The ultimate guide for your

ISO 27001 certification

Content

ISO 27001: what is it?

Today, it is unthinkable for a company to survive in the volatile and competitive global market without the use of information technology. Information technology is necessary for the swift and accurate processing and exchange of data within the context of business transactions. Consequently, information security has become a fundamental condition for business success. Managers and security professionals must adapt to this new situation and take appropriate measures to effectively identify, analyze, and manage risks, regardless of the sector in which their organization operates. Demonstrate that your organization has full control over the security of (confidential) information by obtaining an internationally recognized certification and a quality mark from DEKRA. This will boost the confidence of customers, business partners, and stakeholders.

What is ISO 27001?

ISO 27001 is an international standard covering information security implementation for organizations. It was published by the International Organization for Standardization (ISO) and is established as a globally recognized standard.

Who is ISO 27001 for?

ISO 27001 is suitable for organizations in any sector, as almost every company today uses confidential and privacy-sensitive information. This information is primarily found within IT systems nowadays, making adequate (IT) security of great importance. The requirements of ISO/IEC 27001 are therefore applicable to companies of any size in any sector.

The advantages of ISO 27001

ISO 27001 certification offers you numerous advantages:

- Identify and reduce threats to your organization;
- Manage business and liability risks;
- Keep confidential data and information secure;
- Ensure the trust of customers and business partners;
- Increase your competitiveness;
- Meet the requirements of your stakeholders.

What is information security?

Information security serves as preventive protection from damage and threats to an organization's data and information. With the help of proven technical and organizational measures defined in industry standards, weak points and security gaps can be identified and remedied appropriately. The three core objectives of information security are:

- **Confidentiality:** protection of confidential information against unauthorized access.
- **Integrity:** minimizing risks and ensuring the completeness and accuracy of data and information.
- **Availability:** ensuring reliability and usability for authorized access to information and information systems.

Prepare your organization for the five biggest threats

- Human errors, i.g., unintentional sharing of information, loss of hardware or documents with sensitive information;
- infection with malware via the internet;
- introduction of malware through removable storage devices, such as USB sticks and CDs;
- social engineering: techniques that (cyber)criminals use to entice people into revealing personal or business-sensitive information;
- disabling IT systems by cybercriminals offering so-called 'remote maintenance solutions'.

With an effective Information Security Management System (ISMS), your organization can identify weaknesses in the security of confidential information. You can then develop measures that offer protection against these and other cyber threats and test those measures in practice.

ISO 27001 in relation to **NIS2**

NIS and NIS2: cybersecurity of network and information systems

NIS and NIS2 set requirements for the cybersecurity of information and IT systems. NIS stands for network and information systems. This legislation applies to organizations that provide 'essential services,' such as healthcare institutions, telecom, and energy companies. The original directive dates back to 2016. With the introduction of NIS2 in 2023, more organizations are designated as providers of essential services. This includes, among others, food producers, postal and courier companies, and government services.

Organizations covered by NIS/NIS2 are required to identify risks in the area of cybersecurity within supplier relationships and the supply chain, and to implement adequate security measures for them.

ISO 27001

To meet the requirements of the NIS Directive, the ISO 27001 standard serves as a quality guideline. It helps you to shape your information security management system in a structured manner. DEKRA Audit is pleased to certify you against ISO 27001.

Online training ISO 27001

Gain immediate insights into the latest version of the standard.

The DEKRA ISO 27001:2022 training is an online course that is fully up-to-date with the latest version of the standard. The training is specifically designed for managers, security officers, consultants, and auditors who work with the standard. It helps you understand the ISO 27001 standard and teaches you how to take specific measures based on the standard to secure digital systems and information within your organization. After completing this online ISO 27001 training, you will know what is necessary to take measures for securing confidential information within your organization. Register for this training via the button below.

ISO 27001 training ›

Certification in 7 steps

Are you looking to maximize the effectiveness of your information security measures? DEKRA is here to help by conducting a comprehensive ISO 27001 audit of your information security management system. Our experienced auditors evaluate the processes and measures unique to your organization, ensuring you receive a customized ISO 27001 certification. Alongside our personalized approach, we follow a standardized procedure, guiding you through a 7-step certification process.

Our approach: **People Based Auditing**

What sets DEKRA apart? Our audit process uniquely prioritizes the human factor. With our extensive experience, we understand that it's the people within your organization who play a vital role in implementing processes, systems, and methods.

We call our approach **People Based Auditing**. This method has been highly valued by our certificate holders for many years and is now a standard part of every DEKRA audit. Aspects like behavior and employee awareness serve as critical starting points in the ISO 27001 certification process.

By taking this approach, we go beyond the standard norm to ensure your organizational culture truly aligns with your desired processes.

Behavior is the key determinant of success. With People Based Auditing, you gain valuable insights into this critical factor. This approach invigorates your information security management system, making it more effective and engaging for your organization and employees.

People Based Auditing in practice

During an ISO 27001 certification with our unique People Based Auditing method, you and your organization will benefit from:

- Auditors who take the time to deeply understand your organization, specific wishes, and needs
- A fixed point of contact throughout the entire process
- Comprehensive preparation for the certification process
- Enhanced awareness of service quality

ISO 27001 certification in **7 steps**

1 Introduction

We are happy to visit you or contact you via MS Teams or telephone. In the meeting, we discuss the ISO 27001 certification process. After this, you prepare your organization for the ISO 27001 audit.

2 On-site audit

Our auditors perform an on-site audit to assess and verify the functionality of your management system, ensuring it operates as documented. It's crucial for your organization to clearly demonstrate control over these processes. Should this control not be evident, a further evaluation of corrective measures may be required.

