A Comprehensive Guide to SOC Reports

BUILD CREDIBILITY, CONFIDENCE, AND A COMPETITIVE EDGE

SC&H GROUP

TABLE OF CONTENTS

Common Terms and Brief History 3

SOC Reporting: A Growing Trend 5

What are SOC Reports? 6

How Do I Determine the Type of SOC Report My Business? 7

SOC 1: Focus on Controls Related to User's Financial Reporting 8

SOC 2: Meet the Needs of a Broader User Range 9

SOC 3: Capitalize on a Valuable Marketing Tool 11

SOC for Cybersecurity 13

SOC for Supply Chain 13

SOC Reports: Type 1 vs. Type 2 14

How Do I Choose a SOC Auditor? 15

How Do I Prepare for a SOC Examination? 16

SOC Examination Expectations 17

Value Beyond the Examination 18

Frequently Asked Questions 19

Common Terms

AND BRIEF HISTORY

SARBANES-OXLEY ACT OF 2002 (SOX)

In response to corporate financial scandals in the early 2000s, Congress passed the Sarbanes-Oxley Act of 2002 to help protect shareholders and the public from fraudulent financial reporting by corporations. It mandated new rules for accountants, auditors, and corporate officers, including strict requirements to ensure financial data is accurate and protected against loss.

Section 404 of SOX (SOX 404) requires the independent auditor of a corporation to opine on the effectiveness of internal control over financial reporting, in addition to the fair presentation of the financial statements. It draws attention to processes that feed the financial results and requires corporations to document and evaluate controls that are deemed significant to the financial reporting process. With this, an increased need for internal control examinations.

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS (AICPA)

The American Institute of CPAs is the world's largest member association representing the accounting profession, with more than 428,000 members, and a history of serving the public interest since 1887. AICPA members represent many areas of practice, including business and industry, public practice, government, education, and consulting.

The AICPA sets ethical standards for the profession and U.S. auditing standards for private companies, nonprofit organizations, federal, state, and local governments. It develops and grades the Uniform CPA Examination and offers specialty credentials for CPAs who concentrate on personal financial planning, forensic accounting, business valuation and information management, and technology assurance.

STATEMENT ON AUDITING STANDARDS NO. 70 (SAS 70)

The American Institute of Certified Public Accountants (AICPA) issued Statement on Auditing Standards (SAS) No. 70, Service Organizations, in April 1992. For nearly two decades, SAS 70 served as the authoritative guidance for examinations of a service organization's control objectives and activities.

SAS 70 simplified auditing requirements, enabling auditors to review and test third-party controls, then issue an opinion via a uniform reporting format (Service Auditor's Examination).

STATEMENT ON STANDARDS FOR ATTESTATION ENGAGEMENTS 16 (SSAE 16)

In April 2010, the AICPA issued the Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization.

SSAE 16 updated and clarified reporting processes regarding controls around financial reporting. Further, it replaced SAS 70 Service Auditor's Examination with a System and Organizational Controls (SOC) report.

With the introduction of the SOC reporting format, the AICPA also established three SOC report types (SOC 1, SOC 2, and SOC 3), each designed to meet a specific user need. The AICPA's goal was to build user confidence through more appropriate, comprehensive reporting on service organization controls.

STATEMENT ON STANDARDS FOR ATTESTATION ENGAGEMENTS 18 (SSAE 18)

Effective in May 2017, SSAE 18 updated SSAE 16 in several significant ways, thereby increasing the usefulness and quality of SOC reports. The new standard requires companies to take more ownership of their control environment, including the identification and analysis of risk and management of third-party vendor relationships.

The most significant changes stemming from SSAE 18 impacted the SOC 2 report. Those changes included the reorganization and addition of new trust services criteria, and a set of benchmarks known as the description criteria, to be considered when preparing and evaluating management's description of the system.

A GROWING TREND

SOC Reporting

As outsourcing trends upwards and technology continues to change at a breakneck pace, reporting on internal control is becoming more prevalent. In fact, if you're a growing service organization—whether a technology provider, financial services corporation, healthcare company, or professional services firm—you've likely encountered a request for a SOC report.

Many of today's Requests for Proposals (RFPs) are now requiring these reports, a mandate that will continue to gain traction as scrutiny over third-party controls and legislative requirements, such as the Sarbanes-Oxley Act of 2002 (SOX), increase.

For service providers in most industries, this means that SOC reports are now a competitive necessity essential to gaining client trust in your processes and internal controls. The question is, what type of SOC report does your organization need?

