CYBERGUARD COMPLIANCE

The "Cliff Notes" Guide to a Better Understanding of the SOC 1®, SOC 2®, and SOC 3®Reports

Understanding the Basics of SOC 1®

SOC 1® reports relate to controls at service organizations relevant to user entities' internal controls over financial reporting (ICFR). Yes, that is a mouthful and sounds very convoluted. In layman's terms, if your company provides services to clients which may ultimately impact their financial statements, then a SOC 1® is a great report for you. For example, let's say you operate a payroll company and are tasked with processing payroll on behalf of your clients. Since payroll is a major component of your clients' income statements, they will likely ask your company to produce a SOC 1® report which shows all the key controls related to payroll that you are responsible for performing. The first step towards an SOC 1® audit requires the organization to identify what services and controls are in place which affect the ICFR for clients that utilize their services. Refer to "Understanding the Basics of a SOC Readiness Assessment" for more details on the process of identifying these controls.

SOC 1® reports are restricted use reports, which mean use of the reports are restricted to:

- Management of the service organization (the company who has the SOC 1® performed)
- User entities of the service organization (customers, regulators, business partners, suppliers, etc.)

Both SOC 1® Type 1 and SOC 1® Type 2 reports can be issued depending on the specific requirements and objectives of the service organization. Both report types add value and credibility to a service organization's core activities with the following differences:

- A Type 1 is a report on controls placed in operation as of a specified **"point in time"**. SOC 1® Type I reports evaluate the design effectiveness of a service provider's controls and then confirms the controls have been placed in operation as of a **"specific date"**.
- A Type 2 is a report on controls placed in operation and tests of operating effectiveness for a **"period of time"**. Type 2 reports include the examination and confirmation steps involved in a Type 1 examination, plus an evaluation of the operating effectiveness of the controls for a period of between three and twelve consecutive calendar months. Most user organizations require their service provider to undergo the Type 2 audit for the greater level of assurance it provides.

Understanding the Basics of SOC 2®

SOC 2® reports are best for companies providing services that do not impact their clients' ICFR. SOC 2® reports focus on controls at a service organization relevant to the following Trust Service Principles:

- **Security:** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems andaffect the entity's ability to meet its objectives).
- **Availability:** Information and systems are available for operation and use to meet the entity's objectives.
- **Confidentiality:** Information designated as confidential is protected to meet the entity's objectives.
- **Processing Integrity:** System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- **Privacy:** Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

This means many companies in various industries (e.g. managed service providers, Software as a Service (SaaS), cloud computing, etc.) require a SOC 2® report. SOC 2® reports are restricted use reports, which mean use of the reports are restricted to:

- Management of the service organization (the company who has the SOC 2® performed)
- User entities of the service organization (customers, regulators, business partners, suppliers, etc.)

As with SOC 1® reports, SOC 2® reports are restricted use reports. Additionally, both SOC 2® Type 1 and SOC 2® Type 2 reports can be issued.

Understanding the Basics of SOC 3®

Unlike a SOC 1® and SOC 2® reports (which is a restricted use reports), SOC 3® reports are general use reports, which means they can be freely distributed or posted on a website as a seal for one full-calendar year from the date of issue. However, when producing a SOC 3® report, the CPA firm must conduct a thorough audit with the same rigor as a SOC 2® audit. As such, virtually all service organizations choose to undergo the SOC 2® audit and add the SOC 3® report as an add-on. A SOC 3® report is beneficial from a marketing perspective and allows you to share reports with non-customers to prove your company's commitment to security. Since a SOC 3® report is primarily a marketing tool, ask your Marketing Department for budget for this report as opposed to using the Compliance or IT Departments' budget.

It is important to note that many companies undergoing a SOC 1®, SOC 2® or SOC 3® audit for the first time choose to perform a Readiness Assessment prior to undergoing the Type 1 or Type 2 audit.

