scytale

ISO 27001 FOR STARTUPS

The Ultimate Handbook for SaaS Companies

Contents

INTRODUCTION

When it comes to running a successful startup, it can often feel as if the recipe for success is constantly changing. After all, building a startup is often a learning process in itself, as each business faces unique challenges and hurdles. In fact, no two startups have the same experience with funding, product development, client acquisition, or other critical aspects of launching a business.

So then, amidst the uncertainty and unpredictability of it all, how can startups ensure they have a strong foothold in the marketplace? More importantly, how can startups rest assured that they're staying competitive in a tech-driven landscape, without compromising their data security? We'll keep it short: ISO 27001.

This eBook covers everything you need to know about the most demanded security compliance certification and how to best achieve the security standard with limited resources.

01

Laying the foundation: ISO 27001 for first-timers

Whether you're a compliance guru or a newbie to the world of information security, navigating ISO 27001 can quickly level the playing field. Fortunately, we're here to help you dive into the basics and the nitty-gritty of ISO 27001 and everything you need to leverage it to supercharge your startup and ensure that it fuels your growth trajectory, security, and risk management while meeting growing customer compliance demands.

Unsure if you need to be ISO 27001 certified?

Take a look here for all your answers

What is an ISO 27001 certification?

Let's get the tech jargon out of the way. ISO 27001 is formally known as ISO/IEC 27001:2022 and is an information security standard created by the International Organization for Standardization (ISO). It provides businesses with a framework and guidelines to establish, implement and manage an **information security management system (ISMS).**

Wow, that's a lot. Are you still with us? Let's break it down into human talk.

Your business deals with a whole lot of data. Be it client-related, financial data, system-related, or unique to your core offering and processes. Information touches every aspect of what you do, some of it being sensitive information. ISO 27001 provides the quintessential guide to how businesses can protect themselves and their clients from internal and external threats to the sensitive information in question. This includes setting a standard for risk assessments, staff training, security controls, policies, and processes.

It does this by mapping out the ideal ISMS and providing guidelines, requirements, and controls for businesses to do the same. Once you've achieved this and you've passed your ISO 27001 audit process, a certifying body will give your business the much acclaimed ISO 27001 stamp of approval, and you will be ISO 27001 certified.

This brings us to our next question, why would businesses want to become ISO 27001 certified in the first place, especially if you're still in the startup stage? Let's take a look.

What are the business benefits of ISO 27001 for startups?

From a startup perspective, you may believe that your business can remain under the radar regarding security threats. This couldn't be further from the truth. In fact, almost half of all cyber breaches impact businesses with fewer than 1,000 employees. The only difference is that smaller businesses are generally less likely to survive a security breach or cyber attack.

However, we can't ignore the fact that despite the plethora of fear-striking stats, the small business founder frequently has other priorities and worries that keep him up at night, and often - compliance isn't high on that list. Therefore, despite the significant advantages that being ISO 27001 certified holds from a data privacy and information security compliance perspective, it's worth noting that there's much more to cybersecurity than meets the eye.

ISO 27001 acts as a baseline for regulatory requirements

More often than not, the choice is fairly simple - there is none. Depending on the type of information your business comes into contact with, you may be subject to regulatory compliance. For example, suppose your startup comes into contact with Protected Health Information (PHI), in that case, you may be subject to mandatory HIPAA compliance. Alternatively, you could be subject to other regulatory frameworks such as NIST CSF (Cybersecurity Framework) and the General Data Protection Regulation (GDPR) of the European Union.

Depending on the type of information, location, and industry, you may be subject to specific regulatory frameworks.

Being ISO 27001 certified meets the highest standard of information security to build customer trust by enforcing a security-conscious workforce and creating the ultimate baseline foundation for security policies, processes, and controls.

