Security & Compliance

Complete CXO Guide

assurance LAB

Why standards?

Enterprise security and compliance requirements are snowballing from rising security threats, increasing public expectations and the explosion of digital and data-driven cloud services used by enterprise.

The only way to solve these requirements at scale is through assurance standards. Standards provide a consistent approach to verifying your security and compliance. Through an audit report or certification, you can prove to your current and potential customers that you meet the specified requirements.

When you demonstrate your compliance to industry standards, it makes it easier for enterprises to onboard your product and service. This reduces due diligence questionnaires, shortens your sales cycle and gives confidence to all stakeholders involved that it’s worth the time investment pursuing the deal.

The two leading standards; SOC 2 and ISO 27001, are often non-negotiable requirements of large enterprises. These can take several months, which may result in lost opportunities if you haven’t taken steps towards achieving them.

Which standards are right for your business?
There are several factors that should be considered when determining which standards are right for your business; these are:

- Industry
- Geography
- Purpose

These factors have been mapped against the different information security standards (see next page) and should be considered along with your client’s needs and requirements.

Information Security Standards

				Examples		
Standard	Industry	Geography	Purpose	Data Zoo	Atlassian	AWS
SOC 1	Finance	Global	Satisfying financial auditor requirements (eg. Sarbanes Oxley)	✖	✖	✅
SOC 2	Technology	Global	The most commonly accepted assurance standard	✅	✅	✅
SOC 3	Technology	Global	A published and redacted version of the SOC 2 report	✖	✖	✅
ISO 27001	All	Global	A standard for implementing information security	✅	✅	✅
ISO 27018	All	Global	A standard for implementing privacy practices	✖	✅	✅
HIPAA	Healthcare	US	A regulation for protecting private healthcare information	✖	✅	✅
HITRUST	Healthcare	US	Information risk management and compliance standard	✖	✖	✅
GDPR	All	Europe	Privacy regulation for EU residents	✅	✅	✖
CCPA	All	California	Privacy regulation for Californian residents	✅	✅	✖
PCI-DSS	Finance	Global	Data security for payment card information	✅	✅	✅
CDR	Finance	Australia	Accredited data recipient under the consumer data right act	✅	✖	✖
IRAP	Government	Australia	Stringent security standard for Australian government	✖	✖	✅
FedRAMP	Government	US	Stringent security standard for US government	✖	✖	✅
CSA STAR	Technology	Global	The Cloud Security Alliance (CSA) has the Security, Trust, and Risk (STAR) accreditations and register to track three levels of compliance with the cloud controls matrix (CCM).	✅	✅	✅
ESG	Sustainability	Global	Sustainability reporting (ESG) demonstrates your impacts to positively differentiate your company	✅	✖	✖

Sales playbook

How to use your assurance standards

Your certifications and assurance reports are as meaningful as the way you use them. It's common for enterprises to have limited knowledge of what each standard actually covers with respect to their security and compliance.

Here are a few ways to get the most value from your certifications:

1. **Put the logos on your website and in RFPs.** **Atlassian** and **AWS** are good examples and easy to find when searching to qualify their credentials.
2. **Notify your existing customers.** It's like releasing a new feature that helps third-party risk and security teams manage their requirements.
3. **Brief your sales and marketing team.** Communicating these achievements helps qualify your product to target customers.
4. **Post to your socials.** Aside from the real operational benefits of meeting good practice standards, it also demonstrates your security commitment to your customers.

How to respond to requests for standards

If you haven't achieved any of these information security standards, responding in the right way is especially important. If you simply say "no", it may raise further questions. These standards are often mandated by large enterprises, especially in regulated industries and the more mature US and UK markets. It may be a red flag if your sales narrative talks about other enterprise customers you serve but then your response here doesn't align to that.

