The Essential Guide to SOC 2 for Startups

SHUJINKO

Intro

Are you panicking because your enterprise leads are asking about SOC 2 and you've never even heard of it? Or maybe you have heard of SOC 2, but don't know what's involved to achieve it. Don't feel overwhelmed — lots of other B2B startups are in the same boat. With SOC 2 compliance, you can improve your security posture and pass through vendor approval processes quicker to close more enterprise deals.

This guide to cloud compliance covers everything startups need to know: where to begin, how to achieve compliance, expected budgeting, mistakes to avoid and ways to make the process easier.

Contents

Section 1

What exactly is "cloud compliance"?

We can't talk about cloud compliance, or SOC 2 for that matter, without talking about the cloud and security. The advent of the public cloud represents a truly modern trend in infrastructure. Over the last 10-12 years, even old-line enterprises with on-prem workloads and data centers started moving to AWS, Azure or Google Cloud Platform.

Rather than fronting the expense of traditional hardware and infrastructure, startups born in this era simply adopted the cloud from the get-go. Here's where our story begins.

As the first cloud-native companies, these startups faced a new problem in meeting legal and regulatory security standards. Building architecture in the public cloud had simply never been done before.

> *Cloud compliance refers to the security standards and regulations cloud customers need to follow. These range from HIPAA, GDPR, PCI DSS and many other abbreviated standards. The term describes the process of integrating security best practices and legal policies while building a cloud environment.*

Why bake in security standards *during* the build? Most often, systems that don't meet compliance standards are ones where security practices have been retrofitted after the cloud solution is already up and running. Think of this as the cloud equivalent of trying to wire a house after it's been built. You will save a lot of time — and maybe a few fires — if you read the building code first and design it in from the outset.

Section 2

What do I need to know about SOC 2?

SOC 2 is a security standard written by the American Institute of Certified Public Accountants (AICPA). A SOC 2 audit reviews the security procedures of products or services based in the public cloud. In that way, it falls under the broader umbrella of cloud security and compliance.

There are two flavors of a SOC 2 report: Type 1 and Type 2.

In a **SOC 2 Type 1 audit**, a startup defines its best practices. Type 1 essentially presents a snapshot of security controls at a certain point in time. It collects evidence that shows the security controls that have been put in place and how the company is fulfilling them.

In a **SOC 2 Type 2 audit**, a startup produces a sample set of evidence that proves its security controls have been followed over time. Type 2 is a six-month to a year longitudinal audit that evaluates the constancy of controls through the lens of security.

Do you have to do both Type 1 and Type 2?

Traditionally, on the day that your Type 1 audit is issued, your Type 2 audit period begins. Some startups choose to take a long vacation between audits or forgo Type 2 completely. This is ill-advised.

Let's say you decide to take a six-month break in between completing Type 1 and then starting Type 2. Towards the end of that period, you get a big enterprise lead. They ask you about cloud compliance. You can verify that you were compliant a few months ago when your Type 1 was issued... but your evidence has gone stale in the interim.

> *Most startups need to conduct a SOC 2 Type 2 audit every year to prove their reporting hasn't expired.*

Section 3

What happens if I don’t become compliant?

Clogged sales pipelines

From a basic security best practice standpoint, building your software the right way reduces the risk of a costly breach and the exposure of unprotected customer data.

If you’re chasing enterprise clients, protecting customer data is critical to them. Their reputation is on the line. It’s the enterprise’s name, not yours, that lands in the news in the case of a breach.

So although many enterprises want to work with startups to keep themselves innovative, they perceive young companies as a security hazard. They may love your startup’s product. They still need to evaluate how risky it is to do business with you.

> *In fact, there's a gate around this in the enterprise procurement process. You will not pass go if you don't have a SOC 2 report available or a similar security certification in place.*

Inversely, if you do have a SOC 2 report, you can make air-tight security part of your pitch and get a leg up over your competition.

What happens if you don't become compliant?

