scytale

SOC 2 FOR STARTUPS

If you are up against SOC 2 then this is for you

Contents

INTRODUCTION

SOC 2 (Service Organization Controls 2) is a set of compliance requirements designed for technology-based companies that use cloud-based storage of customer data. However, SOC 2 is not just another compliance obligation. SOC 2 is a voluntary standard that provides an extremely effective way to meet the highest standards of information security and gain a critical competitive advantage.

For startups that want to grow their business, enter new markets, or simply enhance data security, choosing to become SOC 2 compliant can be one of the best business decisions you can make. But becoming SOC 2 compliant can be highly complex. Getting it right depends on careful planning and the strategic use of technology.

We've developed this guide to help startups make more informed SOC 2 decisions and drive sustainable growth.

01

The importance of a SOC 2 report for tech startups

Why is SOC 2 so valuable for tech startups? Here's the short answer:

SOC 2 is one of the best ways to stand out in the crowd and demonstrate that you meet the highest standards of information security. Clients know they can trust your InfoSec processes. And a SOC 2 attestation report ensures you meet even the most exacting procurement policies.

For most ambitious entrepreneurs, that answer is all you need to know. Tech startups don't yet have a proven track record. They need independent verification that their data security controls are up to the task. They have to be able to effectively demonstrate their processes are reliable and secure. Without SOC 2, SaaS startups have very little chance of driving business at scale and breaking into new markets.

Many prospects will not turn into customers without a SOC 2 report. According to the ACA Key Trends and Forces Shaping Risk and Compliance Management in 2021;

44%

of organizations say they are being asked for proof of cybersecurity as part of a request for proposal

Becoming SOC 2 is an effective and comprehensive solution to these problems that gives startups a real competitive advantage.

But there's a deeper reason why implementing SOC 2 at the early stages of a company's life cycle is so invaluable. It relates to the profound transformation that implementing SOC 2 has on a business. That's because SOC 2 Type II isn't simply a snapshot of your current security systems. Complying with SOC 2 Type II is an extensive process that involves developing robust data security, availability and confidentiality controls and in the case of SOC 2 Type II, proving that they operate effectively. For startups, that means building an extremely strong data security foundation which will ensure that, as the business grows, it continues to overcome even the most exacting security challenges.

Of course, it is precisely because SOC 2 is so rigorous that it can be so daunting to implement. Without the right technology and support, SOC 2 can quickly become overwhelmingly complex and time-consuming.

The purpose of this guide is to explain why SOC 2 is important and precisely how it helps startups achieve success in competitive markets. No less importantly, we will outline how to make SOC 2 compliance simpler, easier, and more effective and to outline strategies that enable any business, especially SaaS startups, to achieve SOC 2 success

How SOC 2 makes startups more competitive

As an independent standard, SOC 2 is an objective, detailed report of the controls your company has successfully implemented to ensure your clients' data security. As compliance is verified by an independent auditor, clients don't have to simply take your commitment to information security on trust. But it's more than a question of trust. The SOC 2 audit report is a detailed overview of the controls that you have designed and whether they are operating effectively.

That means potential clients can get a comprehensive overview of your trust service principles you chose, including security, availability, confidentiality, processing integrity and/or privacy. For prospects with very rigorous security procurement requirements, a detailed SOC 2 compliance report may make all the difference. 2022 Statista research on global startups show that:

61%

of startups worldwide offer B2B solutions. It is crucial for these startups to demonstrate their high-level security systems from the start

Furthermore, as of 2022, The United States is the leading country by the number of startups (71,153). SOC 2 compliance is most recognised within the US market and therefore, this statistic highlights how the compliance framework can provide a competitive edge among technology-based startups.

