The 6-Step Guide to Achieving SOC 2 Compliance

strongdm

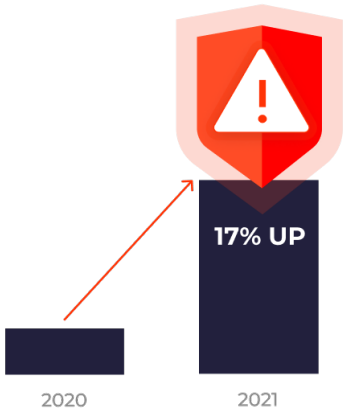
Table of Contents

The 6-Step Guide to Achieving SOC 2 Compliance

Security breaches increased 17 percent between 2020 and September 2021, with no signs of slowing down. So it's no surprise that enterprise customers want their partners to demonstrate the proactive measures they are using to protect customer data. For many customers, this means requesting the results of SOC 2 audits.

If you've never conducted a SOC 2 audit, it can seem like a daunting prospect. Running an audit takes time away from product development and other revenue generation activities, but it will help you attract larger enterprise customers, scale growth rapidly, reduce risk, and create a security-first culture—all of which will make it possible to develop new products and increase revenue in the long run.

In this six-step guide, we'll break down whether you're ready for a SOC 2 audit, who needs to participate in the audit, how to budget for it, and what you'll be doing in the remediation process. Let's jump in.



Step 1

Know When You're Ready to Begin SOC 2

A SOC 2 audit is a time- and resource-intensive process. You'll be doing a deep dive into security, availability, processing integrity, confidentiality, and privacy. The first step is to get executive buy-in. Without executive sponsorship, you won't be able to complete the audit. Executive buy-in is the difference between a successful audit and a smooth experience. To avoid hitting brick walls at every step, ask yourself:

- Is your C-suite on board with SOC 2?
- Are your founders backing you up?
- Will you have the time and resources you need?

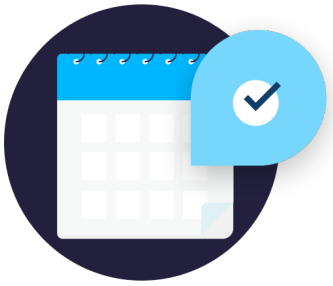
Demonstrating SOC 2 compliance requires controls and processes across HR, recruiting, customer success, and engineering teams. Explain to hesitant executives that the time and resources required will transform the business and the company, and ultimately, you'll come out with better processes and more robust compliance.

Setting expectations with your executive sponsor is critical. Discuss the audit process and create a roadmap for it. You'll need to explain what each step of the audit means and who will be involved. In addition to budgeting and staffing, make sure your executive sponsor understands the market need and can forcefully represent the requirements to the rest of the organization. Your executive sponsor will serve as the strong internal voice that can continue to reinforce your reasons for SOC 2.

Keep in mind that if a SOC 2 audit isn't a "go" right away, there are realistic alternatives: writing security policies, conducting penetration tests, limiting access to databases and resources, and understanding traceability. But SOC 2 is the gold standard to express to customers that you take security and privacy seriously.

Step 2

Set the Timeline



SOC 2 audits take time, and breaking them down into milestones for 30, 90, and 120 days can help you optimize the time you spend with auditors.

THE FIRST 30 DAYS

During the first 30 days, you'll want to understand the scope of your SOC 2 audit. Is it for multiple products, or just one? Will your entire company be audited, or just a particular API or endpoint?

Next, assign teams and interview process owners. Become as familiar as possible with the business: engineering, recruiting, legal, HR, IT, and other departments. Understand where the company is at this moment and where it needs to be in order to comply, so that you can bridge the gaps effectively.

The 30-day period is usually when companies realize how difficult SOC 2 compliance is. A lot of gaps appear, like everyone having access to a tool with limited security controls. And many of those gaps may seem difficult to close, but this new understanding is critical to take into account upfront.

90 DAYS

After you understand the scope of your SOC 2 audit, you can start writing controls. During the first 90 days, you'll make your organization's current security processes as bulletproof as possible. This is where your hard work getting buy-in from other departments will pay off, as teams will be better-equipped to adjust processes across teams.

120 DAYS

Four months in, you'll gear up to start your audit. Before you do, here are some critical items to check off your list:

- Test HR controls.
- Test account management controls.
- Select auditor.
- Risk assessment.
- Prepare for fieldwork.
- Schedule audit

This timeline will help you gauge when you need to bring in outside help and what your company will need to prepare.

Step 3

SOC 2 Team, Assemble!

