Thoropass™

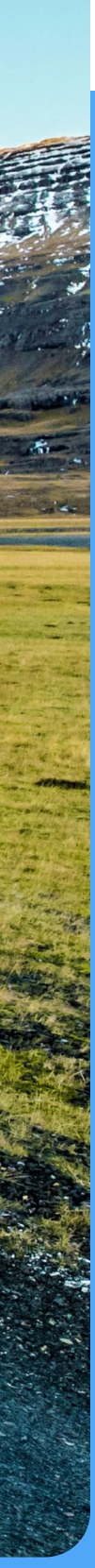
## Unlocking Growth Through Compliance

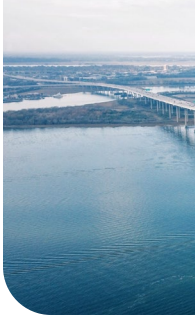
# SOC 2 as a Strategic Business Generator

Most organizations seek a SOC 2 because they have to, or, because they take risk seriously (a.k.a. because they have to.)

Fewer organizations, however, seek ongoing SOC 2 for a more important reason: to enable and differentiate their businesses. These organizations are the smart ones; and whether you're a CISO, IT, Compliance, Procurement, or Legal leader, the fact that you're reading this means you're smart, too. Congratulations.

We've put this guide together to highlight the business outcomes that are possible by attaining and maintaining SOC 2 through an ongoing, scalable solution. From building trust to accessing new markets, a continuing compliance plan guided by SOC 2 can help you so that you can make successful business cases and deliver beyond expectations within your organization.





CHAPTER 1

# SOC 2 as Business Generator

**Receiving a SOC 2 report for the benefit of your stakeholders, and a SOC 2 badge to impress visitors to your website, is only the beginning of how your business can benefit from compliance.**

Attaining and maintaining compliance has both short- and long-term benefits for a business's health. These benefits must be understood at every level of the company, from marketing to engineering, and from analysts to executives. The following list provides a quick glance at the tangible benefits of a healthy SOC 2 and compliance program for a scaling company:

## Building Trust

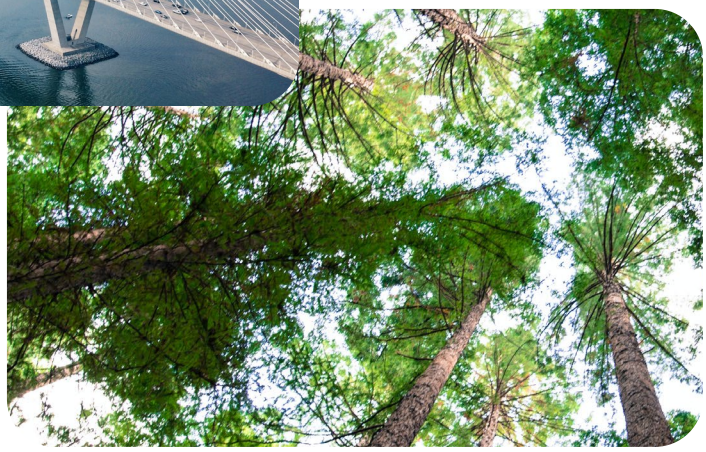
The concepts of trust and reputation are often considered marketing or branding concerns. But Edelman reports[1] that **45% of Americans distrust businesses** as a rule. This means that prospective customers and partners, as well as clients and stakeholders only need one thing to turn them off in most cases and from engaging your partnership no matter how good your product or service is. Consistent and well-documented compliance from a well-respected framework like SOC 2 can be the differentiator.

