Security frameworks / attestations and certifications: Which one is the right fit for your organization?

June 9, 2022 | Bindu Sundaresan

Perspective:

While there is an alphabet soup of compliance requirements and security standards frameworks, this post will focus on the two prevalent certifications frequently discussed for SaaS and B2B businesses. Security and compliance qualifications, like SOC 2 and ISO 27001, demonstrate that you apply good practices in your business. They are often classified as "security" and thought of as the technical security of your systems. However, they are broader, focusing on organizational practices supporting your security and other objectives. That includes availability (system resilience), the confidentiality of data, privacy for your users, integrity of the system processing objectives, scalable process design, and operational readiness to support significant business customers.

So, before we get into which one would you pick, how, and why, let's quickly get aligned on the key benefits of why these certifications and attestations are relevant from a business standpoint.

Background and benefits:

It helps establish brand trust and enable sales: Your customer's looking to use your software, consider your product, and your capabilities as an organization. These qualifications play an essential role in demonstrating your business is "enterprise-ready," providing a reliable service and keeping their data secure.

It helps demonstrate compliance and establish a baseline for risk management: These certifications often become mandates from procurement teams to demonstrate supply chain security. Or they can be used to demonstrate compliance with regulations and satisfy regulatory requirements.

It helps reduce overhead and time responding to due diligence questionnaires: A

Categories

alignment to standards. It provides peace of mind that you are improving your security posture, helps address compliance requirements, and strengthens your essential operational practices.

Which standard is best for these goals?

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

Below, we'll compare the two most common standards, SOC and ISO.

Often, we see that the SOC 2 reports are widely adopted and acknowledged. Many procurement and security departments may require a SOC 2 report before approving a SaaS vendor for use. If your business handles any customer data, getting a SOC 2 report will help show your customers and users that you seriously consider data security and protection. Healthcare, retail, financial services, SaaS, cloud storage, and computing companies are just some businesses that will benefit from SOC 2 compliance certification.

What is a SOC -2 certification?

SOC-2 is based on five Trust Service Criteria (TSC) principles.

Security - making sure that sensitive information and systems are protected from security risks and that all predefined security procedures are being followed

Availability - ensuring that all systems are available and minimizing downtime to protect sensitive data

Processing integrity - verifying data integrity during processing and before authorization

Confidentiality - allowing information access only to those approved and authorized to receive

Privacy - managing personal and private information with integrity and care

SOC 2 examinations were designed by the American Institute of Certified Public Accountants (AICPA) to help organizations protect their data and the privacy of their client's information. A SOC 2 assessment focuses on an organization's security controls related to overall services, operations, and cybersecurity compliance. SOC 2 examinations can be completed for organizations of various sizes and across different sectors.

Businesses that handle customer data proactively perform SOC 2 audits to ensure they meet all the criteria. Once an outside auditor performs a SOC 2 audit, the auditor will issue a SOC 2 certificate that shows the business complies with all the requirements if the business passes the audit. There are two types of SOC 2 audits: Type 1 and Type 2. The difference between

Categories

help organizations establish, implement, operate, monitor, review, maintain, and continually improve their information security management systems.

ISO 27001 details the specification for Information Security Management System (ISMS) to help organizations address people, processes, and technology about data security to protect the confidentiality, integrity, and availability of their information assets. The ISO 27001 framework is based on risk assessment and risk management, and compliance involves identifying information security risks and implementing appropriate security controls to mitigate them. It also includes 27017 and 27018 to demonstrate cloud security and privacy protections and /or do 27701 (privacy management system) as an extension to ISO 27001.

The intent of information protection – a common thread between both SOC and ISO 27001.

Both SOC 2 and ISO 27001 are similar in that they are designed to instill trust with clients that you are protecting their data. If you look at their principles, they each cover essential dimensions of securing information, such as confidentiality, integrity, and availability.

The good news from this comparison is that both frameworks are broadly recognized certifications that prove to clients that you take security seriously. The great news is that if you complete one certification, you are well along the path to achieving the other. These attestations and certifications are reputable and typically accepted by clients as proof that you have proper security. Suppose you sell to organizations in the United States. In that case, they will likely accept either SOC 2 or ISO 27001 as a third-party attestation to your InfoSec program. Both are equally "horizontal" in that most industries accept them.

There are several key differences between ISO 27001 vs. SOC 2, but the main difference is scope. ISO 27001 is to provide a framework for how organizations should manage their data and prove they have an entire working ISMS in place. In contrast, SOC 2 demonstrates that an organization has implemented essential data security controls.

Which one should you go with?

Whatever certification you decide to do first, the odds are as your business grows, you will eventually have to complete both certifications to meet the requirements of your global clientele. The encouraging news is that there are more accessible, faster, and more cost-effective methods to leverage your work in one certification to reduce the amount of work you need to do in subsequent certifications. We are suggesting that you explore compliance with a proactive mindset, as it will save you time and money in the long run.

Categories

Search our blogs

Featured resources

INSIGHTS REPORT

AT&T Cybersecurity Insights™ Report 2023: Edge Ecosystem

Learn more ⟶

SELF ASSESSMENT

Benchmark your cybersecurity maturity

Explore ⟶

From the Blog

Devin Morrissey
Oct 4, 2023

The role of automation in mitigating cybersecurity risks

View all AT&T Business Products ⟶

AT&T Business | AT&T Cybersecurity

Contact us

Categories

Who We Are

Alien Labs

Careers

Contact Us

News

Newsroom

Events

Blogs

Partners

Partner Programs

Partner Portal

Products

AT&T Managed Threat Detection and Response

USM Anywhere

XDR for MSSPs

Open Threat Exchange (OTX)

OSSIM

Solutions

Cloud Security Monitoring

View all AT&T Business Products ⟶

AT&T Business | AT&T Cybersecurity

Contact us

Categories

Vulnerability Assessment

See All Solutions

Resources

Resources

Blogs

Customer Reference Guide

Customer Success

Support & Services

Success Center

Documentation Center

Training

Certification

Contact us

Get price

Free tri