We're here to answer your SOC reporting questions.

In this guide, we break down everything you need to know about SOC reports. From what they are and who they impact to examination preparation and maximizing ongoing internal control value. As a result, you'll be able to easily determine which SOC report is right for your organization and set your business up for greater long-term efficiency, consistency, security, and success.

What are SOC Reports?

SOC reports are a way for companies to verify, via independent third-party assurance, that service providers have appropriate controls in place and are following industry standards before outsourcing a business function to that organization. They afford service providers the opportunity to establish credibility and build trust with customers, investors, business partners, and auditors, while gaining a competitive advantage in the marketplace.

There are six distinct types of SOC reports: SOC 1, SOC 2, SOC 2 Plus, SOC 3, SOC for Cybersecurity, and SOC for Supply Chain. Each report varies but provides valuable information that is required to assess the risks and internal controls associated with an outsourced service provider. An independent, third-party auditor is needed to examine and attest on various aspects of an organization, including, as applicable:

SOC 1: Controls related to financial reporting

SOC 2 / SOC 3: Controls related to the AICPA's five trust services categories: security, availability, processing integrity, confidentiality, and privacy

SOC 2 PLUS: Controls related to the AICPA's trust services criteria, plus additional security framework(s)

SOC FOR CYBERSECURITY: Controls related to an organization's cybersecurity risk management program

SOC FOR SUPPLY CHAIN: Controls related to an organization's supply chain risk management efforts

All SOC examinations are performed in accordance with SSAE 18, specifically:

- AT-C 105 Concepts Common to All Attestation Engagements
- AT-C 205 Examination Engagements

SOC 1 examinations, in addition to the requirements and guidance noted above, are performed in accordance with AT-C 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting.

Whether conducting the examination or advising, an experienced team of auditors will work closely with an organization's leadership to assure that:

- The examination report is tailored to an organization's unique needs, thorough, and timely
- Business operations and internal control processes are streamlined
- Contractual obligations and marketplace concerns are met
- AICPA reporting requirements are met

The SOC examination / SOC attestation process produces a detailed, comprehensive report that not only helps establish the legitimacy of an organization but also uncovers potential weaknesses or gaps that could negatively impact its customers.

How Do I Determine the Type of SOC Report My Business Needs?

There are two primary reasons to undergo a SOC examination:

1. A customer, prospective customer, or auditor requests a SOC report
2. Your organization decides to proactively earn compliance

In the first scenario, it's likely that the requester might specify the type of SOC report needed. In either scenario, an organization must first consider its goals. Typically, the desired outcome for any organization is to demonstrate its commitment to the appropriate design and effective operation of its internal control environment.

In the following pages, we provide an in-depth overview for each type of SOC report to help you determine the right one for your organization.

SOC 1

FOCUS ON CONTROLS RELATED TO USER'S FINANCIAL REPORTING

A SOC 1 report focuses on your organization's controls relevant to a user entity's financial reporting. It's a hyper-detailed examination that requires a specialized understanding of the industry and related control environment. The service organization typically specifies their own control objectives and related control activities based on the specific services they perform. A SOC 1 report generally includes business process controls involving the completeness and accuracy of transactions, as well as general information technology controls, such as network security and logical access.

Given the limited scope, a SOC 1 report is best suited for organizations that must instill confidence in their controls and safeguards over their customers' financial data. It is often necessary when the user entity is publicly traded and must comply with SOX 404 or similar regulations. Examples include:

- Recordkeeping services
- Payroll services
- Medical claims processing
- Lending services

SOC 2

MEET THE NEEDS OF A BROADER USER RANGE

A SOC 2 report is for service organizations whose user entities do not necessarily rely on controls for financial reporting, allowing providers to meet the needs of a broader range of user entities. A SOC 2 examination primarily focuses on how data is stored and protected, specifically controls related to the service commitments and system requirements based on the AICPA's trust services criteria (defined below). It is a more technical, security-focused examination than SOC 1, but since the criteria required are predefined by the AICPA, it is easier to determine what compliance needs are required.

SOC 2 examinations report on the design and/or operating effectiveness of your organization's controls as they relate to five AICPA-defined trust services categories:

1. **SECURITY (COMMON CRITERIA):** The system is protected against unauthorized access, use, or modification. Security (or common criteria) is the minimum requirement for all SOC 2 examinations. The four other categories serve as add-ons to the common criteria, not as entirely separate requirements.
2. **AVAILABILITY:** The system is available for operation and use as committed or agreed.
3. **PROCESSING INTEGRITY:** System processing is complete, valid, accurate, timely, and authorized.
4. **CONFIDENTIALITY:** Information designated as confidential is protected as committed or agreed.
5. **PRIVACY:** Personal information is collected, used, retained, disclosed, and disposed in conformity with commitments in the service organization's privacy notice and criteria set forth in the Generally Accepted Privacy Principles (GAPP) issued by the AICPA.

