SOC 1 GUIDE

TABLE OF CONTENTS

3 What is a SOC 1 report?

4 What are the benefits of receiving a SOC 1 audit?

5 What is the difference between SOC 1, SOC 2, and SOC 3?

6 What's the difference between a SOC 1 Type I and a SOC 1 Type II?

7 Components of Internal Control

9 Frequently Asked Questions

10 Compliance Guidance

11 SOC 1 Readiness Guide

12 How can KirkpatrickPrice help you complete a SOC 1 audit?

What is a SOC 1 Report?

If you have been asked by one or more of your customers to provide a SOC 1 report, it is likely that you are a service organization which provides a service to customers, or user entities, that is relevant to the operation of their business. When a user entity outsources functions that affect its internal control over financial reporting (ICFR), management of the user entity needs to gain an understanding of relevant controls that are performed by the service organization. This is generally accomplished through a SOC 1 engagement.

A SOC 1 audit is an examination that is specifically designed to address controls at a service organization that are likely to be relevant to user entities' ICFR. A SOC 1 report provides management of a service organization, its user entities, as well as independent auditors of their financial statements with information and an opinion on these controls. The report validates your organization's commitment to delivering high quality, secure services to your clients.

Many companies rely on SOC 1 reports to address Sarbanes-Oxley (SOX) and other compliance requirements.

What are the benefits of receiving a SOC 1 audit?

A SOC 1 audit provides assurance by testing the internal controls that a service organization has implemented to ensure the completeness and accuracy of user entities' data, specifically the internal controls that may impact financial reporting. SOC 1 audits are conducted in accordance with the Statement on Standards for Attestation Engagements 18 (SSAE 18) established by the AICPA.

It is important to note that compliance is not achieved by simply completing a checklist; however, this guide will help prepare your organization to undergo a SOC 1 audit. An audit with KirkpatrickPrice will provide assurance to key stakeholders over the controls you have implemented to meet the requirements of a SOC 1 audit and provide your organization with confidence in the effectiveness of those controls.

What is the difference between SOC 1, SOC 2, and SOC 3?

Each SOC report type fulfills a different purpose, and organizations should understand which report will best meet their needs before embarking on the SOC audit process. The System and Organization Controls Suite of Serivices were developed by the American Institute of Certified Public Accountants (AICPA). In the context of SOC reports, internal controls are procedures designed to ensure compliance with policies relevant to company operations, laws and regulations, and financial reporting.

What Is a SOC 1 Report?

SOC 1 engagements are based on the SSAE 18 standard and report on the effectiveness of internal controls at a service organization that may be relevant to their client's internal control over financial reporting (ICFR).

What Is a SOC 2 Report?

A SOC 2 audit evaluates internal controls, policies, and procedures that directly relate to the security of a system at a service organization. The SOC 2 report was designed to provide service organization management, user entities, business partners, and other parties with information about controls at the service organization relevant to security, availability, processing, integrity, confidentiality, or privacy to support users' evaluations of their own systems of internal control. This is also known as the Trust Services Criteria.

What Is a SOC 3 Report?

A SOC 3 report, just like a SOC 2, is based on the Trust Services Criteria, but the major difference between these two types of reports is restricted use. A SOC 3 report can be freely distributed, whereas SOC 1 and SOC 2 reports can only be read by management of a service organization and the user organizations that rely on their services. A SOC 3 does not give a description of the service organization's system, but it can provide interested parties with the auditor's report on whether an entity maintained effective controls over its systems as it relates to the Trust Services Criteria.

When trying to determine whether your service organization needs a SOC 1, SOC 2, or SOC 3 audit, keep these requirements in mind:

- Does your service affect a client's financial reporting? A SOC 1 would apply to you.
- Does your service organization want to be evaluated on the Trust Service Criteria? SOC 2 and SOC 3 reports would work.
- Does restricted use affect your decision? SOC 1 and SOC 2 reports can only be read by the user organizations that rely on your services. A SOC 3 report can be freely distributed and used in many different applications.

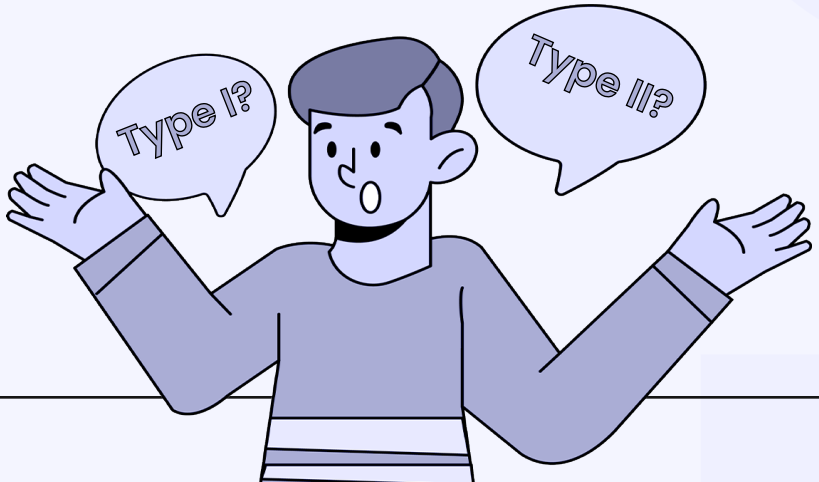
What's the difference between a SOC 1 Type I and a SOC 1 Type II?

