Thoropass™

Everything you need to know to

Get SOC 2 Compliance for Your Startup

thoropass.com →

Chances are your startup will need SOC 2 compliance to close enterprise deals and move upmarket. Also likely—you have no idea where to begin. Becoming SOC 2 compliant isn't an easy feat. It takes significant time, effort, and resources to get that first clean report. What's more, it seems like the bulk of SOC 2 resources are meant for larger, more traditional companies. So, what's a startup to do?

Thoropass (formerly Laika) created this detailed guide specifically for growth-minded founders looking to become SOC 2 compliant for the first time (or for those trying again). This resource provides guidance on how to navigate the complex field of SOC 2 compliance from start to finish. It explains what startups need to know about defining their audit's scope, what to expect in terms of time and cost, how to prepare, and what to do after the report is in.

Get ready to hurdle the SOC 2 learning curve.

Table of Contents

Chapter 1

What Is SOC 2 and Why Is It Important for Your Startup?

Your customers want it. Your competitors (might) have it. What is SOC 2 and why does your startup need it?

What Is SOC 2?

SOC 2 is an auditing standard maintained by the American Institute of Certified Public Accountants (AICPA) to test an organization's internal controls for information security and privacy. It's an objective, third-party system that tells customers that they can trust your startup to handle their information with the utmost care.

This is the compliance audit most commonly sought by startups, particularly SaaS, as it's relevant for any business that uses the cloud to store customer data.

Companies can use this AICPA-approved logo to show enterprise buyers and the world that they've received a clean SOC 1, 2, or 3 report within the last year.

Why Is SOC 2 Compliance Important for Your Startup?

Not only is SOC 2 compliance critical for protecting your business and your customers from data breaches and other company-killing events, but it's also a must-have for startups looking to move upmarket.

Enterprise companies expect startups to meet the same procurement cycles and compliance requirements as other vendors. In many cases, enterprise customers will ask you to become SOC 2 compliant before working with them—that's if they don't move on to a startup that already is.

Savvy startups also use SOC 2 compliance as a competitive differentiator. Compliance doesn't just tell enterprise buyers that you're open for business. It's a powerful brand and marketing message that signals to the world that your startup is more established, credible, and attuned to customer needs.

Companies can use this AICPA-approved logo to show enterprise buyers and the world that they've received a clean SOC 1, 2, or 3 report within the last year.

Chapter 2

SOC 2 Scope—Trust Services Criteria and Type 1 vs. Type 2

To become SOC 2 compliant, your startup needs to undergo an audit and receive a clean report testifying to the quality of your controls. Just what that audit tests depends on which criteria and type you choose.

SOC 2 Trust Services Criteria

A SOC 2 report tests against **5 Trust Services Criteria: security, availability, confidentiality, privacy, and processing integrity**. When you engage an auditor, you decide which of the five you'd like tested, if not all. These decisions are often influenced by what enterprise buyers request.

Thoropass will help identify and prescribe the right steps to accomplish the necessary criterias so you only put in work that is impactful to your business.

SECURITY CRITERIA

Also known as the "common criteria," security is the only criteria required in a SOC 2 assessment.

That's because the security criteria not only sets overarching security standards for your company, but it also overlaps each of the other criteria, setting security controls for availability, confidentiality, privacy, and processing integrity. You can't complete a SOC 2 audit without the security criteria.

→ **What does it test?**

Security focuses on the protection of information and systems against unauthorized access. This criteria tests that your customers' information is protected at all times (collection, creation, use, processing, transmission, and storage) along with the systems that handle it.

→ **Who is it best for?**

All companies that need a SOC 2.

AVAILABILITY CRITERIA

This criteria makes sure your systems are secure and available for customers to use when they expect to. This is important for startups that promise customers access to their data and your services at key times.

→ **What does it test?**

Availability addresses network performance, downtime, security event handling, etc. For example, your team worked hard to get your platform's uptime to 99.31%. By validating your uptime and other availability considerations with this criteria, you're further demonstrating your reliability to your customers.

→ **Who is it best for?**

Companies that need to ensure their uptime—SaaS and data centers in particular.

CONFIDENTIALITY CRITERIA

This criteria ensures the protection of confidential information. Did you agree to keep some of your customers' information confidential? Then this criteria is for you.

→ What does it test?

Confidentiality addresses the handling and protection of information (personal or not) that you've agreed to designate confidential and secure for your customers; for example, proprietary information like business plans, financial or transaction details, legal documents, etc. In addition to the protections outlined in the security criteria, the confidentiality criteria provides guidance for identifying, protecting, and destroying confidential information.

