# A Complete Guide to SOC Examinations: A Proven Process

BARR ADVISORY

# Table of Contents



# SOC Examinations Overview

The SOC framework, as defined by the American Institute of CPAs (AICPA), is a suite of audit engagements which stands for System and Organization Controls. Ultimately, a SOC examination generates a report on the effectiveness of an organization's internal controls while receiving feedback on how to align with best security practices.

As threat landscapes continue to expand, more organizations are at a high risk of compromising personal and customer information. While never required, SOC examinations are becoming increasingly popular, and demonstrating your cybersecurity practices to potential customers has become an expectation of vendors.

## Benefits of SOC

As one of the most common frameworks in cybersecurity, SOC examinations help differentiate your organization by reporting on controls and providing oversight of your governance and risk management process.

When you complete a SOC examination, your organization will not only receive a stamp of approval, you'll also:

- Increase trust and transparency with your internal and external and stakeholders;
- Reduce costs of compliance and number of onsite audits;
- Ensure that your controls are appropriately designed and operating effectively to mitigate risks; and,
- Satisfy your audit requirement to meet your security and compliance goals.

## Types of SOC Examinations

All SOC engagements fall under the AICPA suite of services—offerings provided by a third-party auditor in connection with system-level controls of a service organization or entity-level controls of other organizations.

From these offerings, BARR currently provides four types of SOC examinations.

**SOC 1**: A SOC 1 report, once known as SSAE16, helps service organizations demonstrate their controls specific to the client's financial reporting.

**SOC 2**: SOC 2 reports apply more broadly to operational controls of a service organization covering one or more of the five Trust Services Criteria: Security, availability, confidentiality, processing integrity, and/or privacy across a variety of systems.

**SOC 3**: Much like the SOC 2 report, the SOC 3 examination reports on a service organization's system security, availability, processing integrity, confidentiality, and/or privacy related to the Trust Services Criteria. This report is less detailed and can be distributed on a website for the public to read.

**SOC for Cybersecurity**: Launched in 2017, SOC for Cybersecurity is a reporting framework over an entire entity's cybersecurity risk management program and related controls.

## What is a SOC Report, and Who Needs One?

SOC reports are the final deliverable your organization receives once you complete your examination. While not technically a certification, SOC reports demonstrate to customers and stakeholders that your organization is following best practices to secure valuable information.

SOC reports come in two forms—Type 1 and Type 2.

**Type 1 Report:**

- The SOC 2 Type 1 Report (referred to as a point-in-time report), includes an opinion over the suitability of the design of controls at the service organization at a specific point in time.
- An initial type 1 report often serves as the starting point for subsequent type 2 reviews.

**Type 2 Report:**

- The SOC 2 Type 2 Report (referred to as a period of time report) includes an opinion over the suitability of the design of controls at the service organization and the operating effectiveness of the controls throughout a specified period of time.
- This type of report is often issued annually.

With SOC 1, 2, and SOC for Cybersecurity, you have the option of selecting which report benefits your organization's needs at the time. However, it's important to note that SOC 3 examinations are only available as a Type 2 report.

Examples of organizations who benefit from SOC reports:

**SOC 1**

- Cloud ERP service providers
- Financial services
- Payroll processing
- Payment processing
- Healthcare claims processing
- Data center colocation

**SOC 2**

- Cloud service providers (Saas, IaaS, PaaS)
- Enterprise systems housing third-party data
- IT systems management

**SOC 3**

- Cloud service providers (Saas, IaaS, PaaS)
- Enterprise systems housing third-party data
- IT systems management

**SOC for Cybersecurity**

- Lenders
- Investors
- Analysts
- Insurance providers
- Regulators

## The SOC 2 Examination—A Popular Framework

SOC 2 is one of the most popular security frameworks and intends to meet the needs of a broad range of users that require detailed information and assurance about the controls of a service organization. SOC 2 reports (Type 1 and Type 2) are based on the AICPA Trust Services Criteria.