Understanding the difference between a SOC 1 Type I and SOC 1 Type II is simple; it comes down to the audit period and the extent of testing. While both a SOC 1 Type I and SOC 1 Type II report on the controls and processes at a service organization that may impact their user entities' internal control over financial reporting, the main difference between the two types of audits is the period in which the auditor verifies the effectiveness of internal controls.

For example, if an organization opts to engage in a SOC 1 Type I audit, the auditor will assess and report on the design of their controls to achieve the control objectives included in the report that relate to financial reporting *as of a specified date*. On the other hand, if an organization wants to pursue a SOC 1 Type II audit, the auditor will assess the design and *operating effectiveness* of their controls to achieve the control objectives included in the report that relate to financial reporting *throughout a specified period*.

The type of SOC 1 audit your organization needs depends on your organization's compliance goals. In many cases, clients will not specify which type of audit they want you to have. In these instances, we recommend that organizations begin with a Type I audit and then move onto a Type II audit, if needed.

Beginning with a Type I audit allows your organization and your auditor to focus on the design and implementation of your internal controls, whereas a Type II requires additional time, testing, and resources that might make the audit process more challenging if you've never reviewed your internal controls before.



Components of Internal Control

Various frameworks can be used as established criteria for designing, implementing, and evaluating the effectiveness of internal control. A SOC 1 audit typically evaluates COSO's Internal Control – Integrated Framework. This framework highlights 5 components of internal control and formalizes the concepts into 17 principles associated with the components. COSO defines internal control as a process effected by an entity's board of directors, management, and other personnel designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

The five components that the COSO framework states should be in place to support a company's internal control system are: control environment, risk assessment, information and communication, monitoring activities, and control activities.

What do the five components of internal control mean for your organization?

1

Control Environment

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct.

2

Risk Assessment

Risk assessment is a critical component of a service organization's compliance, which is why the COSO framework incorporates it into the components of internal control. Members of an organization need to understand the risk they are up against and how that risk could affect the achievement of internal control objectives.

3

Information and Communication

When there's a system change, management needs to know how to communicate that change to internal employees and/or external users in an effective and efficient way. Quality information and effective communication enables personnel to understand internal control responsibilities and their importance to the achievement of objectives.

4

Monitoring

Management needs to monitor the operating effectiveness of the organization to be able to address and correct any issues. Ongoing evaluations, separate evaluations, or some combination of the two are typically used to ascertain whether each of the five components of internal control, including controls to affect the principles within each component, is present and functioning. Findings are evaluated and deficiencies are communicated in a timely manner, with serious matters escalated as necessary.

5

Control Activities

This is the largest component of the COSO framework, as it provides the details about the controls that have been put into place to meet internal control objectives. Control activities are the actions which are established by policies and procedures that help ensure the risks identified in the risk assessment are mitigated to achieve objectives. These activities should be performed at all levels of the organization and at various stages within individual business processes, including the technology environment.

Frequently Asked Questions

What system components are evaluated during a SOC 1 audit?

During the planning phase, the auditor will work with you to determine the scope of the engagement. Typically, the components are derived from the people, processes, and technology that support the service(s) offered to your customers:

- **Infrastructure** - operating system(s), database(s), and network(s), including cloud platforms (AWS, Azure, GCP)
- **Software** - application programs and IT system software that support your service(s)
- **People** - all personnel involved in the delivery of your service to your customers
- **Processes** - all automated and manual procedures
- **Data** - transmission streams, files, databases, tables, and output used or processed by a system

What are your auditors looking for?

- A fairly presented description of your system
- The suitability of the design of your controls included in the description
- The operating effectiveness of the controls over a period of time (Type II)

How long does a SOC 1 audit take to complete?

The average SOC 1 audit can take anywhere from weeks to months, depending on a variety of factors, including the scope of the engagement, the nature and level of complexity of your service, the size of your organization, the length of the period being evaluated (Type II), and your level of preparedness and staff's availability for interviews and control demonstrations. To satisfy the AICPA requirements for an engagement, the auditor must validate scope, perform testing procedures, and document conclusions. These steps require time from the service organization's management, which can be compressed or extended to meet your timeline needs.

Who can perform a SOC 1 audit?