ISO 27001 sharpens your competitive advantage

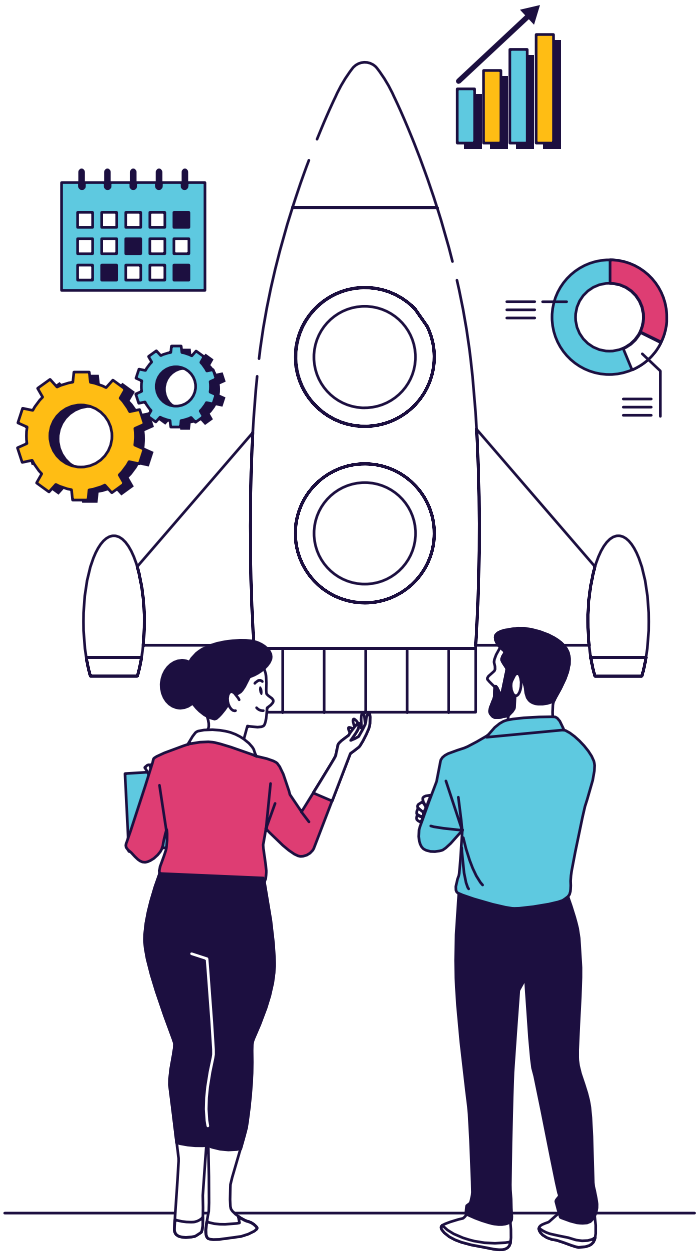
Regardless of the industry, information security is imperative when it comes to onboarding and retaining customers. Why? In a saturated market, choosing between companies often boils down to where clients feel their data and information is most secure. Customers are more inclined than ever to ask hard questions concerning whether they can trust a business with their critical information.

An ISO 27001 certification gives the transparency and trustworthiness they seek. Known as the "golden standard", and proves that your startup differentiates itself from some competitors by showing due diligence and giving you an upper hand over competitors who have implemented another framework or none at all. However, with the importance of infosec becoming non-negotiable, 99% of the time a security compliance framework is requested by prospects, so it becomes a must to have in order to sign deals and grow

Expand into new markets and close deals

Becoming ISO 27001 certified also allows startups to tap into new global markets and close deals without compromising information security or data privacy. In fact, in many cases, prospects request to see proof of due diligence concerning security standards before doing business with you, so it becomes a fundamental need to keep you from losing business opportunities, including enterprise deals. By starting out with the leading security standard, startups don't have to worry about playing compliance catch-up once an opportunity arises. Instead, they can confidently move into bigger projects and new markets, knowing they have strong security standards protecting their business and clients from threats.

With the benefits of becoming ISO 27001 compliant so evident, one would expect more companies (especially startups) to make it their first order of business. Yet, many small businesses struggle to get certified due to common challenges hindering the process.



02

Compliance challenges and solutions for startups

Naturally, things regarding the compliance landscape aren't always as clear or straightforward as expected. For startups, in particular, navigating security compliance for the first time can feel overwhelming.

Why? Well, to be frank, without the proper guidance, it's pretty darn tough - especially if you're still working hard to get your feet off the ground. But despite the challenges, prioritizing security compliance is one of the most fundamental steps in ensuring that your start-up can withstand the headwinds of scaling, cyber threats, and an evolving digital landscape.

To help curb some of the initial uphill battles of starting your journey towards your ISO 27001 certification, here are some of the most common challenges (and solutions, of course) to getting ISO 27001 certified.