### AICPA Trust Services Criteria

- **Security**: Information and systems are protected against unauthorized access and unauthorized disclosure, including potentially compromising damage to systems. Information (or data) should be protected during its collection or creation, use, processing, transmission, and storage.
- **Availability**: Data and systems are available for operation and use. Systems include controls to support accessibility for operation, monitoring, and maintenance.
- **Confidentiality**: The organization should protect information designated as confidential (i.e. any sensitive information).
- **Processing Integrity**: System processing (particularly of customer data) is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- **Privacy**: Personal information is collected, used, retained, disclosed, and disposed of in accordance with relevant regulations and policies.

**In SOC 2 reports, security is the only required criteria**, however, organizations can choose to add other standards within the scope of their audit. For example, it's common for organizations to include Availability and Confidentiality, and larger enterprise organizations may want to add Processing Integrity and Privacy, as those address both internal and external customer requests.

As always, BARR serves as your trusted partner and will walk you through each criteria to help you choose what's best for your organization.

## Sections of a SOC 2 Report

SOC 2 reports contain a lot of information. Like the nutritional facts label on the back of a food and beverage container, SOC 2 reports serve as your "nutritional" security label—a document providing information about the operations and efficiency of your organization. Let's break down the SOC 2 report and how to interpret each section.

- **Section 1**—Auditor's Report
- **Section 2**—Management Assertion
- **Section 3**—System Description
- **Section 4**—Description of Criteria
- **Section 5**—Other Information (optional)

## Section 1—Auditor's Report

Section 1 of your SOC 2 report includes information written by your auditor. This section highlights whether or not your organization "passed" the assessment, which is categorized as either qualified or unqualified.

### Qualified Opinion

"Qualified" may seem like a positive result in most circumstances, however, for a SOC 2 report a qualified opinion actually means that the auditor found at least one issue that did not work effectively throughout the reporting period.

While receiving a qualified opinion for your SOC 2 report can feel daunting, it's not the end-all, be-all. In fact, it's fairly typical for auditors to find issues that deem controls as either 1.) designed or 2.) operated ineffectively. Throughout this process, BARR acts as your true partner, walking you through what we find, and guiding you toward success along the way.

### Unqualified Opinion

Receiving the opinion that your organization is unqualified means you "passed," and the auditor didn't find any issues with the effectiveness of your controls during the specified reporting period.

## Section 2—Management Assertion

Section 2 allows your organization to state that you did, in fact, prepare and implement your system description. It's an overview of your organization stating that:

- The controls stated in the description were designed and implemented within a specific reporting period.
- The controls stated in the description operated effectively throughout the specified reporting period (Type 2 only).

While this section will not contain technicalities, it acts as a precursor to Section 3, where you will write your own system description in greater detail.

## Section 3—System Description

Section 3 includes important information regarding the people, processes, and technology that support your product or service. Companies often write their own description, and it serves as an overview of your organization's systems and controls you have in place.

This section is arguably the most critical section of your SOC 2 report, as your response will help auditors like BARR assess whether or not your system components are effectively protecting your customer data.

Here are the eight components that the AICPA recommends you include in your system description:

1. Types of services provided
2. Principal service commitments and system requirements
3. Components of the system
4. Trust Services Criteria and corresponding controls
5. Complementary user entity controls
6. Complementary subservice organization controls
7. System incidents
8. Significant changes to the system during the period

While writing your own system description might feel intimidating, as your auditor, BARR is here to guide you through the process, working with you along the way.

## Section 4—Description of Criteria

Section 4 is the most detailed section within your SOC 2 report. This is where all your controls that were evaluated are listed. Think of this section like an index where you can easily find the most relevant information from your audit.

Up until now, Type 1 and Type 2 reports will look relatively the same. However, in Section 4, a Type 1 report will contain different information than a Type 2 report.

### SOC 2, Type 1 Report

Because Type 1 reports are a point-in-time assessment, in Section 4 of the SOC 2 report, you'll find a list of controls tested without the auditor's test results. Under the AICPA, Type 1 reports only require the auditor's evaluation if the controls were designed properly within a specific period of time.

### SOC 2, Type 2 Report

Type 2 reports, on the other hand, do include all the controls tested and the auditor's test results. You might find that most people go straight to this section when reading a SOC 2 report. This is because, in this section, you can find any controls that the auditor might have flagged as operating ineffectively.