We probably sound like a broken record when we say that you can't do a SOC 2 audit alone. Having the right team members can ensure the process goes smoothly. Here's who you'll need on your SOC 2 team:

Type	Detail
Executive Sponsor	The anchor for the team. The executive sponsor understands that SOC 2 compliance means the company will sell more and increase its customers base and can articulate that throughout the company–even when the going gets tough.
Writer/Author	Someone to document processes. This team member doesn't have to be a typical writer, but they will be tasked with making sure business processes are thoroughly documented. They will need to comprehend all aspects of how the business operates.
Tech/IT Liaison	A team member specifically focused on the access controls to the company's most sensitive data. The technology team will shoulder a significant burden of the SOC 2 program. Having a technology lead is essential for communication between auditors, outside consultants, and the rest of the company.
Department Liaisons	You will need several people to liaise with other departments like HR. Choose one person from each of these teams to be part of the committee. Since SOC 2 will result in controls on their departments, having the department own their controls, such as background checks or code reviews, will increase the likelihood of success.
Consultant	If you've chosen to augment your team with a third party to help with compliance, include the consultant as part of your team.
Auditor	The auditor's job is to ensure your SOC 2 program meets requirements and review the evidence to make sure it backs up your compliance assertions. Don't be afraid to get the auditor involved with your team.

As the coordinator, it may be difficult to delegate. But you don't want to be the bottleneck; whoever coordinates the SOC 2 effort should feel very comfortable assigning and following up on tasks. The bottom line is that no one person can shoulder the burden of SOC 2.

Step 4

Define the Budget

Figure out your costs before you go into the SOC 2 audit. Here are some line items to include as you define the budget:

- Direct external costs, which are usually the auditor and consultants (if you choose a third-party consultant)
- Salary for the period for the internal employee leading the project
- Readiness assessment, defined as a time cost, not dollar amount
- Legal costs
- Software tools and training
- Regular third-party penetration testing

Side note: Although pen testing is not technically required for SOC 2 compliance, it is often strongly recommended. Since this is a significant line item, we recommend including it as part of your SOC 2 budget.

Step 5

Remediation

You may have to hit the pause button between setting up the controls and performing the actual SOC 2 audit. This is normal for many organizations as they conduct remediation to become SOC 2 compliant. During the readiness assessment, you'll identify gaps in your security program. The remediation stage typically takes about three to six months. Three months is very fast, for example a large company saying, "We need this now." The average organization will take closer to six months, and that's ok! SOC 2 is transforming your business, and allowing adequate time will help the changes stick.

Part of remediation is making the build vs. buy decision. Software tools can help you institute controls. In some cases, building from scratch is the most straightforward solution. However, an off-the-shelf product may get you to compliance faster.

Sometimes, after the auditor comes on board and completes the gap assessment, you might end up with many time-consuming, expensive, useless processes. The right auditing firm will help you understand if the path you're taking makes sense. Ultimately, your goal with SOC 2 is to transform your business to become stronger, not create a bureaucracy or more paperwork.

Step 6

Execute Type 1 SOC 2

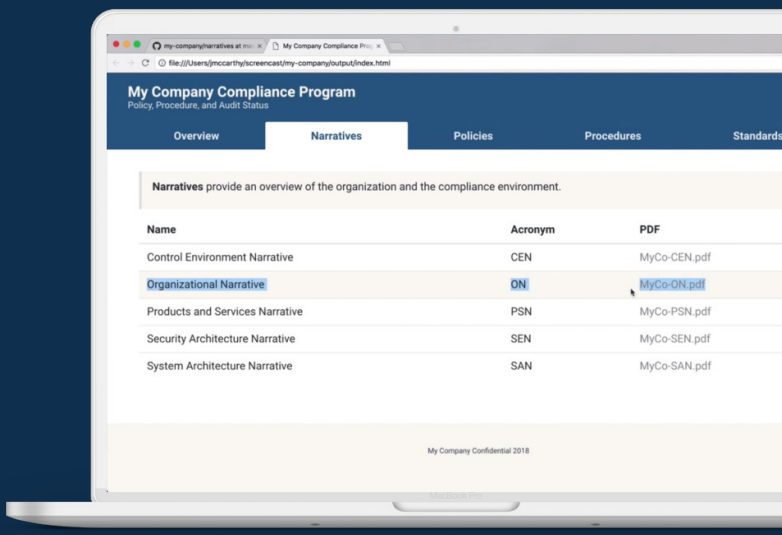
During this period, you will produce evidence that you have the controls in place for SOC 2 compliance, but you're not running tests. Therefore, it is crucial to maximize the time you spend working directly with the auditor. Execution tends to be a constrained time period, so keep it focused. Otherwise, you'll spend weeks or months in this phase.

Be open to collaborating with the auditor. It's a myth that auditors are just out to find problems. They're actually on board to help you become compliant and make the remediation process a way to strengthen your company.

Getting started with SOC 2?

One area that usually requires some remediation is access controls. Most teams don't have answers when auditors ask, "Who has access to a specific database or server and what queries did they execute?" That's why we started strongDM—to manage and monitor access to every database, server, and environment. **Sign up for a demo today**.

Need free, open source templates to assist you on your SOC 2 journey? You can find them at **https://www.strongdm.com/comply**.



strongDM's infrastructure access platform gives every business secure access controls in a way folks love to use. Trusted by the Fortune 500 to fast-growing businesses like Peloton, SoFi, Chime, Yext, and Better, strongDM gives businesses the control and visibility they need at the speed they want with one platform that works for every environment. strongDM is intentionally distributed. Head to **www.strongdm.com** to learn more.