Ready to break through with SOC 2?

If enterprise and public sector prospects struggle to trust you, you've hit the **compliance ceiling.**

SOC 2 is a leading global standard to earn and keep their trust, unlocking your next phase of growth.

VERSION 1 2022

assurancelab

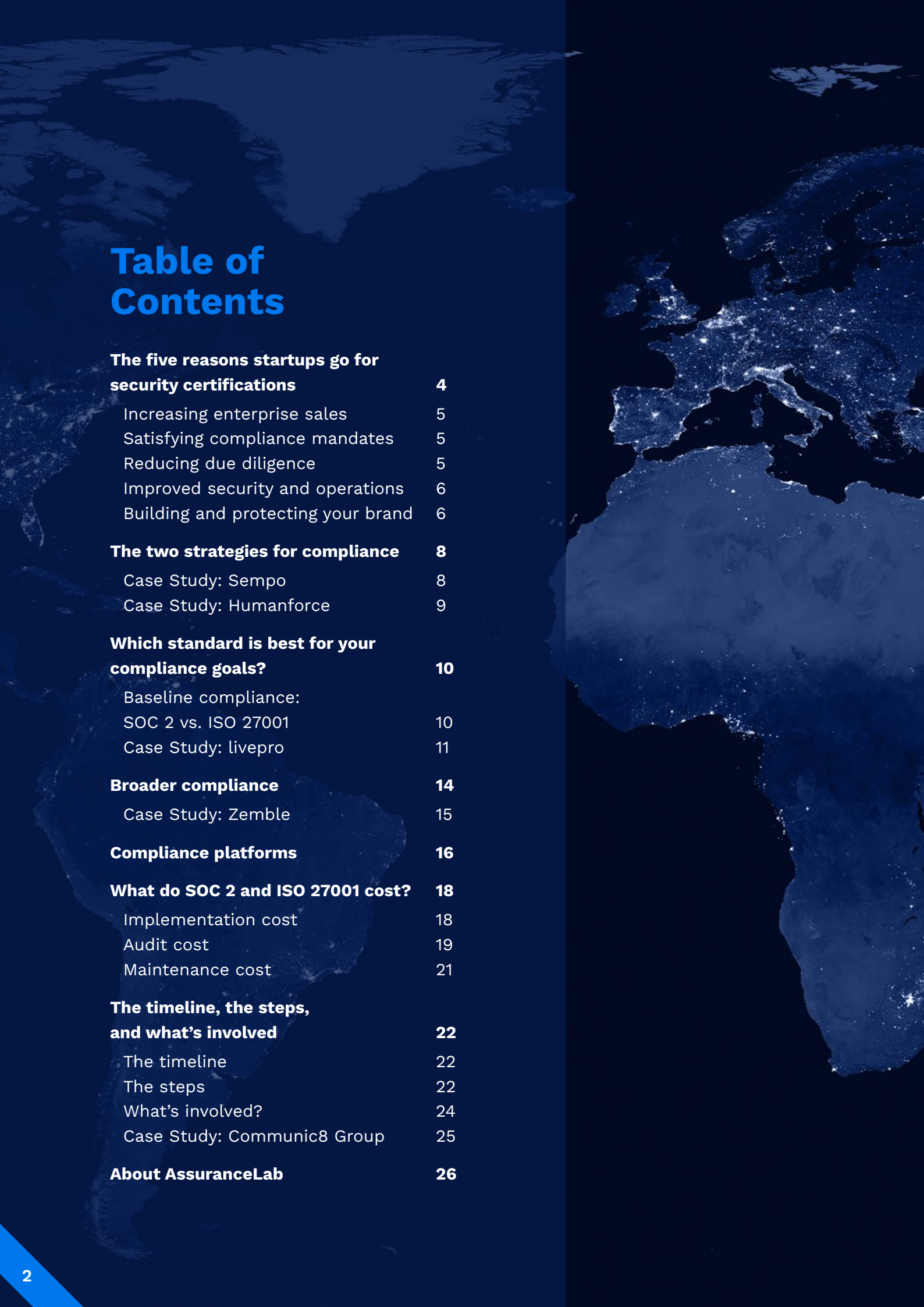


Table of Contents

IMPORTANT NOTICE

This document contains general information only. AssuranceLab cannot guarantee the accuracy, completeness or timeliness of the information contained herein. By making this information available to you, we are not providing professional advice or recommendations. AssuranceLab will not be held liable for any loss or damage arising from reliance on this document, including but not limited to any loss of profit, revenue, reputation, or any consequential losses. Before acting on any of the information contained in this document, you should seek professional advice.

The five reasons startups go for security certifications

Security and compliance accreditations, like SOC 2 and ISO 27001, demonstrate that you apply good practices in your business.

They're often classified as "security" and thought of as the technical security of your systems. However, they're actually broader, with a focus on organisational practices that support your security AND other objectives. That includes availability (system resilience), confidentiality of data, privacy for your users, integrity of the system processing objectives, scalable process design, and generally reflects your readiness to support large and discerning customers.

There are five reasons startups pursue these accreditations, listed in order.

