Vanta

What does SOC 2 compliance certification cost?

The ultimate guide to the cost of SOC 2 compliance certification—with and without automation.

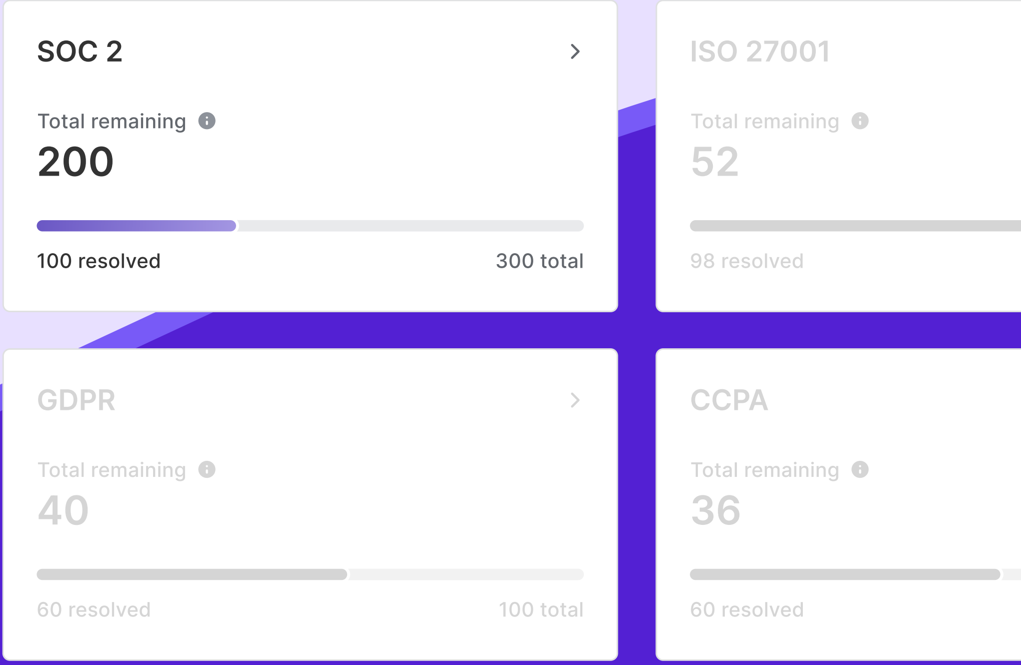
Table of contents

Introduction

Whether you're a startup or a growing company, you've either been asked to provide a SOC 2 report as part of the sales cycle, or you will be asked soon. Your company will need to make the move to get its SOC 2 certification, building and leveraging strong security practices to scale up your business and to sell into the enterprise.

Part of the SOC 2 process is weighing the costs of utilizing software to automate your security monitoring and audit prep, versus taking on SOC 2 by deploying an in-house team to manage and track SOC 2 reporting elements.

The reality is that it takes both time and money to get SOC 2 certified—but these costs can vary substantially depending on your approach. In this guide, we'll consider and compare the costs of tackling SOC 2 with and without automation.



SOC 2
Total remaining
200
100 resolved
300 total

ISO 27001
Total remaining
52
98 resolved

GDPR
Total remaining
40
60 resolved
100 total

CCPA
Total remaining
36
60 resolved

OVERVIEW

SOC 2 and compliance certifications

Let’s first review key security compliance certifications and see where SOC 2 fits in.

A SOC 2 report is a standardized and widely recognized way to assure your customers, prospects, and business partners that you have security guidelines in place and that you follow through on them. Created by the American Institute of CPAs (AICPA), the SOC 2 audit process involves the assessment and documentation of your company’s verified security practices based on five “trust service principles”: security, availability, processing integrity, confidentiality, and privacy.

In the SOC reporting realm, you may have also heard of a SOC 1 report. This report evaluates an organization’s practices and procedures to ensure that financial information is accurate.