> *We've seen startups lose 5-year, $50M contracts simply because they didn't have a SOC 2 audit in place.*

That kind of damage to your sales pipeline is nearly irreversible. And time is your enemy.

Don't be that startup.

Reputational consequences

Security breaches are another blow to your sales pipeline.

> *With reported breaches growing in number and severity (according to Forbes, 2019 saw around 4,000 breaches with over 4.1B records exposed), data protection dominates the public spotlight like never before.*

And yet — even the savviest startups suffer data breaches because they've failed to structure their architecture using best practices. Nothing adds fuel to your competitor's fire like a customer data breach. You can kiss your standing as a company that takes data privacy and security seriously goodbye.

Last to the market

When SOC 2 season comes along, startups typically either have to staff up, allocate heads from existing teams, or bring in expensive consultants.

> *Getting SOC 2 in place requires one or two engineers or more, fully dedicated, for six to eight months. This kind of resource commitment can be life or death for a startup.*

Let’s do the math. You’ve got a year’s worth of funding. You’ve hired just enough engineers to build out a product. You’re working with tight budgets and timelines, racing to hit certain milestones to secure the next round of funding.

But now, with a significant portion of your team tied up in audit preparation, your go-to-market pace slows to a glacial crawl. You’ve promised investors that you’ll acquire and retain N customers, but you can’t advance sales until you’ve completed the audit.

When your sales pipeline is blocked up, your future funding is on the line. Don’t let cloud compliance be a make-or-break issue.

Section 4

Should my startup be SOC 2 compliant?

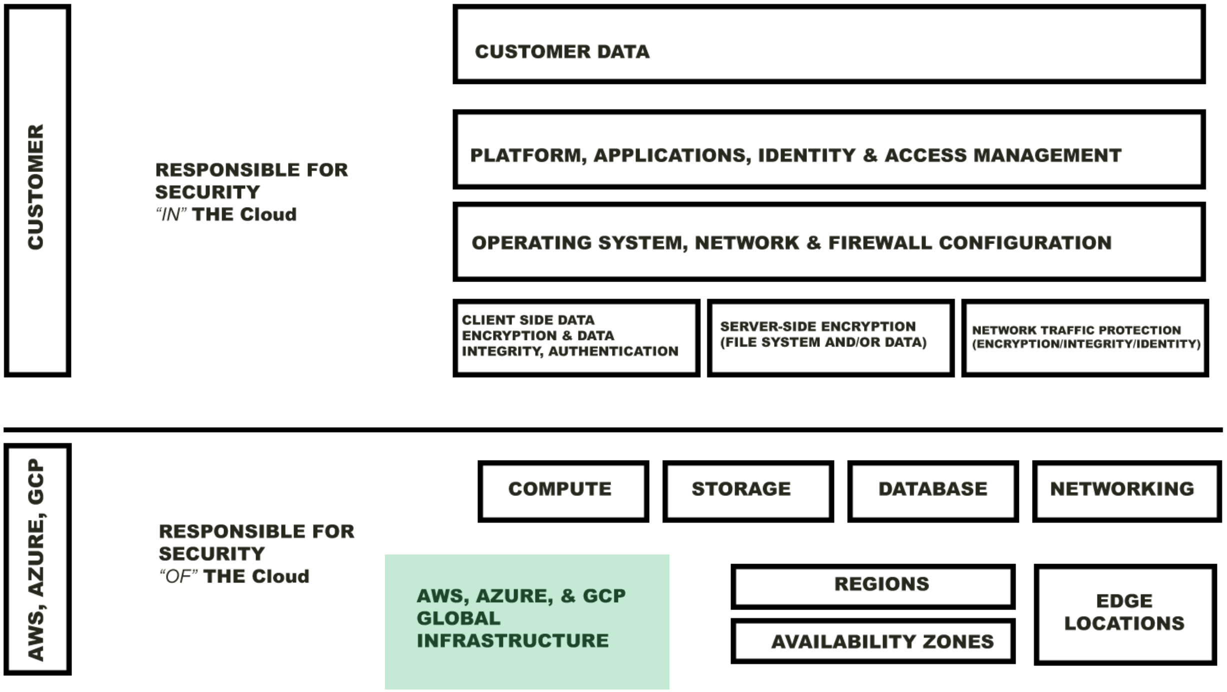
If you store customer information in the cloud, yes.