Building a foundation for long term success

We've discussed the value of an independent compliance security standard from a client perspective. But SOC 2 also provides a powerful guiding light for your own business. SOC 2's robust, exhaustively researched and fine-tuned protocols take the guesswork out of developing your own security controls. By setting the gold standard to which you can aspire, SOC 2 ensures there are no oversights in your security protocols and that your controls really are effective. In other words, SOC 2 takes the guesswork out of security. Plus, your audit partner or SOC 2 consultant will help you develop relevant, effective controls and verify that you have implemented them successfully.

In other words, SOC 2 provides an excellent framework for data security while independent auditing can identify any lapses or shortcomings in your compliance. The result: your company develops truly robust, comprehensive data security systems and best security practices throughout the organization.

And that's not just good marketing. For SaaS companies and for startups that are still building their reputations for excellence, even a single data security breach could destroy your reputation. And if you lose sensitive information, such as medical or personal financial data, you could even be liable for penalties.

Implementing SOC 2 is therefore about more than simply demonstrating that you meet the highest standards of information and organizational security. It's an effective way to ensure you develop resilient controls, without any gaps, that will serve your business over the long term.

02

What's involved in becoming SOC 2 compliant

SOC 2 is flexible, and compliance can be optimized to suit the needs of a wide range of startups. That's a great feature: SOC 2 is adaptable, unlike some more rigid standards. However, that flexibility also means that you need to make some careful decisions. Implementing SOC 2 is not a one-size-fits-all process.

Introducing the 5 Trust Service Principles

One of the first steps in starting the SOC 2 compliance process is choosing which of the five Trust Service Principles you are going to include in your report. The five principles were carefully devised by the AICPA and cover the full range of data security and reliability issues faced by SaaS companies. The Trust Services Principles are:

1. **Security**
2. **Availability**
3. **Processing Integrity**
4. **Confidentiality**
5. **Privacy**

Security is mandatory in any SOC 2 implementation. However, you do not have to implement all of the principles. A business should only include principles that are relevant to its operations.

From readiness assessment to attestation

Identifying the scope of your implementation is just the first step in your SOC 2 journey. Once you have decided which Trust Service Principles you wish to benchmark your systems against, it's time to identify any gaps between your objective and your current systems.

To do this, you start by conducting a Readiness Assessment. This is the process of identifying any shortcomings and then taking the appropriate measures to address them.

The Readiness Assessment comprises two parts:

1

Gap Analysis

The Gap Analysis is a careful evaluation of your current controls and systems. You identify any loopholes between the state of your current controls and how they should be operating, within your chosen scope of the SOC 2 framework.

Again, we can see the value of a gold standard benchmark like SOC 2. You can evaluate your current systems against the controls prescribed by a proven independent standard, and evaluate where you fall short. This is a critical part of developing comprehensive controls, without any gaps.

2

Remediation Period

Once you've identified any gaps in your controls, you need to set to work addressing those shortcomings. To do so, you need to design any missing controls that address shortcomings and complete all action items necessary to remediate any other gaps identified. A good SOC 2 partner will work closely with you to ensure all security gaps and issues are addressed successfully.

A SOC 2 partner, beyond advisory

Startups understand the value of partnering with domain specialists. After all, building a new company from scratch is a learning process, and entrepreneurs are usually keen to learn from experts.

A professional SOC 2 advisory service can be invaluable when you choose to implement SOC 2. An advisory service will help you most effectively determine the scope of audit, advise you on best practices, and guide you towards a successful audit. A good advisory service will provide the knowledge and expertise you need and make sure you use your resources most effectively, so you don't waste time on unsuccessful implementations or devote resources to ineffective or unnecessary interventions.

A 2021 study published by Cloud Security Alliance reveals that a lack of knowledge is the primary cause of SOC 2 misconfigurations and non-compliance issues. Businesses should therefore strongly consider taking advantage of a trusted compliance partner to ensure they get full value from the SOC 2 readiness process, as well as guided each step of the way.

Choosing the right auditor: experience, credibility and reputation

When choosing an auditor to conduct your SOC 2 report, there are certain non-negotiables. Only an independent AICPA-affiliated auditor is permitted to conduct a SOC 2 audit.

