Agency

THE STARTUP COMPLIANCE SERIES · GUIDE

SOC 2

The startup's guide to

# Buying SOC 2

How to get your first SOC 2 report without slowing down your roadmap.

A practical buyer's guide for founders & engineering leaders

© Agency Cyber Inc. 2026

June 22, 2026 • getagency.com

SOC 2 · STARTUP GUIDE

## Why you're reading this

For most startups, SOC 2 doesn't start as a strategic decision. It starts as a blocker.

A promising deal reaches procurement and the prospect's security team asks for your SOC 2 report. Or an enterprise logo says yes — then sends a security questionnaire with a hundred questions you've never thought about. Suddenly a piece of paper stands between you and revenue, and nobody on your team has done this before.

The good news: SOC 2 is a well-worn path. Thousands of startups go through it every year, and the playbook is knowable. The bad news: it's surrounded by jargon, the options look confusingly similar, and the wrong choice can cost you months and a meaningful chunk of engineering time.

This guide is written for the first-timer. No prior compliance background assumed. By the end you'll understand what SOC 2 actually is, the handful of decisions that matter, the three ways startups typically get it done, and how to choose the path that fits your stage. We've kept it high level and practical — a buyer's guide to the lay of the land. It's written by the team at Agency; we've worked to compare the options fairly, and we're upfront that we also offer the operated approach covered later, so you can weigh our perspective accordingly.

---

## SOC 2 in plain English

SOC 2 is an independent audit of how well your company protects customer data. An independent CPA firm (the service auditor) examines your security practices against the AICPA's Trust Services Criteria and issues a report describing what they found.

A few things worth understanding up front:

**It's a report, not a certificate.** There's no badge that says "SOC 2 certified." The deliverable is a report (often 40+ pages) that your prospects' security teams read. You typically share it under NDA.

**You define part of the scope.** Unlike a pass/fail exam with fixed questions, SOC 2 lets you describe the controls you have in place. The auditor then tests whether you actually do what you say. This flexibility is powerful — and a common place where startups over- or under-scope.

**It's built around five "Trust Services Criteria."** Think of these as the categories your controls can be measured against:

- **Security** — the foundation. Protecting systems against unauthorized access. *(Required in every SOC 2.)*
- **Availability** — is your system up and accessible as committed?
- **Confidentiality** — is sensitive information protected?

- **Processing Integrity** — does your system process data accurately and completely?
- **Privacy** — is personal information collected and handled appropriately?

Almost every startup starts with **Security** alone (often called the "Common Criteria"). You add the others only if a customer specifically requires them or your business clearly demands it. More criteria means more work, so don't gold-plate your first report.

**It's an annual commitment, not a one-time project.** A SOC 2 report covers a window of time and then needs to be renewed. The first one is the heavy lift; after that it becomes a rhythm. Plan for the long game from day one.

---

## The one decision that trips everyone up: Type I vs. Type II

There are two flavors of SOC 2, and knowing the difference saves you a lot of confusion.

**SOC 2 Type I** is a point-in-time snapshot. It confirms your controls are *designed* properly on a specific date. It's faster to achieve and can unblock a deal quickly.

**SOC 2 Type II** observes your controls *operating* over a period of time (commonly 3 to 12 months). It's stronger evidence because it proves you actually do these things consistently — not just that you set them up the day before the audit.

What this means for you:

- Most enterprise buyers ultimately want **Type II**. It's the real currency of trust.
- Some startups do a **Type I first** to unblock an urgent deal, then roll straight into a Type II observation window. Others skip Type I and go directly to Type II.
- A Type II requires you to *operate* your controls for the whole observation window, which is why starting your practices early matters more than starting your audit early.

If a customer is forcing the timeline, a Type I can buy you breathing room. If you have a little runway, going straight to Type II avoids paying for two audits.

---

## What the journey actually looks like

Strip away the jargon and the path has four phases:

**1. Readiness.** Figure out your scope, write the policies you're missing, put the right controls in place, and start collecting evidence that they're working. This is where most of the effort lives.

