SafetyCulture

A Comprehensive Guide to the ISO 27001

Table of Contents

- ➔ What is ISO 27001?
- ➔ Why is it Important?
- ➔ What are the Requirements of ISO 27001?
- ➔ Preparing for ISO 27001 Certification in 7 Steps
- ➔ FAQs About ISO 27001
- ➔ How can iAuditor Help Your Organization get Certified?

A Comprehensive Guide to the ISO 27001

What is ISO 27001?

ISO 27001 is an international standard that sets a framework for ISMS or Information Security Management System in the context of the organization. The international standard for ISMS that companies can get certified for, ISO 27001 is officially known as ISO/IEC 27001:2013 and it was created by a committee composed of experts from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

ISO 27001:2013 is not to be confused with ISO/IEC 27000:2018, another ISO/IEC 27000 standard, which intends to define the common terminologies used in the ISMS body of standards.

Why is it Important?

ISO 27001 is important because it sets a benchmark for the kind of ISMS framework that businesses or organizations can implement and fine-tune according to their needs. It sets a minimum standard for information security management system that can be expected of any business, regardless of size, industry, or location, that seeks to be recognized as having a robust ISMS.

A Comprehensive Guide to the ISO 27001

What are the Requirements of ISO 27001?

One of the advantages of implementing ISO 27001 is that it requires proof that existing processes contribute to keeping information secure and that the unique needs of the business in maintaining a strong ISMS are taken into account.

Below are outlined clauses 4.1 through 10.2 which are the core requirements of ISO 27001. They help discover process gaps and assess the readiness of an organization for the ISO 27001 certification.

- **4. Context of the Organization**
  - 4.1 Understanding the organization and its context
  - 4.2 Understanding the needs and expectations of interested parties
  - 4.3 Determining the scope of the information security management system
  - 4.4 Information security management system
- **5. Leadership**
  - 5.1 Leadership and commitment
  - 5.2 Policy
  - 5.3 Organizational roles, responsibilities, and authorities
- **6. Planning**
  - 6.1 Actions to address risks and opportunities
  - 6.2 Information security objectives and plans to achieve them
- **7. Support**
  - 7.1 Resources
  - 7.2 Competence
  - 7.3 Awareness
  - 7.4 Communication
  - 7.5 Documented information
- **8. Operation**
  - 8.1 Operational planning and control
  - 8.2 Information security risk assessment
  - 8.3 Information security risk treatment
- **9. Performance Evaluation**
  - 9.1 Monitoring, measurement, analysis, and evaluation
  - 9.2 Internal audit
  - 9.3 Management review
- **10. Improvement**
  - 10.1 Nonconformity and corrective action
  - 10.2 Continual improvement

A Comprehensive Guide to the ISO 27001

Preparing for ISO 27001 Certification in 7 Steps

It takes a lot of time and effort to properly implement an effective ISMS and more so to get it ISO 27001-certified. Here are some steps to take for implementing an ISMS that is ready for certification:

1. **Review processes and ISO 27001** – Familiarize staff with the international standard for ISMS and know how your organization currently manages information security and information systems.
2. **Get employee buy-in** – Help employees understand the importance of ISMS and get their commitment to help improve the system.
3. **Conduct risk assessments** – Determine the vulnerabilities and threats to your organization's information security system and assets by conducting regular information security risk assessments and using an iso 27001 risk assessment template.
4. **Implement controls** – Information or network security risks discovered during risk assessments can lead to costly incidents if not addressed promptly.
5. **Conduct gap analysis** – Use an ISO 27001 audit checklist to assess updated business processes and new controls implemented to determine other gaps that require corrective action.
6. **Do internal audits and employee training** – Regular internal ISO 27001 audits can help proactively catch non-compliance and aid in continuously improving information security management. Information gathered from internal audits can be used for employee training and for reinforcing best practices.
7. **Contact your auditor for certification** – Prepare your ISMS documentation and contact a reliable third-party auditor to get certified for ISO 27001.

A Comprehensive Guide to the ISO 27001

FAQs About ISO 27001

Is ISO 27001 Mandatory?

ISO 27001 is not universally mandatory for compliance but instead, the organization is required to perform activities that inform their decision concerning the implementation of information security controls—management, operational, and physical. An example of such efforts is to assess the integrity of current authentication and password management, authorization and role management, and cryptography and key management conditions.

What are the principles of ISO 27001?

The ISO 27001 standard bases its framework on the Plan-Do-Check-Act (PDCA) methodology:

- Plan – set objectives and plan the organization of information security, and choose the appropriate security controls.
- Do – implement the plan.
- Check – monitor and measure the effectiveness of the plan against set objectives.
- Act – take action on identified nonconformities for continuous improvement.

What is ISMS?

ISMS is the systematic management of information in order to maintain its confidentiality, integrity, and availability to stakeholders. Getting certified for ISO 27001 means that an organization's ISMS is aligned with international standards. Even if certification is not the intention, an organization that complies with the ISO 27001 framework can benefit from the best practices of information security management.

How can iAuditor Help Your Organization get Certified?

iAuditor by SafetyCulture is used by industry leaders in order to align with international standards such as ISO 27001 and conform with applicable regulations.

iAuditor can help businesses prepare for ISO 27001 certification through the following:

- **Conduct internal audits** to discover process gaps using templates such as the ISO 27001:2013 checklist that users can customize to fit the needs of the organization
- **Capture areas for improvement** and efficiently record the corrective actions done in preparation for certification
- **Secure information** that is accessible only to authorized personnel via the cloud, a system that is already compliant with ISO 27001
- **Maintain compliance** with the standard through regular reviews of the current ISMS