While SOC 1 and SOC 2 reports both have restricted audiences, SOC 2 reports may be given to other parties with insight into the internal controls and nature of the service provided—such as prospective customers, vendor management professionals, regulators, and other key business partners.

SOC 2 Plus

INCORPORATE ADDITIONAL SUBJECT MATTER

Gaining traction are enhanced SOC 2 reports, referred to as SOC 2 Plus reports. They can be used to demonstrate assurance in areas that go beyond just the trust services criteria to include compliance with a range of regulatory and industry frameworks if they meet standards of objectivity, measurability, completeness, and relevance.

A SOC 2 Plus report is a typical SOC 2 report plus an attestation on additional subject matter from industry-specific standards such as National Institute of Standards and Technology (NIST), Cloud Security Alliance (CSA), Health Insurance Portability and Accountability Act (HIPAA), the International Standardization Organization (ISO), etc.

The expanded reports are highly flexible and can create substantial efficiencies for organizations such as a reduction in individual audit requests and customer questionnaires.

SOC 3

CAPITALIZE ON A VALUABLE MARKETING TOOL

Like a SOC 2, SOC 3 reports focus on controls relevant to the AICPA's five trust services categories. However, unlike SOC 2, SOC 3 reports are certified and can be made publicly available, making them valuable tools for marketing the effectiveness of your control environment.

Should you desire a SOC 3 report, your organization must first complete a SOC 2, Type 2 examination (more on report types below). SOC 2 and SOC 3 examinations can be performed on one or more of the trust services categories. SOC 3 reports contain much of the same information included in SOC 2 reports, except with a far less detailed description of your controls related to compliance and operations. They also do not include specific control activities, testing procedures, or detailed results over operating effectiveness.

SOC 1, 2, and 3 Comparison Chart

	SOC 1 REPORT	SOC 2 REPORT	SOC 3 REPORT
Purpose	Report on your controls relevant to the user entity's financial reporting.	Report on your controls relevant to security, availability, processing integrity, confidentiality, and/or privacy.	Same as SOC 2.
A Fit for Your Organization if:	You provide services that can materially affect your clients' financial reporting Your clients will use the report to support an audit of their financial statements Your clients will use the report to comply with SOX 404 or similar regulations	You provide services that require the storage and protection of your clients' data Your clients will use the report to gain confidence in your organization's system that processes user's data and the confidentiality and privacy of the information processed by these systems Your clients want a detailed understanding of your control environment, as well as service auditor tests and results	Your clients want to make the report available (e.g., for marketing purposes) Your clients will use the report to gain confidence in your organization's systems and controls Your clients don't need details regarding your controls or auditor tests and results
Types 1 and 2?	Yes	Yes	No
Audience Restricted?	Yes	Yes	No
Audience	Your organization's management, as well as a user entity's management and financial statement auditors.	Your organization's management, user entity's management, regulators, business partners, stakeholders, and other appropriate parties, including prospective users or business partners who have an adequate knowledge and understanding of the service organization's industry.	Any interested party.

SOC for Cybersecurity

ATTACK CHALLENGES POSED BY DIGITIZATION

In an age of ever-increasing cyber-attacks, the SOC for Cybersecurity provides objective assurance that enterprise controls are in place to manage such an occurrence. The SOC for Cybersecurity report provides senior management, board of directors, investors, and business partners a better understanding of an organization's efforts, allowing stakeholders to make informed decisions.

The SOC for Cybersecurity examination can be performed for any type of organization, regardless of size or industry. It has been designed to cover an entity-wide cybersecurity risk management program; however, it can also be performed on one or more specific business units or functions within a risk management program or on specific types of information used by the entity.

SOC for Supply Chain

MEET COMMITMENTS AND PRODUCT REQUIREMENTS

The frequently complex sequence of processes involved in the production and distribution of a good or service (supply chain) creates significant risks for the organizations involved. The SOC for Supply Chain is a flexible, market driven report that communicates information about supply chain risk management efforts and assess the effectiveness of an organization's system controls that mitigate those risks.

SOC REPORTS:

Type 1 vs. Type 2

All SOC reports (except for SOC 3) can be either Type 1 or Type 2. The difference is primarily based on the time period in scope.

