ISO 27001 certification: what startups need to know

Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), the ISO 27001 standard helps businesses organize their people, processes, and technology. ISO 20071 was designed to ensure the confidentiality, availability, and integrity of information.

Temps de lecture : minute

13 June 2023

The focus of ISO 27001 standard is on a company's Information Security Management System (ISMS), which outlines how they've integrated information security into their business processes.

The ISO 27001 standard requires companies to identify information security risks to their system and the corresponding controls to address them. ISO 27001 comprises 114 controls divided into 14 categories.

There is no requirement to implement the full list of ISO 27001's controls. The ISO 27001 controls represent the possibilities for an organization to consider based on its particular needs.

A primary goal of ISO 27001—as well as other compliance certifications such as SOC 2—is to prove to your clients and customers that security is a top priority.

ISO 27001 is considered the global gold standard for ensuring the security of information and data. *Obtaining an ISO 27001 certification* can help an organization prove its security practices to potential customers worldwide.

Who needs ISO 27001 certification?

To decide whether you need an ISO 27001 certification, first consider the regions in which your company does business: are you primarily working in North America? Are you working internationally or planning to expand your operations?

SOC 2 is a well-known US security standard and has become a common business practice. If your company only performs business with US-based customers, ISO 27001 certification may not be necessary.

If your company focuses much of its work outside of North America, ISO certification may be needed. Additionally, if your clients and prospects have sought proof of your company’s security against an internationally accepted standard, then ISO 27001 certification may also be important.

Your buyers are your best source of information to help you decide which standard to pursue and if ISO 27001 certification is needed. If customers or prospects are requesting an ISO 27001 certification, then your next steps are clear.

If a SOC 2 meets the requirements of your customer in tandem with your own company’s security and compliance needs, you’ll move forward with a SOC 2 instead of an ISO 27001 certification.

Many companies decide they eventually need both a SOC 2 and an ISO 27001 certification based on the demands of their growing customer base. At first, your company may consider a SOC 2 and later pursue ISO 27001 as your business expands.

ISO 27001 certification process and

requirements overview

The 27001 certification process involves:

Scoping and effectively implementing an Information Security Management System (ISMS)

- Establishing an ISMS governing body composed of senior management and key stakeholders from throughout the company
- Performing an internal audit to assess the organization’s ISMS and its implementation
- Undergoing an ISO audit with an external third-party auditor

The internal audit is one of the best ways to ensure that your organization’s ISMS is operating effectively and in alignment with the ISO 27001 standard.

The internal audit is required under the ISO 27001 standard and internal auditors must be objective and impartial. In order to make sure your ISO 27001 certification is up to industry standards, auditors should not be responsible for implementing, operating, or monitoring any of the controls under audit.

Once the internal audit is complete, results should be shared with the company’s ISMS governing body and senior management to address any issues before proceeding to the next step of the ISO 27001 certification process—the external audit.

The external audit is composed of two stages. Stage 1 Audit consists of an extensive documentation review, during which an external ISO 27001 auditor reviews an organization’s policies and procedures to ensure they meet the requirements of the ISO standard and the organization’s ISMS.

Stage 2 Audit consists of the auditor performing tests to ensure that an

organization’s ISMS was properly designed and implemented and is functioning appropriately.

An ISO 27001 certification is valid for three years, however, ISO requires that surveillance audits be performed each year to ensure that the ISMS and its implemented controls continue to operate effectively. This means that every 12 months during the 3-year cycle, an organization’s ISMS must undergo an ISO 27001 external audit, where an auditor will assess portions of the ISMS.

Who benefits from ISO 27001 compliance?

ISO 27001 compliance offers a win-win-win situation: it benefits you, your staff, and your customers in various ways.

The ISO 27001 certification benefits for your business include:

- Positioning your business as a stronger competitor so you can win more customers
- Protection for your intellectual property, brand, and professional reputation
- Retaining more of your customers
- Time savings and cost savings due to having more efficient processes
- Better security against a data breach and the associated costs like investigative costs and lawsuits
- Adherence to security and privacy regulations like GDPR and HIPAA, allowing you to avoid penalties
- Ability to attract stronger, more security-minded staff

When your business is ISO 27001 compliant, it offers certain benefits to your staff too, such as:

- More efficient operations leading to fewer avoidable frustrations

- Comfort of working in a stable company that is at lower risk for financial devastation
- Clear and predictable policies and procedures

The biggest winners of all, though, may be your customers, who stand to gain several benefits from your ISO 27001 compliance:

- Assurance that their data will be managed safely and securely
- Lower risk of their data and their end users' data being exposed in a data breach
- More streamlined onboarding when they sign on with you as a vendor

Next steps

Vanta's trust management platform automates up to 90% of the work for SOC 2, ISO 27001, GDPR, HIPAA, and more — getting you audit-ready in weeks and saving you significant costs (up to 85%!).

Vanta helps you build a list of controls tailored to your company, then connects to your company's software, admin, and security systems to continuously monitor your systems and services.

Download the *free ISO 27001 Compliance Checklist* from Vanta to get started, and *watch the on-demand demo* to learn more about how Vanta can get you audit-ready in just weeks.

Article by Maddyness, with Vanta