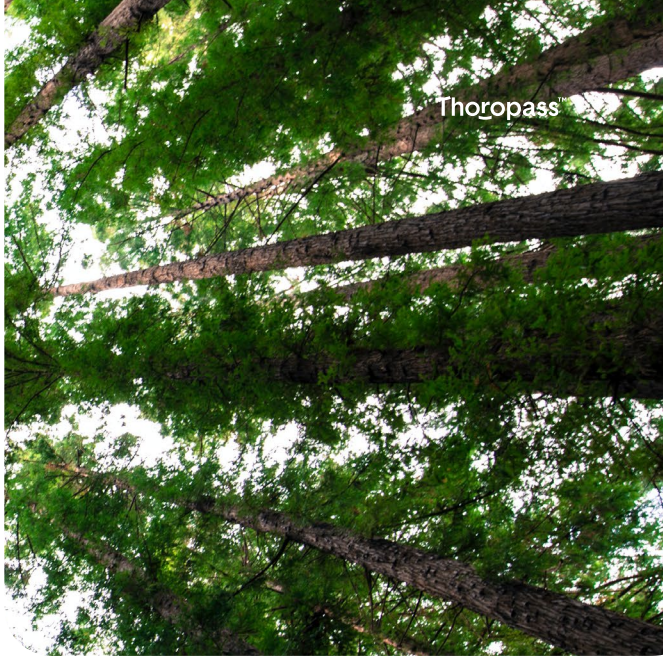
## Managing Risk

The need for data and IT security are well accepted in businesses, as data breaches have expanded by 15% since 2020, with the average breach in 2023 costing over $4.5 million dollars. But the flipside is less widely known, that, according to IBM, **a company can save $1.76 million dollars a year** by using security automation tools.[2] Having an extra few million dollars on hand could be the difference between good and great years.

## Stretching Resources

Companies save money by automating their compliance process, thereby reserving headcount and resources for more important, strategic tasks. The average security analyst makes around $100k annually, while **cybersecurity staffing faced a 3.4 million employee shortfall** to start the year.[3] This means companies are increasingly paying more for less available talent, making compliance harder and more expensive without tools to help in the process.






## Security as Strategy

Better use of resources creates efficiency and productivity that businesses can use to leverage predictable growth plans amidst unpredictable times in cybersecurity. In a recent survey,[4] nearly **3 in 4 business leaders said security and compliance positively impacted** their business's productivity and success despite the uncertainty in macroeconomic conditions, staffing challenges, and new technology disruptions like the wide adoption of AI.
Are your leaders of this mindset?

## Accessing New Markets

No industry requires SOC 2, which is why it is an **instant differentiator**. However, many industries, such as government and SaaS, are increasingly asking for a SOC 2 report to ensure security. Demands for strict compliance jump considerably as you look at enterprise companies, especially those who deal with hundreds, if not thousands, of vendors. These companies will often make buying and partnering decisions based on compliance controls and certificates, often with timing being the deciding factor. Staying compliant and offering quick sales cycles erases this as a barrier to entry.

## Doing Good

Within the past 5 years, **90% of companies in the S&P 500 have published social responsibility reports**, up from just 20% a decade ago.[5] The reason is simple: prospective customers, employees, and partners care, not just about sustainability and social issues, but about how their personal data and privacy are handled. Companies that demonstrate compliance likewise demonstrate corporate responsibility in ways that go beyond managing risk; they signal to new generations that they're built to last with integrity at their cores.

CHAPTER 2

# Is SOC 2 Enough?

**Because SOC 2 is not strictly required for all organizations, it can be difficult to know if you're compliant "enough." For example, if you have a SOC 2 Type 1 report, you may want to consider Type 2. Likewise, if you have a SOC 2 report and are considering global business (especially in EMEA) then adding ISO 2700x to your frameworks is a smart investment.**

You may not be in the market for more security frameworks. Regardless if it's the right time for your organization or not, SOC 2 is an excellent first step in exploring multiple frameworks. The controls and audits involved in SOC 2 can either be directly applied to other frameworks or do the heavy lifting that makes follow-up compliance journeys much easier.