But when you bear in mind that you are under no obligation to undergo a SOC 2 audit and that your goal is to get the most out of the process as possible, then it stands to reason that you want an auditor that will provide a detailed, comprehensive report detailing your SOC 2 achievements.

For that reason, it's critical to select an auditor with extensive SOC 2 audit experience and detailed working knowledge of your industry. **SOC 2 should never be a mere box-ticking exercise, and the last thing you want is a generic audit report.**

The auditor's reputation also plays a major role - if you plan to sell to corporations you may want them to know and trust the CPA firm that performed the audit. BIG4 firms are well known globally and their standards are high so clients can trust them. On the contrary, engaging with well known CPA firms may come with a pricing proposal, so startups with limited budgets may choose with a smaller CPA firm.

It is important to take under consideration what your customers' requirements and expectations are.

03

Is SOC 2 compliance affordable?

Implementing SOC 2 is a detailed process that involves a considerable investment of time and money. For startups, in particular, implementing SOC 2 is likely to involve a large proportion of the workforce.

However, working out the affordability of the SOC 2 process is no simple matter. There's the opportunity cost of having key members of your team involved with the compliance process rather than their core roles. Fortunately, this can often be effectively managed with the appropriate compliance automation technology. We will discuss automation in more detail in the next section.

At the same time, you need to also account for the opportunity cost of not implementing SOC 2. In other words, your initial outlay should be balanced against the gains in securing new clients and successfully entering new markets.

In fact, according to a 2011 study by the Ponemon Institute and Globalscape, non-compliance costs increased by a sobering

45%

in 6 years

following that study, and these costs are expected to be even higher in 2021 and beyond.

Additionally, in a 2022 study performed by Statista,

over

50%

of respondents agreed that the most critical cybersecurity area is privacy.

The risk of security breaches is a great worry. They could ultimately be catastrophically expensive, as well as lead to reputational damage and lost trust amongst customers and prospects.

The type of SOC 2 audit you undergo will also determine the cost of compliance. SOC 2 Type I is considerably less expensive. However, SOC 2 Type II is universally recognized as a much higher standard of data security.

The type of SOC 2 audit you undergo will also determine the cost of compliance. SOC 2 Type I is considerably less expensive. However, **SOC 2 Type II is universally recognized as a much higher standard of data security.**

Calculating time-savings

The table below compares the number of hours spent on SOC 2 compliance, the manual,administrative way versus the automated way. It outlines the time-savings for SMBs per year by utilizing automation to achieve SOC 2 compliance:

	MANUAL COMPLAINTS	WITH AUTOMATION
Employees hours	200-250 hours	20-50 hours
Policies and procedures	50-100 hours	5-10 hours
Audit management	25-45 hours	8-16 hours
System description	20-40 hours	4-8 hours
Evidence collection	50-150 hours	10-20 hours
Readiness period	3-12 months	2 - 12 weeks

04

Opportunity cost and automation

Compliance automation makes compliance smarter, faster and greatly reduces human error. It also saves money. An integrated compliance system means you can reduce your investments on additional technologies. With built-in information security modules such as risk assessment and security awareness training, automated evidence collection and solid audit management - you can trust on a smart one single source of truth to manage your SOC 2 workloads. But let's not just think in terms of efficiency gains, but the opportunity costs of employees spending massive amounts of time managing SOC 2.

Many startups choose to implement SOC 2 early in their growth cycle, to build a robust security foundation for the business. As SOC 2 helps you break into competitive markets, compliance is also important for startups looking to accelerate growth and scale faster.

However, in the early phases of development, the team is often building and fine-tuning their products. Diverting the majority of the team's resources to managing extremely time-consuming manual compliance processes effectively means that the startup's productivity is put on pause. For many startups, this may simply be an unjustifiable use of resources.

When we consider the practical everyday realities of startups, we can appreciate that, in many cases, compliance automation is a game-changer. Without automation, most startups simply do not have the capacity to implement SOC 2. Compliance automation does more than save you time, it enables your team to stay laser-focused on product development, hiring and sales with minimal distraction or investment of time.

