

Thoropass™

A Founder's Guide:

**Deciphering the Right
Compliance Framework
for Your Startup**

Table of Contents

The Growth Strategy Most Founders Overlook

- Compliance Unblocks Sales 4
- Compliance and Security Give Your Startup a Competitive Advantage 5
- Compliance Protects Your Startup’s Finances and Reputation 5
- The Top-Line Cost of Ignoring Compliance..... 6

Choose the Right Compliance Framework for Your Startup

- What Is a Compliance Framework?..... 8
- What You Should Know About the Common Compliance Frameworks 8
- How to Choose the Right Compliance Framework(s) for Your Startup 14
- Find a Guide You Can Trust and Stick with Them..... 16

The Growth Strategy Most Founders Overlook

What many founders don't realize is just how important compliance is in growing a startup. By prioritizing compliance and security, you're positioning your startup to close the bigger deals you need to move upmarket. What's more, compliance is a powerful marketing message that helps startups stand out from the competition as well as an important safeguard against company-killing events.

Still unconvinced? Here's a closer look at how compliance helps startups grow.

Compliance Unblocks Sales

Chances are your startup will need to [move up-market to succeed](#). This means transitioning sales to close bigger deals with enterprise companies. Too often, though, startups hit a roadblock as they start sales conversations with this new breed of customer. A lack of data security and privacy leaves them woefully underprepared to meet enterprise needs.

Large companies want to work with innovative startups. Nike, Bayer, Microsoft, BMW, Pepsi, and Johnson & Johnson, for example, all invest in partnership, mentorship, or incubator programs for startups. [Adidas recently partnered with Carbon](#), a digital 3D-manufacturing startup, to create a new 3D-printing technique for its new product line, [Futurecraft 4D](#).

In 2015, Coca-Cola partnered with [Wonolo](#), an on-demand staffing platform, to find a solution for the corporation's staffing woes. The partnership cut Coca-Cola costs by 75% per outlet and boosted Wonolo's funding round by \$5.7 million, according to [StreetFight](#).

Startups tend to underestimate the preparation they need to do before engaging corporate clients. Enterprise buyers expect startups to meet the same procurement cycles and compliance requirements as other vendors.

For example, say your startup decides it's ready to [move beyond selling to SMB customers](#). As you initiate sales conversations with enterprise companies, a pattern emerges. The enterprise

loves your product and is keen to work with you, but they can't do business with you until you fill out their 100-question security assessment. And, in order to fill that out, you need to have a compliance program in place.

Founders in healthcare, finance, and other regulated industries tend to anticipate compliance challenges early on, as that's a clear barrier of entry to working within those fields. But if you're outside of regulated industries, it's easy to miss the need for compliance until it's too late.

This reactive approach to compliance not only blocks enterprise sales, it sends teams scrambling to find a solution. Unfortunately, compliance takes time. It's not something you can jump on last-minute, nor can you expect a promising enterprise customer to wait until you're finished. With proper planning and a compliance platform like Thoropass (formerly Laika) to guide you through the process, founders can complete an audit in three or four weeks. But on your own, pressured by standstill sales and unsure of how to proceed, the process can take [up to 18 months at the extreme](#).

Procurement cycles tend to be long at large companies—[7+ months](#), depending on product and industry. By investing in compliance before starting conversations with enterprise prospects you position your startup to meet enterprise expectations and empower your sales team to do what they do best. The faster you can get through security, the more you can focus on selling.



Partnerships are attractive to both parties because startups bring innovation, and corporations bring scale.

Ritam Ganhi
Founder and director of Studio Graphene and former consultant for Accenture and Bank of America Merrill Lynch.



Compliance and Security Give Your Startup a Competitive Advantage

Compliance isn't just a requirement for working with enterprise customers. It's a powerful marketing message and competitive differentiator.

You can use compliance as a selling point to help your startup stand out from the competition. By having a compliance program in place, you're telling prospects that not only do you have all of the innovative products/ services and the agility of your competitors, but you also ensure their data is handled in accordance with regulatory requirements.

Startups can further demonstrate their commitment by pursuing a stage-appropriate security program. This isn't just important for sales conversations with enterprise prospects. With data breaches and privacy concerns dominating headlines on a regular basis, consumers are generally more aware

of the need for strong security protocols and [expect a higher level of internal controls](#).

Quality security processes signal that your startup is more established, credible, and attuned to customer needs.

It isn't easy for consumers or businesses to evaluate how secure or private their vendors' practices are. A compliance attestation from third-party CPAs, however, makes it easy to build trust at a glance. Your prospects can go to your startup's website, see the AICPA-approved logos, and immediately know that your company is equipped to protect their information. Equipped with an auditor's report, you can use that information to tell a more compelling story about how third-party experts stand by your company's security practices.