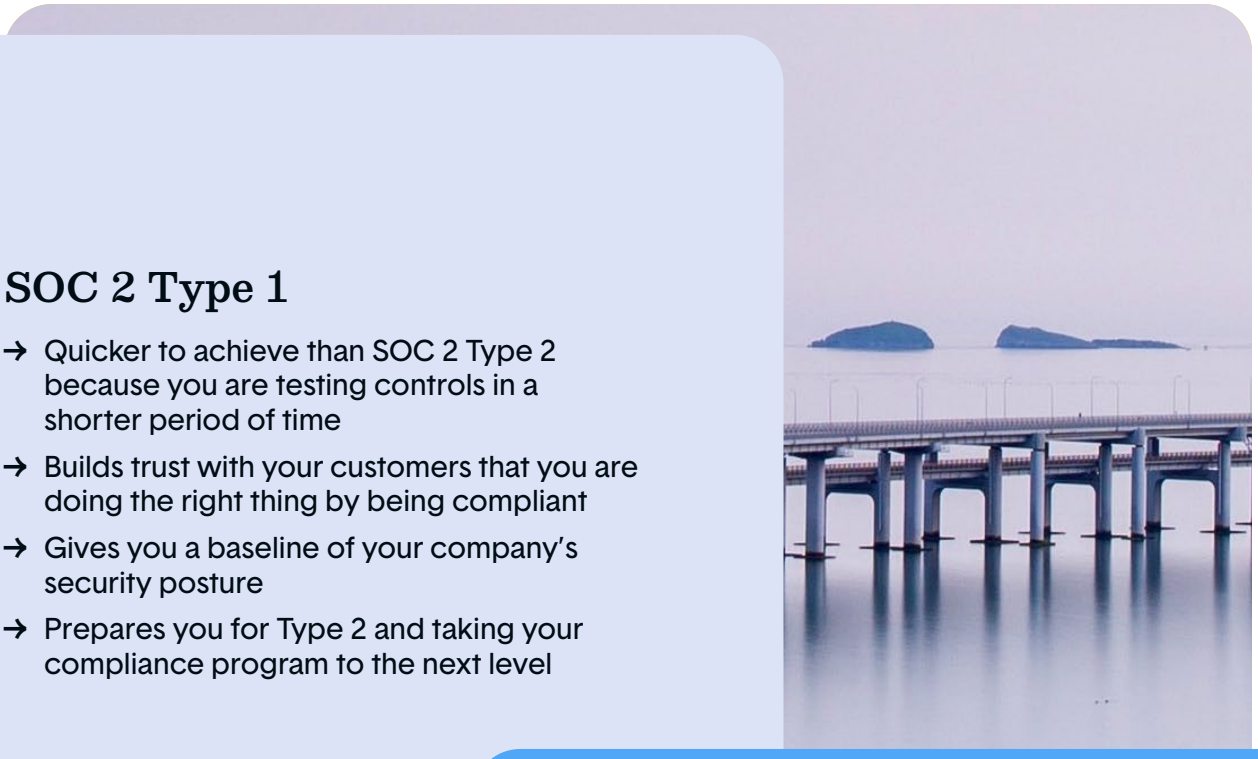
As you (re)consider whether or not your organization is compliant enough, consider how a SOC 2 can prepare you with these extra layers of protection:

## SOC 2 Type 1 vs. Type 2

**SOC 2 Type 1** is a stepping stone for some enterprise customers. But if your business is growing exponentially and wants to work with enterprise customers that require a more complete picture of their compliance, then you'll need to pursue SOC 2 Type 2.