1 Increasing enterprise sales

Large businesses, when looking to use your software, consider your product AND your capabilities as an organisation. These qualifications play an important role in demonstrating your business is “enterprise ready”, providing a reliable service, and keeping their data secure. They often require these accreditations to support their own compliance, so if you are unable to furnish an accreditation you may be excluded from their consideration.

Catherine Fromont, People and Operations, FileInvite:

For us to grow as a company, we needed to know what gaps we had within our business to ensure we were covering all our bases and had the confidence to get our bigger enterprise customers onboard and ensure they could trust us with their data.

2 Satisfying compliance mandates

These information security accreditations help you verify and demonstrate that you meet your compliance obligations. That can include what you contractually sign up to in your service agreements with customers, as well as industry-specific regulations for privacy, financial services, healthcare, and more, that are underpinned by effective governance and information security.

Alfonso Marquez, CTO, Zemble:

As a vendor for highly-regulated industries, compliance is very important for our customers. Certifications such as ISO, HIPAA and SOC are necessary to our customers as part of their vendor assessment.

3 Reducing due diligence

A major pain point for software companies is the relentless due diligence that goes with serving enterprise customers. Hundreds, even thousands of “security questions”, and vendor audits, are common. Standards like SOC 2 and ISO 27001 are designed to have a single independent audit process that satisfies broad end user requirements, to reduce this due diligence burden.

Simon Gillson, Project Manager, JAVLN:

We required an assurance report to streamline our clients’ due diligence processes when they evaluate our services. That could be hundreds, even thousands, of questions from each customer when considering the use of our cloud-based insurance software, which takes a lot of time from the team and slows down the time to get customers on board.

4 Improved security and operations

Comparing to industry standards is a means for improving the way you operate. These standards are based on “good” or “best” industry practices. Auditors have a lot of experience seeing these applied in different environments and can guide you on how best to apply them in your context. It’s common to see companies scale without spending adequate time defining the right processes and governance, which notoriously leads to growing pains and failures along the way.

Adrian Loke, Director of Security, Dropsuite:

We needed a 3rd party audit to assure ourselves as well as our clients that we have good data governance policies and practices in place. (We wanted) better confidence in our data management and security processes.

5 Building and protecting your brand

There are myriad other stakeholders that also favour these accreditations. Investors, regulators, partners, boards, your management team, and even employees benefit from implementing and validating your alignment to standards.

It provides peace of mind that you are secure, compliant, and provides clarity on what your key operational practices are. We often hear these accreditations being used for “defensibility” - you can’t always stop things going wrong and, if they do, you want to be able to show best efforts were made to avoid that. Standards are an objective way to show you’ve invested in your information security and effective governance.

Brad Shaw, CEO, livepro:

The market we target are security conscious. We felt we needed SOC 2 so that our customers had the confidence in selecting livepro as their provider. It gave livepro (a smaller company) a level of security prestige within the market. It also helped tighten up operations by providing clear guidelines on the best practice for managing a business, so we know we’re doing the right things.

The two strategies for compliance

We now see companies opt for one of two compliance strategies:

1 Generic

Compliance automation platforms, like Drata, allow for a more standardised way to implement your compliance. Audit firms that partner with the platforms, like us, can offer generic audits aligned to that strategy.

This is best suited to companies that want:

- **The simplest, shortest path to compliance**
- **Self-preparation following a playbook**
- **Lowest cost audits**
- **Minimum control requirements**

Case Study: Sempo

Sempo delivers aid into developing nations through blockchain technology in partnership with charities like Oxfam. Sempo operates at the intersection of humanitarian aid and finance, with high operational standards. SOC 2 helped Sempo meet those standards.

Starting SOC 2 as a three person company, Tristan Cole, CTO, explains: It's definitely doable, but you do need to dedicate resources and time to make it happen - so make sure it's worthwhile for your organization. Leveraging external tools assists in automating compliance with some of the trust criteria. I'd particularly recommend a platform for organizations who haven't completed a SOC 2 like standard before and/or are time restrained. Some weeks are busier than others and SOC 2 is something that takes time. And you won't see immediate benefits. Thus, for us, being able to prioritise SOC 2 during weeks when we had less urgent deadlines was important. AssuranceLab's approach fit well with that.

2 Customised

Whether or not you use a compliance platform, in this strategy, the controls and the audit process are aligned to your unique way of operating.

With a team of in-house experts and trusted consulting partners, AssuranceLab is well placed to assist clients who wish to achieve compliance in a tailored way. We use technology for maximum efficiency and to ensure compliance at scale, but also add more personal service and ongoing support to help you maintain and incrementally improve your compliance program.

