CyberGuard Compliance, LLP

SOC 2 Report Overview

Report on Controls Related to Security, Availability, Processing Integrity, Confidentiality, and Privacy

About SOC 2 Reports

Whereas SOC 1 audits comprise internal controls over financial reporting, SOC 2 audits focus on controls at a service organization relevant to the following five Trust Services Principles and Criteria:

- **Security:** The system is protected against unauthorized access, use, or modification;
- **Availability:** The system is available for operation and use as committed or agreed;
- **Processing Integrity**: System processing is complete, valid, accurate, timely, and authorized;
- **Confidentiality:** Information designated as confidential is protected as committed or agreed; and
- **Privacy:** The system's collection, use, retention, disclosure, and disposal of personal information are in conformity with the commitments in the service organization's privacy notice and with criteria set forth in the Generally Accepted Privacy Principles (GAPP).

For companies which have used SOC 1's in the past, you should now consider a SOC 2 report (e.g. managed service providers, Software as a Service (SaaS), cloud computing, etc.). SOC 2 reports are restricted use reports, which mean use of the reports is 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.)

The AICPA has outlined essential elements that must be incorporated in the SOC 2 report:

- Service auditor's opinion (prepared by CyberGuard Compliance)
- Management's assertion letter (prepared by client with advice from CyberGuard Compliance), which includes:
  - Management's description of the service organization's system fairly presents the system that was designed and implemented throughout the specified period (or in the case of a Type I report, as of a specified date)
  - The controls related to the control objectives stated in management's description of the service organization's system were suitably designed throughout the specified period (or in the case of a Type I report, as of a specified date)
  - When included in the scope of the engagement, the controls operated effectively to provide reasonable assurance that the control objectives stated in management's description of the service organization's system were achieved throughout the specified period (Type II only)

- A description of the service organization's system (prepared by client with advice from CyberGuard Compliance), which includes:
    - Description of the services provided, including classes of transactions processed
    - Description of the procedures by which services are provided, including transaction initiation, authorization, recording, processing and reporting
    - Description of the process used to prepare reports and other information, which is provided to customers
    - Description of other significant events that affect transaction processing
    - Any changes that occur during the audit period
- Service auditor's tests of controls and results of tests (Type II report only) (prepared by CyberGuard Compliance)
- Other supplemental information not covered in other sections (prepared by client with advice from CyberGuard Compliance)

Both SOC 2 Type I and SOC 2 Type II reports can be issued:

- Type I – a Type I is a report on policies and procedures placed in operation as of a specified point in time. SOC 2 Type I Reports evaluate the design effectiveness of a service provider's controls and then confirms that these controls have been placed in operation as of a specific date.
- Type II – a Type II is a report on policies and procedures placed in operation and tests of operating effectiveness for a period of time. SOC 2 Type II Reports include the examination and confirmation steps involved in a Type I examination plus include an evaluation of the operating effectiveness of the controls for a period of at least six calendar months. Most user organizations require their service provider to undergo the Type II level examination for the greater level of assurance it provides.

Readiness Assessment Process

We understand that completing an audit initiative for the first time can be a daunting task and is a significant investment in time and money. Our clients have many questions around the scope, documentation requirements, and internal resources needed to complete the engagement. Clients 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. Here is our process:

- We sit down with your process owners, obtain an understanding of the risks associated with the services you provide your customers, and walk through each critical business function. We then help you identify the controls you have in place to mitigate applicable risks.
- Once the controls have been identified, we perform a walkthrough of each control and provide you with a gap matrix of failed controls.
- Our gap matrix provides a detailed action plan which allows you to remediate the gaps.
- After control gaps have been remediated, we will re-perform walkthroughs for each control that initially failed.
- Once all gaps have been remediated, we then proceed to the audit phase.

The readiness assessment allows our firm to assist your team prepare for the audit, while gaining critical knowledge of key processes. This unique combination of services allows CyberGuard Compliance to gain efficiencies, which ultimately reduces audit fees.

The Engagement Approach

At CyberGuard Compliance, our unique approach will be to conduct each engagement using our proven, three-phased methodology within the standards established by the AICPA. Before we execute our proven methodology, that our engagement team first obtain a thorough understanding of your business. Additionally, we coordinate the logistics of the engagement with your personnel to acquire the necessary information to complete the engagement objectives. Our proven three-phased approach is as follows:

<u>Phase I – Planning and Scoping</u>

- The objectives of this initial phase are to refine and finalize the scope of the audit work to be performed and to develop a suitable work plan. This will take into account business requirements and constraints of your company, including identifying controls based on our risk assessment.

<u>Phase 2 – Fieldwork</u>

Once controls have been identified and documented, fieldwork begins. We will:

- Confirm that stated control procedures are still valid and apply to the environment;
- Test the stated control procedures for design and/or operating effectiveness; and

- Document the results and conclusion.

Phase 3 – Reporting of Results

Once fieldwork is completed, we prepare and provide a draft audit report to client management for final input. Once all input is received, we will issue the final report.

The Benefits of Completing the SOC 1 Audit

Unlike most audits, which can be painful and agonizing, SOC audit can have a real ROI. Here are some benefits to consider when deciding on whether or not to pursue the SOC audit:

1. The SOC audit provides a competitive advantage with a proven return on investment and increases your prospective client base, organizational productivity, and customer retention.
2. The SOC audit is a single audit that is completed annually. This prevents the external auditors of your clients from continuously contacting your personnel for independent audits throughout the year.
3. The SOC audit increases trust and transparency with clients. Your clients are more likely to trust your organization with their data or performing an important business process on their behalf because they will have the ability to review your SOC report and verify the effectiveness of your controls.
4. The SOC audit increases investor confidence around your internal controls. Many_investors, including venture capitalists and angels, require the companies they invest in to perform annual SOC audits.
5. Finally, having an SOC audit will enable your company to respond to more RFP's with confidence and not face the possibility of being eliminated from the bidding process.

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 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 Compliance, HITRUST Compliance, 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 their professionals has over 10 years of relevant experience at “Big 4” and other large international or regional accounting firms, and most carry the designation of Certified Public Accountant (“CPA”), Certified Information Systems Auditor (“CISA”), Certified Information Systems Manager (“CISM”), or Certified Internal Auditor (“CIA”). CyberGuard Compliance treats its staff as valued and highly talented peers, while omitting avoidable layers of management and associated costs.

CyberGuard Compliance has a diverse client base, ranging from Fortune 50 clients to government agencies to start-ups in Silicon Valley. Many of their clients are companies undertaking the audit for the first time. They pride themselves in working closely and collaboratively with their clients to ensure all service related risks are addressed with appropriate criteria and control activities. Their detailed approach helps to identify opportunities for improvement within their clients’ operations. CyberGuard Compliance’s proven methodology, flexible delivery methods, efficient economic operating model, and focus on adding value for their 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 their 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 top tier leadership to help their clients through the SOC for Cybersecurity process. For further information regarding SOC reports, or to request a fee proposal from CyberGuard Compliance, please visit their “Contact Us” page to submit an informational form or call 866.480.9485 today. Or, feel free to contact the SOC Practice Leader directly:

Tim Roncevich, CISA | **Principal**

T/ 866.480.9485

E/ ContactUs@CGCompliance.com