Ariel Diaz Follow

3x Entrepreneur. Founder/CEO at Blissfully.com. Previously Founder/CEO at Boundless and YouCastr. NYC, by way of Boston, Frankfurt, Chicago, Hanover, Miami.

Mar 26 · 6 min read

Why We Did SOC 2 a Month After Our Seed Round

Most companies wait until their B or C round (or later) to start tackling key industry security audits and compliance certifications.

I think that's a mistake.

In fact, we started our SOC 2 Type II process just a month after closing our Seed round.

Data security and privacy more important than ever

Information security and data privacy is more important than even. Hackers (Russians) have recently compromised cities, companies, credit agencies, and elections. Plus, there is a growing backlash over questionable privacy policies, controls, and "breaches" at Facebook. Ignoring these trends and risks for your business is simply reckless.

Starting early embeds it into your culture and processes

Strong security is fundamental to our vision of the company we wanted to build. Our mission is to simplify how organizations manage IT, and this means being deeply embedded in their organization, and having access to sensitive information. Getting companies to work with us requires trust. And achieving SOC 2 compliance helps us demonstrate to our customers that we are trustworthy, and take security, privacy, and compliance seriously enough to invest in it. We did it so early in our company lifecycle because we wanted to create a culture that treats security as a central tenet from the start, not something that we bolted on years later with some outside consultants.

Understanding SOC 2: Don't be intimidated

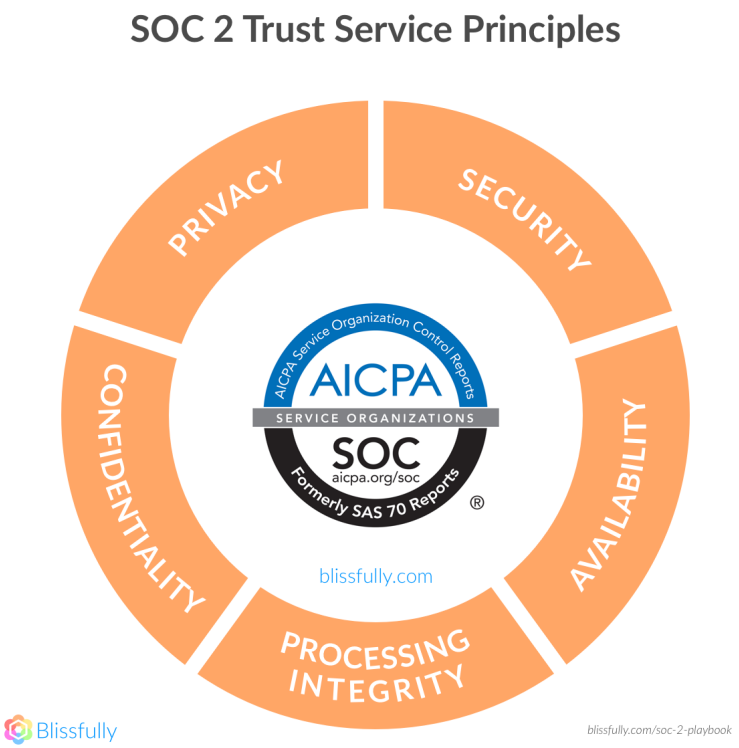
Our first step in preparation was to get a good understanding of what the audit was going to require. We spent weeks figuring out what being compliant meant to us as a company. For us, achieving SOC 2

compliance at an early stage meant that we were truly internalizing these policies and procedures and baking them into our corporate ethos, rather than just fulfilling a checklist. Waiting until later to go through this process seemed far more difficult to us, since we'd have to start breaking bad habits, rather than establishing good ones from the outset.

Brief SOC 2 Overview

We chose to start SOC 2 because it's broadly applicable to SaaS companies, widely recognized across the industry, and creates a good foundation to build on and potentially add others (e.g. ISO 27001).

SOC 2 is a framework that is built on 5 key "trust principles":



There are a set of criteria across all principles (the "Common Criteria"), and a few additional criteria specific to each principle that depend on your audit scope).

