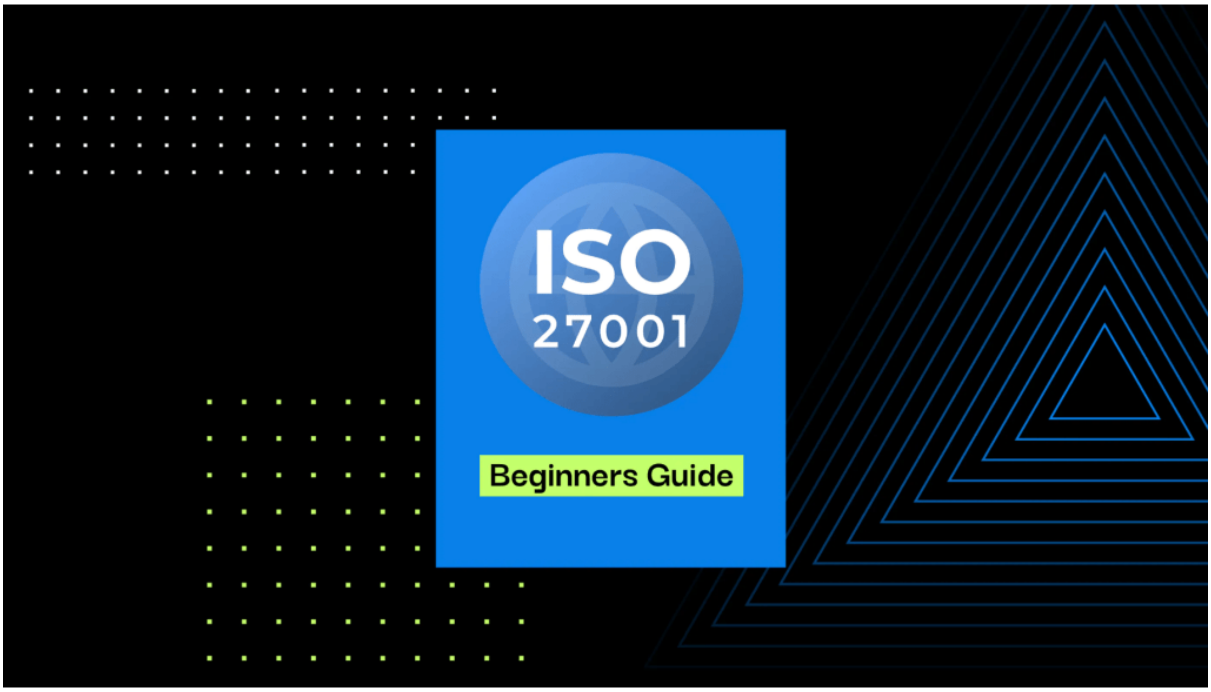
What Is ISO 27001? A Beginner’s Guide

By Ishaq Firdaus from Paireds.com



The effect of implementing of personal data protection law which was inaugurated on 17 October 2022 regulates directly for companies that access, store and manage sensitive data to immediately implement ISO 27001

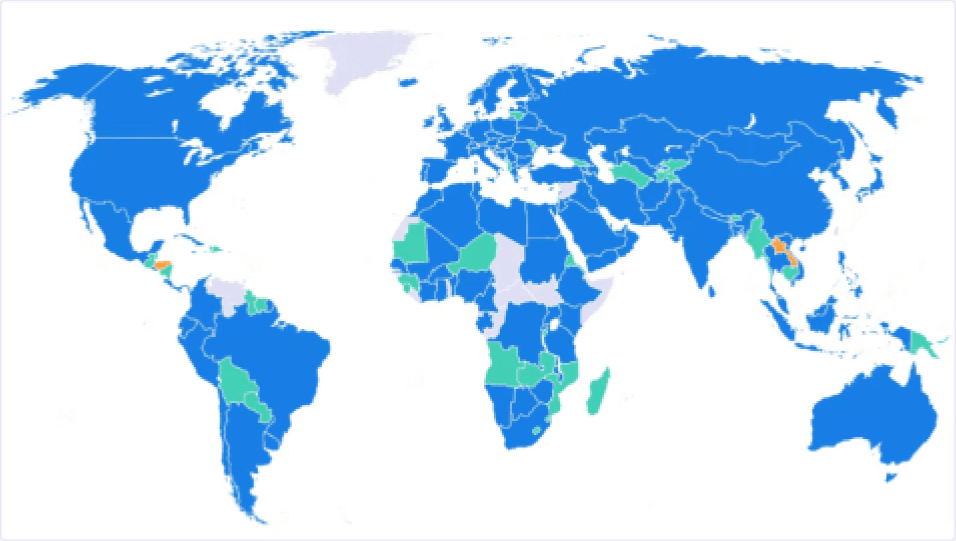
So, what exactly is ISO 27001 certification? And how can ISO 27001 protect your organization from data breach threats?