In the MetricStream State of Compliance Survey Report 2021,

44%

of organizations say their top compliance management challenges are handling compliance assessments, undergoing control testing, and implementing policy and process updates.

However, with compliance automation, these tasks become very easy to manage and organizations are able to achieve compliance much faster.

05

Automation + Advisory: The best of both worlds

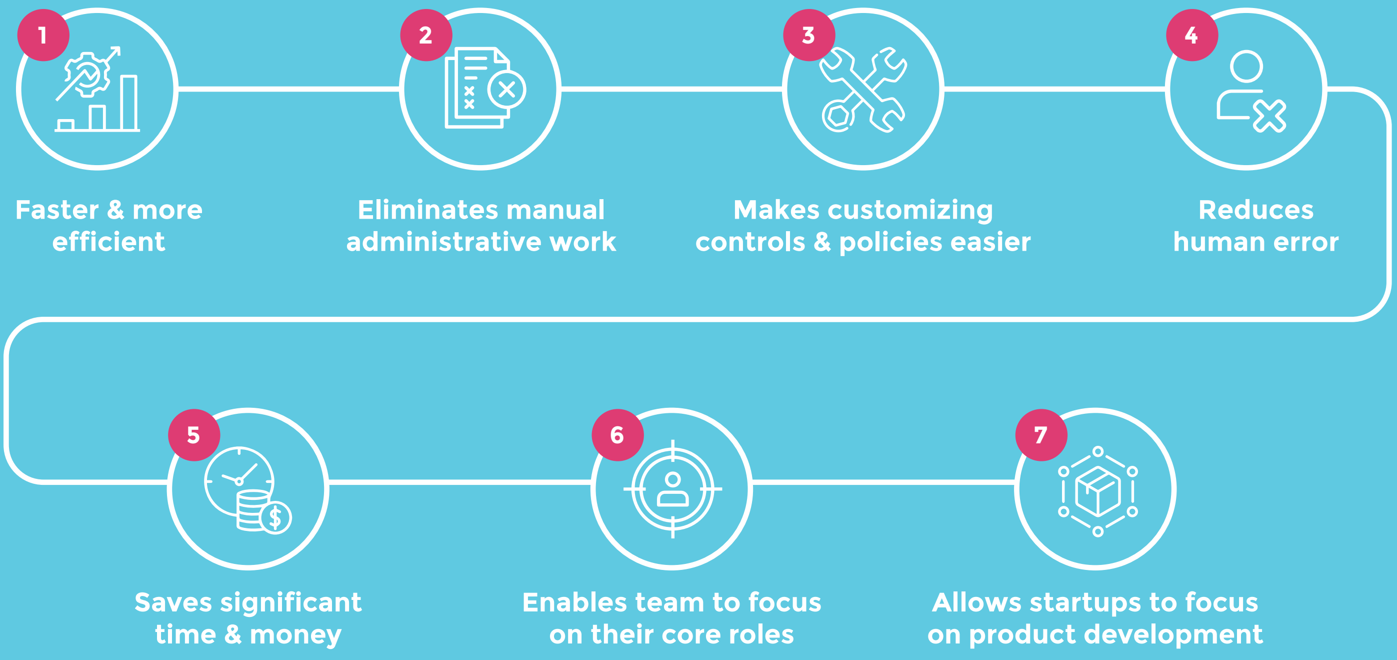
Startups are in a unique position. You are developing the practices and systems that will define the business as it grows. Equally, however, startups lack the resources of established firms and don't usually have recourse to an in-house security team. How do you navigate the unknown complexities of SOC 2 compliance, while still running a streamlined compliance process?

In these cases, the invaluable input of an advisory team, supported by specialized compliance automation technology, is a powerful combination that is more than the sum of its parts.