Maybe you're thinking:

> **"We use AWS, and AWS is SOC 2 Type 2 compliant. That should cover us."**

Cloud service providers like AWS will have a number of certifications, but they don't apply to your own applications or internal policies. AWS still requires users of their platform to implement security measures for secure use of their products.

Shared Responsibility Matrix


CUSTOMER
RESPONSIBLE FOR SECURITY "IN" THE Cloud
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT SIDE DATA ENCRYPTION & DATA INTEGRITY, AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORK TRAFFIC PROTECTION (ENCRYPTION/INTEGRITY/IDENTITY)
AWS, AZURE, GCP
RESPONSIBLE FOR SECURITY "OF" THE Cloud
COMPUTE
STORAGE
DATABASE
NETWORKING
AWS, AZURE, & GCP GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

"Shared Responsibility Model - Amazon Web Services (AWS)." Amazon Web Services, Inc., 2017, https://aws.amazon.com/compliance/shared-responsibility-model/.

4.3 Your Security and Backup. You are responsible for properly configuring and using the Service Offerings and otherwise taking appropriate action to secure, protect and backup your accounts and Your Content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Your Content from unauthorized access and routinely archiving Your Content.

Maybe you’re thinking:

**“We have great security.
I’m sure we’re
compliant already.”**

That’s a good start. However, **great security doesn’t equal compliance.**

Or maybe you’re thinking:

**“We’ve been fine without
SOC 2 so far. Why go through
the headache now?”**

You might have been able to slide under the radar during R&D mode. But the minute you try to sell to an enterprise, you’ll be exposed in the procurement cycle and stamped out of the deal. Better to win the customer… and spare yourself the pain of missed opportunity.

Section 5

When should I start a compliance program?

Here’s when *not* to start a compliance program: when you’re in the middle of a deal and realize you need it.

> *The best time to start is while you’re designing an application. Then, when it comes time for an inspection by an auditor, you’re all clear. We call this “compliance by design.”*

Being compliant by design means building security into your cloud environment during your development sprints. In most organizations, compliance action items are either pushed to the backlog and forgotten entirely or never factored into the workload at all. Compliance becomes an afterthought. Retrofitting an app to meet security standards is a much more complicated process than simply designing the product properly in the first place. As a bonus, when you bake compliance into your sprints, you’ll be able to keep up with the regular two-week delivery cadence in perpetuity — no returning for backfilled security tasks.

Section 6

What does a compliance program involve?

At the baseline, a SOC 2 report will audit your startup against two essential factors:

1. Whether the policies, procedures and controls you have in place meet the minimum security requirements.
2. Whether your policies, procedures and controls effectively meet your system requirements and service commitments.

Policies, procedures, controls... clearly these are key terms. So what's the difference?

- **Policies** are high level statements around what security you have in place. An example might be a firewall or network configuration: systems that demonstrate how you've established and adhered to compliance standards.

- **Procedures** are the ways you maintain and implement your policies, which are written into your policy statements. Maybe you have an onboarding procedure that states you'll perform a background check on every new hire.

- **Controls** are the execution of those procedures. It means you actually perform that background check and collect evidence to prove to the auditor that you've done so.

Within the report, you'll also be audited against how you meet certain criteria. The AICPA dictates companies participating in SOC 2 compliance must select a focus for the audit. It groups security policies and procedures into five principles called "Trust Service Criteria."

1. **Security** is considered "common criteria," meaning it must be included in the report. Security refers to the protection of the system against unauthorized access such as breaches, software misuse or data thefts.