ISO 27001 is a security framework created by the ISO (International Organization for Standardization) institution that assesses a company’s ability to keep its data secure. To achieve certification, companies must complete an audit to verify that they comply with the stringent ISO 27001 standards.

Perhaps you have heard the term “building a proper company”? Actually, with the implementation of ISO 27001 you have built a proper company based on agreed international standards.

This article will thoroughly examine the meaning of ISO, its length and benefits, its goals and process as well as the detailed cost and work timeline.

Introduction



A map of standards bodies who are ISO members as of February 2015 Key:

- 🟦 Members
- 🟩 Correspondent members
- 🟧 Subscriber members
- ⬜ Other places with an ISO 3166-1 code who are not members of ISO

1. What is ISO and ISO 27001 stands for?

ISO stands for “International Organization for Standardization”.

ISO is a global entity founded in 1946. Delegates from 25 countries come together to ensure that national boundaries do not interfere with humanity’s ability to develop reliable technology.

Today, ISO brings together the standardization boards of 166 countries and reports to the central government in Switzerland. and regulates almost all standardization of industrial activities, companies from the smallest scope to life-related security and data protection.

If in terms of IT security, ISO 27001 certification is one of the most respected international standards. The full name of ISO 27001 is “ISO/IEC 27001:2013” and it was revised in 2017 and 2022 in collaboration with another certification body called the International Electrotechnical Commission (IEC).

2. What is the benefits of ISO 27001?

Benefits of ISO 27001 certification
Protect customer data
Comply with laws and regulations
Improve overall security posture and business processes
Avoid costly data breaches
Send positive signals to investors & shareholders
Enhance brand reputation & win new customers

The ISO 27001 framework is useful for determining whether an organization has established an Information Security Management System (ISMS) capable of protecting sensitive data.

The Information Security Management System (ISMS) is useful for more than just managing the hardware and software used to maintain information security. The ISMS also regulates a whole set of rules about how you use information, how you store and retrieve it, how you assess and reduce risk, and how you can continuously improve data security in the future.

If an independent auditor verifies that your company’s ISMS meets the standards, you will receive an ISO 27001 certificate.

Once you get ISO 27001 certified, you will have access to clients or partners who were previously hesitant to work with you. You will show all your customers that you take their personal information seriously. ISO 27001 can also help your organization comply with other regulations such as the GDPR (although adopting ISO does not mean you are inherently GDPR compliant).

But most importantly, you will have a system that you and all your partners can trust and you will make TRUST your main competitive advantage.

Following are some of the advantages and benefits of having ISO 27001 certification:

- **Gain the advantage of entry into competitive markets, especially internationally**
- **Have an advantage in seeking agreements against competitors who do not meet ISO 27001 requirements**
- **Speed up the sales cycle by eliminating the doubts about security and compliance requirements that potential clients often question**
- **Able sell to large companies (fortune 500) because they have gained the trust of ISO 27001**
- **Strengthen customer trust by proving that your services are safe. A certified ISMS offers solid assurance about your overall security posture**
- **Laying the foundation for a strong ISMS that strengthens security and business processes**
- **Build a proper company safety and compliance culture**
- **Create a framework for managing security risks across the enterprise**
- **Increase the trust of investors and partners**
- **Streamlining the due diligence process by potential buyers or investors**

What is the purpose of ISO 27001 certification? Is ISO 27001 Mandatory?