This is best suited to companies that want:

- **Strong foundations for security and operations**
- **Alignment to your unique way of operating**
- **Hand-holding support and iterative feedback**
- **Flexibility for bespoke requirements and multi-standard**

Case Study: Humanforce

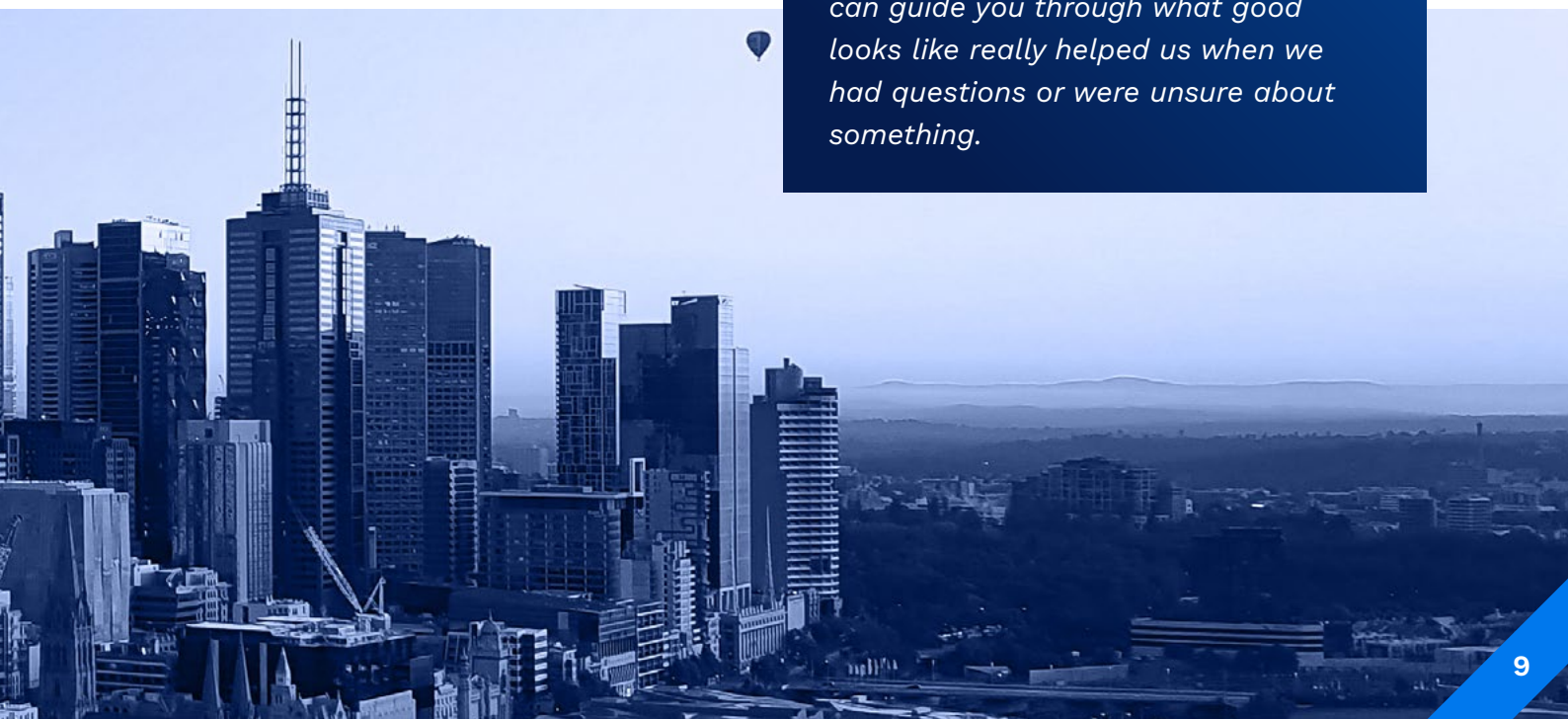
Humanforce uses AI-powered technology for workforce engagement with easy onboarding, auto-rostering, smart time capture and more. Humanforce achieved both SOC 2 Type 1 and SOC 2 Type 2 in a 7-month period in order to satisfy their large business customers and support their enterprise sales.

Jason Fischer, CTO, shared his top tips for others starting out:

Things to remember when planning to kick off SOC 2:

Define and document what you do today. That's probably 80% of what you need. Start documenting all actions. This can be simple meeting minutes. Ensure the person running the evidence gathering has all the business touch points they need and that everyone in the business knows to assist. Security and Privacy are everyone's responsibility, not just one person or team.

Working with AssuranceLab who can guide you through what good looks like really helped us when we had questions or were unsure about something.



Which standard is best for your compliance goals?

Each standard has different requirements, nuances in how they are applied, and perceptions in the market. This impacts how they help you achieve the goals above as well as which one may be best for your business.

Our CXO Guide to Security and Compliance has a table of the various global standards that commonly apply to software companies. Post-covid, we've seen a large increase in multi-standard compliance. It's common to start with one of the below two standards, but increasingly important to consider a future roadmap that factors in where additional standards may be needed.

Baseline compliance: SOC 2 vs. ISO 27001

SOC 2 and ISO 27001 are the two most common global information security standards, each rising from a family of standards that date back decades. Most large enterprises will recognise either standard interchangeably. There's about 80% overlap between the two standards in the information security practices they cover. That said, there are some quite significant differences in how they work in practice.

The customer view

Regulated industries, like finance and healthcare, tend to prefer the SOC family of standards. Less regulated customers generally prefer the ISO family of standards. SOC 2 is more prevalent in the US. ISO 27001 is more prevalent in Europe. Most companies start with one of the two standards, but it's pretty common to adopt both in order to cover all bases and reduce friction for customers that have a preference one way or the other.

