Sensiba

WHITE PAPER

Getting Your First SOC 1 Report

Table of Contents

OVERVIEW

Introduction

What we call a SOC 1 report has been around, in different forms, for decades. Back in the day, it was referred to as a SAS 70 report and it had, and still has, a very specific use case. These reports were designed for companies that provide outsourced services, known as service organizations, a tool to manage requests from their customers —and, more importantly, their customer's auditors.

The SOC 1 report describes how the service organization's system processes information and records and reports transactions outsourced to the service organization, affecting their customer's financial reporting.

Some classic examples of service organizations that obtain SOC 1 reports include payroll providers (such as ADP or Paychex), third-party administrators of employee benefit plans (Fidelity Investments), or service organizations that perform complex accounting calculations for their customers such as stock-based compensation (Carta) or SaaS revenue and billing solutions (Maxio).

Over the last several years, we're seeing more instances where SOC 1 requirements are being placed on companies as part of vendor compliance, similar to how the need for SOC 2 arises. While this is not necessarily consistent with the intent of SOC 1, it provides a compelling reason to consider obtaining a SOC 1 report on your system.

This paper will discuss how to obtain a SOC 1 audit, with an emphasis on getting to SOC 1 from the starting point of a completed SOC 2 audit. The reason this approach makes sense is because there is overlap between SOC 1 and SOC 2 reports that can be leveraged, and many companies that need SOC 1 often also need, or already have, a SOC 2 report.

There are a lot of similarities between SOC 1 and SOC 2 reports. Both are audit opinions, provided by a licensed CPA firm, on your company's internal controls. Both include a written management assertion as well as a system description—a written narrative that describes what the service organization's system does, how it operates, the data it processes, and other key details. Both reports also include a listing of controls and the results of the testing of those controls by the auditor.

The Importance of SOC 1 in Auditing

The example service organizations cited above are larger companies that provide services that would very likely affect their customers' financial reporting significantly. They also have customers that need audited financial statements.

To avoid dealing with each customer's financial statement auditor, these service organizations will have their system audited and described in the form of a SOC 1 report they can share with the customer's auditors. This is the true purpose of the SOC 1.

When performing a financial statement audit, the auditor is required to understand the company they are auditing. This includes how the company processes its transactions. If this function has been outsourced, the auditor is required to follow procedures to understand how the outsourced service organization processes transactions.

To gain this understanding, the auditors will read the service organization's SOC 1 report, especially the audit opinion (i.e., you want a clean opinion). This will often satisfy their requirements. The auditor may still want to follow up with questions on how the system processes transactions or how reports are created, but this is rare.

If you don't have a SOC 1 to hand to your customers, you may get requests for detailed, and potentially time-consuming, walkthroughs of how your system works to process transactions.

How SOC 1 Interplays With SOC 2

The SOC 2 [1] report began life about 15 years ago as the AICPA saw how SAS 70 reports were often being used by service organizations to attest to the security of their datacenter and computer service operations for the emerging application service provider and co-location businesses that were evolving in the 2000s.

While many of these service organizations were providing services that had little to do with financial reporting, their ability to provide an audit report describing their solution was seen as a valuable way to prove to their customers their systems had been tested and thus offered a "secure" place for customers to entrust their data. The AICPA responded to this market need by rewriting the SAS 70 standard to effectively split the SOC 1 and SOC 2 reports for these different business purposes.

This is how the AICPA and accounting and auditing firms got so heavily involved in the information technology world. Ultimately, SOC 2 demand led to the creation of a huge market, and as a result, currently there are many more SOC 2 reports issued than SOC 1 reports with the transformation to the cloud over the last decade.

As we noted above, a SOC 1 report is a report on business processes and internal controls over financial reporting. A SOC 2 report examines controls related to the Trust Services Criteria (Security, Availability, Confidentiality, Processing Integrity, and Privacy), with the primary emphasis on Security.

Over the past several years, there has been almost exponential growth in SOC 2 due to vendor risk management considerations.

A SOC 2 is often a specific request as companies evaluate the security stance of the service organizations to which they are outsourcing custody of their data. Due to this market growth, there are numerous SOC 2 readiness platforms, many with significant funding and broad marketing reach.

SOC 2 has a structured framework for reporting based on the Trust Services Criteria. With this structured framework and the readiness platforms out there, the path to getting the first SOC 2 is well-defined.