For example, your platform manages a customer's documentation about their trade secrets and intellectual property. For obvious reasons, they only want people within the company (and only some of them) to have access to this sensitive information. The confidentiality criteria signals that you're set up to protect that information and secure access as desired. It also shows that you're set up to appropriately destroy confidential information if, say, the customer decides to stop using your platform.

→ Who is it best for?

Companies with customers that want some of their data kept confidential.

PRIVACY CRITERIA

This criteria focuses on the protection of personal information. Similar to confidentiality, the privacy criteria tests whether you effectively protect your customers' personal information. Confidentiality, on the other hand, applies to any information you agreed to keep confidential.

→ What does it test?

Privacy addresses the secure collecting, storing, and handling of personal information, like name, address, email, Social Security number, or other identification info, purchase history, criminal history, etc.

→ Who is it best for?

Companies with customers concerned about their personal information.

PROCESSING INTEGRITY CRITERIA

This criteria makes sure you provide the agreed-upon services as promised in an accurate, authorized, and timely manner.

→ What does it test?

The processing integrity criteria addresses processing errors and how long it takes to detect and fix them, as well as the incident-free storage and maintenance of data. It also makes sure that any system inputs and outputs are free from unauthorized access or manipulation.

For example, the processing integrity criteria demonstrates to customers that your data, processes, and system work as intended, so they don't have to worry about inaccuracies, delays, errors, and whether only authorized people can use your product.

→ Who is it best for?

Companies that provide e-commerce services, financial services, transactional features, etc.

Choosing Which SOC 2 Trust Services Criteria to Test

Even though only the security criteria is necessary for a SOC 2 audit, you may choose to test the other criteria that are relevant to your startup and how you serve your customers. Thoropass's team of dedicated experts will help you identify what will make the most impact for your current and projected business needs.

Enterprise customers want to work with startups that are SOC 2 compliant in security and confidentiality. If you're struggling to decide which criteria to tackle in your first audit, security and confidentiality make a good starting point. Otherwise, add on the criteria your target customers want and are asking for.

SOC 2 Type 1 vs. Type 2

The next decision founders need to make is whether they want a Type 1 or Type 2 SOC 2 audit. **Be careful not to mistake Type 1 for SOC 1 or Type 2 for SOC 2.** They all mean something different.

There are two types of audits (Type 1 and Type 2) for SOC 1 and SOC 2. That means you can get: a SOC 1 Type 1 audit, a SOC 1 Type 2 audit, a SOC 2 Type 1 audit, AND a SOC 2 Type 2 audit. Thoropass can help you achieve them all, including multi-framework progress to eliminate duplicative work.

SOC 2 Type 1 vs. Type 2: What's Best for Your Startup?

Each type comes with its own benefits and challenges. Type 1 is faster and cheaper than Type 2. Also, the requirements aren't as strict as Type 2, as you just need to prove your compliance program meets audit standards, not provide evidence that you're using it effectively over time. Type 2, however, points to a higher level of compliance.

Type 1 is enough for some enterprise customers, making it a sufficient option for some startups. That is until a startup wants to work with enterprise customers that require a more complete picture of their compliance. In that case, you'll want to pursue SOC 2 Type 2.

vs

SOC 2 Type 1

A SOC 2 Type 1 audit tests the design of your compliance program. It assesses your compliance at one point in time. Typically, this involves checking to see that you've identified and documented the controls you have in place, as well as provided sufficient evidence that your controls are functional at that point in time.

SOC 2 Type 2

A SOC 2 Type 2, on the other hand, tests not only your compliance program but whether you follow it by executing on the controls over time. Usually, a Type 2 audit assesses your compliance over a six to 12-month review period, with your first audit typically lasting six months.

Chapter 3

Time and Cost of SOC 2 Compliance for Startups

How long is this going to take, and how much is this going to cost me? Good questions.

How Long Does SOC 2 Compliance Take?

Weeks? Months? Years? As with many important and complicated things, the answer is—it depends.

The deciding factor here is complexity. How many employees work for your startup? How many systems do you run? Do you have multiple locations? What's your startup's revenue like? How sensitive is your customer data? All these things come together to determine your compliance timeline. It's why big Company A and small Company B, despite doing the exact same things, endure different SOC 2 timelines (and costs). However, Thoropass's team of experts help you set goals and stay on track, including your team of Thoropass auditors who understand your tech stack, making the audit that much faster. Excessive back-and-forth between the company and auditor will also put a hold on the progress. This happens when the startup and the auditor struggle to clarify requirements.