2. **Confidentiality** refers to the protection of customer information in regards to how it's used by your services. For example, this principle might examine if you're meeting your agreements around Personally Identifiable Information or Protected Health Information.

3. **Availability** refers to whether customers are able to access your system as agreed or expected, which often applies to SaaS, PaaS, and IaaS services.

4. **Processing Integrity** refers to providing services in a timely, accurate and authorized manner. This mainly applies to services highly transactional in nature, such as finance or e-commerce.

5. **Privacy** refers to how customer data is collected, used or retained. The privacy principle looks to see if you're handling this data per privacy policies and legal regulations.

How do I know which principles to include in my report?

Most enterprises accept reports focused on Security, the Common Criteria. However, if your service is highly transactional, for example, the Processing Integrity and Privacy principles might come up in sales conversations — enterprise clients will want to ensure vendors have taken the right steps to protect customer data.

Section 7

How do I achieve SOC 2 compliance?

Take a deep breath. No one has called this a “fun process.” Ready? Okay.

January

Most of the time, the decision to begin the process comes from the sales or leadership team (for ease, let’s say it’s the CTO). They just heard from a potential customer that you need SOC 2 Type 1 before you can move forward in the sales process.

The first thing they do is a Google search to look for an auditor. They start researching options.

February-April

The CTO learns that the firm performing the actual audit must be an independent CPA firm and can’t help the company with implementing policies, procedures and controls. They can’t audit their own work, so they can only provide limited additional services to help you get ready. You'll need a second vendor if you do not have in-house expertise and staffing.

The second vendor can provide audit "readiness" that is comprised of three steps: discovery, gap assessment, and remediation. First, they assess, or discover, your current security posture as it relates to the SOC 2 Type 1 requirements. They identify what needs to be in place versus what *you currently* have in place. That's the gap assessment. Then they do remediation to fill the gaps and help you build policies, procedures and controls that will pass the audit. While your auditor can help you with some of the discovery and gap assessment steps, they are barred from helping with remediation.

May-October

Now it's time for the onsite audit. The audit firm comes in and asks to review the collected evidence and have meetings with your engineering staff. You may have to re-collect items you already gathered during the readiness phase. The engineering team is tasked with uploading 300-400 pages worth of evidence to the audit firm's evidence portal. While the audit firm is onsite, they make you walk through every single one of your controls to ensure there aren't any gaps. Onsite audits usually take between one and three weeks, but can go even longer depending on the size of the audit.

Once they've gone through all the evidence and you've fixed any gaps they've identified, then they offer you your report. The report takes the firm a full month or two to create.

You've finally reached the finish line. It's taken the best part of a year to get SOC 2 Type 1. You might think you can do it faster than other startups. Fair enough — but it's not you doing this work, it's the consultants with your in-house people working on it with them. Even shaving a month or two off will still delay deals for six months.

Section 8

How much time and resource should I commit?

If you barely made it through reading that last section, you can imagine how bad the real process is.

Maybe you think we're being dramatic. Here's a breakdown of average time and resource expenses so you can see exactly what you're in for.

Economic Comparison

Area	Manual Traditional Compliance	Automated Shujinko Compliance	Savings
Staffing (FTE hours)	10 FTE months	2 FTE months	8 FTE months
Productivity Cost	$160K	$32K	$128K
Readiness Consult Fees	$10K-$50K	$0	$10K-$50K
Total Audit Prep Time	6-8 months	2-3 months	3-6 months
Audit Report Fees *	$20K-$50K	$20K-$50K	

*** Independent auditor fees required; vary by firm**

> *Of all the manual compliance fees, the hidden costs to productivity should be your biggest concern.*

The manual compliance process always falls on the laps of the engineering team — the same people on the hook to develop products. They come to work excited to build new capabilities and infrastructure, not to capture, document, and upload evidence. The worst part is, since devs have to re-do evidence collection every year, they can't help but feel like they're being asked to reinvent the wheel. The Herculean manual compliance process isn't just devastating to app development timelines, it's also a blow to morale and employee retention.