SOC 1, however, is much more of a blank sheet and the nature of the controls to be reported on will be highly dependent on the nature of the service organization's system, the business processes involved, and how information is generated. Further, the overall market for SOC 1 is a fraction of SOC 2, so the tools and platforms for SOC 1 readiness are limited.

As such, getting to SOC 1 readiness can be, and often is, a more challenging and wide-open process than obtaining a SOC 2 report.

[1] Learn more about comparing SOC 1 and SOC 2

Types of Controls

Taking a closer look at the controls, there is even more overlap between SOC 1 and the SOC 2 reports. As most service organizations are developing their solutions using computer-based—often cloud—systems, many of the controls in a SOC 1 report will cover the computer/cloud operations of that system. For future reference, these computer controls in SOC 1 are referred to as Information Technology General Controls (ITGCs).

Another type of control common to both SOC 1 and SOC 2 reports are what are called "entity-level" controls, which describe how the service organization is governed and managed. Examples of entity-level controls would include written policies and procedures that are trained out to the employees. These often include controls over on-boarding and off-boarding of employees, proper tone at the top, proper governance of the organization, and other key processes and policies.

(See Appendix 1 for sample entity-level controls.)

SOC 1 and SOC 2 reports will both have entity-level and ITGC controls.

At this point the SOC 1 and SOC 2 controls will diverge, with the SOC 2 having more specificity in their controls to meet the TSCs and the SOC 1 will likely have controls over the service organization's business processes that are specific to financial reporting. These controls are referred to as ICFRs (internal contros over financial reporting).

Entity Level (Applicable to both SOC 1 and SOC 2)	
The company has a documented Information Security Policy, and makes it available to staff on the company intranet.	A risk assessment is performed on an annual basis to identify and rank potential threats to the system.
ITGC (Applicable to both SOC 1 and SOC 2)	
Customer data at rest is encrypted.	System changes must be approved by an independent technical resource prior to deployment to production.
ICFR Controls (SOC 1 Specific)	
New client setup information is reviewed by management for completeness, accuracy and timeliness through completion of a mock payroll run for new clients.	On a daily basis, the Payroll Treasury Manager performs a bank reconciliation of payments booked against the bank transactions for the previous business day.
SOC 2 Specific Controls	
The company uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.	Vulnerability scans are performed on a quarterly basis to identify vulnerabilities and management takes action based on the results of the scan.

SOC 1 Starting Point Scenarios

When discussing getting to your first SOC 1, there are three relevant starting places to consider and some pointers to consider. While specifics will depend on your company's situation and needs, common scenarios include:

SCENARIO 1

If your company already has a SOC 2 report:

- Leverage entity-level and ITGC controls from your SOC 2 by mapping those controls over to your SOC 1 report.
- Evaluate the relevance of ICFR controls and add those control objectives and controls to complete your SOC 1 report.
- Revise the system description from your SOC 2 report to the proper presentation for SOC 1.
- If you use a SOC 2 readiness platform, consider customizing the readiness platform to track your SOC 1 compliance.

SCENARIO 2

If your company does not have a SOC 2, but has SOC 2 compliance in mind along with getting a SOC 1 report:

- If SOC 2 is on your radar, even if it isn't a priority, it might make sense to pursue SOC 2 readiness first. This would be especially true if you're in the cloud, where the utilization of a SOC 2 readiness platform would be beneficial.
- Using this approach allows for the company to benefit from the SOC 2 readiness platform to build the foundation for SOC 1 while moving the SOC 2 initiative forward.
- If this scenario is applicable, you can refer to the pointers in Scenario 1 above.

SCENARIO 3

If your company only needs SOC 1:

- In this instance, it may make sense to obtain project management resources to work with the company on the core elements of a SOC 1 control environment, such as policies and procedures, entity-level controls, and other key details. Someone with SOC and controls experience can greatly benefit the company.
- Where there is no previous SOC 2 to leverage, you will need to create the entity-level controls, risk assessment processes, process and policy documents, and other important processes, documents, and procedures necessary to support the control environment from scratch.

Approach for ICFR

As noted previously, the SOC 1 report does not have a defined framework, so the needed controls in your SOC 1 report will really depend on two factors:

1. The type of services offered by the service organization.

2. The risks that customers and their auditors are concerned about related to the transactions processed and reports generated by the system.