CHALLENGE 1

A lack of expertise

Most startups don't hit the ground running with an inhouse CISO, security compliance manager or an ISO 27001 compliance guru, and that's perfectly normal. However, due to the complexity of ISO 27001 information security management requirements, it's also one of the most significant drawbacks and challenges for startups.

To overcome this, we recommend leveraging **experts** who have experience and knowledge around the specific audit requirements involved in getting ISO 27001 certified and provide excellent resources in order to gradually educate your team on best practices.

CHALLENGE 2

Third-party dependencies

As startups establish themselves, they often rely on third party service providers. However, without the proper third party risk management, this can quickly expose a startup to compliance risks they may have been unaware of.

As your startup is preparing for your ISO 27001 certification, be sure to keep in mind that the information security practices of any third parties will also fall within your scope of responsibility. To overcome and mitigate these risks, many startups opt-in for **automation tools** that include regular third-party risk assessments.

CHALLENGE 3

Budget and resource constraints

Overcoming budget and resource constraints is one of the most significant challenges for startups who want to get (and stay) ISO 27001 compliant. So, what's the solution if you only have so many hours in a day, a small team, and a (very) limited budget? Let's take a look.

We get it; throwing all your efforts into obtaining an ISO 27001 certification may seem like it could disrupt critical business processes, something that you just can't afford to do. Who says it has to? For startups, in particular, running the ISO 27001 process alongside other business objectives and day-to-day tasks with minimal disruption to your workflow while maintaining a consistent momentum towards achieving ISO 27001 within specific time requirements is critical.

Here are a few ways you can achieve ISO 27001 amidst budget, resource, and time constraints:

For starters, consider your resource implementation. Unfortunately, you can't just designate anyone with the capacity to manage and maintain your ISO 27001 compliance. Although start-up teams are comfortable juggling many responsibilities and wearing different hats, without the proper internal experience and expertise - you could potentially spend more time and resources than needed while simultaneously incapacitating your team. Be sure you have a few experts helping you obtain ISO 27001 (hint-hint).

Additionally, be sure to invest in security compliance training and resources to help equip your team with the tools to incorporate best practices throughout your organization daily.

But first, if ISO 27001 costs are still stressing you out and keeping you from diving into the process, we've got you covered with

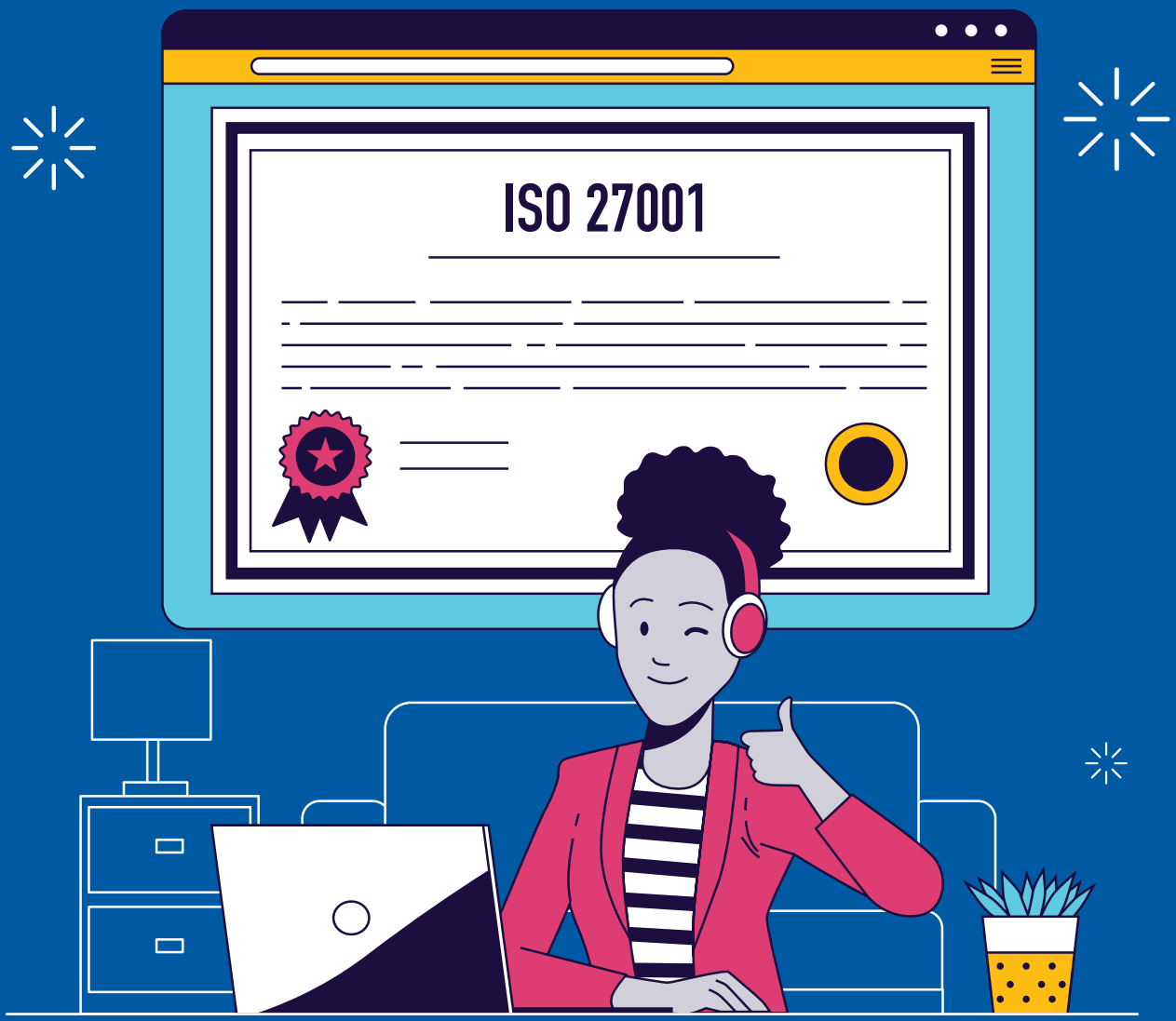
a breakdown of ISO 27001 certification costs for companies.