Our recommendation is to conduct an initial gap assessment of the standards that are relevant to your geography and industry. AssuranceLab offers free readiness assessment software to make this easy. It's a one-hour exercise to prepare an automated output report with gap analysis. You can then say you have started working towards these standards. Often, this is enough to satisfy their initial due diligence requirements and may respond by saying their license agreement is conditional upon a certification or assurance report to follow in a reasonable timeframe (often 12-18 months).

Frequently asked questions

Will these standrds burden my business?

The most common concern we hear about compliance with these standards is the operating burden on your agile and high-growth business. It is true that these standards require a level of formality and maturity that may be beyond the way start-ups operate. These standards bridge the gap to what's expected and important to the enterprise customers you support. That doesn't mean you need to operate like a traditional enterprise though!

Principles-based standards like SOC 2 and GDPR are more flexible without prescribing "documentation heavy" approaches. They allow for the scope and nature of compliance activities to be based on the risk and what makes sense in practice. For smaller, simpler and cloud-native businesses, many of the security risks are less significant and easier to address with out-of-the-box features from your cloud provider. That makes SOC 2 a popular choice of standard for software-as-a-service in particular.

What are 'assurance' standards?

Assurance is the concept of providing third-party trust. Beyond just saying you meet a particular standard, you're able to prove it in a way that your customers and other stakeholders can rely on. That comes in various forms that are most commonly referred to as certifications. The SOC standards are actually "attestation reports" with an independent auditors' opinion. Regulations like GDPR and HIPAA do not have certifications but can be demonstrated in assurance reports with third-party cerification. There is subjectivity, complexities and judgement involved in every standard. Assurance is how end-users achieve the outcome they need, which is to know your information security has been verified by a qualified provider.

What steps are involved?

The following steps are performed for achieving and verifying information security standards:

1. **Assessment:** reviewing your current state to identify any gaps in what's required
2. **Remediation:** implementing additional practices to address the gaps
3. **Audit:** independent validation of your compliance
4. **Report:** issuing an assurance report or certification to verify your compliance to third-party stakeholders.

What is the timeline?

The timeline varies based on the information security standard(s) covered, the resources and priority you put into it. More flexible standards like SOC 2 can be achieved in as little as one month, with an average of three months. More prescribed standards like ISO 27001 and HITRUST have defined phases to complete sequentially that can take longer. ISO 27001 is typically a six-month engagement for the three phases through to initial certification. HITRUST, FedRAMP and IRAP are usually an 18–24 month program.

We often see a scramble to get these completed quickly when it's linked to a live sales opportunity or an overdue commitment to a customer. Allowing more time for the project can achieve better outcomes for your business by incrementally and more organically working towards a good fit of compliance that makes sense for your business.

Who is involved?

There are various models of responsibility for these projects. Often the Chief Technology or Operating Officer will be the accountable owner and delegate to others in their team and across the business as required. The best way to map this out is to conduct a readiness assessment to identify the individual areas, requirements and who is best placed for each. Some clients choose to have a project manager or compliance lead coordinate it all, while others will deal directly with individual area owners that are usually part of the management team (CXO, Head of).

What do I need to do as an Australian SaaS business?

As a tech company operating solely in Australia, it's generally acceptable to choose one standard to satisfy your customers - SOC 2 or ISO 27001. The exception is in financial services where SOC 1 or SOC 2 may be mandated on top of ISO 27001 to satisfy their regulatory obligations like APRA CPS 234.

If you are operating in Europe, ISO 27001 and GDPR will be expected or mandated. If you are operating in America, SOC 2 will be expected or mandated. There's industry specific requirements for healthcare in the US (HIPAA or HITRUST), for government (US - FedRAMP, AU - IRAP), payments (PCI-DSS), or participating as a Data Recipient in Australia requires CDR accreditation.

Which standard is best?