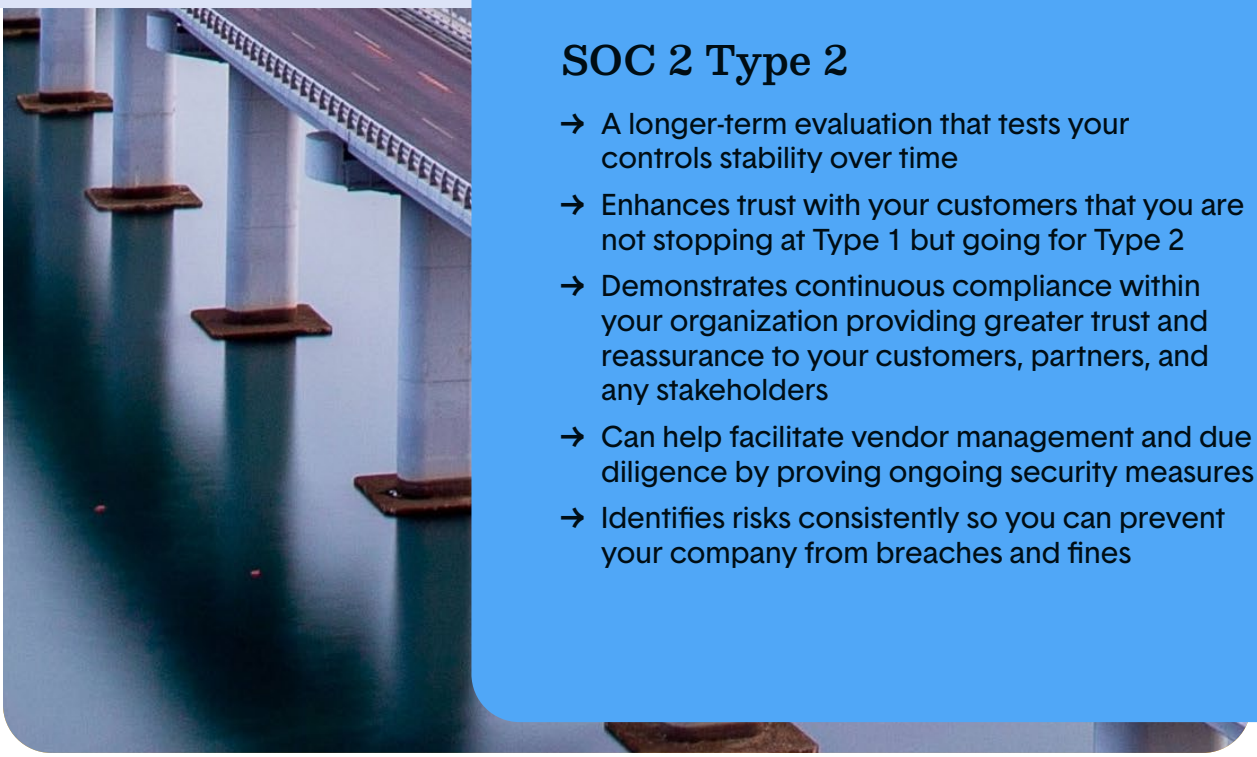
**SOC 2 Type 2** includes all the features of SOC 2 Type 1, but with an additional examination of the effectiveness of controls over a specified period of about six to twelve months, thereby proving the stability of your controls over time. Once you prove the stability of your controls, SOC 2 Type 2 gives you the opportunity to transparently provide valuable reassurance to your customers and partners that you take your compliance seriously.

Since SOC 2 Type 2 covers a specified period of time, it encourages maintenance. This maintenance is a building block to help build a reputation that your business is continually improving and has an ongoing commitment to security.



## SOC 2 Type 1

- Quicker to achieve than SOC 2 Type 2 because you are testing controls in a shorter period of time
- Builds trust with your customers that you are doing the right thing by being compliant
- Gives you a baseline of your company's security posture
- Prepares you for Type 2 and taking your compliance program to the next level



## SOC 2 Type 2

- A longer-term evaluation that tests your controls stability over time
- Enhances trust with your customers that you are not stopping at Type 1 but going for Type 2
- Demonstrates continuous compliance within your organization providing greater trust and reassurance to your customers, partners, and any stakeholders
- Can help facilitate vendor management and due diligence by proving ongoing security measures
- Identifies risks consistently so you can prevent your company from breaches and fines

## Other possible frameworks

**SOC 2 is a widely accepted framework that also can be applicable to other popular frameworks. While there are many frameworks available—such as NIST, FedRamp, or CSA Star—the ones listed below are widely accepted and liable to deliver serious ROI for your business.**

SOC 2 contains many transferable controls that can save your company time and money as you consider investing in one (or more) of the following frameworks.

### SOC 1

Whereas SOC 2 focuses on security, SOC 1 is dedicated explicitly to services that may have an impact on financial statements. As your business ecosystem grows, having a SOC 1 provides instant credibility to your ability to manage risk across multiple financial stakeholders.

### GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) regulation concerning the protection of personally identifiable information (PII) of EU citizens. It sets guidelines for data protection and privacy with strict regulations. If you operate or are thinking of operating in the EU, GDPR is increasingly seen as essential for serious companies.

### ISO 27001

An international standard for implementing an effective Information Security Management System (ISMS), you might want to start your ISO 27001 if you're aiming to establish a more robust compliance program at your company. You may also want to consider ISO 27001 if a country or region you operate in or want to expand operations into requires you to comply with ISO 27001 regulations.

### HIPAA

HIPAA, the Health Insurance Portability and Accountability Act, sets the standards for healthcare organizations in the US to ensure the protection and privacy of patient health information. If you operate in the healthcare or HealthTech industry, it is a must to show you are operating ethically. Even if not explicitly required, HIPAA is considered a minimum bargaining chip by many companies and investors.