As Guido Santo, VP Cybersecurity, Rokt explains: We were already ISO 27001 certified, but SOC 2 was an important step in further maturing Rokt's compliance program. Most of our business is conducted in the U.S. market and clients there typically want to see SOC 2 reports. We wanted to avoid potential sales blockers.

The business perspective

The SOC 2 standard is more flexible, more operationally focused, and sets a less stringent minimum bar. That makes it appealing to cloud software companies in particular. Often these companies want to minimise the burden on their teams, with less documentation and less administrative burden that can slow them down. ISO 27001 by contrast can take out some of the guesswork. It's a more prescribed standard with a mature market of consulting providers, templates, and guidance, so it can be easier to just follow the script. It would be remiss of us to omit that ISO 27001 audits are often described as extremely painful. The

greater focus on face-to-face audit work, and carving out large chunks of time for the audits, can cause more business disruption and be really tiring for everyone involved.

Case Study: livepro

livepro is a Customer Experience Knowledge Management system used by organisations as their single source of truth to deliver "answers" to customers, not long documents or PDFs. The SOC 2 report gave livepro (a smaller company) a level of security prestige within the market. It also helped tighten up their operations by providing clear guidelines on the best practices for managing a business. Their CEO, Brad Shaw, shared his tips for others undertaking SOC 2 similar projects:

"Taking things in bite-sized chunks enables you to action things within the business as you go, rather than having a big bang approach. It allowed me to continue to run the business while also using the SOC 2 process to identify best practice management processes. Lots was achieved without the stress of deadlines."

- Brad Shaw, Founder & CEO, livepro

The deliverables

ISO 27001 is a certification where you receive a one-page certificate to share with customers. If it's an accredited certification - by an accredited certification body - it's also reflected in an online register that can be searched by customers. In some cases, you might also share your statement of applicability (SoA) that details which controls you have implemented.

SOC 2 is an attestation report, which is often confused with a certification. It's a detailed report that overviews your company, your services, and the scope of your "system". The system is your infrastructure, software, data, people and processes that support the service(s) being reported on. It also includes your control activities mapped to the criteria, and important elements of what is out of scope; the reliance on critical third-parties, and where end users have important responsibilities like managing their own access to your software.

The TL;DR, a SOC 2 report gives further detail to end users, which is favoured when it comes to due diligence and covers more of what they want to know.

The cost

It can be challenging to compare the costs of SOC 2 and ISO 27001 as they are not like-for-like. They also vary significantly between countries and providers. ISO 27001 is a three-year certification cycle. The costs are larger in year 1 for initial certification, and lower in years 2 and 3 when you conduct surveillance audits.

SOC 2 is not defined by a certification period so you can choose when to issue the reports. The industry standard is a Type 1 report in Year 1,

followed by a Type 2 report; either later in Year 1, or in Year 2. It's usually every 12 months thereafter as an annual recurring report.

The SOC 2 audits tend to cost more than the ISO 27001 audits, at least when factoring in the three-year timeframe. However, it's important to also consider that ISO 27001 tends to rely on consulting support to help you implement it and conduct the required internal audits. That means overall the cost of ISO 27001 can be higher or similar with all parts factored in.

The scalability

The compliance landscape is rapidly evolving, where multi-standard compliance is becoming the norm. It's increasingly important for companies to plan forward with their compliance requirements, considering the geographies, industries and future expectations that will impact their compliance requirements. When it comes to SOC 2 vs. ISO 27001, the SOC 2 standard is more flexible, which allows it to fit well with other standards. It has become common to see SOC 2 + HIPAA, GDPR, Californian Privacy, Consumer Data Right, CSA STAR, or other standards and regulations that may also be required.

SOC 2 also has the additional Trust Services Criteria areas for Availability, Confidentiality, Processing Integrity and Privacy. Enterprise customers often place a lot of focus on the Availability (reliability) element, and Privacy is a rapidly emerging area of concern as well.

ISO 27001 does link well with other ISO standards, like ISO 27701 to cover Privacy, however, not as well with other standards outside of the ISO family.

The bottom line

Both SOC 2 and ISO 27001 are great, globally recognised, cross-industry standards that build an effective compliance foundation. Based on their differences above, many companies do both. There are synergies and additional benefits of doing so. If you do prefer to choose one, it's important to consider your customers' preferences, what works best for your team, and how it fits with your future plans.

Broader compliance

If you're a globally focused software company, especially if you have a cross-industry focus, you'll want to consider additional compliance standards. These standards open new opportunities: expanding into markets with local privacy regulations, serving customers with industry-specific requirements like HIPAA, and even just better appealing to a global customer base with the varying standards favoured in each region.

SOC 2 or ISO 27001 creates a good global baseline to build trust with enterprise customers. SOC 2 in particular is nicely compatible with additional standards that are commonly combined, and also offers the additional criteria for Availability, Confidentiality, Processing Integrity, and Privacy, that can be optionally added.

SOC 2 and ISO 27001: despite the same purpose and a lot of overlap, these remain the most commonly combined standards. They complement each other in strengthening your information security, create a perception of greater commitment and rigour in this way, and just appeal to a broader customer base globally where there are different preferences for one or the other of these leading standards.