When thinking about ICFR, you should understand the process, how it is performed, and what is done to ensure the process is performed correctly. It can be very helpful to document the process via a walkthrough, process narrative, (see Appendix 2) and a flow chart.

When writing the controls for the relevant business processes, the following template can help you organize what you will need to gather for SOC 1.

How Many and What Types of ICFR Controls Do I Need?

The good news is that there is no mandatory number of controls or control objectives. As every system is different, there is no specific requirement to meet as a minimum. In fact, there are instances where there are no specific ICFR controls.

In these instances, the covered controls would be the entity-level, risk assessment, and computer operation controls, and those could be sufficient.

Instances where this would be sufficient would include computer-based systems that have only automated controls (i.e. do not involve human intervention). You don't need to have a control for everything the system does. A system with strong entity-level and computer operation controls provides assurance that the system and the automated controls built into the system will operate correctly.

Types of ICFR Controls

When looking at the controls to include as part of ICFR, you would look to:

- Controls that rely on human input, calculations, or verification.
- Controls with very complex calculations that are difficult to perform.
- Reports the system produces that have significant impact on your customer's financial reporting.
- Other automated controls that often make sense to include [2], such as:
  - Audit trail functionality (i.e., immutable transactions that require reversing transactions to correct or change).
  - Role-based logical security, especially functionality that enforces proper segregation of duties. For example, requiring separating the role of the transaction initiator from the role of transaction approval.
  - Data validation controls. These are input controls to prevent the entering of information or transactions outside of specified ranges or other requirements.

[2] These examples are controls that often make sense to include as they speak to risks the financial auditor would be worried about. These controls are all automated, which makes them relatively easy to test.

Scoping Your First SOC 1

Scoping a SOC 1 engagement involves defining the boundaries of the audit and determining the systems and controls that are relevant to the services provided by the service organization that impact their clients' financial reporting.

The scoping conversation takes place early in the SOC 1 process and typically involves the auditors. Often times, the scope of the SOC 1 can be determined by the purpose of the SOC 1, who is requesting the SOC 1, and what business functions they want coverage over. Additionally, identifying the people, processes, and technology involved in providing the services to clients is important. Once the scope is determined, the auditors can begin readiness to help develop control objectives and relevant controls.

Conclusion

Obtaining your first SOC 1 report is a significant step for any service organization. The SOC 1 demonstrates your commitment to robust internal controls over financial reporting while enhancing your credibility with customers and their auditors.

By leveraging the similarities between SOC 1 and SOC 2, you can streamline the process and make it more manageable—especially if you already have a SOC 2 report.

The journey to SOC 1 readiness can be complex, but it is manageable with careful planning and the right resources. Whether you start from a SOC 2 report or from scratch, focusing on the key controls and processes that impact your financial reporting is crucial.

Engaging with experienced professionals can provide valuable guidance and ensure your SOC 1 report is comprehensive and meets all necessary standards.

As the demand for SOC 1 reports grows, driven by vendor compliance and customer requirements, staying ahead of the curve is essential. By understanding the intricacies of SOC 1 and how it interplays with SOC 2, you can better prepare your organization for the audit process. This proactive approach will not only save time and resources but also build trust with your stakeholders.

About Sensiba

Sensiba's comprehensive accounting, tax, and consulting services help businesses and people solve problems, navigate complexity, and build a foundation for sustainable growth. A top-100 U.S. firm, we're passionate about collaborating with clients to increase efficiency, mitigate risk, and prepare to embrace emerging opportunities.

Our Risk Assurance professionals understand your challenges and help you identify, analyze, and manage potential risks. We'll work with you to customize risk models and provide support to will help you protect and enhance the value of your business. Our System and Organization Controls (SOC) audits help you build trust and credibility with customers and prospects, improve data security and regulatory compliance, and unlock market opportunities.

Contact Us

Appendix

APPENDIX 1

Entity-level controls are policies, procedures and standards of behavior for members of the board of directors, company officers, management, and employees. The behavior of upper management usually sets the tone, and working examples, for behavior throughout the organization.