Compliance Protects Your Startup's Finances and Reputation

And what happens if something goes wrong? Say, a middle- or upper-level manager makes a mistake and triggers a lawsuit or your company suffers a data breach, privacy violation, or business ethics scandal? These things aren't pleasant to think about, [but they happen](#), and they can kill your company.

The [Verizon Data Breach Investigations Report](#) analyzed 41,686 security-compromising events that occurred this year alone. 2,013 of those were [confirmed data breaches](#) where data was actually obtained by an unauthorized party and not just exposed. They also found that:


71% of breaches were financially motivated



29% of breaches involved use of stolen credentials




25% of breaches were motivated by the gain of strategic advantage (espionage)



56% of breaches took months or longer to discover



32% of breaches involved phishing



69% of breaches came from external attackers



Data from the [Verizon Data Breach Investigations Report](#)

In 2016, human resources startup, Zenefits, learned first-hand the perils of growing quickly without proper ethical and sustainable compliance standards in place. The promising startup drew \$1 million in revenue in its first year, and attracted interest from top venture capitalists, raising \$500 million at a \$4 billion valuation the year before its CEO stepped down amid scandal, according to [The New York Times](#). Accused of cheating state online broker license courses and other scandals, [Zenefits paid \\$11 million to the state and \\$450,000 to the SEC](#), and the company's focus on growth pivoted to survival.

The startup Timehop fell victim to a breach in 2018 when an [unknown attacker used a Timehop employee's credentials](#) to get access to over 21 million user records. The attack compromised users' names, email addresses, birth dates, and phone numbers.

Compliance protects your startup against devastating financial and reputation losses. It ensures your company is built on solid processes that remain strong and secure as your team grows, your product becomes more complex, and you take on bigger clients. Without it, you put yourself, your startup, and your customers at risk of losing it all.

The Top-Line Cost of Ignoring Compliance

Strong compliance and security provide obvious risk mitigation benefits. For example, a well-designed process for writing, testing, and shipping high-quality code reduces the likelihood of introducing errors that impact your startup's revenue. The benefits are so obvious, in fact, that early-stage teams often frame their commitment to compliance and security purely through a bottom-line calculus around risks. That's a mistake. **The biggest benefit of compliance comes from its impact on your top line, particularly on your ability to move up-market.**

Enterprise customers take on risks when deciding to work with startups, especially startups that don't appreciate the size and scope of security issues for larger companies. To mitigate some of that risk, they build in security reviews and contract negotiations that often last months

or longer. They hone in on compliance and security questions throughout the buying process. If you're unprepared, you stand the risk of having to agree to terms that aren't ideal for your startup or losing the opportunity entirely.

Corporate buyers know when founders misrepresent (deliberately or inadvertently) their security, processes, and earned certifications; they've seen it all before. Such interactions not only tarnish your brand's reputation, they cancel your chances of earning enterprise trust and expanding your top line. **Ignore compliance at your own risk.**

Choose the Right Compliance Framework for your Startup

You need to understand the compliance frameworks to select the right one for your customers and business. Choose right and you stand to close bigger deals and move upmarket. Make the wrong call and you risk holding up your compliance investment and overall company growth. The stakes are high.

The burden is on founders to understand the use cases and benefits of each compliance type to make an informed decision. Here's how you can cut through the vague and verbose legal speak to do just that.

It doesn't seem like compliance frameworks are meant to be understood by busy founders or even mere mortals. For example, take a look at this excerpt from an AICPA guide on SOC 2. Not exactly bedtime reading.

SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.

2.01

An understanding of the process for determining the risks that would prevent the service organization's controls from providing reasonable assurance the service organization's service commitments and system requirements were achieved, and for designing and implementing controls to address those risks, may assist the service auditor in identifying deficiencies in the design of controls. Some service organizations have a formal risk assessment process based on the applicable trust services criteria. In those circumstances, the service auditor may be able to inspect the risk assessment and controls documentation prepared by management to obtain an understanding of this process.

From SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.

What Is a Compliance Framework?

A compliance framework provides a set of guidelines that companies can adhere to when building their IT security controls.

If a company decides to pursue an audit, the auditor or regulator will test the company's processes and operations for security, stability, longevity, and compliance with laws and regulations based on the chosen framework.

Each Compliance Framework Is Different

Compliance frameworks focus on different considerations. PCI, for example, governs the handling of payment card data. HIPAA deals with the privacy of protected health information. COSO, the framework used for SOC 2 reports, looks at how well a company's internal controls meet a broad range of standards.

Some compliance frameworks define their standards more explicitly than others.