Understanding the Basics of a SOC Readiness Assessment

Undergoing a SOC audit for the first time can be a daunting task and is a significant investment in time and money. Clients have many questions around the scope, documentation requirements, and internal resources required to complete the engagement and want assurances the audit outcome will have a high likelihood of success.

With so many uncertainties, it is prudent to perform a Readiness Assessment prior to beginning your engagement. The Readiness Assessment will include:

- Sitting down with your process owners, obtaining an understanding of the risks associated with the services you provide your clients, and walking through each critical business function to identify the controls you have in place to mitigate applicable risks.
- Performing a walkthrough of each control and providing you with a gap matrix of failed controls. The gap matrix provides a detailed action plan which allows you to remediate the gaps.
- Re-performing walkthroughs for each control that initially failed.

Once all gaps have been remediated, you may then proceed to the audit phase.

The readiness assessment allows your team to prepare for the audit, while gaining critical knowledge of key processes. This combination of Readiness Assessments and Audit services allow CyberGuard Compliance to gain efficiencies, which ultimately reduces overall audit fees.

Benefits of Successfully Completing a SOC Audit

- Improves the security posture of your company
- Demonstrates your organizations commitment to investing in security measures
- Improves your marketing and competitive advantages
- Builds trust with your clients
- Improves your organizational performance and productivity
- Improves your ability to perform outsourced services for public and private companies
- Potential clients are more likely to trust your company over competitors who do not have a SOC report.

SOC 1®, SOC 2®, and SOC 3® reports should be viewed as an annual investment into your company with a proven ROI, helping generate new clients while increasing operational efficiencies and overall security posture. For more information, or if you have questions, please contact CyberGuard Compliance today.

About CyberGuard Compliance

CyberGuard Compliance is based in the United States but serves clients around the globe. The firm's leadership team has over 150 years of combined business management, operations and related information technology (IT) experience. CyberGuard Compliance has performed over 1,000 SOC audits, and unlike most traditional CPA firms which focus on financial statement auditing and tax compliance, CyberGuard Compliance only focuses on cybersecurity and compliance related engagements. These engagements include, but are not limited to, SOC 1® Audits, SOC 2® Audits, SOC 3® Audits, SOC Readiness Assessments, ISO 27001 Assessments, PCI Compliance, HIPAA Attestations, HITRUST Certification, Vulnerability Assessments, and Penetration Testing.

CyberGuard Compliance was founded with the goal of providing clients with top professional talent from a boutique-style professional services firm. Each of our experienced professionals carry one or more of the following designations: Certified Public Accountant (CPA), Certified Information Systems Auditor (CISA), Certified Information Systems Manager (CISM), Qualified Security Assessor (QSA), or Certified Information Systems Security Professional (CISSP).

CyberGuard Compliance has a diverse client base, ranging from Fortune 50 clients to government agencies to start-ups in Silicon Valley. Many of our clients are companies undertaking the audit for the first time. We pride ourselves in working closely and collaboratively with our clients to ensure all service-related risks are addressed with appropriate criteria and control activities. Our detailed approach helps to identify opportunities for improvement within our clients' operations. CyberGuard Compliance's proven methodology, flexible delivery methods, efficient economic operating model, and focus on adding value for our clients has enabled the firm to be one of the most highly sought-after Cybersecurity, SOC Audit, and IT compliance-focused CPA firms in the United States.

As a Public Accounting Oversight Board (PCAOB) registered and licensed public accounting firm, CyberGuard Compliance is subject to an independent peer review on our auditing practice by a recognized and approved peer review program. This ensures the firm is held to the strictest of audit standards.

Contact CyberGuard Compliance

CyberGuard Compliance has assembled a top tier team to help clients through the SOC process. For further information regarding SOC reports, or to request a free consultation from CyberGuard Compliance, please visit the "Contact Us" page on the CyberGuard website to submit an informational form, or by phone or email listed below.

T/ 866.480.9485

E/ ContactUs@CGCompliance.com

W/ www.cgcompliance.com