HIPAA: SOC 2 and HIPAA fit together like puzzle pieces. Even better. There's so much overlap, you'll find adding HIPAA can be included in the same attestation report and only adds about 20% to the controls and audit work involved.

Consumer Data Right (CDR): also a great fit with SOC 2, as CDR is built on the same family of SOC standards. While CDR is Australian, it's similar for Open Banking in the UK and likely to fit well with new open data standards coming in the US, NZ and other countries. Adding CDR to the SOC 2 scope adds about 25% (even though its scope is smaller than SOC 2) based on the more prescriptive controls that often aren't required for SOC 2 (like data segregation, and application whitelisting). These can be covered in the same report. ISO 27001 gives you a leg up, addressing about half the requirements, but requires a separate report and assessment of the ISO controls to ensure they align.

CSA STAR: the CSA STAR cloud controls matrix (CCM) for level two accreditation was conveniently designed to leverage SOC 2 or ISO 27001 seamlessly. It can follow that attestation or certification format accordingly, recognised as the same accreditation outcome. CSA STAR is more comprehensive for cloud security so it almost doubles the scope.

GDPR and CCPA: these privacy regulations, for Europe and California respectively, are two of the most influential privacy regulations. The relevance for software companies is that, if you can't demonstrate you comply with these regulations, enterprise customers (data controllers) will be at risk of fines

and reputational damage for using your product as they are responsible for that compliance. SOC 2 and these regulations fit seamlessly, like HIPAA above, and covers the baseline information security that privacy practices are built on. ISO 27001 also works well, with the ISO 27701 standard able to be added for a Privacy Information Management System (PIMS) that can directly address the privacy regulations that apply.

Case Study: Zemble

Zemble is a web-based SaaS platform for mapping and executing complex, highly-regulated processes like claims and complaints, that involve many stakeholders, steps and materials. With configurable workflows and real-time collaboration, Zemble acts as a single source of truth for every case.

Zemble undertook a combined SOC 1, SOC 2 and HIPAA engagement with AssuranceLab, with the intent to integrate ISO 27001 in the future that had already been certified.

As Alfonso Marquez, CTO, explains: “As a vendor for highly-regulated industries, compliance is very important for our customers. Certifications such as ISO, SOC and HIPAA are necessary to our customers as part of their vendor assessment.”

When asked about the benefits of combining these standards with a single provider, and into a single audit process, Alfonso’s response was: “One was of course the cost of the bundle. In terms of the work involved, it was helpful to know in advance the overlap and differences between different standards. This way, we could organize our information better in our internal compliance tools.”

Compliance platforms

The compliance industry has gained pace in the last few years. That's in part driven by strengthened regulations, increased enterprise customer and public expectations, rising security threats, and the networking effects of compliance standards. It's also being driven by the rise in platforms and automation that help companies achieve compliance faster.

There are two types of platforms used, that have some natural segregation based on the independence boundaries of audits.

Security and compliance platforms: Drata, Sprinto and Vanta are examples of a growing category of software that supports compliance with security standards. They integrate with other software, automate compliance monitoring, and provide governance, risk and compliance (GRC) features for risk assessments, vendor management, and managing policies and other documentation for the compliance audits. By centralising your compliance documentation in these platforms, and inviting your auditor in, you can keep things in one place. Your auditor may also want to add their audit software in the mix, to fill any gaps, and leverage some of the additional features and benefits of that category of software.

Audit software: A-SCEND, Laika, Fieldguide, and our own platform, Pillar, are examples of the other large category of software that supports the compliance audit process. There's overlap with the above category, but audit firms require separate record-keeping and have various other processes required to comply with audit standards. The features built into these platforms power more effective audits, lower costs, and a better customer experience; even if their clients don't use this software directly (instead using the above category to directly manage their compliance). The main beneficiaries of this software are the audit firms, but that passes on benefits to their clients when it works well.

In our case, we generate major savings in multi-standard compliance this way, provide a collaborative audit experience our clients love, and are moving to continuous audit to reduce business disruption.

Our perspective

We've worked with various compliance platforms for years, and continue to support our clients that are embedded in those platforms. But as they've become more advanced, we've seen benefits in more closely aligning. We landed on Drata as the key platform we work with. Our clients led us in that direction, and it works seamlessly with our audits, especially now with our Drata-exclusive audit playbook designed to leverage all the platform's automation to best effect in our audits.

Whichever audit firm you work with, their audit software will be used, even if you don't know it. You may not need

to consider that at all if it just sits in the background, but it's worth asking what audit software is used and the potential benefits for you.