PCI, for example, is regarded as a compliance framework with a stricter set of rules. HIPAA and

CCPA are federal and state laws, respectively, while GDPR is a European Union law. SOC 2 and other frameworks, on the other hand, are more industry best practices than hard-and-fast rules, though they still indicate that a company takes security and privacy seriously.

Choosing the Right Compliance Framework Matters

Deciding which frameworks will best benefit your startup is one of the first decisions you'll make as you start to invest in compliance. This decision is important, as it determines the amount of time, money, and resources you'll spend.

The more compliance frameworks you use within your startup, the longer and more expensive the process. (Though there are ways to make multiple audits more efficient, which we talk about in a later section!)

What You Should Know About the Common Compliance Frameworks

There are five compliance frameworks founders should familiarize themselves with as they start moving toward compliance. These frameworks are the "bread and butter" of compliance for startups and cover the most common needs.

SOC 2 (COSO)

Chances are you will need a SOC 2 audit at some point in your startup's life, especially if your business does anything with data and software (which one doesn't?).



What does it test?

SOC 2 uses the COSO framework to test your internal controls against five Trust Services criteria: security, availability, confidentiality, privacy, and processing integrity.

Who needs it?

In many cases, enterprise buyers require their vendors to get SOC 2 compliance. This makes a SOC 2 audit particularly important for B2B startups that are starting to attract enterprise customers in order to grow upmarket (see: [The Growth Strategy Most Founders Overlook](#)).

Today, more startups than ever choose to pursue SOC 2 in order to satisfy enterprise customers' needs. In fact, Deloitte saw a 25% increase in SOC 2 engagements between 2017–2018 alone.

Who manages it?

The American Institute of Certified Public Accountants.

ISO 27001

This is another security-focused standard that enterprise buyers often require. It's internationally recognized, making it more important for startups that cater to customers outside of the U.S.



What does it test?

ISO 27001 tests how well you create, implement, maintain, and continue to improve on an information security management system that's appropriate for your company. It also sets standards for assessing and addressing information security risks.

Who needs it?

Startups looking to grow by working with enterprise customers, particularly those overseas.

Who manages it?

The International Organization for Standardization.

SOC 1

Does your startup impact your customers' financial statements? Your customers will likely require you to invest in SOC 1.



What does it test?

SOC 1 hones in on internal controls that impact customer financial reporting. While **SOC 2 evaluates security** based on five Trust Services criteria, SOC 1 tests your controls based on objectives you and your auditor agree to. These objectives depend on what your customers need for their own financial reporting.

Who needs it?

Typically, any public company or large non-public company will require their service providers to get SOC 1 if they impact their financial reporting, even indirectly.

For example, say your SaaS startup provides billing services to large companies. Chances are your customers will require you to become SOC 1 compliant as your billing impacts their payables, and their payables impact their financial statements.

Who manages it?

Like SOC 2, **SOC 1 is published by the AICPA.**

PCI DSS

If your startup deals with customer credit, debit, prepaid, or other payment cards in any way, you'll likely want to add PCI DSS to your arsenal of compliance. Thankfully, many payment and security vendors (e.g., [Stripe](#), [Very Good Security](#), etc.) can help startups meet strict PCI standards.



What does it test?

The PCI framework tests controls for companies that host cardholder data, receive card payments, or save cardholder information.

Who needs it?

PCI is for companies that handle payment cards like credit cards. It's often used by startups in the financial technology community that process payments or store/handle credit card information.

Who manages it?

The [PCI Security Standards Council](#).

HIPAA

Unlike the above frameworks, compliance with HIPAA is not a choice. HIPAA is a federal law, and if your startup handles [protected health information \(PHI\)](#) in any way, it must abide by HIPAA's regulatory rules. Fail to comply with HIPAA, and you could face criminal charges.



What does it regulate?

HIPAA is a federal law that defines how companies keep PHI private and secure. It defines how your company is allowed to manage and disclose PHI internally and externally. It also sets strict policies and controls for managing data security, risk assessments, and responding to incidents like data breaches.

Who needs it?

Expect to meet HIPAA regulations if your startup deals with patient data or information about consumers in the healthcare space.

Who enforces it?

The Office for Civil Rights within the U.S. Department of Health and Human Services.

How to Choose the Right Compliance Framework(s) for Your Startup

To reap the best benefit from your investment, it's important to find the right mix of compliance frameworks that fits your startup's needs.

Select Your Compliance Type(s) Based on the Services You Provide

Designing a compliance program is all about understanding which frameworks fit your business based on your startup's size, industry, business model, data, and customer needs. When it comes to choosing which audits to pursue, simplify your decision by focusing on the services you provide to your customers.

Information security and privacy for data stored on the cloud are must-haves for all startups, so you'll likely want SOC 2, at least. Other than that, startups need to focus on the regulations within their specific industries.

