work — bench

SOC 2 COMPLIANCE

Enterprise Playbook Series

INTRODUCTION

As early-stage enterprise technology investors, Work-Bench has worked with dozens of enterprise startups navigating SOC 2 audits. Although “SOC 2 audit” have become dreaded words for these leaders, it’s an inevitable process you’ll be faced with at some point - we like to think of it as an enterprise startup right of passage.

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?

This Enterprise Playbook **collates the best practices within the SOC 2 industry to help enterprise startup leaders stay ahead of their organization’s internal controls for information security and privacy, and be able to remain competitive in the market.**

If you’re an enterprise startup whose been through the SOC 2 process and has feedback or a successful game plan that you’ve rolled out, we would love to hear from you! **Additionally, you can watch our webinar recording on this topic here.**

work — bench

Authored By

MATT CATALANO
Director of Growth, Laika
matt@heylaika.com

KIRA COLBURN
Head of Content, Work-Bench
kira@work-bench.com

LAIKA

work — bench

TABLE OF CONTENTS

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.

WHO NEEDS IT?

SOC 2 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. While most startups seek out a SOC 2 audit once reaching their Series A or B, it may be beneficial to do so beforehand if you've already begun selling into enterprise customers.

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 customers expect startups to go through the same sales procurement processes and meet the same security, privacy, and compliance requirements as other vendors. In many cases, enterprise customers will ask you to become SOC 2 compliant before working with them.

Savvy startups also use SOC 2 compliance as a competitive differentiator. Compliance doesn't just tell enterprise customers 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.

SOC 2 SCOPE

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.

TRUST SERVICES CRITERIA (TSC)

A SOC 2 report tests against five Trust Services Criteria:

1. SECURITY
2. AVAILABILITY
3. CONFIDENTIALITY
4. PRIVACY
5. PROCESSING INTEGRITY

PRO TIP

In our experience, most 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 are good starting points. And add any criteria your target customers are asking for.

CHOOSING WHICH SOC 2 TRUST SERVICES CRITERIA TO TEST

When you engage an auditor, you decide which of the five you'd like tested. Even though only the Security criteria is necessary for a SOC 2 audit, you may choose to test other criteria that are relevant to your startup and how you serve your customers. These decisions are often influenced by what enterprise buyers request. One potential enterprise customer may ask for a particular TSC, another may ask for other TSCs. You don't want to be in a position where your SOC 2 does not ultimately satisfy a broad range of prospective customers. So, it is best to get advice and guidance on what TSCs are most relevant given what your startup does.

#1: SECURITY

Also known as the “common criteria,” security is the foundational criteria that is required in every SOC 2 assessment.

That’s because the security criteria not only sets over-arching 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 NEEDS IT?

All companies that need a SOC 2.

#2: AVAILABILITY

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 99.31percent. By validating your uptime and other availability considerations with this criteria, you're further demonstrating your reliability to your customers.

WHO NEEDS IT?

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

#3: CONFIDENTIALITY

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 NEEDS IT?

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

#4: PRIVACY

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. Given the rise of privacy regulations such as GDPR and CCPA, many enterprises want assurances that their vendors protect personal information.

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 NEEDS IT?

Companies with access to personal information.

PRO TIP

GDPR (EU), CCPA (California), and PIPEDA (Canada) are data protection and privacy regulations. If you need to be compliant with one of these regulations, there is a lot of overlap with the Privacy TSC. Start by working towards these regulatory frameworks then work on the Privacy TSC.

#5: PROCESSING INTEGRITY

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 NEEDS IT?

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

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. The key difference between Type 1 and Type 2 is design versus operating effectiveness.

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. This involves checking to see that you've identified and documented the controls you have in place, and 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.

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.

SOC 1 VS. SOC 2

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.

For more info about SOC 1, check out **A Founder's Guide to Deciphering Which Compliance Type is Right for Your Startup**

SOC 2 TIMELINE

HOW LONG DOES SOC 2 COMPLIANCE TAKE?

The deciding factor of your compliance timeline is the complexity of your product and company, including:

- 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?