Ours, Pillar, includes:

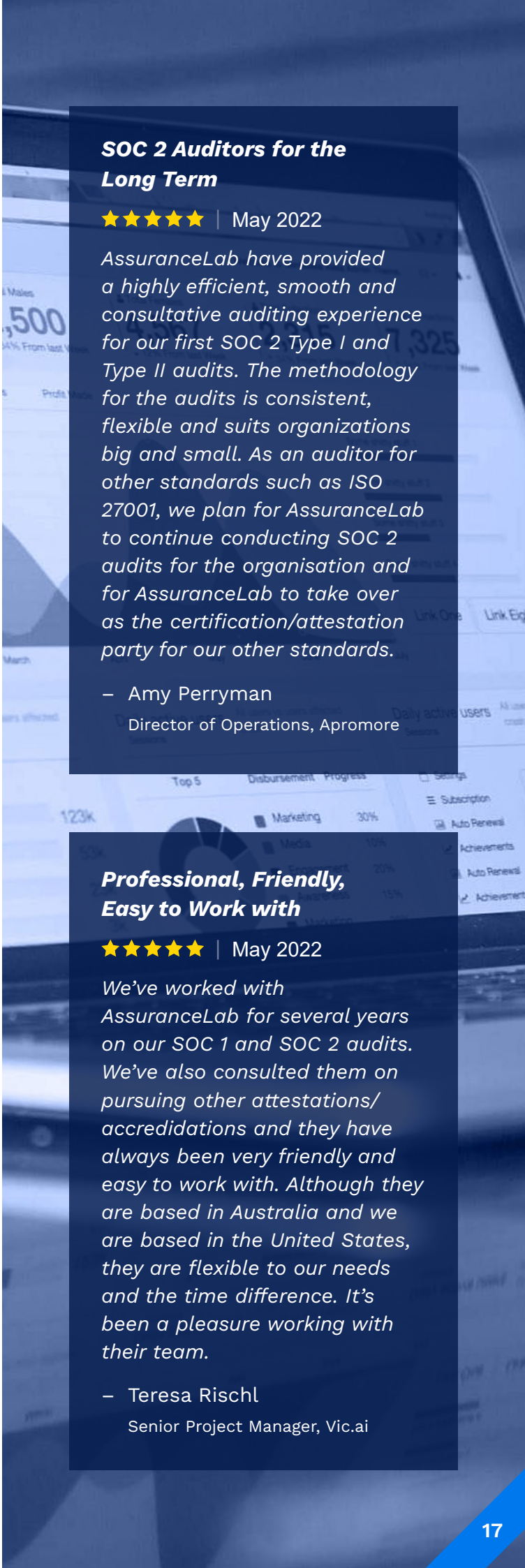
- **Free readiness assessments (optional)**
- **Advanced policy and system description automation**
- **Features to enable an agile and collaborative audit process**
- **Consolidated multi-standard audits and flexibility to completely customise your compliance activities.**

Which combination is best for you?

We see two segments of the market in terms of their preferences:

1. Those that want the simplest, lowest cost, minimum requirements for their compliance. For these clients, we put Drata front and centre, with Pillar working in the background to enhance our audit practices, satisfy our own requirements under the standards, and provide future options like continuous audit and multi-standard.

2. Those that want a stronger foundation, customised to their way of operating, and potentially multi-standard compliance. For these clients, we put Pillar front and centre, leveraging a compliance platform's automation (optional) in the areas those cover.



SOC 2 Auditors for the Long Term

★★★★★ | May 2022

AssuranceLab have provided a highly efficient, smooth and consultative auditing experience for our first SOC 2 Type I and Type II audits. The methodology for the audits is consistent, flexible and suits organizations big and small. As an auditor for other standards such as ISO 27001, we plan for AssuranceLab to continue conducting SOC 2 audits for the organisation and for AssuranceLab to take over as the certification/attestation party for our other standards.

– Amy Perryman
Director of Operations, Apromore

Professional, Friendly, Easy to Work with

★★★★★ | May 2022

We've worked with AssuranceLab for several years on our SOC 1 and SOC 2 audits. We've also consulted them on pursuing other attestations/ accredidations and they have always been very friendly and easy to work with. Although they are based in Australia and we are based in the United States, they are flexible to our needs and the time difference. It's been a pleasure working with their team.

– Teresa Rischl
Senior Project Manager, Vic.ai

What do SOC 2 and ISO 27001 cost?

It's hard to compare the total costs of compliance between different options. Let's take a look at why that is, how you can effectively understand the costs, and guidelines on the costs to expect.

Despite a lot of overlap, there are significant differences between SOC 2 and ISO 27001. We cover the practical and a more technical view in our popular comparison posts:

A practical comparison of SOC 2 and ISO 27001

SOC 2 vs. ISO 27001

For the purposes of comparing costs, there are three key differences to note:

The audit process - ISO 27001 follows a three-year certification cycle with a larger audit in year 1, and smaller surveillance audits in years 2 and 3. SOC 2 has an optional smaller Type 1 audit in year 1, and otherwise has the full Type 2 audits annually (typically, but it's not prescribed by the standard; it's up to you to decide).

The expertise required - SOC 2 is more operationally focused on embedded security related to your systems and services, while ISO 27001 is a management system for information security. The latter requires more expertise, which is commonly addressed by using third-party consultants, which forms a significant part of the cost.

Pricing for risk - ISO 27001 has defined audit days that can be adjusted +/- 30% depending on complexity factors. Costs are usually a day rate cost multiplied by those audit days. SOC 2 might be informed by similar factors, but it's less defined, more variable, and carries greater pricing risk. There's also more liability assumed by CPA firms to the end users of the SOC 2 reports. The calculation of ISO 27001 audit costs are generally easier to perform and understand than SOC 2.

So with that in mind, what do these standards cost and how can you think about those costs?