Let's say your startup not only manages your customers' data in the cloud, but you also process their credit cards for purchases. That means you'd need SOC 2 and PCI. And yes, healthcare startups need HIPAA, but not only healthcare startups—if you sell insurance, for example, you need to be HIPAA compliant, too. Do you want to do business in Europe or even hire a European citizen? Then you'll want to consider GDPR. The more customer services your startup provides, the more likely you'll need to target multiple compliance frameworks. Salesforce, for example, complies with SOC 2, HIPAA, GDPR, ISO 27001, PCI DSS, and [more](#).

Decide How to Handle Multiple Frameworks

Pursuing multiple frameworks at the same time can overwhelm founders, especially without expert guidance. Compliance frameworks are nuanced, difficult to navigate, and expensive to audit. However, common compliance frameworks often overlap each other, so you can save time and money by knocking them out at the same time.

For example, SOC 2 and ISO test similar controls like:

- Securing your physical space
- Assigning appropriate information access to each employee
- Basic employee security training
- Human resources functions (onboarding, employee termination, etc.)

Your SOC 2 auditor can use the same control sample for PCI compliance as well, as long as you schedule your testing periods around the same time. This not only eliminates extra work for the auditor, but it also minimizes the disturbance to your own team.

If you can only invest in one framework at a time, you'll want to pick based on what your customers need and request most.

Keep in mind that the work you do to become compliant for one framework can help you progress in another, regardless of whether you tackle all of your frameworks at once or one at a time.

Thoropass benchmarks your implementation so your efforts toward one framework can be reused for another. You can track your progress toward each framework in your [Knowledge Base](#) and access all of your [policies and documentation](#) based on how they help you achieve each compliance requirement.

Understand Stage-Appropriate Compliance

While the compliance standards are the same for all businesses, the implementation of those rules varies drastically from small to large companies. So, don't be alarmed when you dive in and realize that the legal language is far more generic than helpful.

For example, a common compliance standard is making sure your physical space is secure. A small lock on an office door and a doorman who handles building security would be sufficient for a six-person startup. An AWS data center, on the other hand, would need much more.

We often get questions from founders asking us for guidance on what's enough for their startup. Unfortunately, the answer is often, "It depends". One way founders can start thinking about translating compliance frameworks to meet their startups' needs is to consider what makes the most sense based on their current stage.

[As Forbes illustrated earlier this year](#), your infrastructure security needs will change as your startup matures. Stage-appropriate compliance might look like database backups and basic encryption when you're pre-seed. If you're on your way to Series A funding and have hired a dozen engineers, you may want to replace your team's shared accounts with individual accounts with strict permissions and start regular infrastructure penetration tests. And you'll likely want to invest in a security information and event management tool post-Series A.

Seek Professional Guidance

The complexity of compliance makes it all the more important to look for help in understanding what's actually important in each framework and what's not. It's also critical to understand what makes sense to implement and how to fulfill the requirements appropriate for your stage.

Unfortunately, there aren't many resources online for startups seeking compliance. Yet, as more tech startups demonstrate a need and interest in compliance, companies like Thoropass are bringing the focus to startups.

The Thoropass team are the experts, so you don't have to be. Pairing easy software that's always getting smarter with expert guidance and continuous monitoring, Thoropass integrates into your process to prepare you to pass any audit, every year, with flying colors. With Thoropass, our in-app audit combines a seamless audit readiness program with CPA auditors that specialize in information security and infosec audits, not taxes like most other CPA firms. Our auditors will conduct your compliance audits and issue your reports, without ever leaving the Thoropass platform.

You can also reach out to a certified public accounting (CPA) firm specializing in information security. A CPA will conduct your compliance audits and issue your reports; however, selecting the right one can be challenging. CPA firms handle a variety of tasks (bookkeeping, taxes, etc.), so it's important to find one that's experienced in infosec audits.

Find a Guide You Can Trust and Stick with Them

Compliance is complicated enough without changing your guide halfway through the process. Regardless of the type of compliance you choose, it's important to find an expert team or vendor you trust and stick with them throughout the process.

Because of the complexity of compliance frameworks and how they apply to your unique startup, there's a bulk of knowledge that vendors need to know about your company and its situation at the beginning. That need for company-specific knowledge continues to grow as you step through this process, and your startup continues to grow.

Stepping through the knowledge-sharing stage again can cause you to lose your momentum and increase your time and cost investment.

When choosing your compliance partner, never sacrifice quality for speed—as tempting as it may be. Ensure your guide [offers a sophisticated platform with thorough preparation and continuous monitoring](#) that sticks with you along every stage of your compliance journey.

**Don't just pass.
Thoropass.**

Thoropass™

[Get in touch →](#)