When dealing with a complex process like a compliance audit, it's sometimes challenging to collect not only the right evidence but also the right amount of it. Thoropass's technical deep dive sets you up for success by telling you exactly what you need to prepare before the audit and provide during the audit, so you don't waste time understanding what's required or collecting evidence you don't need.

How Much Does SOC 2 Certification Cost?

We've seen **SOC 2 audits start around $20,000 for startups and cost hundreds of thousands for larger companies**. Again, your cost will depend on a number of factors:

- → Team size and distribution
- → Lack or abundance of control documentation
- → Complexity of services as well as the number and complexity of processes
- → Scope of your audit (Trust Services Criteria and Type 1 or 2)
- → Reputation of your auditor

Expect to pay a premium for working with the "Big Four:" KPMG, Ernst & Young, Deloitte, and PricewaterhouseCoopers. The good news is that for most startups, your auditor's reputation only matters to a certain extent. We talk about this in the Who Can Perform a SOC 2 Audit? section.

For the audit alone, expect to pay:

SOC 2 Type 1 $10–$30K

SOC 2 Type 2 ~$30K

Again, these are starting costs, and your audit price will ultimately depend on the factors outlined above. Also, these estimates don't take into account additional compliance-related expenses like your:

- Dedicated in-house employee(s) or consultant
- Readiness assessment]
- Legal fees
- Any technical work, training, or cultural changes you need to put proper controls in place.

Since your Thoropass subscription includes the SOC 2 Type 2 audit, we keep costs down to much less than 3rd party audits.

How Long Does SOC 2 Compliance Last?

Your SOC 2 report lasts for one year. That means, once a year passes from your completed audit, you will need to undergo the process again.

Startups grow, processes and systems become more complex, and teams change. It doesn't take long for an ambitious startup to outgrow its audit. This means the evidence you gather and the controls your auditor tests in your subsequent annual SOC 2 audits will likely look different from your first.

While there's no obligation to pursue compliance to begin with, much less every year, you run the risk of upsetting customers and blocking sales, particularly bigger enterprise deals, by operating on a stale SOC 2 report.

Remember, many enterprise customers won't consider working with a startup without SOC 2 in place. Thoropass's continuous compliance programs grow with your team to ensure each year's compliance easily scales as you do, without the extra work.

Chapter 4

How to Prepare Your Startup for SOC 2 Compliance

Now that you understand the process from a high level, let's dive into what you need to successfully prepare for your SOC 2 audit.

When Should You Start Preparing for a SOC 2 Audit?

Here the adage rings true: It's never too early to start thinking about compliance.

The precise time to initiate the certification process depends on your industry, the sensitivity of your data, and when you want to start pursuing bigger opportunities. However, it's much **easier to** build a compliance culture **from Day 1** than it is to course-correct when you're 50 people and growing. By putting the policies and procedures in place early, you're making sure your startup grows on a strong foundation. If you have a deadline, give yourself some wiggle room.

There's a lot to learn when you pursue your startup's first SOC 2 audit. With a dedicated support team at Thoropass, you get to leave the complexity to the experts, and only need to understand what's relevant to you and your business.

We provide a gap analysis that identifies clearly outlined remediations processes to close gaps before the actual audit to make an efficient path towards the audit.

Who Can Perform a SOC 2 Audit?

Only a CPA firm can conduct your SOC 2 audit. However, that doesn't mean that every CPA firm is a good fit for your startup's SOC 2 audit.

Certain auditors are more startup friendly than others. **Find a CPA that understands the specific needs of tech-focused startups** over more traditional companies, like a credit union or manufacturing plant. For example, you'll want to work with an auditor who understands the impact cloud-based information storage, co-working spaces, and other unique considerations have on compliance.

Thoropass customers get the opportunity to work with a tech-first well-regarded and vetted CPA firm that specializes in compliance for startups. While working with that firm isn't required to take advantage of Thoropass's enterprise-ready compliance platform, it makes the task of selecting the right auditing firm for your startup much less of a headache, and it minimizes duplicative work, and the potential for endless email loops of submitting evidence.

Do I need to work with one of the Big Four?

While the opportunity to work with the biggest and the best might seem appealing at first, it's overkill for most startups undergoing their first SOC audits.