Each standard was created for different purposes and in the context of the requirements of their industry and geography. The two main global and cross-industry standards are SOC 2 and ISO 27001. SOC 2 is the most commonly accepted assurance standard for international tech providers like cloud software-as-a-service. ISO 27001 is the most widespread internationally in other industries. Most global software companies comply with at least one of these two standards, often both. Read more detail in our **SOC 2 vs. ISO 27001 article.**

Can I cover multiple standards in one project?

Yes! It's increasingly common to combine standards for time and cost savings. As a CPA firm we offer multi-framework audits through our tailored multi-framework audit approach. For example you can cover SOC 2 and ISO 27001 in the one audit.

What scope is covered by the standards

Different standards define the scope from different angles. The SOC family are focused on the services you provide to customers. The ISO family of standards are focused on business entities. The Consumer Data Right and privacy regulations like GDPR are focused on the scope and uses of the relevant data. Whichever method is the central focus, the following system components are considered as it relates to those:

- **Infrastructure:** the configuration and security of your cloud or on-premise infrastructure
- **Software:** in-house developed products and third-party software
- **Data:** the sensitive data collected, processed and stored
- **People:** your employees and contractors including endpoint devices
- **Processes**: the relevant business practices applying to the above components and compliance requirements.

What audit evidence is required?

There are a few types of controls and audit evidence:

- **Policies and processes:** documentation of the established business practices
- **Configurations:** system design features, settings and technical configurations
- **Actions:** steps and activities by your people related to the security and compliance areas

Most of the evidence we look for are in the form of screen shots, PDFs and Excel documents. Screenshots are becoming increasingly common for the automated system functions and where the audit evidence is automatically captured by the software you use. In some cases, our clients give us direct access to systems so we can capture what we need directly.

What software solves compliance?

Modern software solutions automate, simplify and provide 'out-of-the-box' solutions to information security compliance. It's best to set up a call with our team to talk about what products you already use and whether additional solutions are a good fit for your goals. There are platforms specifically designed for SOC, ISO, HIPAA and other frameworks like Drata. Your existing products in your cloud infrastructure, and other software products like Atlassian and Bamboo HR, have in-built features that support your compliance when configured or licensed accordingly.

Should we use templates?

One of the most painful parts of compliance, is documenting policies and processes. We often see clients choose to use templates to avoid "reinventing the wheel". This is particularly useful for more prescribed standards like ISO 27001 and HIPAA. Standards like SOC are more flexible. The downside to templates is they can create misinformation in your business, a culture of compliance being a standalone function, or just skipping past the important step of establishing the way your business should operate. We created **PolicyTree,** to help you generate tailored policies that are fit-for-purpose and make sense for your way of operating.

What does it cost?

There are three costs to consider when it comes to standards:

- The costs to achieve compliance
- The cost of your team's time
- The external auditor fees

The costs to achieve compliance can be low if you choose to manage it in-house without expensive consultants or software licensing. The cost of your team's time can be significant. That is why software, consultants and specialised auditors are worth the investment to save that time. The external auditor fees can vary a lot with different approaches, cost structures and ways of presenting the fees. It's worth asking firms to compare their fees to other providers that have quoted you, and to clarify what's included and what's not.

What role does AssuranceLab play?

AssuranceLab is an independent audit provider. We conduct the audits and are a CPA accredited firm allowing us to quality review and issue your certifications.

We cannot design or implement your policies or controls for you. We have a range of how-to guides and examples. We work closely with our clients to guide them on doing "enough" but also not "too much", through iterative feedback and collaboration. The target state for these compliance projects is finding the right business fit that doesn't overburden your business with compliance. Most clients see our team as a trusted partner to help them navigate security, compliance and a broader fit of operational practices aligned to their individual needs and objectives.

Get in touch with our friendly consultants for complimentary guidance on standards and to discuss options for solving your compliance goals.

assurance LAB

AUS HQ: 3/11 York Street, Sydney, NSW, 2000
US HQ: 1400 Lavaca Street, Suite 700 Austin, Texas 78701
E: info@assurancelab.com.au
W: assurancelab.cpa