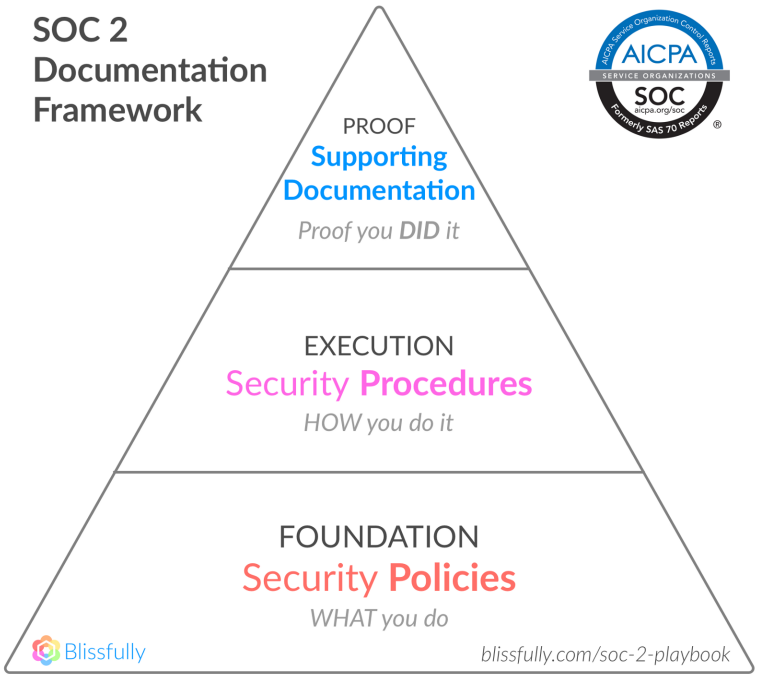
Documentation Framework

Overall, when completing a SOC 2 compliance audit, there are three key types of documentation:

- **Security Policies (WHAT you're gonna do):** This documents how you approach all the compliance requirements, and

documents your goals and plans. Typically this is defined in a (massive) “Information Security Policy” document. Ours is 10,000 words. Sophisticated vendors will ask to see this. as will the auditor.

- **Procedures (HOW you do it)**: These define the specifics of how you actually do the things you outlined in your policies. Things like who is responsible for communicating security breaches, how do you enforce laptop security, and which tools do you use to execute it. We recommend using as much software as possible to automate the process.
- **Supporting Documentation (Proof that you did what you said you’d do)**: What are the proof points that show the procedures you’ve set up fulfill the policies you’ve laid out as a company?



Preparing for the Audit

We decided to complete a Type II SOC 2 audit instead of a Type I audit, since we knew we eventually wanted to strive for a Type II certification (Type II means audits your compliance over a period of time, typically 6 months or more, Type I looks at a moment in time). Choosing to go directly to Type II was faster and cheaper for us in the long run, because if you completed both audits you’d end up spending about 1.5x the cost of just doing the six-month audit the first time around.

We spent the next phase looking at our own internal processes. My cofounder and I drafted and revised a security policy that coincides with each area of the compliance framework. We then went through our workflows in the areas of people ops (HR+IT), including employee onboarding and off-boarding, plug engineering processes and security. We went deep in each area, spending several weeks examining things including our onboarding and training process, how we monitor and check code changes, and how we manage computers and our physical office space. From there, we modified our key procedures before we even started the clock on our SOC 2 audit.