A good advisory service will guide both to make the process as efficient as possible and ensure you get the most value out of the SOC 2 process. Your SOC 2 partner should also work with you to ensure you are fully trained in your compliance platform, get the most out of the technology and that everything is customized for you - to work as your work and smartly support your business objectives.

At the same time, the technology helps ensure that you are able to execute the advice of your advisory team efficiently and effectively. In other words, automation enables you to get the most out of your advisory partner; and a good advisory team will guide you each step to make sure your SOC 2 automation delivers maximum results.

The benefits of guided automation:



1. Faster & more efficient
2. Eliminates manual administrative work
3. Makes customizing controls & policies easier
4. Reduces human error
5. Saves significant time & money
6. Enables team to focus on their core roles
7. Allows startups to focus on product development

Additionally, in the **ACA Key Trends and Forces Shaping Risk and Compliance Management in 2022,** firms identified

the top 5 risk and compliance functions that can benefit from technology as the following:

1

54% Vendor oversight

2

41% Marketing reviews

3

41% Compliance policy/ activity tracking

4

32% Trade surveillance

5

24% Regulatory reporting

06

Avoiding SOC 2 pitfalls

It may be your first time implementing SOC 2 but you can learn from the experience of others. Of course, there is no substitute for an expert guide who will ensure you follow best practices and will tailor a SOC 2 program to meet your startup's specific needs.

However, there are also a number of common pitfalls that many businesses make, especially if they try to cut corners. As experts who have identified common implementation errors that all startups should avoid.

A lack of SOC 2 leadership

SOC 2 is a complex process that involves a large number of personnel and organizational structures. Indeed, implementing SOC 2 in a startup may involve input from everyone in the business. Strong leadership is critical, as you need someone to coordinate compliance across the organization and liaise with all partners and stakeholders.

Ideally, SOC 2 leadership should be formalized, with an employee specified as project manager.

In addition, senior leadership needs to be involved in the process, assigning authorization for all necessary interventions and ensuring clear lines of communications are established between teams.

Underestimating the readiness assessment

Failing to effectively assess whether the startup is ready for audit is the surest way to experience a negative report. The readiness assessment isn't simply a useful diagnostic. It's a critical part of the SOC 2 implementation process. By performing a smart gap analysis you can detect vulnerabilities and ensure you allocate the appropriate resources to remediate them in less time.

Thinking SOC 2 is a one-off achievement

SOC 2 audits need to be renewed once a year since the audit period will cover 3-5 months (first report) to 12 months following the first report issuance. You can't simply implement SOC 2 once and then rest on your laurels. To gain an ongoing competitive benefit, it's important that your SOC 2 audit is up to date.

More fundamentally, becoming SOC 2 compliant is all about ensuring your business maintains impeccable compliance security standards. That's not a one-off box-ticking exercise, but an ongoing process. The right automation tool will offer continuous audit and 24/7 controls monitoring, ensuring your compliance is in force all year round. If there are any non-compliance issues, you allerted instantly.

Trying to figure it all out on your own

Implementing SOC 2 for the first time is a complex undertaking, full of unknowns. As startups often lack a dedicated compliance team, they face plenty of guesswork with relatively limited resources. This is where choosing the right SOC 2 partner makes all the difference. The best SOC 2 partner won't just advise you on best practices and guide you through all the complexities - they can also customize the compliance process specifically designed to meet your business's operations and goals, making the process smooth and efficient.

Doing it manually

Startups are all about being lean and working faster since time is critical. However, manual SOC 2 compliance is often slow, inefficient, and extremely resource-intensive. For that reason, startups, in particular, should prioritize SOC 2 automation that makes compliance fast and efficient, guarantee successful results and customers trust.

According to research performed by Cybint,

95%

of cybersecurity breaches are caused by human error, meaning they were likely preventable

07

A SOC 2 solution for startups

As we've discussed in some detail, startups have a unique set of SOC 2 requirements. They need flexible, cost-effective, and efficient solutions that help them stand out in highly competitive markets.