The below costs and guides are based on the startup and SMB market. For larger enterprises, there can be a factor of 10X or more, but the drivers and principles are the same.

There are three parts to consider that are relevant to any compliance program:

Implementation cost

This is the cost to get the right documentation, systems and processes in place that meet the requirements for the audits. There may be a few parts within this:

A. Internal time costs: This is like the bottom of the iceberg when considering the total costs of compliance. It's easy to compare the costs of consultants, platforms,

and audit fees, but really important to recognise that the internal time costs are invariably the largest cost - at least when you consider the opportunity costs of your time. Regardless of what approach you take, there's significant internal time involved, so it's important to consider options to reduce that and ensure you have the best support throughout the process.

For our SOC 2, it took about 80 hours, split between the Co-CEO (~50), Head of Product and Engineering (~20), and our other two cofounders (~5 each). That was with a lot of outsourcing and using great service providers! When we assessed how long ISO 27001 would take, we estimated 120 hours, as well as a similar +50% on the maintenance of it when compared to SOC 2.

Our clients sometimes use more junior personnel. We regularly see months of their full-time allocation, as well as material involvement of the executive level as the accountable owners. Some CTOs have reported spending ~200-300 hours on SOC 2 and ISO 27001 (separately), so there is a lot of variation.

B. Consultants: In order to reduce the internal time and access the expertise required, consultants may be used. This is especially prevalent for ISO 27001 as more expertise is required and it's generally heavier on documentation. For either SOC 2 or ISO 27001, you'll be looking at $20,000-$50,000+, increasingly framed as monthly retainers and even multi-year arrangements.

C. Internal audit: For SOC 2, it's often a self-assessment of controls by the accountable owners, so there's no additional cost here. ISO 27001 requires internal audits by independent and experienced personnel, which often requires engaging third-party providers. The costs for internal audit can range from $5,000-$20,000.

D. Compliance platforms: The market leading platforms, like Drata, start at $15,000 p.a. (you may be able to access discounts through partners like us). There are many platforms out there; while you may find cheaper ones, they may not offer the same benefits and/or the ones you nee d. The point of using these platforms is to reduce the internal time involved, which is usually the largest cost.

Audit cost

Let's start with ISO 27001 since it's more clear cut. You'll typically pay $1,000-$2,500 per audit day, and you can calculate the audit days yourself using ISO 27006 guidelines. That's the initial certification cost, and then surveillance audits are about 1/3 of that, plus a bit (to cover overheads like planning and client relationship management).
For SOC 2 it's more complex, so we'll skip straight to the going rates in the market for various scenarios.

A. For a platform-specific, generic audit, without "risk advisory", the cost is between $5,000-8,000 for Type 1, between $7,000-10,000 for Type 2, and $10,000-14,000 to combine

both. These scenarios require using the relevant compliance platform, eg. Drata; you get limited support and guidance from the auditor, and the controls are generic rather than customised to you.

B. For a platform-centric audit with "risk advisory", the cost is between $7,000-10,000 for Type 1, between $10,000-14,000 for Type 2, and $12,000-18,000 to combine both.

C. For a tailored audit with "risk advisory", that works with any system setup, the cost is typically between $8,000-12,000 for Type 1, between $12,000-15,000 for Type 2, and $15,000-20,000 to combine both.

Note: all of the above are based on audit firms that specialise in startups and SMB cloud software companies. We see traditional audit firms like Big-4 and mid-tier accountancy firms that may have significantly higher costs, lower savings when combining Type 1 and Type 2, and limited support for the compliance platforms.

Maintenance cost

The audit costs above include the ongoing costs, so this category of costs is limited to your own ongoing internal compliance activities. If you use a compliance platform or have engaged consultants, again those costs were described above and may continue as an annual recurring cost, or taper off after you've achieved compliance and have less of a need accordingly.

The ongoing maintenance includes performing your control activities and working through the audits. These costs can vary quite significantly based on how you've set it up during your implementation. If you take shortcuts there, it generally adds to the maintenance where you need to operate more compliance-specific activities rather than having those integrated with the standard way you operate. Or having audit issues that take more time to work through and resolve.

We set up our controls to really fit the way we operate, with the help of our auditors, MJD Advisors, our infrastructure implementation with the Citadel-One, and using the Drata platform to help us automate some of the compliance activities. With that, it's only about 5-10 hours per month to maintain. We do hear it can be more like 20-40 hours if it's not set up as well, or the process design is more arduous in general.

The timeline, the steps, and what's involved

These three topics go hand-in-hand. We often hear audit firms and platforms claiming it will take you *insert unrealistic expectation* to achieve SOC 2.

The timeline

We spent 80 hours on our own SOC 2. That's not including time spent on related activities that weren't performed specifically for compliance, e.g. implementing our infrastructure security and employee performance review process. That 80 hours could theoretically be done in a week or two, but there are practical reasons it doesn't work like that.

1. Compliance is never the top business priority. It often takes a back seat, which slows progress.

2. It touches many different business activities, often with multiple people and lead times involved.

3. The audits require back and forth. Even with our agile and collaborative audits to optimise this, it's dependent on your team providing the right evidence and clarifications.