Among potential compliance certifications, SOC 2 is the most commonly accepted framework for demonstrating security in the United States. ISO 27001 is the global benchmark for demonstrating an effective ISMS; for businesses selling to customers outside the US, a well-defined ISMS may be required by local law, and potential buyers will likely ask to see an ISO 27001 certificate prior to purchasing. As well, companies that create, access, store, or share PHI must comply with HIPAA legal requirements or potentially face steep fines and penalties.

If your company stores customer data in the cloud and sells to other businesses, you’ll likely be asked to prove your security via a SOC 2 report.

Other compliance certifications you may be considering include ISO 27001 and HIPAA.

ISO 27001

ISO 27001 is a globally accepted international standard that was developed to help organizations protect their information and supporting assets through the implementation of an Information Security Management System (ISMS). The ISO 27001 security standard is designed to support information security management by organizing people, processes, and technology to ensure the confidentiality, availability, and integrity of information.

HIPAA compliance

HIPAA compliance involves fulfilling the requirements of the initial Health Insurance Portability and Accountability Act (HIPAA) of 1996, its subsequent amendments and additions, and any related legislation. According to HIPAA, covered entities and business associates with access to protected health information (PHI) are obligated to ensure administrative, physical, and technical safeguards are in place to maintain the security of patient data; these entities are also obligated to demonstrate that they are in compliance with HIPAA Rules.

SOC 2 certification without an automation platform

If your company chooses to go through the SOC 2 preparation and audit certification process without engaging an automation platform, there are a number of costs to take into account.

01

SOC 2 audit preparation

Companies prepare for a SOC 2 audit by assessing their security gaps, putting security controls and practices in place, and documenting those practices. This process typically takes anywhere from one to six months, depending on the scale of the company and whether they choose to hire a security consultant to help draft policies and define controls.

If your company plans to conduct its SOC 2 certification processes without the use of an automated platform, you will want to establish which members of your team will support this work. They will need to strategize and organize all security tracking and evidence manually or through the use of org-specific business processes.

SOC 2 audit preparation:

- ✓ Assess security gaps
- ✓ Put security controls in place
- ✓ Put security practices in place
- ✓ Document practices

Acquiring and allocating in-house team resources

You will want to assemble an in-house SOC 2 team, which may be comprised of current team members and may be augmented by new hires with expertise in security and compliance. Some people on this team will be full-time security representatives, others will allocate a portion of their time away from their regular organizational duties.

Targeted roles or dedicated staff time that you will want to build into your SOC 2 team include executive leadership, SOC 2 project management, a lead author who will take on technical writing, input from your legal team, and significant IT/security team representation. You may also need to work with a third-party consultant to support your company throughout the SOC 2 process.

Development and documentation of controls

Your SOC 2 team will need to develop a list of security controls, or rules, that your company plans to follow. While you can pay an outside expert to develop the list, it's also possible for an employee or team to research and produce the list on their own. The full list might include dozens or even hundreds of rules. You'll need these rules to conform to AICPA guidance.

Policies and procedures

Document your organization's policies and procedures, and prepare to make that documentation available to your auditor. Your organization will tailor its policies to your industry, your customers, and the type of service you provide. It can be a very time-consuming process to develop the ecosystem of your organization's policies, but this documentation is a critical complement to your company's security controls.

You may decide to outsource this work to a security consultant; these costs can easily be another $10K or more. If you decide to take care of this work in-house, plan for at least four to eight hours of time per policy (typically 15 to 30 policies for an SMB) plus the cost of staffing this internally.

Vendor management

Your security team will also want to create a vendor management policy. Regulators have expanded security and data management requirements in various sectors to ensure that companies are effectively and proactively managing supply chain risks. It is a best practice for any organization working with sensitive data and customers' personally identifiable information to build a comprehensive list of all vendors—every third-party, contractor, or associate with whom you do business—to develop a policy to review all vendors, and to establish requirements for the level of information security that vendors should maintain.