1. The purpose of ISO 27001

ISO organization created ISO 27001 to counter increasingly sophisticated cyber-attacks against information systems. To protect sensitive personal data, companies need to adhere to a strict set of security standards.

Emerging information security regulations have also fueled the adoption of ISO 27001. Laws such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union and the Personal Data Protection Act in Indonesia which also enforces strict penalties for preventable data breaches.

Those who do not comply also face very high penalty fees. For example In July 2019, British Airways was fined £183 million for failing to prevent a phishing attack using a fake version of its website. Marriott hotels were fined £100 million just two days later after hackers stole sensitive data from improperly secured guest records.

2. Is ISO 27001 Mandatory?

The short answer is no, but following government regulations is mandatory

Even though the government does not require all companies to undergo an ISO 27001 audit, most IT companies registered with PSE Kominfo in Indonesia (or similar compliance in other country) are required to implement ISO 27001, and also the easiest way for us to comply with other laws such as the PDP Law is to implement ISO 27001

On the other hand, if your business model relies on providing IT services to other companies, you may find that many clients do not want to work with you if you do not have ISO 27001 certification, this is also the reason that implementing ISO 27001 is mandatory.

However, many companies that understand the importance of ISO 27001 still do not get certified because they are worried about the complexity of the ISO 27001 certification process.

If you’re still unsure, keep reading to learn exactly what ISO certification requires for information security.

How long does it take to get ISO 27001 certification?

The answer to this question really depends on the size of your company and the complexity of your data and sector, IT companies in the e-commerce sector are of course different from finance, companies with 10 employees are of course different from 100 and so on.

But as an illustration, an MSME company can be expected to be ready to be audited in an average of four months, then go through the audit process in six months. Larger organizations may need a year or more.

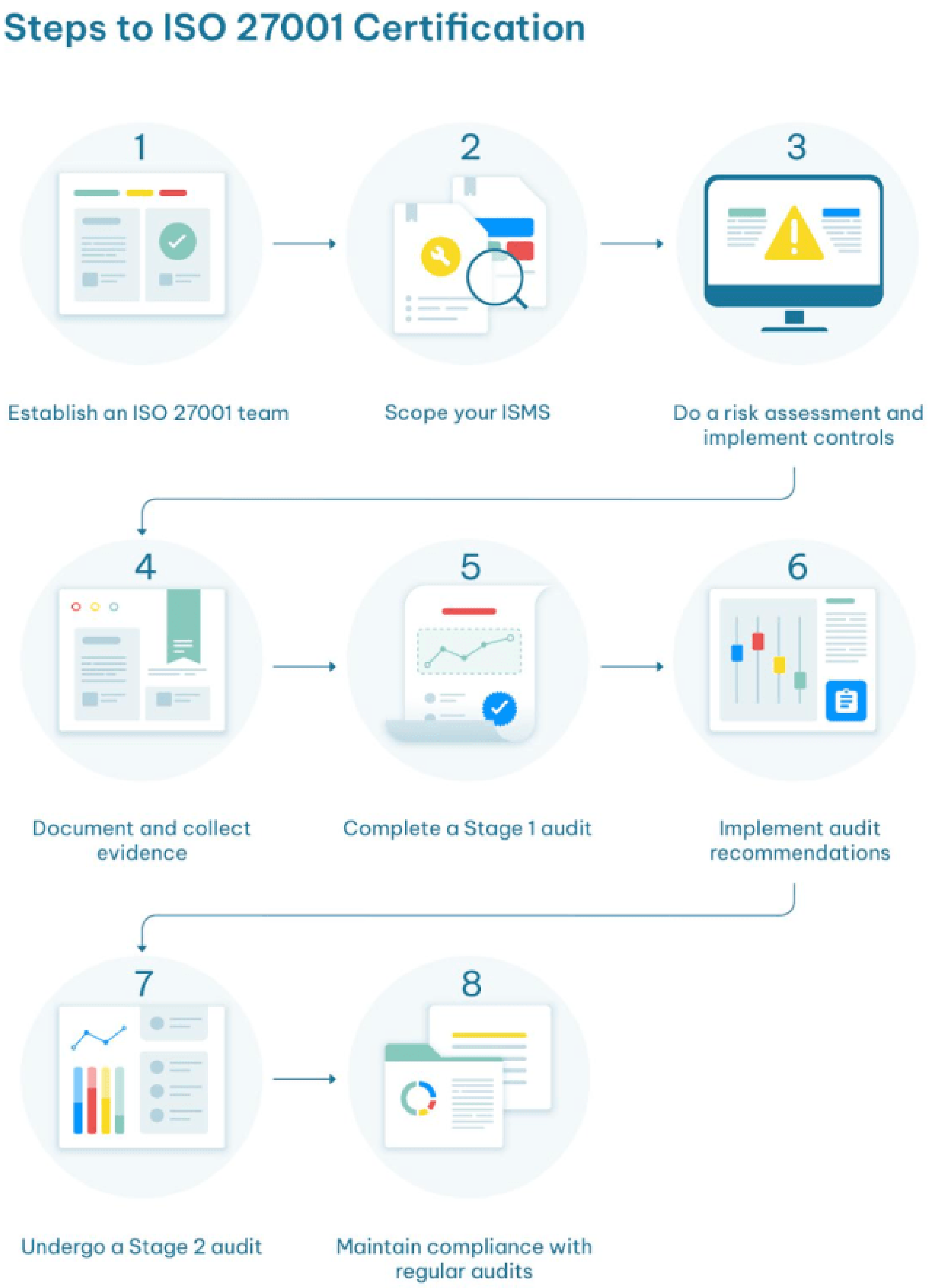
The four months of preparation for the audit typically involve scoping your ISMS, conducting a risk assessment and gap analysis, designing documents and implementing implementation controls, training staff, and preparing evidence documentation.