**2. The observation window (Type II).** Your controls run for a set period while evidence accumulates — access reviews happen, backups run, alerts get triaged, onboarding and offboarding follow the process.

**3. The audit.** An independent firm examines your evidence, asks questions, and tests samples. You answer requests and close any gaps they find.

**4. The report — and renewal.** You receive your report and share it with prospects. Then the clock resets: SOC 2 is continuous, so the practices need to keep running for next year's report.

The single biggest predictor of a smooth audit isn't the auditor you pick — it's how well-run your day-to-day security operation is during the observation window. Evidence you generate naturally beats evidence you scramble to reconstruct.

---

## The three ways startups get SOC 2 done

Here's the part most guides skip. Once you understand what SOC 2 requires, the real question is *how you'll actually do the work*. There are three common paths.

### Path 1 — DIY without a GRC platform

You manage the whole thing with spreadsheets, shared drives, and calendar reminders. You write your own policies, track controls by hand, and collect screenshots and exports as evidence.

**Who it can fit:** Very early teams with a strong technical lead who has done this before, a simple stack, and more time than money.

**The honest tradeoffs:** It's deceptively expensive in the currency that matters most to a startup — founder and engineer hours. Evidence collection is manual and easy to let slip. Spreadsheets drift out of date. When the auditor asks for access reviews spanning the full observation window, you're reconstructing history instead of pulling a clean trail. For most startups, the "free" path quietly becomes the most costly one in time and stress.

### Path 2 — Buy a GRC platform (e.g., Vanta or Drata) and run it yourself

GRC automation platforms like **Vanta** and **Drata** connect to your cloud, identity provider, and other tools to continuously monitor controls and gather evidence automatically. They give you a controls dashboard, policy templates, and a clear picture of where you stand.

**Who it can fit:** Teams that want structure and automation, and have someone in-house with the time and judgment to operate the platform, interpret what it's telling them, and drive the work to completion.

**The honest tradeoffs:** This is a big step up from spreadsheets, and these platforms are excellent at what they do. But it's important to understand what they *are*: they automate **evidence collection and monitoring**. They are not a person. The platform will show you a red control — it won't decide how to fix it, write the remediation, configure your cloud, chase a vendor for their report, or sit across from the auditor on your behalf. A dashboard full of green checks still requires someone who knows which checks matter, how to interpret an exception, and how to translate "task" into

"done." Buy a platform expecting a tool, not a teammate, and you'll get the value. Expect it to run your program, and you'll be disappointed.

### Path 3 — Have it operated for you

Instead of just buying software, you bring in a team that *runs* the program end to end — typically on top of a platform like Vanta or Drata, not instead of it. They handle scoping, write and tailor your policies, implement and remediate controls, collect and validate evidence, manage vendor risk, and coordinate directly with the auditor. You get the dashboard *and* the people who act on it.

**Who it can fit:** Startups who would rather their engineers ship product than become part-time compliance managers — and who want SOC 2 done right the first time, with security maturity that holds up beyond the audit.

**The honest tradeoffs:** You're adding a partner rather than doing it all internally, so it works best when you value speed, certainty, and keeping your team focused on the roadmap. The upside is that the work that usually lands on your most expensive people — judgment calls, remediation, audit wrangling — gets handled by people who do it every day.

---

## The work a platform doesn't do

This is the gap that surprises most first-timers, so it's worth making explicit. Whether you go DIY or buy a platform, *someone* still has to:

- Decide the right scope so you're not auditing things you don't need to.
- Write and tailor policies to how your company actually operates — not just accept generic templates.
- Implement the real technical controls in your cloud and applications, and **remediate** the ones that are failing.
- Interpret monitoring alerts and exceptions, and know which ones actually matter.
- Run access reviews, manage onboarding/offboarding, and keep the human processes consistent.
- Chase your vendors for *their* reports and assess third-party risk.
- Assemble evidence the auditor will accept, and manage the back-and-forth with the auditor through to the final report.
- Keep all of it running for next year.