BEST-CASE SCENARIO

In a best-case scenario, a SOC 2 audit for a startup can take as little as 4-6 weeks to draft. However, startups usually spend much more time preparing for the audit. This preparation stage includes learning about and selecting compliance frameworks, gathering documentation and policies, undergoing a readiness assessment (pre-assessment), and vetting auditors.

The exact time depends on the scope of your audit. Testing multiple Trust Services Criteria rather than only the required security criteria will mean gathering more evidence. Likewise, you'll have to wait longer for your report for a Type 2 audit, which tests your controls over a 6- or 12-month period, than a point-in-time Type 1 audit.

PRO TIP

There are 3 key elements to shorten the runway to audit. One, know your assets, both physical (e.g. devices) and virtual (e.g. servers). Two, understand what data lives where, it's criticality, and how it will be handled. Three, establish key roles for your team, then assign data and system access based on need.

SOC 2 TIMELINE

SOC 2 TYPE I TIMELINE

SOC 2 TYPE II TIMELINE

THE BIGGEST COMPLIANCE ROADBLOCKS?

Completing a SOC 2 audit is a large undertaking that requires time from multiple people across the company. Audits can drag on longer than necessary when not properly prioritized and prepared for by the team. Excessive back-and-forth between the company and auditor can also put a significant hold on progress, causing long delays. This happens when the startup and the auditor struggle to clarify requirements and communicate with each other.

HOW LONG DOES 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. In the normal course of business you will fall out of compliance as you hire new people, open a new office, evolve your infrastructure, develop your product. This means the evidence you gather and the controls your auditor tests in your subsequent annual SOC 2 audits will 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.

PRO TIP

In order to avoid audit nightmares and minimize delays, you need to invest in preparation and ensure the right folks in your organization prioritize this effort. Between SOC reports, audit firms sometimes issue 'Bridge Letters' to serve as intermediate validation that can be useful for your sales and security diligence conversations.

SOC 2 COST

SOC 2 Cost Relies On:

- Team size and distribution
- Lack or abundance of control documentation
- Complexity of services as well as the number and complexity of processes
- Type of personal or confidential data you process or store
- Scope of your audit (Trust Services Criteria and Type 1 or 2)
- Size of your auditor

As an example, for a Series A startup based in the U.S. with 25 employees going after two TSC's (Security & Confidentiality), for the audit alone, you can expect to pay around:

- $10,000 to $30,000 for a SOC 2 Type 1 audit
- $30,000+ for a SOC 2 Type 2 audit

Additional compliance-related expenses like your:

- Dedicated in-house employee(s) time
- Consultants or other vendors
- Readiness assessment
- Legal fees
- Any technical work, training, or cultural changes you need to put proper controls in place

SOC 2 PREPARATION

WHEN SHOULD YOU START PREPARING FOR YOUR 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.

There's a lot to learn when you pursue your startup's first SOC 2 audit. With that in mind, it makes sense to start earlier then anticipated to give yourself time to understand what exactly is needed from you and to button up any gaps in your controls.

Say you learn from your readiness assessment (more on that later) that you have gaps in your controls. You then need to follow up with a remediation process to close those gaps before the actual audit. Depending on the size of the tasks, this alone can take several months.

PRO TIP

Cost and time are two big challenges for every startup, and often cited as reasons to bump compliance down the roadmap.

Early adoption of security and compliance best practices goes a long way to securing your organization and minimizing disruption. Build a compliance culture and mindset into your foundation. You can right size your compliance program to where you are as a company and build things that will scale as you grow. If cost is a factor, figure out how to be creative with low cost or open source products.

Always understand what you're protecting and why. Always have a strong narrative as to why you've made certain choices.

HOW TO SELECT YOUR AUDITOR

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 generally understands the impact cloud-based information storage, co-working spaces, and other unique considerations have on compliance. It's ok if your auditor does not have enterprise tech expertise, but it will likely slow down the audit process.

- If you're unsure where to begin, try asking your investors and other network connections for recommendations.

- 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.

- Keep in mind the importance of sticking with one vendor throughout the compliance process regardless of the type of compliance you choose.

PRO TIP

The "Big 4" firms will be more expensive, but that doesn't necessarily mean a more comprehensive or 'better' audit. There is a price premium there and most startups don't need all the resources a massive firm provides to get through the SOC 2 process successfully.