The six-month certification audit is divided into two phases. During the Stage 1 audit, the auditor reviews the ISMS documentation to ensure policies and procedures are properly designed. They can also provide suggestions on how the organization can improve its ISMS to make it more secure.

During the Stage 2 audit, the auditor reviews business processes and controls to ensure compliance with the requirements of ISMS and Annex A of ISO 27001.

The ISO 27001 certification process

The ISO 27001 certification journey will take you through the following steps:


Steps to ISO 27001 Certification
1
Establish an ISO 27001 team
2
Scope your ISMS
3
Do a risk assessment and implement controls
4
Document and collect evidence
5
Complete a Stage 1 audit
6
Implement audit recommendations
7
Undergo a Stage 2 audit
8
Maintain compliance with regular audits

1. Preparation Phase

In this phase, preceded by an implementation kick off activity, the consultant (if using a consultant) together with the company's main management team performs:

a. Creating an ISO 27001 team

Designate a member of your staff to be in charge of the certification process.

The ISO 27001 team will define the scope of your ISMS, establish processes for documenting it, get support from senior management, and work directly with auditors and consultants, among other tasks.

b. ISO 27001 Introduction Training

This training is a basic training required for all personnel. Trading materials include:

- **Introduction of ISO as a management system**
- **Application of information security management system principles according to ISO 27001:2013 version**
- **Introduction to how to implement an integrated system ISO 27001:2013**
- **Introduction to the requirements needed to implement an ISO 27001:2013 management system**

c. Gap Assessment

Gap Assessment Is an activity to compare the requirements needed in implementing ISO 27001: 2013 with the actual and actual conditions that have been implemented in the company by conducting interviews and collecting actual company data and documents.

2. Development Phase

This phase is the development phase of the management system and the necessary tools in the form of standard documents, studies and forms. ISO 27001 requires companies to document active and ongoing efforts to identify and mitigate threats.

Document development is useful for fulfilling the requirements of the standards to be applied, as well as fulfilling the business development and processes at the ISMS company based on the results of the gap analysis that has been carried out during the preparation process.

At this stage the Documentation process can be a painstaking job without the help of automation, so it's better to start early. Undergo an internal audit as a dress rehearsal for the real thing.

During this phase, your ISO 27001 team should educate your general staff about information security, your ISMS, and specifically ISO 27001 certification. By getting your entire staff to work together, you greatly reduce the chances of leaving gaps unaddressed in your ISMS.