However, it would also be a mistake to focus too narrowly on a startup's short-term objectives. Ideally, startups need a fully scalable solution that both builds a foundation for successful growth and meets the challenges of the business as it expands.

Scytale has developed powerful security compliance technology that supports SaaS companies for rapid scale. Scytale difference is about ensuring all customers get the training, hands-held support, and expert advisory they need to get the most out of SOC 2 automation - now and as they grow.

After all, Scytale doesn't just want to help customers grow, Scytale wants to ensure they grow sustainably and effectively. **And that means that their security controls are always robust, resilient, and designed to meet the business's strategic goals.**

So while Scytale is able to offer unmatched technology and support to clients ranging from small startups to multinationals, we also appreciate that each business is a dynamic entity that needs flexible, innovative security compliance solutions. That's the Scytale difference.

08

SOC 2 Dos & Don’ts: A checklist for startups

With automation, good advice, and careful planning, any business can get SOC 2 right the first time, as efficiently and affordably as possible.

For startups, with limited resources and tight timelines, getting it right the first time is especially important. Here’s are some of the key Dos and Don’ts to consider when implementing SOC 2 in your business:

.

Don’t:

Dont try to rush the process. In our experience, haste truly does make waste. By contrast, carefully planning is the key to immediate success and long-term growth.

Dont waste your team’s valuable time with manual processes. Automation means a more productive workforce and more efficient SOC 2 implementation.

Dont try to do it alone. Getting expert SOC 2 advice is one of the most effective ways for startups to manage a complex undertaking like SOC 2.

Dont simply treat SOC 2 as a box-ticking exercise. SOC 2 is an opportunity to bulletproof your security and become more competitive as a SaaS provider and boost sales. For startups, it’s an excellent opportunity to refine your security controls and ensure you are not overlooking important compliance issues.

Do:

Strategically identify Trust Service Principles that are relevant for your business. SOC 2 is a flexible framework, and you should adapt it to suit your goals

Gap Analysis. Invest time to customize everything to work for you, build organizational knowledge around required processes and procedures that don’t build on a single individual, reduce human errors and unclarity.

Appoint a senior project lead. There are a lot of moving parts, and you need to ensure there is precise coordination between stakeholders and partners to streamline the process smoothly.

Get the right partners. Choosing the right auditor, automation and advisory provider could mean the difference between a frustrating SOC 2 experience and a rewarding process that delivers ongoing value.

Automate wherever possible. Startups don’t have the time, resources, or manpower to waste time on costly, painstaking manual compliance processes. Why waste time and money when you can automate?

Manage properly. Working with multiple versions of word and excel docs, emails, and dozens of shared folders will create mess, confusion and delay. Trust on a single source of truth to centralize all work into one place.

09

Internal survey conducted among our customers

The following outlines data collected during the onboarding process of new customers, the majority of whom are SaaS startups:

1

33.7%

have their CTO lead the SOC 2 project

2

68.2%

urgently need a SOC 2 Type II report

3

67.7%

are between 1-50 employees in size

4

68.9%

do not have policies and procedures properly implemented

5

78.6%

do not have any internal security controls

6

52.6%

do not conduct internal InfoSec procedures

Key takeaways from the survey:

1

Startups are in need of SOC 2 automation and expert guidance in order for key employees to continue with day-to-day responsibilities.

2

Startups and SOC 2 first-timers need a partner to help them build core information security best practices and ensure oversight across the company.

3

Compliance becomes increasingly more relevant and crucial for small companies.

CONCLUSION

SOC 2 for startups is achievable when you know how

It would be an overstatement to say that implementing SOC 2 is easy. But with the right technology and guidance, it's much more achievable than many business operators realize. This eBook was designed to show how startups can implement robust security protocols and set themselves up for long-term business success when they have access to SOC 2 automation and expert guidance.

Automation means you can develop robust security controls right at the start of your business journey, without losing focus on your core product. For SaaS startups, that's the ultimate recipe for long-term success.