A TYPE 1 REPORT describes a service organization's suitability of the design and implementation of controls at a *specific point in time.*

A TYPE 2 REPORT ensures that defined control activities are consistently operating effectively over a *defined period of time*—thus yielding improved operational performance.

In many instances, a service organization will begin with a Type 1 report to define the control activities, as of a point in time. Once controls are designed and implemented, the Type 2 report would follow. As the Type 2 report covers a period of time (i.e., 6 or 12 months), this report is more valuable to users because it provides assurance that, during a period of time, controls were operating effectively. An organization typically engages an audit firm to complete the Type 2 report, annually.

How Do I Choose a SOC Auditor?

No matter where you stand in the process of becoming SOC compliant—the readiness/gap identification stage, just starting an examination, or continuing annual compliance—working with a value-add licensed CPA firm is imperative. An auditor will add continual value to your organization and to the report being delivered to your customers and stakeholders.

SOC reporting is not inflexible. Your auditor should work with you to leverage existing processes within your control environment to determine the best approach needed to meet defined control objectives and trust services criteria. As part of your due diligence in selecting an audit firm, we recommend that you ask the following:

- Who will be working on my examination and how experienced are they?
- What differentiates you from other public accounting firms?
- What is your typical examination process?
- How do you gain efficiencies during the examination process?
- How can you add value beyond the examination?

The answers to these questions can assist your organization in making an informed decision.

How Do I Prepare for a SOC Examination?

When starting your first SOC examination, it is beneficial to work with your selected third-party auditor to perform an initial readiness assessment, allowing you to remediate any gaps prior to the start of the SOC reporting process. Taking this step yields a more efficient examination, and much of the initial assessment can be leveraged for the SOC examination.

While each SOC report is different in scope, there are certain areas of focus essential to all SOC examinations. By focusing on the following tasks, an organization can start preparing their employees for a stronger control environment and therefore a more efficient SOC examination.

DOCUMENTATION

From an auditors' perspective, if it's not documented then it doesn't exist. Although there may be strong internal controls in place, the evidence of occurrence may not be memorialized. Ensure documentation is maintained to support all controls in place (e.g., approval for access grants, employee acknowledgements, maintenance of populations, etc.)

DEFINED POLICIES AND PROCEDURES

To ensure all relevant parties understand their responsibilities to meet organizational objectives, ensure fundamental processes and procedures are documented. This provides a resource for both employees and the auditors to understand the organization's intention within the control environment. The scope of policies should include:

- Organizational procedures to meet contractual obligations (SOC 1; SOC for Supply Chain)
- Means of meeting principal service commitments and system requirements (SOC2)
- Risk management approach (SOC for Cybersecurity)

RISK ASSESSMENT

A formalized process facilitated by an annual risk assessment discussion and approved by the board of directors or executive management should exist. In place of a formal annual risk assessment, an organization may also elect to hold quarterly meetings to discuss changes in threats, business operations, etc. and their impact on the overall risk assessment. The risk assessment should include defined risk levels (i.e., low, medium, and high threat) and the Company's remediation approach (i.e., accept, mitigate, or eliminate) with detail as to how the Company has responded or plans to respond in the future.

SOC Examination Expectations

While each SOC report has different requirements and objectives, each is generally performed following seven main stages:

PROCESS STAGE	KEY PARTICIPANTS	KEY MATERIALS
1 **Scoping**	Management Auditors	Background on organizational needs and customer requirements
2 **Walkthrough and Control Design**	Auditors Process and Control Owners	Existing policies and procedures, materials from time spent with each process owner
3 **Gap Assessment**	Auditors Process and Control Owners	Preliminary documentation to support remediation roadmap
4 **Remediation**	Project Manager Process and Control Owners	Documentation for validation of the control environment
5 **Examination/Testing**	Auditors Project Manager Process and Control Owners	Process documentation, examination evidence
6 **Report**	Management Auditors	Policies and procedures, draft feedback, response to feedback and exceptions
7 **Issuance**	Auditors	SOC report

Even with first-year examinations, most of the stages can be accomplished within a defined timeline, though the most unpredictable of the stages is remediation (stage 4). The level of effort spent on remediation is determined based on the results of the gap assessment (stage 3). During the assessment stage, your audit firm will provide a remediation roadmap to ensure compliance with the applicable SOC criteria. By creating a strong control environment prior to the start of the examination, you are setting the foundation for an organized, minimally disruptive audit.