There's a price premium to working with KPMG, Ernst & Young, Deloitte, or PricewaterhouseCoopers, and most startups don't need all the resources a massive firm provides to get through the SOC 2 process successfully.

Don't expect a lot of hand-holding throughout the SOC 2 auditing process. While auditors are experienced with first-timers—startup customers may provide some general guidance (like a SOC 2 template or an overview of the process)—they have their objectivity to uphold.

As they're the ones assessing your controls, it would be inappropriate to act in any way that could signal a vested interest in the results of your report. And so you shouldn't expect them to go out of their way to guide you to a clean SOC 2 report.

How to Set up Your Internal SOC 2 Team

While your auditor can't do all the work for you, Thoropasss' dedicated team of experts have insight into what your auditor will ask for, providing you with the correct answers before the actual audit starts While you'll need to rely on your team to gather the documentation and evidence your auditor requires, Thoropass's platform streamlines the evidence gathering process and automates most of the undertaking.

BENEFITS (AND CHALLENGES) OF TACKLING SOC 2 IN-HOUSE

Usually, we see startups handle as much of their compliance prep as possible in-house. This means assigning one or more employees to eat, sleep, and breathe SOC 2 for a week or two (or more). This is an effective way to keep costs down. However, there's an opportunity cost to diverting resources away from your startup's day-to-day.

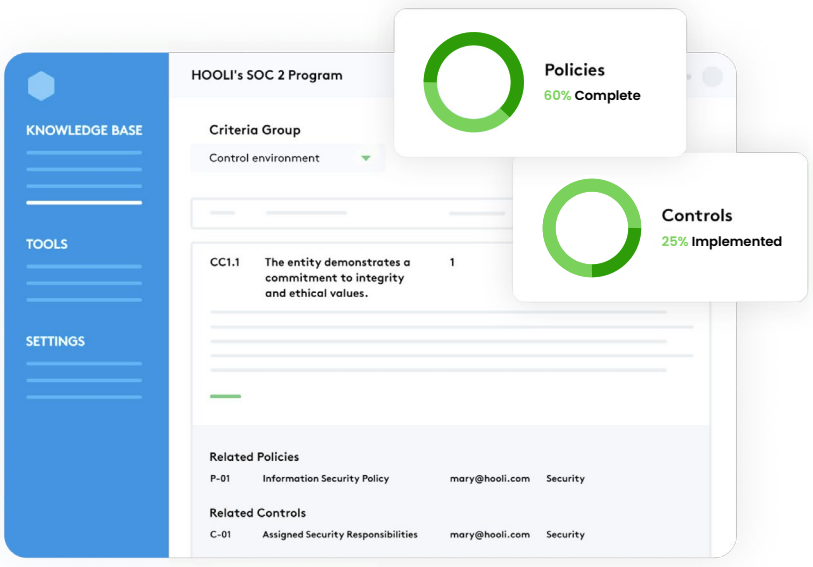
This in-house approach also benefits from the knowledge stored within your company. You don't need to spend your time teaching an outsider about all the ins and outs of your startup to get started with SOC 2.

EMPOWER YOUR IN-HOUSE TEAM WITH THE RIGHT COMPLIANCE SUPPORT

One way to efficiently and effectively prepare for SOC 2 in-house is by using a compliance solution like Thoropass.

Thoropass works directly with startups (regardless of their SOC 2 expertise) to design a compliance program based on your goals, whether it's to pass a specific prospect's procurement process or work towards a clean compliance report. Our program takes into account your profile and your company's context, so you're set up to do the right thing and only the right thing from the start, not just made to check a box.

With Thoropass concierge service, experts answer your questions in real time, so you don't need to spend hours digging through complex AICPA guides to find the answers. We also handcraft your policy drafts and provide a detailed implementation guide as well as the software tools to manage your compliance efforts. We also guide you through the audit, providing you with a tech-first dedicated audit team once you're ready.



WHO SHOULD BE ON YOUR SOC 2 TEAM?

As compliance doesn't start and end in engineering, you will need involvement from all aspects of your startup, including HR, sales, and legal. Your team should be comprised of members from each department. This not only allows you to leverage your startup's varied expertise, but it also helps cultivate a culture of compliance and ownership within teams for their controls.

You'll also need:

- A team lead to delegate and drive progress.
- A tech lead to act as a liaison between the auditor and the rest of the team for more technical matters.
- Someone who is comfortable documenting a lot of your company's processes. This person doesn't need to be a writer, but they should expect to do a lot of writing.