### HITRUST

Specifically designed for healthcare organizations, HITRUST is a comprehensive framework that includes security standards, regulations, and best practices. Seen as a benchmark, you should consider HITRUST if operating in the healthcare and HealthTech space to reassure healthcare partners, stakeholders, and clients that your business is committed to their security. Whereas HIPAA is often self-reported, HITRUST requires a more robust audit process that many large companies and insurers require.

### PCI DSS

Payment Card Industry Data Security Standards (PCI DSS) is required by the largest payment and credit card companies to ensure the security of any cardholder data while simultaneously preventing credit card fraud. If your business takes credit card payments, this framework can show your customers that your company operates securely.

# IRL Capitalize

## A FinTech company's use of SOC 2 to build credibility and grow their client base

Compliance isn't the first thing you think of when trying to compete in a highly regulated, competitive industry like FinTech, but that's exactly what Capitalize did. Capitalize is a retirement savings company, specializing in, for example, helping employees move old 401ks to IRAs with simplicity and speed. They used their SOC 2 to both demonstrate their compliance journey as well as unlock new partnerships and deals. They did it by:

- Taking advantage of a **frictionless experience**: Capitalize met with their in-house auditor on the first day of working with Thoropass. From there, all evidence collection, communication, and management was done on the same platform.
- Getting their entire organization to be **compliant-conscious**: Capitalize onboarded their employees as they were being onboarded to the Thoropass experience. They strengthened this by instituting ongoing internal education and training so that everyone in the company understood how compliance fits into their business strategy.
- Managing their **third-party vendors**: As a scaling business, Capitalize realized that they were only as strong as their weakest vendors. As a result, they focused on vendor management as part of their compliance journey, making sure that their business relationships were reflected in their documents, contracts, and ongoing monitoring related to the safety and security of their third-party vendors.
- Seeking **enterprise-level partners and customers**: Seeking larger partners and clients is often a main part of scaling a successful business. While many organizations consider SOC 2 as table stakes for doing business, Capitalize was able to tap into deals where it wasn't, and accelerate deals where it was.

> "Thoropass was our complete compliance solution. The best part about working with Thoropass was that it's the perfect blend of technology and people to take a complicated process and make it accessible and easy.

Hear more from Chris →

CHAPTER 3

# SOC 2 Time and Cost Expectations

**Even for organizations who have been adhering to SOC 2 for years, it's easy to lose track of what is considered "normal" or "best" when it comes to expectations related to time and cost. Most compliance experts will leverage their network to compare benchmarks. Whether you don't have that network, or just want an honest and objective take on these important questions, we've got you covered:**

## How long should your SOC 2 attestation take?

As with many important and complicated things, the answer is—it depends. Before seeking out a timeline from a costly company (or the Oracle of Google search), make sure you have honest and up-to-date answers for the following questions:

- How many employees do you currently have?
- How many employees do you plan to have in the next year?
- What type and how many systems do you run?
- Do you operate your systems in multiple locations?
- What sensitive customer data are you storing?
- What Type of SOC 2 report are you preparing for?
- Are you planning for another SOC 2 Type and/or framework (e.g. ISO 2700x) in the near future?
- What is the current state of your SOC 2 journey versus the state needed to go to audit?

Depending on your answers to these questions—and whether your current evidence and compliance programs are all up to date and in one place—you could reasonably expect to be audited for SOC 2 Type 1 in a handful of weeks while SOC 2 Type 2 can take longer. And while some audits might take a few months—and annual attestation could be seen as a year-long process of collection and education—the moral of the story is that the fewer moving parts the quicker the timeline.

If you're still doing audits the old way, by collecting your evidence and managing your controls manually via spreadsheets and screengrabs, and only then passing it along to an audit firm, then you're likely wasting valuable time (and money) for your SOC 2.

Even most modern SaaS companies who supposedly offer compliance platforms to help you with your audit still rely on manual labor combined with certain automation features that lead to a hand-off to a third-party auditor whom you've never met before. This adds time and doubt to your compliance journey, especially if/when the auditor comes back with questions about your controls or requirements that your SaaS compliance solution never prepared you for.

Thoropass is the only compliance and audit solution with in-house auditors performing the audit on a single platform. This not only saves you valuable time, it makes future compliance for different Types or frameworks faster still.

## How Much Does SOC 2 Attestation Cost?

If you've gone through a SOC 2 attestation in the past, you already know that the audit can be expensive. Even years ago, a SOC 2 audit starting at $20,000 wasn't unusual, with costs in the hundreds of thousands of dollars for enterprise companies being fairly typical.

