SECURICY

How to Get Ready for a SOC 2 Audit

SECURICY

What's Inside

SECURICY

An Overview of SOC 2

Passing a SOC 2 audit can be a big deal if you sell to enterprise companies that are looking to weed out risky vendors with a weak information security posture. The certified badge of a SOC 2 report shows a qualified third-party reviewed and validated your security controls. Overall, it helps companies feel like you're a vendor they can trust with their data.

If you're just starting to get questions about SOC 2 compliance, or even customers demanding a SOC 2 audit report — you likely have some questions yourself. If you're trying to get up to speed about what SOC 2 is and why it matters, read on to get all the essentials you need to know about SOC 2 and audits.

What is SOC 2?

Service Organization Control 2 audits were designed by the AICPA (American Institute of CPAs) as an auditing process to check the existence and effectiveness of data security, availability, processing integrity, confidentiality, and privacy controls at vendor organizations.

The reports from a SOC 2 audit are commonly used to assess, provide information, and verify a third-party vendor's data management processes.

SECURICY

The SOC 2 Timeline

SOC 2 reports are among the most common compliance requirements for technology-focused companies and service organizations that store customer data in the cloud.

If you've determined that you need a SOC 2 audit, here's what happens next.

Planning for SOC 2

Preparing for SOC 2

The SOC 2 Audit

Your SOC 2 Report

Planning for SOC 2

This is a big step. Before you do anything, you need to know: what will your audit cover? This is when you define your system description for the auditor and determine the audit scope. Planning for SOC 2 is a critical step you can't overlook.

Your planning here will influence the controls, policies, and procedures that you need to prepare ahead of the SOC 2 audit (the next stage we'll look at). These two components, the system description and audit scope, will later be included at the beginning of your final SOC 2 audit report. They will also influence the cost of your SOC 2 preparation, time to get certified, and auditor fees.

SOC 2 Type 1 or Type 2?

Another consideration is whether you're getting a Type 1 or Type 2 audit.
A SOC 2 Type 1 audit gives you a point-in-time report that evaluates and tests the design of your information security controls.

A SOC 2 Type 2 audit is completed over an extended period of time (the timeframe depends on the scope of your audit, usually between 6 to 12 months) to test the implementation and effectiveness of your information security program.

Writing Your System Description

For the system description, you'll need to tell the auditor what to review and explain what your system is designed to do. It's an overview of your operations, product offerings, any tiers of your product offering, what it is, exclusions, and more. Should the auditor review just one application? Or do you have multiple products?

You need to write up this system description for the auditor. It could amount to a couple of paragraphs or over ten pages. It depends on your business and the complexity of your services, but you can expect to have at least one paragraph per product (think about it like unique SKUs).

Example:

Let's say your business has a bookkeeping application — a free trial and two paid versions (a basic version and a deluxe version). In this bookkeeping example, you'll need a minimum of 3 paragraphs (or more) to describe your system. If you have a SKU with an API and one without the API, then you would also need to make sure you explain that API system, what it does, and where it is included.

Defining Your Audit Scope

This planning stage will also be when you define your regulatory requirements, contractual commitments, and what Trust Services Criteria apply to your business.

Do you have clients located in the European Union, which means GDPR requirements apply? Do you sell software to the healthcare industry with legal obligations of the Securicy and Privacy rules under HIPAA? A SOC 2 audit can help prove this regulatory compliance to clients or prospects who need to verify your security posture.

Trust Services Criteria

You'll want to determine which of the five Trust Services Criteria that the auditor should use in the assessment. Security is the one Trust Service category that is always included and is also called the Common Criteria. (You'll see this coded as CC in Securicy's security controls.) The other four criteria are optional: Availability, Confidentiality, Privacy, or Processing Integrity. You can select which — if any — of these additional Trust Services Criteria that you and your clients need to be assessed in this audit.

Preparing for SOC 2

After you've defined your systems and your audit scope, you begin "doing" the preparation.

The majority of your preparation will be ensuring that you are ready to produce whatever documentation the auditor requests as soon as the audit begins. The auditor will start out by requesting a list of items called "Common Population." This is a gigantic pile of documentation and data, which they will then comb through during the audit.