4. Your compliance implementation is the best opportunity to get things set up right. You may be able to box-tick for the sake of compliance, but a little extra time goes a long way for real business benefits AND ensuring it will actually pass the audit.

We spent 80 hours over 3 months, after some initial planning and "starting it" 3 months earlier. The median timeframe we see for our clients is 3 months; range 3 weeks to 18 months. Sure you can do it in a week if you don't sleep, make it the top priority, and forgo the opportunity to get real benefits from it, but we don't recommend that!

The steps

The steps below were traditionally performed sequentially. In modern compliance they are often all going on in parallel; that's the purpose of our agile and collaborative audit process that gives more timely feedback, end-to-end guidance, and all stakeholders a clear view of progress. These steps to consider are:

1. **Planning**: Which standards will you target? Which audit firm will you use? Will you use a compliance platform? What resources are required? What timeline will you target?

2. **Readiness Assessment**: You can use a compliance platform like Drata, or a free tool like our readiness assessment software, to see where you do and don't comply with your chosen standards.

3. **Implementation**: You put in place the necessary activities to meet the compliance standards

(ie. close any gaps), and ensure you can prove those to your auditor.

4 **Evidence Gathering**: You collect and provide the evidence of those activities for your auditor to independently verify.

5 **Audit**: The auditor reviews and provides feedback, asks additional questions, and ultimately signs off on your compliance.

6 **Reporting**: The report (SOC 2) or certification (ISO 27001) is issued to share with your customers.

7 **Maintenance**: You manage your compliance activities in business-as-usual, until the next audit, or as part of a continuous audit process that follows.

What's involved?

The activities covered for your compliance can vary greatly. That's a good thing; although it can make it harder to understand compliance and what's required, it means you can do things in a way that makes sense for your company with optionality of which activities you do and don't want to perform. This is where some companies opt for the generic strategy to compliance, covered earlier, to keep it simpler and take out the guesswork.

Compliance activities include the following types:

Systematic controls (10-35%)

Systematically configured functions are tested with automation or screen shots. These include:

- **Infrastructure (e.g. AWS):** Encryption, firewalls, system monitoring and logging.
- **Enterprise software (e.g. Google Workspace):** Tracking your people, information assets, and enforcing MFA for logins.
- **Code repository:** Restricting access, enforcing peer reviews, and oversight of the code changes for software development.
- **Mobile device manager:** Enforced policies on user devices like operating system updates, anti-virus software, device firewalls and encryption, screen timeout.

Policies, procedures and plans (20-35%)

Documented responsibilities, business requirements and the design of processes and plans that support your compliance requirements.

Event-driven activities (15-30%)

When events occur, managing those events in accordance with defined policies, procedures and plans. For example, when new joiners are onboarded: conducting background checks, employment contracts, and security awareness training. This also includes when incidents occur, changes are released, vulnerabilities are identified, and assets are disposed of, to ensure they are managed effectively.

Periodic meetings and reviews (20-30%)

Board and management meetings, risk assessments, and vendor governance reviews are conducted periodically (quarterly, annually) to maintain oversight of the organisation. There are also penetration tests, business continuity and disaster recovery exercises, and other periodic tests to check the compliance activities are effective.

Other ad-hoc items (~10%)

This category is here for completeness. There are a few things that may not fall into the above, like having a documented architecture diagram, customer contracts or terms of service, and cyber insurance.

Case Study: Communic8 Group

Communic8 offers the latest innovation in digital engagement that's providing organisations a better way to connect, inspire, analyse and align employees and customers. Communic8 services the communication needs of many of the world's largest enterprise organisations. With that level of service, clients expect that their data is securely managed and require the assurance accordingly.

Communic8's CEO, Bryon Westmoreland, shares their insights from achieving both SOC 2 Type 1 and SOC 2 Type 2 in a 9-month period:

"Set expectations and the correct mindset with your team from the very beginning. Make your team aware that this process adds value to the organisation, and ultimately, will make their job easier (and help them sleep at night).

Delegate tasks to people within your organisation who are most knowledgeable or responsible for the particular control and set reasonable expectations and offer support.

Google Drive can quickly become the wild west of documentation. Develop an information management strategy and stick to it. Establish procedures around the retention and clean-up of documents, versioning, file, and folder nomenclature.

We found that simple, shared calendar entries were most helpful in linking to documentation or resources that were being reviewed or executed and invited the individuals that were needed for the review."

About

assurancelab

AssuranceLab is your modern cybersecurity audit partner. Unlock new opportunities and power your international growth with trust.

We have developed a modern, cloud-native approach to efficiently carrying out cybersecurity audits in your business. While you can always opt for one-off audit engagements as needed, we also offer monthly compliance packages that empower you to create a culture of trust and continuous, incremental improvement across your operations.

We've spent the last five years developing and validating our innovative approach with trailblazing startups that needed to invest in trust to go further. In working with us they've unlocked new growth potential – and they've actually enjoyed the process.

We're the auditors you wouldn't cross the street to avoid!

Our clients use security and compliance accreditations to:

Win large customers to grow revenue

Satisfy customer and regulator requirements

Improve security practices

Achieve operational excellence

Build trust and protect your brand

w www.assurancelab.com.au

e info@assurancelab.com.au

ABN: 25 633 120 108