Strike Graph

5 Things Founders Should Know about a SOC 2

If you are like us, you wish you had a SOC 2 Fairy Godmother to guide you through the convoluted SOC 2 compliance process. We have something better - Free Advice! In other words, we'll tell you the things we wish we knew when we were Founders.

We want to share our lessons with you because we firmly believe that compliance doesn't need to be complicated, and the journey to a SOC 2 does not have to be painful.

01 Start early.

You don't need a start date to begin the process, but if you do have a tentative timeline or milestone in mind, great! Now take that timeline or milestone and toss it out the window because you are starting *now*. Why *now*? While setting up a decent, appropriately-sized security compliance function is possible in 4-6 weeks, we wish we had methodically chipped away at our looming audit by planning key security tasks in Sprints. Set yourself up for success and avoid the last minute compliance rush. Better to chip away at security *now* then to lose valuable coding hours because all hands are on deck to get prepared for an audit.

You are most likely going to be asked for a SOC 2 when you sell to your first mid-sized or enterprise customer. While it is hard to predict when that first customer will surface, you can come prepared with basic security already in place.

02 Hire or outsource with security in mind.

As you hire, look for applicants who are passionate and practical about security. You will have a leg up! Their passion will make it easier for your organization to put good practices in place. The practicality will be in efficient, appropriately sized security processes - you do not want to put in processes to simply check a box, but rather, because it is the *Right Thing To Do* to win a customer's trust and improve sales. If security is a mystery, consider outsourcing different components that are outside your area of expertise. For example, consider outsourcing the operations and security over the network infrastructure, or a person or solution that can handle your HR/ Operational practices. Focus on what you do well and let others help pick up any slack.

03 Aspire for 'Good Practice', not 'Best Practice'.

You are small, so it's ok to approach your security in steps. The key is to have a solid (aka 'good') baseline. You are nowhere near having a fully staffed enterprise security function, so do not shoot for 'Best Practice' yet. Security will be an evolution - it may not make sense to implement the currently hyped Glossy Marketing Campaign if you have no revenue or customers to support it or especially if that Glossy Campaign is on a provider's roadmap for release 18 months out. Address each security risk as cost-effectively as you can, even if it is temporarily manual and painful.

Unlike more rigid frameworks (NIST, ISO), the beauty of a SOC 2 is that YOU define the controls that you want the auditor to test. You still need to ensure that you have appropriate controls in place to address the SOC 2 'Criteria', but the controls you choose to demonstrate this coverage are up to you. Don't let your auditor convince you to adopt Best Practice when Good Practice will provide you the

04 Where to start?

We do suggest that every startup begins with a solid Change Management Process that can grow as your team grows. Do not start by writing policies - some will not be relevant to your organization and it will become a wasted effort. The policies that will apply to your organization can come later (link to Risk Assessment POST).

In your early days, you are not in the business of formal policy writing - you are busy creating The Next Big Thing. You need to focus on what matters the most as you get off the ground. Once you have your prototype, implement independent testing AND independent code review - this will ensure that no untested code gets migrated without a second set of eyes on it. Set these baseline expectations early. Then, as you grow, you can add other change management practices such as SAST or DAST, etc.

Also, think about your back end infrastructure (It might be appropriate to outsource the management of this in your early days). Set up the basics: a firewall, VPN access, intrusion detection, encrypted email, and configure each container with the CIS Benchmarks. When someone has a free moment, start the practice of running vulnerability scans on a set cadence. Define who and how soon Severe and High vulnerabilities will be addressed. (Medium and Low vulnerabilities can come later when you have more staff to handle them.)

These foundations establish a solid base from which you can add controls for logical access, system monitoring, back ups, vendor management, and all of the operational controls that are appropriate for the SOC 2.

05 Operationalize.

Setting up good security practices is only half the battle. These practices now need to be followed and maintained. Be prepared to have new processes thrown into your start up mix. Also be prepared for a bit of backlash from employees as they adapt to more robust processes. (That key new hire that's passionate about security will come in handy here!) Use collaboration tools (Confluence, Google Docs, etc.) to set up SOPs, or play books that are living documents and can be refreshed as

We hope this information is useful as you embark on your startup journey. Contact us if you have more important things to do than PM a security

ABOUT STRIKE GRAPH

Strike Graph is an IT compliance SaaS solution simplifying security certifications such as SOC 2 Type I/II or ISO 27001. These certifications dramatically improve revenue for B2B companies. Facilitated by the Strike Graph platform, Key actors in the process inducing Risk Manager, CTO's, CISO's and Auditors can work collaboratively to achieve trust and move deals. For more Information Visit https://www.strikegraph.com