Fortunately, just as automation has made compliance faster, it's also decreased costs. Determining your costs comes down to a few basic factors:

- Team size and distribution
- Lack (or abundance) of control documentation
- Complexity of services as well as the number and complexity of processes
- Scope of your audit (Trust Services Criteria and Type 1 or 2)
- Reputation of and relationship to your auditor

Again, these are starting costs, and your audit price will ultimately depend on the above mentioned factors. Also, these estimates don't take into account additional compliance-related expenses.

Once you've collected your evidence (racking up resources and man hours from your own company) it's time to turn to an auditor. The most recent figures for a SOC 2 audit are eye-popping, with SOC 2 Type 1 averaging $15–30k and SOC 2 Type 2 going up to $40–80k on average.

If your company is using a third-party auditor when going through your SOC 2 journey, these are only the start of upfront costs that may not include:

- Dedicated in-house employee(s) or consultant
- Readiness assessment
- Legal fees
- Any technical work, training, or cultural changes you need to put proper controls in place

Not all auditors charge flat fees either, so when using a compliance platform who outsources to a third-party auditor, be wary of hidden time and costs that can sneak up on your estimates.

Again, this is where Thoropass's in-house auditors and single-solution platform can help you to save money and make accurate, predictable statements across your organization. By limiting timelines and third-parties, you can eliminate surprise costs.

## A reminder on your SOC 2 report longevity

While technically your SOC 2 report does not expire, you should be re-audited every 12 months. This includes either Type regardless of the auditor.

As your company continues to grow and evolve, processes and systems become more complex, and teams change. It doesn't take long for a company to outgrow its audit year after year. This means the evidence you gather and the controls your auditor tests in your subsequent annual SOC 2 audits will likely look different from your first-ever SOC 2.

However, just because the attestation needs to happen annually doesn't mean the process has to take as long in future years. Compliance is continuous, and by keeping everything in one place, you keep the process simple and predictable. Skipping a year or delaying compliance can have unforeseen consequences even if short-term priorities change.

## A MedTech company's use of SOC 2 to shorten sales cycles to accelerate growth

AcuityMD lives where healthcare, medicine, and technology converge. Needless to say, it can be a busy corner of the market, especially in such highly regulated industries, but by leveraging a SOC 2 early and keeping compliance at the forefront of their business strategy, they've been able to accelerate deal velocity and cement their credibility as a player here to stay. They did it by:

- Making themselves **attractive to do business with**—Even large companies are potential vendors, and AcuityMD identified that their most viable partners and customers cared deeply about data retention and backups. By signaling that they're up to date with compliance, potential partners bypass the scrutiny to get to the strategy.
- Increasing **sales velocity**—When dealing with buyers—especially IT ones as is the case for AcuityMD- having a SOC 2 report allowed the Sales teams to negotiate on their terms instead of playing catch up. It'd estimated that 15% of buyers leave compliance till implementation. Ensuring that a company is active in their compliance journey (and that it's cleared annually with no hiccups) means sales are faster and more confident.
- Collecting evidence and **completing audits at speed**—For both initial and follow-up audits, AcuityMD leveraged a single platform and auditor team to keep everything in one place. This meant they could collect as they go with confidence that it was all contributing to the same outcome. The result was a significant amount of time saved to focus on go-to-market strategies.

> It's become table stakes in the industry to have that SOC 2 stamp of approval.

Hear more from Mike →

CHAPTER 4

# How Can You Best Leverage Your SOC 2 Report?

**Even if you've successfully received multiple SOC 2 reports, there's a sweet sense of relief each year when you receive an updated report. Beyond internal congratulations (and bittersweet preparations for next year's audit), organizations should waste little time in leveraging their most recent report(s) to their advantage. Here are some tips to keep the momentum going:**

## Keeping your SOC 2 report on hand

Your 30–40 page SOC 2 report is not intended for direct consumption by prospects, customers, partners, vendors, or internal stakeholders. It's meant to be read, understood, and evaluated by other compliance or information security professionals.