Once the control activities are defined and the first-year examination is complete, the audit process will only consist of stages 5-7.

Value Beyond the Examination

MARKET YOUR ORGANIZATION

Beyond the value gained from the results of a SOC examination, the SOC report can also be used as a tool to market your organization to gain a competitive advantage in the marketplace. A common tactic is to apply for the SOC for service organization logo through the AICPA website once your examination is complete. This logo symbolizes the successful completion of a SOC 1, SOC 2 or SOC 3 examination and can be applied to assets like your website, sales and marketing collateral, and social media.

SECURE FUNDING OR PARTNERSHIPS

A SOC report, as previously shared, demonstrates your commitment to meeting customer needs through accurate, complete, and secure data. This type of information and activity appeals to potential stakeholders or investors and can be leveraged to secure funding or gain business partners.

COMPLY WITH ADDITIONAL SECURITY REQUIREMENTS

Lastly, once the core of the control environment is set to meet the needs of a SOC examination, an organization can leverage the work completed to expand on the scoping/documentation needed to meet further security requirements. As a result of the AICPA's flexibility in meeting SOC examination requirements, it is a good starting point to create centralized reporting and/or compliance with more robust control frameworks such as NIST, CMMC, and others.

Frequently Asked Questions

? What if a client requests a SOC report that differs from what we think is needed?

This is a more common occurrence than many executives realize. We regularly consult with service organizations to evaluate their client needs and determine the appropriate SOC report based on the services they provide. In most scenarios, a SOC 2 report is needed, even when the client initially requests a SOC 1 report.

? Does a SOC 2 examination require significantly more effort than a SOC 1 examination?

It depends. Given the in-depth technical and security-focused nature of SOC 2 examinations, they are typically more time consuming than SOC 1 examinations. However, SOC 1 examinations require more upfront time to determine scope, since the SOC 2 criteria is predefined. For organizations with complex financial processes and controls (e.g., certain mortgage lenders and healthcare claims processors), SOC 1 reports can exceed the time requirements of some SOC 2 reports.

? Why Do Organizations Request SOC Reports?

Any organization that outsources services will typically request a SOC report from a current or prospective service provider to ensure the provider has controls in place to protect their data and/or delivery of services. The need to do so often depends on the nature of the work to be performed and the access the provider has to the customer's financial information, individuals' personally identifiable information (PII) or other sensitive information (e.g., trade secrets), and/or the importance to the organization's service level agreements.

Common scenarios that trigger a request for a SOC report:

- Outsourcing payroll, credit-card processing, recordkeeping, etc.
- Using software as a service (SaaS)
- Storing sensitive data with a cloud service provider
- When infrastructure / data are hosted or managed by an external third-party system

Any company with a business model based on providing a service to another company can benefit from a successful SOC examination.

? What are the biggest issues facing an organization as they prepare for a SOC examination?

Failure to have effective controls in place is an obvious issue. Less obvious, but no less problematic, is having a policy that hasn't been formalized, or a procedure that is insufficient or missing documentation evidencing it occurred. Auditors not only require evidence of what the control is, but also documentation about when and how it was adopted by management.

Another issue we confront when preparing for a SOC examination is getting buy in from not only management, but also from the people performing the controls. Having an internal champion who understands the SOC audit process and educate and prepare the organization for the examination is helpful as you prepare. Learn more about common pitfalls and how to ensure your organization is ready for a SOC examination.

ABOUT SC&H

SOC Audit Services

Our experienced team advises service organizations on AICPA SOC reporting requirements. We provide valuable information that customers, prospects, and auditors require to assess the risks and internal controls associated with an outsourced service provider.

As a qualified firm in this space, we have had innumerable conversations around education, value, and efficiencies. We take pride in working with organizations who have specific needs, competing priorities, time constraints, and other unique objectives. We understand the value of time, appropriate planning, and education that ensure an examination seamlessly progresses.

YOUR SOC AUDIT TEAM

Paul Shifrin
Director

Jodi Harris
Principal

TELL US ABOUT YOUR SOC NEEDS

About SC&H Group

SC&H Group is a nationally recognized audit, tax, and management consulting firm serving rapidly growing private sector businesses to Fortune 500 companies. With more than 300 employees, SC&H Group has a strong foothold along the east coast, a client base representative of global brands, and a client approval rating nearly five-times the industry average (Net Promoter Score = 84.4). We've advised over 1,800 organizations, spanning numerous industries, on accounting, tax, profitability, and business process solutions.

TO LEARN MORE, VISIT WWW.SCHGROUP.COM.