## Section 5—Other Information (optional)

This section is available as an optional part of your SOC 2 report where your organization can provide additional information relevant to your audit. Within this section, you might find details like a response to any exceptions found during the SOC 2 report. For example, if the auditor lists a specific gap in Section 4, in this section, your organization can provide additional context for why that gap might exist.

# Getting Ready for Your SOC Examination

## The Readiness Assessment

Many organizations choose to complete a readiness assessment prior to their SOC examination. The readiness period of your SOC audit is meant to prepare your organization's policies and procedures so your assessment runs smoothly. Think of it like the dress rehearsal for your examination—you're making sure everything's running smoothly and in place before the big performance.

## Choosing Your Path: Readiness Assessment Versus Automation

When preparing for your audit, there are two options you can choose prior to examination reporting:

1. Readiness Assessment: Plan and conduct the preparation work manually. This typically consists of interviews, a deep dive into your cybersecurity processes, and a gathering of materials that showcase how your company meets your security controls.

2. Automation Platform: Use a third-party automation platform to help streamline the process of documenting your policies and procedures. BARR partners with top security and compliance automation companies and can connect you with the platform best suited for your organization.

With either option, both you and BARR are responsible for providing specific information throughout your SOC audit:

## What you provide:

- **Complete your system description**. The system description provides an overview of your company's operations and control environment for the in scope system.
- **Review control wording**. Controls are documented processes in your environment relevant to your in scope system that helps achieve your in scope trust service criteria. BARR will provide you with template controls to test during the engagement. It is important you review the controls and modify them to reflect your current control environment.
- **Provide information requests**. BARR will request documentation via our tool called *taskBARR*. Information requests must be submitted within predetermined timeframes that will be established by the engagement team.

## What BARR provides:

- **Support and knowledge**. We are here for you during the engagement kickoff meeting and provide you with the support and knowledge you need to complete your engagement.
- **Solutions to information requests**. We will review information requests as they come in and hold walkthrough meetings with you to gain an understanding of your control environment and ensure we obtain the correct documentation to evidence your compliance with applicable trust services criteria. Any issues we identify will be reported to you immediately and we will work with you to identify possible solutions.
- **Type 1 or Type 2 Report**. At the conclusion of our fieldwork, we will issue a draft report.

## What to Expect from Readiness Assessment Meetings

If you choose the option of a readiness assessment, BARR will connect with you on a 30-minute call to determine your needs. We will then send a proposal to confirm this understanding which will be sent within one day after the call.

BARR will provide three key deliverables to assess the readiness of your audit: System Scope, Prioritization of Gaps, and Key Controls. This is accomplished as follows:

1. **Readiness Meeting 1:** You will be introduced to your dedicated BARR engagement manager to schedule the first readiness meeting. After meeting the team and confirming expectations, you can expect to provide a demo of the target system.

2. **Readiness Meeting 2+:** Your engagement manager will schedule a minimum two-hour meeting that works for you to get an overview of your key processes, including change management, access management, and vulnerability management. Additional meetings may be necessary depending on complexity.

3. **Remediation & Engage:** You will develop and execute remediation plans to get your environment ready for your engagement, but don't worry, your engagement manager is here to help with any questions. Based on your remediation timeline, your manager will work with you to plan your engagement timeline and resources. An engagement letter for the examination will be executed with the confirmed timelines and key dates.

4. **Readiness Meeting 3:** Once your engagement manager has an understanding of your processes, they will provide a prioritized list of observations and recommendations and will go over the list in a one-hour debrief meeting.

Once the readiness period is complete, you are ready for your examination. Like the readiness assessment, BARR will guide you through the process to ensure you pass with flying colors.

# The Process: SOC Assessments to Final Report

## SOC Assessments

The assessment phase is the meat to obtaining your SOC report. It's the main event of your examination, and this is where you'll work with your engagement lead to create a plan and assess your controls through walkthroughs which leads to your final deliverable.