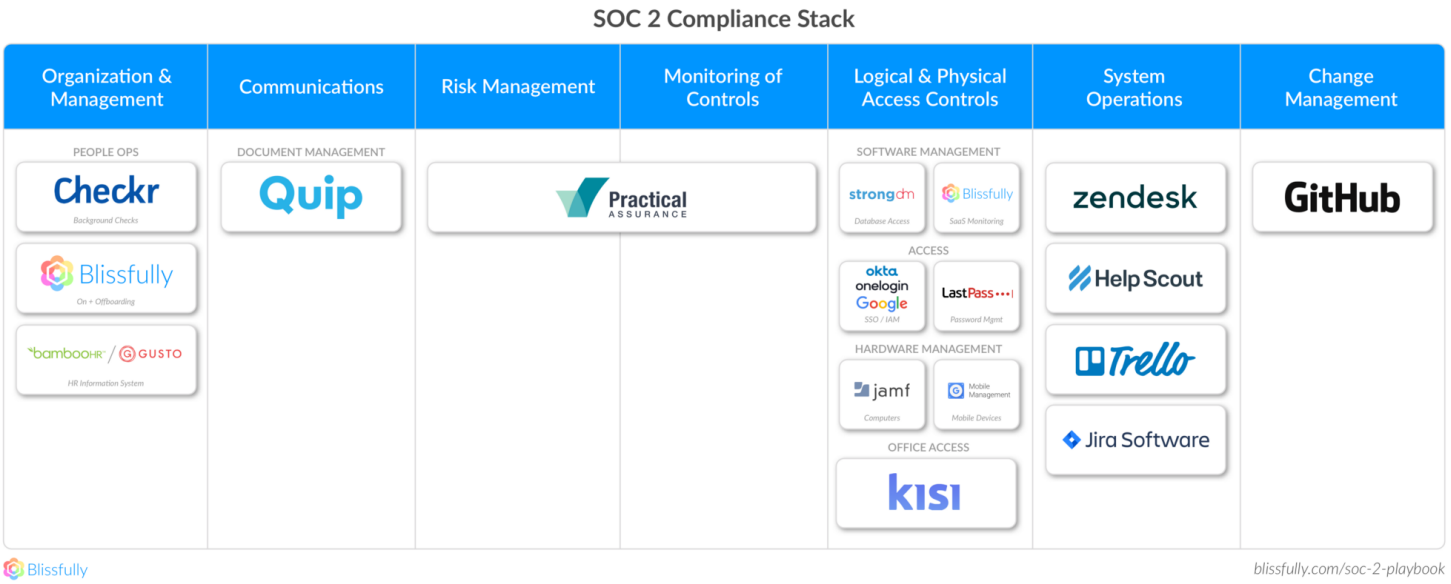
For example, on the HR side, we ended up adopting BambooHR as a human resources information system (HRIS) on employees that would help fulfill the personnel compliance checklist. All paperwork flows through the HRIS, which minimizes the use of random spreadsheets to track our workflow.

The experience of going through our workflows step by step helped inspire new functionality in the Blissfully app. Subsequent audits should now be easier, since app provisioning workflows are tracked in Blissfully. We also built in employee onboarding and offboarding for SaaS apps, complete with an audit trail of who's accessing which services. This functionality gives you the ability to quickly give employees access to the tools they need, and remove access when they leave the organization.

Choosing the right tools

Historically a lot of the SOC 2 documentation (especially the supporting documentation) was handled manually by a bunch of spreadsheets or forms. Being techies, we wanted to leverage software automated workflows wherever possible. We adopted (and later on built) software to do just that.

Here's an overview of what we used and recommended:



Our recommended SaaS Stack for SOC 2 compliance—broken out by Common Criteria

You can see more details on the full stack and tools in our SOC 2 Compliance Playbook.

Completing the Audit Itself

When an auditor arrives on site, you can expect him or her to go through each of the three core areas: policies, procedures and documentation. The auditor will look at how each of these areas are handled in your organization, and ask important questions along the way. The review of the policies and procedures will be to make sure you cover all the required criteria.

Most of the work will focus on the “Supporting Documentation”. For example, on the engineering side, an auditor will dig into how your organization living up to the policies you’ve laid out for your team. How are software code changes tracked? If you have had a security breach, how did you communicate that to customers and partners? How do you insure your cloud infrastructure is highly available? How would you restore service in the case of a disaster? If you’re prepared, it should be easy to clearly and deeply answer the questions they’re asking with the right proof points to back it up.Because we used tools for most of our processes, our supporting documentation was pretty easy to prepare. It was typically screenshots or exports from the tools we use (e.g. a Pull Request from Github to showcase “change management”).

We are happy to be able to say that we passed our SOC 2 audit on the first go with flying colors, mainly due to the automation tools and built-

in documentation that form the core of how we work.

You can see more about SOC 2 and the compliance certification process in our Blissfully SOC 2 Playbook:

Blissfully SOC 2 Compliance Playbook

. . .

Originally published at www.blissfully.com on March 26, 2018.