3 Report and evaluation

Our auditors will share the results of the audit with you in the form of an audit report.

4 ISO 27001 certification

Upon successful completion, you will receive your ISO 27001 certificate. The certificate is valid for a maximum of three years.

5 First follow-up audit

Within a year, we will conduct a follow-up audit in which we assess whether your management system is still operating in accordance with the standard.

6 Second follow-up audit

Approximately a year later, we will conduct a second follow-up audit. We will again assess whether your management system is operating according to the standard.

7 Recertification

In the third year following the ISO 27001 certification, we schedule an audit for recertification. Should the recertification be successfully completed with a positive result, the certificate will be renewed for another three-year period. After recertification, the annual audit cycle will continue.

☑ ISO 27001 **checklist**

With our checklist, you can quickly and easily find out whether your organization is properly prepared for certification as per ISO/IEC 27001 for an integrated information safety management system. The following questions are arranged according to the basic structure for management system standards.

If you can answer a question with yes, mark it with a check. That way you can see instantly which areas of your company already comply with the requirements, and which areas require more attention.

Context of the organization

- ☐ You have mapped out the structure of your organization (e.g., in the form of an organizational chart).
- ☐ You have defined the scope of your ISMS (Information Security Management System), particularly for stakeholders.
- ☐ You have drawn up a statement of applicability (SoA), which documents the decisions about implementation of measures, and the reasons for those decisions.
- ☐ You have conducted an environmental analysis for the integration of the ISMS within your organization.
- ☐ You have conducted a requirements analysis about the different interest groups (stakeholders).
- ☐ You have compiled an overview of all relevant legal, regulatory and contractual requirements that have an effect on your information safety strategy and the ISMS.

Management

- ☐ You have clearly defined and documented the business aims and requirements relating to the information safety policy within your organization.
- ☐ You have defined a concrete strategy for information security.
- ☐ You have defined your “top management”; this group is responsible for controlling the ISMS of the organization and decides how resources are deployed.
- ☐ You have implemented an information security policy.

Planning

- [ ] You have a documented risk assessment procedure.
- [ ] You have comprehensive documentation of the risk assessment process and the risk handling process/plan.
- [ ] All records and results from risk assessments and risk analyses are available to you.
- [ ] You have documented all records and results from risk handling.
- [ ] You have defined all the safety targets for your organization and stakeholders.

Support

- [ ] You have a strategy in place for handling documented information.
- [ ] You are able to provide the personnel and infrastructure required for the implementation and control of the ISMS.
- [ ] You have defined a procedure for internal and external communications.
- [ ] You have created documentation for the awareness and training concept regarding the ISMS.
- [ ] You have training documents for the ISMS and are able to provide proof that your employees have participated in relevant training.
- [ ] You have a communication plan or matrix for documenting all communications within the organization that relate to information safety.
- [ ] You have prepared detailed descriptions of the roles of employees to whom the ISMS applies (such as the information security board, the CISO, or the data security board) and can prove that you have verified their competencies.

Operation

- [ ] You have documentation about internal audit programs and audit results.
- [ ] You have comprehensive documentation on the measuring structure for all KPIs (key performance indicators), as well as on the measurement results and the resulting management reports for escalation.
- [ ] You have defined an Incident Response Plan (IRP) that includes current contact lists and escalation plans.
- [ ] You have verification that the ISMS processes were executed correctly, and that the ISMS is controlled and its performance measured.
- [ ] You have proof of the types of non-compliance, of all implemented reactive measures, and of the results of all corrective measures.
- [ ] You have an overview of the results of risk assessments (e.g., risk assessment reports, risk key figures) and risk handling (e.g., control test reports, penetration test reports).
- [ ] Your documentation comprises behavioral rules in the event of safety-relevant irregularities, process descriptions and work instructions for securing proof, and reports about information safety incidents.

Learn more about **ISO 27001**

Our experts are ready to guide you through the introduction of an ISO 27001-compliant information security management system. Request an informational conversation online, ask for a quote directly, or visit our website to learn more about ISO 27001 certification.

ISO 27001 quote ›

DEKRA Audit
Meander 1051
6825 MJ Arnhem
salesaudit.nl@dekra.com
+31 88 96 83016

About **DEKRA Audit**

Active. Diligent. Visionary. Whether you need more efficient business processes, more reliable products and systems for international market success or qualified auditors, DEKRA Audit has over a thousand specialists worldwide ready to provide you with comprehensive services.

Our services cover all aspects of quality and performance, safety and health, sustainability, and responsible business practices. Approximately 30,000 companies in over 50 countries rely on our certifications, tests, and inspections to achieve their objectives efficiently and seamlessly.

Learn more about us on **dekra.nl**

All audits and quality labels ›

Our method › | **All DEKRA services ›**

DEKRA Audit certifications and quality labels

We offer our clients certification services to the following standards (among others):

BORG
BRL 100
BRL 6000
BRL 6000-25
CO2 Performance Ladder
CO2 Reduction management
CSR Performance Ladder
Double-counting verification
Entry verification
Evacuation Alert System Certification
Fire Alarm Installations Regulations
HKZ certificate
ISCC Corsia
ISCC EU
ISCC Plus
ISAE 3000
ISAE 3402
ISO 14001
ISO 2000-1
ISO 45001
ISO 55001
ISO 9001
MedMij label
NEN-EN 15224
NEN 7510
NEN 8009
NTA8080
NVKL
Security Quality Mark
Social Enterprise Performance Ladder
SCIOS
Safety Culture Ladder
VCA company certificate