Now, let's get to the fun part (and yes, ISO 27001 can be fun, okay?)

03

How to get/stay ISO 27001 compliant

Regardless of the approach you take, achieving your ISO 27001 certification will involve multiple steps. It's also important to keep in mind that each startup's journey towards ISO 27001 will look different depending on how prepared they are and the existing state of their ISMS (if any). However, there are a few general guidelines that apply to most ISO 27001 certification processes.



STEP 1

Assess your ISMS

eed a quick refresher? Your ISMS is your Information Security Management System. It's the crux of ISO 27001. Naturally, the first step is to gauge your ISO 27001 readiness by **conducting an internal gap analysis** before an auditor joins the party. You can do this by conducting a gap analysis, a process that helps you test your startup's current posture against the ISO 27001 controls.

STEP 2

Develop (or fix) your ISMS

Now that you've pinpointed those gaps, you'll have a much clearer picture of what you need (and how to get it). Step two involves creating a solid ISMS - one that will pass an external audit. Developing your ISMS is probably the most critical step during the process and involves various substages to ensure nothing slips through the cracks. This includes determining your ISMS scope and **conducting a thorough risk assessment** to identify and prioritize the unique security risks that may apply, assessing vulnerabilities, and determining the potential impact of incidents.

STEP 3

Implement your ISO 27001 controls

The proof is in the pudding, right? And your controls are the sweet stuff. Now, it's time to put in place the security controls and measures that you defined in your ISMS documentation. However, this step goes far beyond simply implementing the correct access controls and processes.

Hold up. Let's take it back a notch. For beginners, security controls may feel like a whole new language. In fact, perhaps you're not even sure which controls apply to your startup. For a closer look into identifying controls for your ISMS, Annex A of the ISO 27001 provides clear guidelines.

During this stage, businesses are also required to create a Statement of Applicability that outlines which Annex A controls are applicable to your organization and therefore, included in your scope.

A Statement of Applicability should:

- List the controls an organization has selected to mitigate risk
- Explain why these controls were chosen for your ISMS
- State whether the controls have been fully implemented
- Explain why any controls were excluded

STEP 4

Find an accredited auditor

In order to become ISO 27001 certified, a reputable certification body accredited for ISO 27001 certification must conduct your audits. Yes, there are multiple. Apart from your internal audit, your startup will ultimately have to undergo four external audits, so best make sure you're teamed up with the right auditor.

These four external audits include a ISMS design review, certification audit, surveillance audits and recertification audits. During the certification audit stage, you'll (finally) get certified! Your auditor will review your processes and controls and confirm whether they meet ISO 27001 requirements. The external auditor will assess if they've been implemented correctly. If approved, you're eligible for your full ISO 27001 certificate - congratulations!