Common entity-level controls may include the organization's:

- MISSION STATEMENT
- CODE OF ETHICS
- STATEMENT OF VALUES
- CODE OF CONDUCT
- AUDIT, TESTING, AND REPORTING REQUIREMENTS
- EMPLOYEE HANDBOOK OR RULEBOOK
- TRAINING MANUALS
- INTERNAL COMPLAINT PROCEDURES
- CONTINUING EDUCATION REQUIREMENTS
- EMPLOYEE REVIEW PROCESSES

APPENDIX 2

Sample Process Narrative

Performing a walkthrough of a process from initiation through recording in the financial statement is one of the most efficient ways to learn how an entity processes transactions and information. This sample includes a brief process narrative and the controls identified during the walkthrough.

Sample Financial Management Process

As part of the organization's financial management process, the controller develops an annual financial plan and budget that includes predicted results and detailed analysis of key areas within the company. After the plan is developed, the CFO conducts an independent review and meets with the controller to evaluate the plan's assumptions and conclusions.

CONTROL 1

After completion, the CFO reviews the controller's work on the budget and financial plan. This control, designed effectively and implemented properly, is selected for testing.

Each month, the controller prepares a detailed gross margin analysis for the monthly board meetings.

CONTROL 2

Before presenting to the board, the controller reviews the gross margin analysis, which is performed as part of a more general review of actual results vs. budgeted results (Key Performance Indicator Analysis).

Control is designed effectively and properly implemented. This control is not selected for testing.

At monthly board meetings, the CFO and CEO review actual operating results at each month-end (including the detailed gross margin analysis) and question variances from budget. All results and variances are discussed in a monthly meeting of the CEO, CFO, and the controller.

The CEO, CFO, and the board review each financial statement line item for reasonableness. All accounts that require management estimation, such as reserve accounts, receive additional scrutiny.

CONTROL 3

The CEO and CFO review the gross margin analysis and actual results monthly and compare them with the budget (Management Review). Control is designed effectively and properly implemented. This control is selected for testing.

CONTROL 4

At the board meeting following the end of the quarter, the CEO, CFO, and board review each financial statement line item and accounts that require management estimation (Management Review). Control is designed effectively and properly implemented. This control is selected for testing.

Sample Identified Controls

The following controls have been identified:

CONTROL 1

After completion of the budget and financial plan, the CFO reviews the controller's work (Management Review).

CONTROL 2

Before presenting to the board, the controller reviews the gross margin analysis, which is performed as part of a more general review of actual results vs. budgeted results (Key Performance Indicator Analysis).

CONTROL 3

The CEO and CFO review the gross margin analysis and actual results monthly, and compare them to the budget (Management Review).

CONTROL 4

At the board meeting following the end of the quarter, the CEO, CFO, and the board review each financial statement line item and accounts that require management estimation (Management Review).

APPENDIX 3

Control Objective 10: Data Validation - Controls provide reasonable assurance that data entry is consistent.*						
Ref	**Company Description of Controls**	**Test Results**	**Operating Effectively**	**Automatic/ Manual****	**User Control Considerations*****	**Example Evidence provided**
10.1	Company system maintains the customer price list(s) for users' reference and constrains users' pricing inputs when generating new orders to the pricing and discount ranges in the customer's approved price list(s). As such pricing rules are enabled to be set by set price or tier-based pricing. Company system will only allow for customers to be generated from the ERP master customer list.	Inquired of Lead Software Engineer as to the company systems' ability to constrain pricing to price lists and discounts that are defined by user entities. Observed the configuration screen in the company system providing for this functionality.	No exceptions noted.	No exceptions noted. Does the control happen automatically without human intervention? If it is manual how many times does it operate? We will need to sample	Are there any specific things your customer needs to do for this control to operate?	Screenshot/report or other evidence. Please explain and reference
10.2		Inquired of Lead Software Engineer who verified that customer information is pulled from the associated ERP system. Observed the generation of a new order whereby customer data was linked to ERP data.	No exceptions noted			
10.3	Data Integrity checks					

* Control Objective language is up to you.

** As auditors, we need to understand how the control operates. If it is a computer-based control (i.e., automatic), we only need to see evidence of the control operating once. However, if there is human intervention (manual), we need to understand the population (i.e., how many times does the control operate – ad hoc, annually, quarterly, daily). We will need a listing of the times the control operates so that we can sample from it.

*** You may want to have specific language to tell the reader of the report that you must do this for this control to operate. There is no need to state obvious or best practice items. If there is something specific or not obvious that the customer needs to do, an explanation should be considered. The determination of what is a required Complementary User Entity Control is judgment-based and not formulaic.

Sensiba