Keep in mind that partnering with Thoropass means you are provided with a dedicated project manager, coupled with in-app project management tools, to fill in any gaps and keep you on track.

There's a bulk of knowledge that vendors need to know about your company and its situation in the beginning. That need for company-specific knowledge continues to grow as you step through this process and your startup continues to grow.

If you change halfway through the process, you need to step through the knowledge-sharing stage again.

How Do You Know If Your Startup Will Pass the SOC 2 Audit?

How do you know your existing controls are enough to meet your SOC 2 auditor's expectations? **A gap analysis or readiness assessment before the audit can help you close any lingering gaps in your compliance.**

Used interchangeably, a gap analysis or readiness assessment alerts you to anything that might cause you to receive less-than-favorable results in your SOC 2 report. It gives you an opportunity to right these missteps before the official assessment.

Let's say you forgo a readiness assessment and skip straight to the SOC 2 audit only to realize that to comply with SOC 2 criteria, you need a risk committee that meets every quarter.

Suddenly, you're scrambling to decide who will make up the committee, when they'll meet and where, what the agendas look like, how to document the meetings and put decisions into practice, etc. That takes a while to organize, putting a halt to your SOC 2 audit and distracting you from the day-to-day priorities of running your business.

A readiness assessment brings these potential blocks to your attention sooner, preventing last-minute scrambles, as in the scenario above. Thoropass's readiness assessment, for example, gives you over 90% confidence that you're ready for SOC 2 before the audit even starts.

Chapter 5

What Happens Once You Receive Your SOC 2 Report?

Finally! You spent the time scoping, preparing, and delivering countless documents to your auditor. Now all your hard work is about to pay off. Here's what to expect.

What Is a SOC 2 Report?

A SOC 2 audit report is a 30–40 page document that describes your organization's controls and whether they stand up to scrutiny. Written by your auditor, your report serves mainly as auditor-to-auditor communication. It's meant to be read, understood, and evaluated by other compliance or information security professionals.

For example, enterprise customers that require startups to meet SOC 2 compliance before working with them will request a copy of your report, so their procurement or compliance team can review it.

Unless driven by detailed procurement processes, most people won't want to sift through your audit report to know your startup is safe to work with. Instead, you can show off your startup's commitment to compliance by adding the appropriate AICPA-approved logos and other certification seals to your website. To see this in action, check out Slack's dedicated security page.

Slack dedicates an entire page to showing off all of its compliance certifications. This approach tells customers that you take their security needs seriously.

This tells potential customers, at a glance, that your startup is serious about protecting their information and serving them as promised. It's a powerful, trust building marketing message that can help you stand out from the competition. Thoropass's platform centralizes all of your reports so you can access it at any time and be ready to take on any enterprise deal.

What Happens If You Fail SOC 2?

Don't worry; you won't! Instead of receiving a failing grade, **you just won't get a completed SOC 2 report at all**.

Usually, your auditor will alert you if they suspect your startup may not pass a SOC 2 audit. Very rarely will an auditor continue on with an audit for a service organization that isn't secure. If this happens, your audit will go on hold while you close the gaps that are preventing you from passing. Once you tie up the loose ends, you start again.

Chapter 6

My Startup Is SOC 2 Compliant. Now What?

Finally, after putting in the time, energy, and resources, my startup is SOC 2 compliant. My work here is done...right?

Not quite! **Compliance isn't a one-and done affair**. It takes ongoing work to maintain controls and cultivate your team's compliance culture, not counting the preparation needed to renew your SOC 2 next year.

The most efficient and effective way to remain compliant is to keep it a priority. This prevents your team from having to scramble to get ready for your annual audits. So, instead of going back to old habits after receiving your SOC 2 report, **do what you need to do to keep your controls in place and start preparing for next year**.

- → Keep gathering the documents for your next audit and maintain a process that documents new policies as your startup grows and becomes more complex.
- → Back up your data every quarter (or as otherwise instructed).
- → Ensure new employees receive appropriate training.
- → Continue to build up a compliance culture in your startup by making compliance a priority rather than just a bunch of checklist items.

By completing your first audit and continuing to keep compliance in mind, you build a strong foundation to support your startup as it takes on bigger customers and matures. Leveraging Thoropass's continuous compliance program, our monitoring and automated evidence gathering platform minimizes work for you to tackle audits for years to come.

Let Thoropass change the way you think about compliance.

Thoropass™

Get in touch →