Internal testing and readiness assessment

As the name suggests, a readiness assessment helps you determine when your security practices are ready for an audit. Your SOC 2 team will need to review each rule to determine which ones are being upheld and which ones need to be addressed. While it's possible to conduct a readiness assessment in-house, many companies outsource this work to a consultant; their output is often a long task list.

The cost of an external readiness assessment starts at $10K and scales with company size. If you decide to develop the readiness assessment in-house, plan for 20 to 40 hours of time plus the cost of staffing for this project.

Procure and implement security tools and practices

Your SOC 2 team should then recommend the implementation of new practices to fulfill your stated rules. This step can require buying new security tools (e.g. laptop management software to ensure laptop hard drives are encrypted), changing internal practices (e.g. instituting code review for all commits), and adopting new processes (e.g. performing background checks on new hires) to bring your systems into compliance. These tools may cost another $10K or more per year per product on the low end.

Choose to pursue SOC 2 Type I or Type II

An additional factor to consider is whether to pursue a SOC 2 Type I or a Type II. A Type I report is issued on a specific date and represents an auditor's review and approval of your systems at that moment in time. A Type II report shows not only that you understand the necessary security procedures, but that you follow them over a period of several months.

A Type I is faster than a Type II, but it's worth noting that if you start with a SOC 2 Type I, you'll likely also need to get a SOC 2 Type II report at some point, since many enterprise customers require the stronger Type II report. If a SOC 2 Type II is your goal, it is usually more cost-effective to start there and avoid the cost of the Type I.

If you are preparing for your SOC 2 Type II without automation, your security team will need to manually gather this information over time to meet audit requirements. They will need to set up processes in order to manage recurring annual audits.

SOC 2 preparation without automation:

- ✓ Develop and document security controls and practices
- ✓ Develop and document policies and procedures to support security controls
- ✓ Periodically review and refresh documented policies and procedures
- ✓ Develop internal tracking tools and processes to manage third-party vendors
- ✓ Periodically review and refresh status of third-party vendors' security
- ✓ Test your organization against its established controls
- ✓ Purchase and/or implement new tools and practices to fulfill security controls

STAFF TIME:

8+ weeks

FINANCIAL COST:

Minimum annual cost of $30K plus the cost of staff hours

02

The SOC 2 audit

Process and cost of an auditing service

To conduct your SOC 2 audit, an auditor will examine your list of controls and assess whether you are following those rules. You'll need to produce a "paper trail" of evidence for each security control—a process that you can expect to take a few weeks of dedicated time and paperwork.

Your auditor is likely to ask questions of key employees, request screenshots of configuration dashboards, and either visit your office or join your engineering team's leadership on a video call. You'll then guide the auditor through your systems and processes, which can take full days—even weeks for large companies—and will require dedicated time to go through your company's security and engineering practices in detail. Your engineering team may also be asked to provide additional evidence as needed. The duration of your audit will also vary depending on availability of your team members who must be a part of the process.

Audit fees can vary significantly depending on the size of the company being audited, the auditor's brand, and the complexity of the audit. Typically, the fees for a SOC 2 audit will range between $10K to $50K.

When developing the SOC 2 report without automated processes, it can take weeks for your auditor to finalize and deliver your report detailing your adherence to your security controls.

Your SOC 2 report is generally valid for one year and audits are typically conducted annually, which means incurring these costs each year.

Total cost of SOC 2 audit preparation and SOC 2 audit

Between prep work and the audit itself, the total cost of achieving a SOC 2 can range from $40K to $180K or more.

SOC 2 audit without automation:

- ✓ Company produces evidence for each security control, e.g. screenshots
- ✓ Internal SOC 2 team reviews security and engineering practices with auditor
- ✓ Auditor examines full list of controls and assesses adherence to controls

STAFF TIME:

80 hours

AUDITOR TIME:

120 hours

FINANCIAL COST:

Two weeks of staffing cost, plus the audit cost

Potential costs of noncompliance

The cost of noncompliance, paired with the risk of a security breach, can vary widely. Some of the most likely consequences of a data breach include financial penalties in the form of fines that can reach into the thousands of dollars—and even millions—depending on the scale of the breach, as well as potential legal action against your company in relation to a breach.