A SOC 1 audit can only be performed by an independent auditor at a CPA firm. CPAs must adhere to the specific standards that have been established by the AICPA and have the technical expertise necessary to perform SOC 1 engagements.

Compliance Guidance

This exclusive SOC 1 compliance guide outlines the typical areas that will be evaluated by your auditor during your SOC 1 audit. Use this guide to learn what your auditors are looking for and how to prepare for your SOC 1 audit.

Keep in mind, you don’t have to have everything perfectly in place to start your audit; this guide should be used as a tool to help you prepare for your audit. If you need help putting any controls in place, contact one of our experts today! We want to make sure you feel ready to successfully complete your SOC 1 audit!

SOC 1 Readiness Guide

- [ ] Define system and/or service(s) offered to customers
- [ ] Determine report type (Type I or Type II) and period (Type II only)
- [ ] Define relevant business processes
- [ ] Define the systems(s) in place that support service delivery
- [ ] Define relevant location(s)
- [ ] Define relevant third parties that support service delivery (Subservice Organizations)
- [ ] Determine who is receiving the report (user entities)
- [ ] Determine relevant personnel and ensure they are available for client-visit week activities
- [ ] Ensure a Risk Assessment is performed at least annually
  - [ ] Potential threats (internal andexternal) to the system or service have been identified
  - [ ] The significance of the risks associated with each threat has been analyzed
  - [ ] Controls have been designed and implemented to address the risks identified
- [ ] Define control objectives
- [ ] Regular vendor management assessments are performed
- [ ] All organizational controls are documented with policies and procedures
- [ ] Physical and logical access controls are in place
- [ ] Access to data, software, functions, and other IT resources is limited to authorized personnel based on roles
- [ ] Physical access to sensitive locations is restricted to authorized personnel only
- [ ] An access control system, as well as monitoring to identify intrusions, has been implemented
- [ ] Incident response procedures have been developed and tested
- [ ] Software, hardware, and infrastructure is updated regularly as necessary
- [ ] A change management process is in place
- [ ] Backup and recovery policies are in place
- [ ] Environmental risks have been addressed
- [ ] Your disaster recovery and business continuity plans have been tested and documented

How can KirkpatrickPrice help you complete a SOC 1 audit?

At KirkpatrickPrice, we care about helping you reach your security goals. That includes supporting you from audit readiness to final report. When you choose to undergo a SOC 1 audit with KirkpatrickPrice, you get access to experienced professionals who will help you identify the scope of your project, will thoroughly test your controls, and will communicate with your client's auditing partner until the project is completed.

Audits are a team effort. You'll work with a dedicated audit team made up of your client success manager, your auditor(s), and one of our in-house report writers. This team will ensure that you receive a high-quality audit, an on-time report you can show off, and an audit experience that makes all of your efforts worth it.

A Thorough Audit Makes a Difference

When you choose KirkpatrickPrice for your SOC 1 audit, you won't simply receive a checkbox audit that is left solely to automation. Our team will work with you through our compliance tool, the Online Audit Manager (OAM), and in person to gather evidence, answer your questions, and track your progress. We believe in actually evaluating controls, reading your policies and procedures, and assessing your environment to make sure you're doing everything you can to keep your organization secure.

Audits are hard. We make sure they're worth it.

At KirkpatrickPrice, we know that when it comes to threats you want to make sure that you're ready. In order to do that, you need quality cybersecurity and compliance audit reports and results you can trust. The problem is SOC 1 audits are hard because the process is complicated and feels overwhelming. We believe if you're going to do it, that audit should be worth it. We've been in your shoes and know how hard audits can be, but we've issued over **20,000 reports** to **2,000 clients** worldwide, giving them the assurance they deserve.

When you work with KirkpatrickPrice, you can stop feeling like you are going to miss something or be surprised when a client or attacker finds something that wasn't in your report. You can stop feeling worried that you're wasting your time using someone who's not advanced enough to thoroughly test your environment. Instead, you'll have a report that gets you ready for your next steps, allows you to say yes to client requests, and provides you the assurance you deserve. Cybersecurity and compliance will no longer be a mystery.

To get started on your SOC 1 audit, call one of our experts today at **800-770-2701** or visit **www.kirkpatrickprice.com.**

About the Author

Logan Sizemore

Director, Audit Delivery

CPA

Logan R. Sizemore, MAcc, CPA currently serves as Director, Audit Delivery at KirkpatrickPrice. In his role, Logan is focused on managing the delivery of quality audit and attestation engagements and subsequent reports, including SOC 1 and SOC 2 reports. Logan serves as a subject matter expert both within the firm as well as with our clients, and he has experience with clients of all sizes and across a variety of industries. Logan previously worked at Deloitte, where he provided IT and Specialized Assurance services for clients across the Life Sciences & Health Care, Consumer & Industrial Products, and Retail industries.

Connect with Logan on LinkedIn