STEP 5

Find the right support

For first-timers, taking on the ISO 27001 certification journey alone is a risky bet, and one that you don't have to take. For startups specifically, expert guidance can make or break your compliance. Therefore, it's best recommended to gauge experts that can help ease the burden and guide you through each and every step. Additionally, delegation is imperative. Be sure to appoint an inhouse project manager who will take the lead in getting ISO 27001 certified.

04

Staying ISO 27001 compliant - always

The number one mistake that many organizations make (from startup to enterprise) is to treat ISO 27001 compliance as if it's a one-time box to tick. In reality, getting compliant means incorporating certain methodologies into the DNA of your business. Ultimately, the point of putting in all the effort towards getting compliant is to create a security posture that becomes your greatest asset, not a liability. Therefore, in order to leverage the benefits of ISO 27001, you need to ensure that you not only get compliant, but you stay that way, especially through **continuous control monitoring.**

So, how can startups ensure that all their efforts aren't in vain?

Continuous monitoring and measurement

Most security breaches stay hidden and unidentified until it's too late. Invest in a continuous monitoring process that allows you to keep tabs on all controls and processes 24/7 to ensure nothing slips through the cracks.

Regular security awareness training

As you scale, it may be more challenging to maintain a security conscious culture within your team. Not only is awareness training a necessary ISO 27001 requirement, but regular and effective training programs are a surefire way to regulate internal risk and maintain consistent compliance.

Onboard experts

You don't have to be an information security compliance guru to stay compliant, but someone has to be. Leveraging the support and guidance from experts in the field is one of the most effective ways to stay compliant while incorporating leading infosec strategies and controls for your specific industry.

That sounds great, but really taxing. Is there another way to stay compliant as a scaling startup (with a lot going on)?

If you're thinking, "Wow, that doesn't sound like something we can take on by ourselves," you're probably right. Getting (and staying) compliant can be an all-consuming process. So then, how can leading startups balance it all while maintaining a bulletproof security posture? Can we let you in on a secret? Most of them don't. At least not without leveraging automated technology to uncomplicate and lessen the burden. Here's how.

05

Leveraging technology for ISO 27001 compliance

We don't need to remind you about the importance of time and resource management. So, in the spirit of saving it - we'll get to the point: Security compliance was not designed for the faint of heart and regular startup founders don't have the capacity to train themselves to become designated compliance experts. Fortunately, they don't have to.
Cue **ISO 27001 automation.**

To do business in a modern and digital landscape, you've got to be two things: compliant and fast. Unfortunately, relying on manual processes to get ISO 27001 certified generally encourages error-prone, highly-administrative and time consuming processes. Not only does this drag out the process of getting certified, but it usually disrupts employees' key responsibilities and delays company growth quite significantly.

Here's why most startups leverage the powers of compliance automation to supercharge their information security.

Free up your team so they can focus on their key roles and business growth.	**Remove the risk of human-error**	**Track all ISO 27001 workflows in a centralized place.**
Stay current with changing requirements in ISO 27001 landscape	**Stay compliant with continuous control monitoring (CCM)**	**Automate evidence collection and streamline the entire audit-readiness process.**

Automate ISO 27001 compliance with Scytale

What if reading this ebook is the most time-consuming thing you have to do within your entire ISO 27001 certification process? At Scytale, we help startups get (and stay) ISO 27001 certified up to 90% faster. Through our smart automation technology, we provide quick, simple and streamlined compliance while teaming you up with designated compliance experts to provide guidance and support every step of the way.

Automate the entire process, and gain expert partners in compliance in a few clicks without having to compromise your time or people.

Wait, I still have a few questions!

You're not alone. In fact, here are some of the most common FAQs concerning ISO 27001 compliance for startups.

1

Are there any alternatives to ISO 27001 for startups?

While ISO 27001 is considered the leading security standard, there are other frameworks or regulations that could apply to your business. A common alternative is SOC 2 compliance.

2

Is ISO 27001 certification recognized internationally?

It is, especially in Europe, making it an excellent choice for startups looking to expand globally.

3

How long does it take to get ISO 27001 certified?

This depends entirely on the approach you decide on and can vary depending on company size, risk landscape, and whether or not you decide to onboard third-party services or automation tools to help speed up the process.

Keen to see how Scytale can revolutionize your compliance management?

Experience Scytale here