facilitate the required annual risk assessment, 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 is designed to audit the internal controls over financial reporting. This report is the successor to the SAS 70 report format. This report format is still accepted for IT general control audit purposes.

A SOC 2 report addresses a service providers stated 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 your customers are requiring for assurance. The SOC 2 report is currently the standard for security assurance testing, and most customers will ask for this report by name.

SOC 3

A SOC 2 report contains a detailed description of the client's operation and security controls in place. This report is only provided to existing customers.

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.

Type I or Type II

A type I report is a point in time report (example: as of December 31, 2019) where AuditOne LLP assess your security controls and determine if the controls are sufficiently designed. No collection of evidence is performed. Customers may not accept a type I report due to the lack of audit review.

A type II report is a time period-based report (example: January 1, 2019, to December 31, 2019). AuditOne LLP will assess your 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 typically six months. Your stated security controls need to be in place during this period.

The AuditOne LLP SOC Program Process

- Risk assessment and penetration test performed prior to review period
- Audit kick off meeting – 2 to 4 weeks before audit start
- Bi-weekly scheduled meetings when audit begins
- Audit and evidence gathering phase – 2-3 weeks
- Report issued in as little as 90 days form end of review period

SOC Audit Advantages

- The SOC framework is industry and regulator agnostic.
- The SOC 2 framework is a globally recognized report format.
- Audited controls are your controls and based on existing processes in place.
- SOC audits are significantly less costly than PCI-DSS or ISO.
- SOC audit time commitments are significantly less than PCI-DSS or ISO
- AuditOne LLP has over a decade of experience delivering SOC audits.

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

https://www.AuditOneLLP.com