Look for a mid-level firm that has a good reputation. Ask if they have worked with tech-forward, VC-backed companies. Ask if they are comfortable with doing most of the attestation remotely. There are plenty of great firms out there for startups that don't come at too high of a cost.

RECOMMENDED RESOURCES

RECOMMENDED COMPLIANCE COMPANIES & TECHNOLOGY SOLUTIONS:

There is a growing landscape of tools to help startups with implementing controls, maintaining your compliance program, securing your data, protecting your organization, and attaining a SOC 2 certification.

COMPLIANCE PLATFORM	PASSWORD MANAGER	ENDPOINT SECURITY	CHANGE MANAGEMENT	HUMAN RESOURCES	ASSET MANAGEMENT
Vanta LAIKA	1Password DASHLANE	Bitdefender	GitHub Clubhouse Jira	GUSTO JUSTWORKS.	jamf JumpCloud

RECOMMENDED CPA FIRMS FOR TECH-FORWARD STARTUPS:

A-LIGN blumshapiro COALFIRE GRASSI ADVISORS & ACCOUNTANTS KP KirkpatrickPrice

WHO SHOULD BE ON YOUR INTERNAL SOC 2 TEAM?

Your auditor can't do all the work for you. You'll need to rely on your team to gather the documentation and evidence your auditor requires.

As compliance doesn't start and end in engineering, you will need involvement from all aspects of your startup, including sales, operations, HR and legal (if you have these departments already built out). 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.

PRO TIP

Most early stage startups will not have a dedicated risk and compliance team member, that's ok.

Assign a lean team (2-3 people) to the project, including one highly technical person (can be the CTO depending on your team's size) and an ops-focused person.

HOW DO YOU KNOW IF YOUR STARTUP WILL PASS THE SOC 2 AUDIT?

We recommend doing a gap analysis or a readiness assessment before your audit. These 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 report. It gives you an opportunity to right these missteps before the official assessment.

For Example

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

- If you fail to perform these assessments properly you may fail to notice there is a control missing such as a change management procedure that could potentially impact the security of your application. This could cause you significant delays as you will need to remediate the issue, write the policy and procedure, and then implement it.
- Readiness and risk assessments bring these potential blocks and issues to your attention sooner, before the audit. If you wait until the auditor points out issues, it could take months to close some of the gaps identified, and will only add amplify the disruption to your team's day-to-day priorities in running your business.

LAIKA PRO TIP

A SOC 2 is not pass or fail, per se, but the more prepared you are the less headache there will be and the sooner you will make it through the audit.

Proper audit prep helps to minimize the loops required to remediate issues identified by the auditor, this is where extensive delays occur.

Gap assessments on the front end can help project manage what needs to be done to implement SOC 2 controls. Then a risk assessment, after implementing all controls, policies, and procedures can minimize any loops needed during the audit process in order to "pass."

ONCE YOU GET THE 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.**

LAIKA

ABOUT LAIKA

Laika helps growing companies implement and manage compliance, obtain security certifications, and build trust with enterprise customers. Through a modern compliance platform coupled with dedicated experts, Laika minimizes the time, cost, and headaches for early stage companies to implement scalable, audit-ready compliance programs.

Laika streamlines audit prep and management for SOC 2, as well as other security certifications and regulatory frameworks. Through an expert-in-the-loop model, Laika performs gap and risk assessments, provides implementation guidance, and automates document and evidence collection to ensure a smooth audit process.

Check out Laika's comprehensive compliance solution to streamline your SOC 2 process.

www.heylaika.com | /LaikaHQ | hello@heylaika.com

work — bench

THANK YOU

Work-Bench is an enterprise-focused venture capital firm based in New York City. Work-Bench was founded in 2013 with a unique, thesis-driven approach that flips traditional enterprise venture capital upside down by first validating Fortune 500 IT pain points through our extensive corporate network and then investing in the most promising companies addressing these challenges.

Sign up for the Work-Bench Enterprise Weekly Newsletter, to stay up-to-date on all things enterprise tech with 18K+ subscribers.

www.work-bench.com | /work_bench | hello@work-bench.com