What's a SOC 2 certification?

Ah shit, it's the auditors again

Justin
Apr 13, 2021

The TL;DR

Companies get a SOC 2 report to **show off how secure and compliant their processes are** to potential customers.

- Larger companies demand **high security and compliance standards** from their vendors (companies they buy things from)
- **SOC 2** is a **report** issued by a **third party auditor** certifying that your company meets a set of standards
- Most SOC 2 standards relate to things like **software best practices**, **company governance**, and **system security**

As more startups start to focus on moving up-market and selling into enterprises, SOC 2 has been having a moment – pretty much every company I've worked at has gone through the report process.

SOC 2 – the why

Security certifications and such aren't just for giant companies - even small (like literally, 5-person) startups are thinking about SOC 2 these days. So what's changed?

1. **Startups moving up-market** – companies are starting to think more about how to sell into larger organizations earlier in their lifecycles (that's where the money is!). And those larger orgs have more stringent security requirements.

2. **Security's general awareness** – tight requirements for security and compliance and moving *down* market, as even small to mid sized companies hold their vendors to high standards.

SOC 2 isn't *technically* a certification, since there's no central body that decides which startups get bestowed with the honorary "SOC 2 crown." Instead, it's a **report** issued by a third party auditor that verifies "yes, this company is decently not terrible at security and compliance."

> 🚨 **Confusion Alert** 🚨
>
> SOC 2 technically has **two types** - Type I and Type II (creatively named). Type I assesses your security chops at a point in time, while Type II does so over a longer period of time (typically 3 to 12 months). Usually, companies start with a Type I and get their Type II done subsequently.
>
> 🚨 **Confusion Alert** 🚨

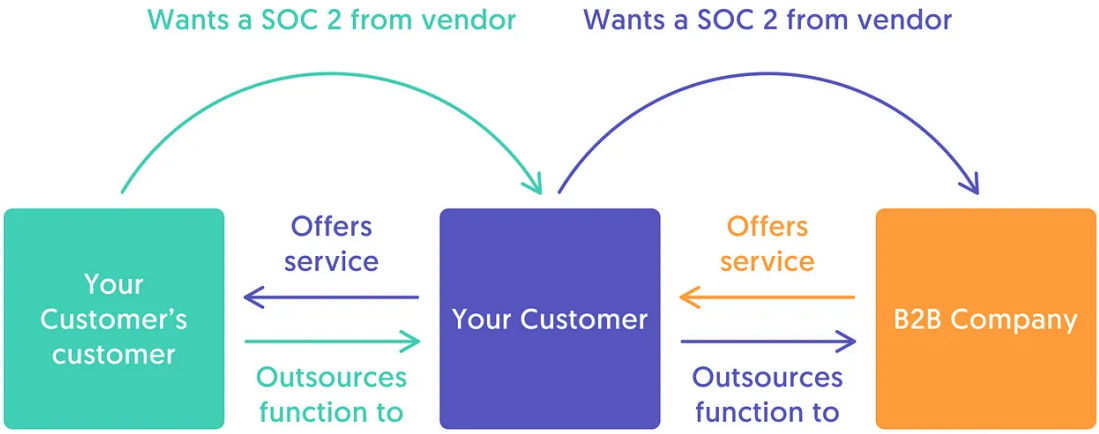
The standards that auditors look for, though, *are* determined by a central body – it's called the American Institute of Certified Public Accountants (AICPA), an organization we can only imagine parties hard on the weekends.

SOC 2 – the what

Ah yes, the section you've been waiting for - what does this CeRtIfIcAtIoN actually mean? There are basically two pieces of governance and security that auditors look for:

1. **Organizational** – things like performance reviews, maintaining an org chart, and security awareness training
2. **Technical** – things like running vulnerability scans, encrypting your data at rest, and tracking your software development lifecycle

Your auditor will give you an itemized list of things your company needs to do, and your team needs to give them proof that you actually do those things. And if you don't do them yet (for example, you don't have issue tracking set up for your codebase), you need to set them up.



If you're wondering why Technically is covering SOC 2 (we are *not* a compliance newsletter), it's because SOC 2 reports tend to cover *a lot* of tech stuff. Engineering teams need to be heavily involved in the reporting process, because auditors are looking for very specific controls on the software development process. A few examples:

- Issue tracking of software features and bugs with something like JIRA or Linear
- Change management for releases (e.g. a Git workflow, multiple environments)
- Encrypting customer data at rest
- Basic application performance monitoring with something like Datadog

At the companies I've worked with who went through SOC 2 audits, there was usually a **developer lead** responsible for handling most of this stuff. And they have to do a lot of manual, kind of annoying non-technical things, like tracking down information, taking screenshots of settings, etc. Teams are starting to use SaaS like Secureframe to automate that process, but more on that later.

And if you're interested in diving deeper into the technology piece here, I wrote about it on the WorkOS blog a while back.

> 🔍 **Deeper Look** 🔍

> For larger companies, SOC 2 reports can be quite large, and have decently well-known auditors. A good example is the SOC 2 report that Carta got from their auditor, BDO.
>
> 🔍 **Deeper Look** 🔍

How to get SOC 2 certified

The word "audit" is very scary, but getting that SOC 2 report doesn't need to be a nightmare. Standards are generally very straightforward, and while you need to put time into it, it's a predictable cycle. In general, budget:

- **3-4 months** and a decent amount of time per week from a few core team members (you can shorten this by a lot with a decent automation tool)
- **$10-40K** for audit costs
- **$3-30K** for a pen test (not fully necessary, but good)

In other words - it's a serious investment, but one that pays off and shouldn't consume all of your time.

→ Finding an auditor

The first step to getting that elusive report is finding an auditor to work with. There are literally thousands, which can be a bit overwhelming – a basic Google search is your friend, or consider working with a company like Secureframe that can connect you with a vetted auditor network, plus help with the details via an in-house compliance team.

→ Working with a technology partner

Because the tech part of SOC 2 tends to be the most tedious and specific of the audit requirements, you can outsource pieces of it to companies like Secureframe or Vanta. They'll connect to your tech and infrastructure (e.g. AWS, Rippling, Github) and automate some of the process (or proof) that your auditors are looking for.

→ Alternative certifications

As you try and expand your customer base, it becomes evident that SOC 2 is just the *start*. Larger and larger enterprises ask for more specific certifications and reports, often specialized to arenas like healthcare or finance. A few examples:

- ISO 27001, a SOC 2 like standard popular outside the U.S.
- HIPAA compliance for healthcare data
- PCI for payments data
- CMMC for Department of Defense contractors

2 Comments

Write a comment...

Nathan Xiao Apr 15, 2021

FedRAMP is another notable certification for government contractors, similar to CMMC - DOD is looking into getting FedRAMP and CMMC reciprocity.

♡ 2 Reply Gift a subscription Collapse •••

Nick E. Writes Nick's Vital Few May 8, 2021

Whenever I see the auditors, I say "Awwww SHIT!!"

♡ 1 Reply Gift a subscription Collapse •••