Beyond financial losses and legal action, your company can expect to confront damage to its reputation, a cost that is harder to quantify but is likely to result in lost business as potential clients seek to build relationships with competitors doing business more securely.

Logistically, a data breach is also likely to lead to operational downtime and the loss of sensitive data. Broadly, these costs can be more difficult to estimate (note the fine structure specific to HIPAA compliance) but should be understood as real potential costs with impacts on your business beyond direct financial fines.

Budgeting for SOC 2 costs annually

Remember that the process of getting a SOC 2 audit and keeping your security compliance updated is an annual process, which means all of the costs described here are incurred each year.

SOC 2 audit preparation and monitoring with automation

Engaging an automated security and compliance platform will cost you between $25k to $75k, depending on company size. You can compare this cost to the annual and ongoing expense of staff time to monitor security operations and reallocate time from regular roles and business operations to prepare for your annual SOC 2 audit.

Use of an automation platform will support your company through much of the prep work for a SOC 2 audit, saving both time spent on collecting evidence and money spent on hiring security consultants to perform readiness assessments, customize controls, and write security policies.

An automation platform offering continuous monitoring will also take a lot of the guesswork out of obtaining a SOC 2 Type II, such that companies may opt to forego a Type I—ultimately saving them money while presenting a stronger security posture to their customers.

An automation platform also simplifies the audit for auditors, meaning your audit fee will be lower. With an automation platform like Vanta, for example, you can expect to pay approximately $10K to $35K+ for the audit, depending on company size.

Engaging an automated security and compliance platform will cost you between

$25k – $75k

Make the choice: manual or automated SOC 2 preparation and audit

Today, a company’s proof of security is a requirement for doing business, making the expense of security and compliance monitoring a baseline cost—whether you accomplish it with the ongoing effort of an in-house team or whether you engage automation to get the job done. A small startup team may find that it is more reasonable to implement automated security systems early on, baking strong and reliable security into a company’s practices sooner rather than later.

Save time and money with automation

If your company is ready to engage in the valuable process of securing a SOC 2 report, and you’d like to save time and money on what you know could be an expensive and time-intensive manual process—consider pairing an automated security monitoring platform with a trusted audit firm to deliver a streamlined and successful SOC 2 audit.

Automation with Vanta

Vanta's dashboard tracks audit readiness

The core of Vanta's product is a dashboard that provides an up-to-date view on security practices across your company. You'll have instant feedback on what's looking good—and what could be touched up. By the time you speak with an auditor, your systems will be airtight.

Vanta eliminates the need for a readiness assessment, since Vanta's monitoring and alerting replaces those spreadsheets.

Vanta offers tools to close security gaps

Every company needs to change something before their audit, from writing down de facto policies to changing AWS or GCP configurations. Vanta offers tools and guidance, like policy documents, laptop monitoring, and vulnerability management, that help companies close gaps faster.

Vanta allows your company to spend less time with the auditor

Your auditor will have access to Vanta ahead of time and will understand your system. This limits the back-and-forth required, and allows your team to answer specific questions from the auditor, rather than needing to bring the auditor up to speed on every detail of your system.

Security and compliance become continuous operations running in the background

What used to be a costly and time-consuming process of proving system configuration over time is transformed into an automated background process supporting your business—saving you time and money in comparison with typical SOC 2 audit processes.

Vanta

Vanta is the easy way to get and stay compliant. Thousands of fast-growing companies depend on Vanta to automate their security monitoring and get ready for security audits in weeks, not months. Simply connect your tools to Vanta, fix the gaps on your dashboard, and then work with a Vanta-trained auditor to complete your audit.

REQUEST A DEMO

VANTA.COM