Companies can use Securicy to customize and generate the bulk of this documentation, manage implementation, and report on SOC 2 readiness. We're on a mission to make SOC 2 preparation as painless as possible.

Policies and Documents You Need for a SOC 2 Audit

- Policies: Expect for them to ask for the full text of all your policies that address the security controls listed in the SOC 2 framework.

- Procedures: You'll need to describe your team's activities or actions to meet the control requirements, with records of the dates and people who are designated to complete those tasks. (Like account creation procedures or offboarding.)

- Implementation: Ensure you've implemented all those policies and procedures before the audit begins (get your pen test results, update your risk assessment, hold security awareness training, etc.).

- Operations: You'll need additional items like a list of current employees, your organizational structure, various changes documented, and lists of any recent security incidents within the audit period. Here is an easy one to forget — the auditor will also require you to disclose any new business partners within the audit period or new third-party vendors you started using.

The SOC 2 Audit

Once you're confident that you have the correct security controls in place, you'll need to research and evaluate third-party auditors to engage for your audit. Only an independent, certified CPA firm can conduct a SOC 2 audit.

How Much Will an Audit Cost?

The cost of a SOC 2 audit will vary based on the audit's scope and the certified auditor you hire. Typically, you'll find auditor fees in the $20,000 to $45,000 range.

However, you'll also want to budget for the cost of audit preparation — you'll need to plan for whatever time, resources, outside expertise, and additional tools you need to get your security program into compliance with the SOC 2 Common Criteria and any additional controls in the scope of your audit.

Scheduling the Audit

At this point, you're ready to schedule and conduct the audit. You may be able to request a pre-audit readiness assessment, which can help you identify trouble spots in advance. Your auditor will also provide additional information and details, which will help set your expectations on the audit timeline and how they will conduct the audit.

So how long will the audit take? The amount of time needed for the actual audit will depend on your scope: a SOC 2 Type 1 audit will take less time as it is a point-in-time audit, while Type 2 takes between 6 to 12 months.

Sharing Documentation

Ahead of this stage, you'll need to determine how you will securely share documentation and records with the auditor when they request them.

If you are using Securicy, you can invite your auditor to review your content about your security controls using Audit Connect. It's secure, fast, and helps you simplify the process to get through your audit. With a lot less hassle.

Getting Your SOC 2 Audit Report

Finally! You got the SOC 2 report! Once you have the results, you can start sharing it with clients and sales prospects that requested a copy of your SOC 2 report.

Since the report contains sensitive information about your security program, you should never make it publicly available to download. It's a best practice to require the requester to sign an NDA before sending over a SOC 2 report. Some companies will watermark reports with the requester's name or email to ensure the person receiving it does not share or post it online.

If you were well prepared, your SOC 2 report might be spotless. But you'll want to look carefully for insufficient areas that you need to remediate. Did they find not all of your employees have completed the mandatory awareness training required by your policies? Discovered poor asset inventory management? For any noted issues, you'll want to prepare in case questions come up and you need to demonstrate corrective action.

SOC 2 Renewal & Ongoing Compliance

Keep in mind that after you have your audit results — you can't let employees drop the ball on following security policies and procedures. Companies need to maintain ongoing security compliance. Auditors recommend that companies opt to renew their SOC 2 certification and get an annual SOC 2 report to prove continuous compliance.

Technically, SOC reports don't expire, but sharing years old reports with prospective buyers may not instill confidence in your security posture.

Security procedures require ongoing action, monitoring, or an annual activity (such as a penetration test). Depending on how old your SOC 2 report is and your buyer's data security requirements, you may need to answer additional security questions or show more recent reports verifying your current procedures.

Chat with an Expert

Need help getting your organization SOC 2 compliant?

Talk to our security experts about the SOC 2 Audit Readiness in the Securicy platform.

Get the tools you need to generate policies, while efficiently achieving, maintaining, and reporting on your compliance status.

Talk to us and book a demo at securicy.com/demo.

About Securicy

Securicy is an information security management platform for businesses selling to large enterprises.

The Securicy platform uses industry-leading best practices to generate information security policies and automatically create implementation tasks. Securicy acts as your command center, providing access to the tools, resources, and advisors your business needs for building and maintaining security compliance.