Section 9

What do startups get wrong about SOC 2 compliance?

These are the most common mistakes startups make around cloud compliance (but not your startup, right?)

Mistake #1: thinking SOC 2 will be a breeze.

Lots of startups see compliance as an easy best practice checklist. They overcommit to customers, investors and boards of directors that they can slam out a SOC 2 audit in a few weeks with the resources they have on hand. Then, once they get into it and realize how arduous the process is, they have to manage back everyone's expectations.

Mistake #2: architecting cloud environments incorrectly.

Technical controls actually impact your cloud environment, and if you've arranged your design just to get through the audit, you'll find yourself spending months changing that architecture afterward.

Mistake #3: failing to delegate gap assessment to-do lists.

The gap assessment does exactly what it sounds like it should: it finds what necessary technical capabilities and organizational processes you're missing. Once these are identified, it's on your team to implement the solutions. That's where the disconnect happens. Teams rarely assign out a defined task list. This simple misstep keeps them up till the 11th hour trying to implement grueling technical controls, like web application firewalls or anti-malware.

Mistake #4: budgeting too conservatively, both in time and finances.

Most startups are shocked when they find out how much auditing and remediation costs. From a staffing perspective, the pain of surrendering two engineers to a nearly year-long manual compliance process will be felt at every turn.

Mistake #5: underestimating CTO and leadership time required.

Not all SOC 2 tasks and responsibilities can be delegated to engineers and other staff. Some requirements, such as risk assessments and employee training, require startup leadership time that is already spread thin between many competing priorities.

Mistake #6: trying to fast-track manual compliance to meet a tight deadline.

You can lose half a million dollars attempting to finish the process in less than six months.

Mistake #7: treating SOC 2 as a “nice to have.”

Compliance is a need to have — it’s an essential capability. Take it on the chin as a cost of being a B2B company building software.

Section 10

What do I have to gain from compliance?

Getting a SOC 2 report isn't all doom and gloom. There's a lot of light at the end of the process. Here's what you have to look forward to:

Benefit #1: reduced risk to customers.

Consider yourself a custodian of customer data. It's your job to protect that data by following security best practices.

Benefit #2: accelerate your engineering team.

Treating compliance as an afterthought saddles engineers with backfill security tasks, which stalls their velocity. Building those capabilities during a sprint enables dev teams to maintain their regular delivery cadence. Compliance by design ultimately lands you the speed-to-market advantage.

Benefit #3: winning the enterprise sales upper hand.

Customer data, including sensitive personal data, is already the lifeblood of many companies. With cloud computing becoming increasingly important and datasets growing bigger and bigger, security standards will only become more rigid. If the enterprises you pitch don't yet have a compliance gate in their procurement process, expect them to very soon — and expect that gate to get narrower. Compliance enables you to sail past a barrier impeding your competitors.

Conclusion: How do I make the auditing process easier?

Throughout this guide we've talked about "automated compliance" as an alternative to the manual compliance process. This antiquated method of preparing for and passing an audit is clearly time-consuming, inefficient and costly. And frankly, engineers hate it.

> *Automated compliance is the go-to option for startups that need to achieve and maintain SOC 2 compliance in order to sell to enterprise customers.*

The writers of this guide are engineers who speak audit. We built Shujinko, a SaaS platform that automates infrastructure compliance and audit preparation so that startups can become compliant in a faster, easier way.

Shujinko is automating SOC 2 cloud compliance, reducing the time and cost by 3x. We've simplified the process by:

- Provisioning compliance-ready cloud templates that support thousands of configurations
- Automating deployment of a compliant environment from container to cloud in under 15 minutes
- Generating smart 'to-do' lists and gap assessments that roadmap and remediate gaps to audit readiness
- Mapping uploaded evidence to satisfy all related tasks
- Finding, uploading and organizing evidence automatically on an ongoing basis (future capability)

Want to free up your engineering teams and ensure your audit is done right and done fast?

Let's Get In Touch