**A SOC assessment will typically take 3-12 months to complete.**

## Create a Plan

A kickoff call is scheduled to confirm everyone is on the same page with the scope, timelines, deliverables, and personnel needed for the assessment. You will be responsible for confirming control wording and drafting your system description. BARR will provide information requests based on the agreed scope and controls.

**This happens within 60-120 days until the end of the examination period.**

## Assess your Controls

Your engagement team will schedule a walkthrough with your team to assess the controls and any preliminary issues. Your time is valuable, so in order to leverage our efficiencies, BARR will review your provided information requests and control activity in compliance automation software prior to walkthroughs.

**Walkthrough duration is dependent on your environment complexity and size; however, four hours is the typical time commitment.**

## Walkthroughs

A walkthrough is a meeting, or series of meetings, to discuss the design and operation of your organization's control environment. This is a time for the engagement team to ask questions concerning how the controls are designed and how they operate, providing the engagement team with a deeper understanding of your control environment to support our assessment.

Depending on your reporting period, walkthroughs are most effective in the following time periods:

- **30 days before period end (3 month reporting period)**
- **60 days before period end (6 month reporting period)**
- **90 days before period end (12 month reporting period)**

## What You Gain—The Final Report and More

You've made it through your examination—now what can you expect? BARR will provide a draft of your report no later than 30 days after the examination period ends. After you've reviewed the report, we perform a final editorial and quality review. You'll then sign off on the management representation letter.

Once you receive your report, BARR will provide you with a comprehensive promotional package to share with customers, partners, and other company stakeholders. For SOC 1, 2, and 3 reports, you can proudly display the AICPA SOC logo on your website and in marketing materials to demonstrate your milestone of compliance and security.

And finally, we not only celebrate with you but optimize your experience with improved security and next steps for continued success.

## Why Choose BARR for Your SOC Examination

With thousands of SOC reports issued, BARR not only serves as your auditor—we're your trusted security partner. Throughout the process of your SOC examination, we'll show you how to use security and compliance as a differentiator, leveraging our services to guarantee your organization successfully reaches its goals.

### What Sets BARR Apart

***Human First Approach***
Cybersecurity, at its core, is about humans feeling safe and protected. We will educate and empower your people using real talk to raise awareness, change behavior, and embed best practices into your company culture.

***Perspective***
BARR is a trusted advisor to hundreds of SaaS and enterprise-level clients across all industries. No matter your organization's stage of growth, we can help you stay secure and compliant at every stage of your growth.

***Connections***
Through our global network of partners, we will connect you with best-fit experts. These partners are integrated into our own tools, processes, and services. They drive innovation, so why wouldn't we share them with you?

# About BARR Advisory

At BARR Advisory, we build trust through cyber resilience. We help protect the world's data, people, and information networks through a human-first approach to cybersecurity and compliance. Businesses looking for the accessibility of a boutique firm with the tools and expertise of a global consulting firm will find a partner in us.

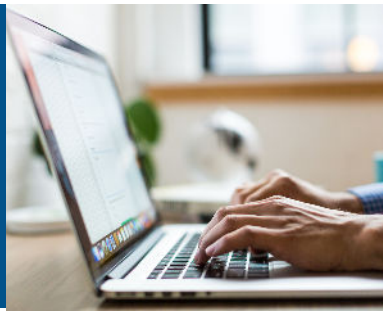
Specializing in cybersecurity and compliance for companies with high-value information in cloud environments like AWS, Microsoft Azure, and Google Cloud, BARR has the global network of partners, the perspective, and deep expertise every thriving SaaS provider to world-class enterprise needs to stay secure and compliant at every stage.

## Our Services

- **SOC Examinations**
  [SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]
- **Healthcare Services**
  [HIPAA/HITRUST]
- **ISO 27001 Assessments**
- **FedRAMP Security Assessments**
- **PCI DSS Assessment Services**
- **Penetration Testing and Vulnerability Assessments**
- **Virtual CISO Services**
- **Compliance Program Assistance**

## Connect with BARR

Interested in learning more about BARR's SOC examination services and how one can benefit your organization? Contact us today for a free consultation



Contact Us | 888-532-2004 | barradvisory.com | engage@barradvisory.com