Automation removes the busywork of *gathering* evidence. It doesn't remove the **judgment** of running a security program. The three paths above are really three answers to one question: *who is going to do this work?* — your team with spreadsheets, your team with a platform, or a dedicated team operating a platform for you.

## How to choose: a quick framework

Run your situation through these five questions.

1. **How urgent is the deal?** If a contract is gated on SOC 2 *now*, you need either a Type I to unblock fast or an operated approach that compresses the timeline. Pure DIY is the slowest.
2. **How much engineering time can you actually spare?** Be honest about what a founder or senior engineer running compliance part-time really costs — in dollars and in roadmap. Compliance work tends to expand to fill (and overflow) the time available.
3. **Do you have in-house expertise?** Has anyone on your team owned a SOC 2 before? A platform assumes a competent operator. If that person doesn't exist, a tool alone won't close the gap.
4. **Is this one report or the start of a program?** If ISO 27001, HIPAA, or more frameworks are on the horizon, build for an ongoing security operation now rather than a one-off scramble.
5. **What's the cost of getting it wrong?** A messy first audit, a report with exceptions, or a missed renewal can damage trust with the exact enterprise buyers you're trying to win. Sometimes the cheaper-looking path is the expensive one.

A simple rule of thumb: **the more your engineers' time is worth, and the more certainty you need, the further down the path from DIY → platform → operated you should look.**

## Common first-timer mistakes to avoid

- **Over-scoping.** Adding Trust Services Criteria nobody asked for, multiplying the work for no commercial benefit. Start with Security; add more only when required.
- **Starting the audit before starting the practices.** A Type II proves controls operated over time. You can't backfill a clean evidence trail the week before.
- **Treating a tool as a team.** Buying a platform and assuming the work is now handled. The dashboard surfaces the work; it doesn't do it.
- **Underestimating the engineering tax.** "We'll knock it out in a couple weekends" is the most expensive sentence in compliance.
- **Ignoring vendor risk.** Your auditor will ask about your subprocessors. Gathering their reports late is a classic last-minute fire drill.
- **Letting it lapse.** SOC 2 is annual. Treating it as one-and-done means re-running the scramble every year instead of building a rhythm.

## What "good" looks like

A healthy SOC 2 program, regardless of who runs it, tends to share a few traits:

- Scope is **right-sized** to what your customers actually need.
- Policies reflect **how you really work**, so the team can follow them without friction.
- Evidence is generated **automatically and continuously**, not reconstructed under deadline.
- Someone clearly **owns** the program and has the time and authority to drive it.
- The audit is **a confirmation**, not a surprise — because the operation was already running well.
- Year two is **easier than year one**, because the system is in place.

If your plan doesn't get you to most of these, it's worth rethinking the path before you start.

---

## A note on doing this without distracting your team

Most startups don't fail SOC 2 because the requirements are impossible. They struggle because the work quietly pulls their best engineers off the roadmap for months — implementing controls, gathering screenshots, interpreting a dashboard, and negotiating with an auditor — none of which is why those engineers joined.

That's the case for the operated approach, and it's worth being upfront that this guide comes from **Agency**. We're a security and compliance team you don't have to hire — U.S.-based forward-deployed engineers, supercharged by our own AI, who run your program end to end on top of the tools you already trust like **Vanta** and **Drata**. Virtual CISO, control implementation, evidence collection, continuous monitoring, vendor risk, and audit coordination — included, without adding headcount. Agency has served more than 1,000 companies and is backed by Y Combinator.

Whichever path you choose, we hope this guide makes the decision clearer. If you'd like a second opinion on your specific situation — scope, timeline, and the fastest path to audit-ready evidence and a report without avoidable exceptions — we're happy to talk.

**Want to see what an operated SOC 2 would look like for your startup?**
Talk to our team for a no-pressure walkthrough of your scope and timeline.

**Assemble your GRC team ›**

---

*This guide is for general educational purposes and isn't legal, audit, or compliance advice. SOC 2 requirements depend on your specific business, systems, and customer commitments.*