However, it's also a useful document for internal training of new employees, source material for communicating your compliance journey to the C-Suite and Board, and as a key to unlocking conversations with other businesses. For example, enterprise customers that require a business to have a SOC 2 attestation before working with them will request a copy of your report so that their procurement or compliance team can review it. Ensuring your report is up to date and available is incredibly important in order to maintain a speed advantage.

## How do I leverage my SOC 2 Report?

Your SOC 2 report is a milestone and a reassurance to all that your organization is committed to security and protecting sensitive information. While it may seem obvious, keep in mind how important it is to every level of stakeholder. The value of your SOC 2 is important to each stakeholder for different strategic reasons:


Of course, unless driven by detailed procurement processes, most people won't want to sift through your audit report. Instead, you can show off your business's commitment to compliance by adding the appropriate AICPA-approved logos and other attestation seals to your website. This approach is a powerful, trust-building marketing message that can help you stand out from the competition by enhancing your reputation within your market.

CHAPTER 5

# Maintaining your SOC 2 report and your compliance journey

**As anyone who's attained a SOC 2 report understands, maintaining compliance—whether it be through an annual attestation or expansion to other frameworks—can be a full-time job.**

But most companies don't have headcount to dedicate to that job. That's where automation and an ongoing relationship with your auditor (who in turn has familiarity with your controls) can be the difference between accelerating your business or regularly slowing it down. From keeping pace with changing regulations to maintaining a disaster recovery plan, maintaining your SOC 2 keeps your business ahead of non-compliant or slow competitors. Here's how to leverage that advantage:

1. **Compliance is always-on**

   Maintain efficiency and momentum but keeping compliance a priority, both for your team, as well as stakeholders from the C-Suite to your Sales team. Using tools like Thoropass's continuous monitoring features can be hugely beneficial.

2. **Plan ahead**

   Annual renewals and/or expansion to other frameworks (e.g. ISO 2700x) can be planned in advance to minimize interruption and allow you and your team to maintain focus on other security and strategy projects.

3. **Maintain your controls**

   Controls are where the rubber meets the road for your compliance journey; make sure that they're documented, functioning as designed, and understood by relevant stakeholders.

4. **Always be gathering**

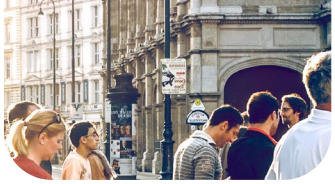
   Make evidence collection and process documentation a part of your business scaling process throughout the year.

5. **Regularly back up data**

   Backing up your data is an important safety check that is surprisingly overlooked or pushed off. Prioritize it in case you need to put a business continuity plan into action.

6. **Update and educate**

   Compliance becomes easier when everyone understands it and its importance in your company's growth plan. Make sure new employees are onboarded and continuing employees are part of the continuing process. You can also update maturing controls year over year (you don't want to stay stagnant).



## 7 Build a compliant culture

When employees and investors share an outlook of compliance-driven strategy, your job becomes easier as every corner of the business documents changes as they happen.

## 8 Do compliant business

You have a choice in who you do business with. Demand compliant and secure third-party vendors even if they don't officially have a report. Your business is only as strong as your weakest partner; make sure their flaws don't hold you back.

## 9 Advertise your compliance

Be sure to work with your Marketing team to display your attestations on your channels (e.g. website homepage) and your Sales team to engage prospects and partners around the idea of how secure your company is to do business with.

## 10 Relax! It's only an audit

If you work with Thoropass, you'll meet your auditor on the first day, and you'll keep your evidence and ongoing management all on one platform; whether you think about it every day or only every so often, we'll be here to ensure your success.

Thoropass is the only compliance and audit solution that provides customers with everything they need without gaps, surprises, or unnecessary third parties. In-house auditors join customers on Day 1 of their journey and manage all evidence and communication without leaving the platform. The result is a **frictionless, closed-loop experience** that is easy to predict and respected across industries.

Thoropass™

# Let Thoropass change the way you think about compliance.


1 https://www.edelman.com/trust/2023/trust-barometer

2 https://www.ibm.com/reports/data-breach

3 https://www.isc2.org/Research/Workforce-Study

4 https://www.forbes.com/sites/deloitte/2023/04/20/navigating-the-future-of-cyber-business-strategy-cybersecurity-training-and-digital-transformation-are-key/?sh=3c1fb69629c1

5 https://online.hbs.edu/blog/post/corporate-social-responsibility-statistics


Get in touch →