3. Implementation Phase

This phase is a trial phase of the system that has been tried to be developed in the previous phase. In this phase, SMKI companies at all levels will apply work standards and programs that have been announced and make the necessary improvements to achieve the goals that have been set.

4. Internal Audit and Remediation Phase

In this phase, it has taken 2-3 months to undergo the preparation process for the previous phases and the ISO 27001 success team together with all components such as consultants, employees carry out activities including the following:

a. Internal Audit Training

This training is intended for the ISO 27001 success team appointed by the ISMS company as an internal auditor with the aim of

- **As one of the prerequisites for ISO 27001:2013 management standards**
- **As a means of obtaining the necessary information and methods for auditors to carry out the audit process internally**

The material that will be presented in the internal audit training includes:

- **Further understanding of the requirements of the ISO 27001:2013 standard**
- **Understanding of internal audit methods correctly**

This training will at least be conducted for a maximum of 1 (one) day interspersed with other workshops related to the internal audit process.

b. Internal Audit

This stage is an evaluation stage of the system that has been implemented by the company for some time by the auditors selected through previous internal audit training with the aim of:

- **Knowing the weaknesses and strengths possessed by the company from the system that has tried to be implemented**
- **Knowing the potential improvements needed to perfect the system that has been implemented**
- **As one of the mandatory requirements of the implemented management system**

c. Management Review

Management review is one of the activities of the standard to be applied. This management review activity is in the form of a meeting attended by representatives of departments and management which discuss the results of the implementation of the management system with a specific agenda according to standard requirements.

d. Remediation

Improvements were made by referring to the findings of the internal audit results, and the results of discussions at the management review meeting. Improvements are needed in order to improve the management system that has been implemented and at the same time as a means to prepare for certification

5. Stage 1 Audit and Remediation

This phase. It has been about four months now, and you are finally ready to invite an external auditor to review your ISMS. Your ISO 27001 auditor will be from a certification body with ISO accreditation.

At this stage the accreditation auditor will carry out an initial check of the completeness of the documents required during the stage 2 audit. After carrying out the stage 1 audit process, make improvements to all aspects of your ISMS marked by the auditor for improvement and improvement so that in the stage 2 audit the process will run smoothly.

6. Stage 2 Audit and Certification

This time your auditor will check how your information security functions. Their goal is to see if you practice all the rules regarding your Information Security Management System (ISMS).

After a successful Stage 2 audit, you will receive ISO 27001 certification, which is valid for three years.

7. Maintenance and Surveillance 1&2 Phase

After obtaining ISO 27001 certification, make a regular internal audit plan. ISO 27001 requires organizations to conduct an annual “surveillance audit” to ensure their commitment to the appropriate ISMS has not expired.

At the end of the third year, you can complete a recertification audit to maintain your ISO 27001 certification for another three years.

Each company’s path to ISO 27001 certification can be slightly different. Some may choose to hire a consultant or opt for penetration testing over vulnerability scanning. But this overview should give you an idea of the ISO 27001 certification steps and why the process can take up to 12 months.

8. Recertification Audit

The recertification audit occurs during the year of ISO 27001 certificate expiration. Similar to Stage 2, this audit evaluates the evidence to prove your ISMS and controls are effective, and that they meet the ISO 27001 requirements. Passing a recertification audit will renew the ISO 27001 certification period for the next 3 years.

How much does ISO 27001 certification cost?

ISO 27001 audit fees can vary widely depending on the size and scope of your company and your information security management system.

The biggest cost associated with ISO 27001 compliance is that you have to remove employees from other projects or hire new ones. You will also have to pay for the security training materials and the audit itself.

In total, the average company can expect to pay between USD $10.000 to USD $50.000 this fee includes pre-certification preparation, for the certification audit itself, and another USD $5k-10k per year for maintenance and supervision audits after obtaining certification, but these costs do not include the required software tools and the salaries of ISO 27001 special internal team employees

Conclusion

ISO 27001 may seem daunting at first, but its benefits far outweigh the effort.

To speed up your certification process, the compliance automation platform offered by Paireds can make the ISO 27001 certification process much faster and more economical, you can see an overview of the process yourself and monitor the progress of your process. Schedule a demo now to learn more.