FAQ – Frequently Asked Questions About ISMS Certification According to ISO 27001

DEKRA
On the safe side.

If you would like to optimize information security in your company and obtain ISO/IEC 27001 certification but still have some questions on this topic, we have compiled frequently asked questions and answers for you here.

1. 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 has established itself as a globally recognized standard.

2. What is information security?

Information security serves as preventive protection from damage and threats to organizations' 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

3. What are the top 5 information security threats a company must be prepared for?

Infection with malware via the internet continues to top the list, followed by the introduction of malware via removable

media such as USB sticks or CDs. Human error and social engineering also constitute threats to your information security that should not be underestimated. Last but not least, attackers repeatedly succeed in crippling IT systems via remote maintenance access and thus obtain confidential information or data.

With an effective information security management system (ISMS) you enable your company to identify weak points and to derive and test measures designed to protect against these and other IT threats.

4. What is an ISMS?

The abbreviation ISMS stands for Information Security Management System. The ISMS defines rules, methods and measures to control, manage and ensure information security. An ISMS can be implemented in your company within the scope of certification according to ISO 27001 and checked for its effectiveness.

5. Why should I certify my company against ISO 27001?

ISO 27001 certification offers you numerous advantages:

- You minimize your company and liability risks
- You reduce your costs
- You identify and reduce threats to your business
- You protect your confidential data and information
- You secure the trust of customers and business partners
- You increase your competitiveness
- You meet the requirements of auditors

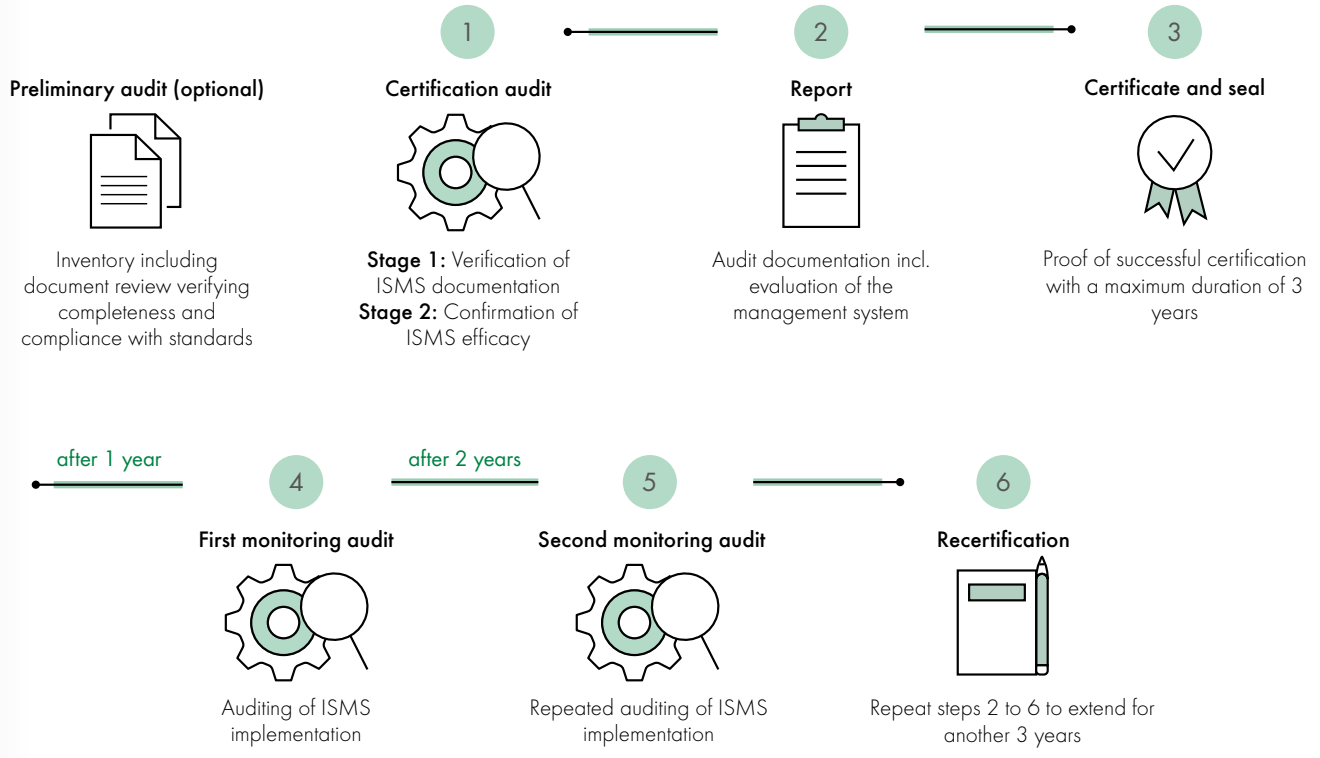
6. Which industries should be certified according to ISO 27001?

ISO 27001 is suitable for every industry, since today almost all companies use information technology systems and depend on their security. The requirements of ISO/IEC 27001 are designed to be applicable to any company, regardless of industry or size.

With our checklist, find out now with how well your company is prepared for ISO 27001 certification.

7. What is the certification process for ISO 27001?

We certify your company according to ISO 27001 in the following steps:



8. What does the ISO 27001 certification process involve?

Among other things, the certification process includes:

- Client's preparatory activities
  - Determining the scope of the ISMS
  - Defining information security guidelines and goals
  - Developing a risk assessment and risk treatment methodology
  - Preparing a declaration of applicability
  - Preparing a risk management plan and risk assessment report
  - Defining security roles and responsibilities
  - Creating a list of assets
  - Ensuring acceptable use of assets
  - Defining guidelines, e.g. for access control according to Annex A of ISO 27001
- Implementation of the certification audit
  - Stage 1: We examine the ISMS documentation and determine whether the company is ready for certification (readiness analysis). This includes inspection of the company and an interview with the ISMS manager.
  - Stage 2: We perform an audit to check the effectiveness of the ISMS by interviewing the relevant managers and employees in the various areas of your company.
  - The auditors prepare a report documenting the audit and evaluating your company's ISMS. The certificate and seal are then issued for a maximum term of three years.
  - The first surveillance audit takes place within one year and the second surveillance audit in the following year. A recertification audit must be carried out and completed before the certificate expires at the end of 3 years. This is followed by a first and second monitoring audit as described above.

Do you have further questions about the certification of your information security according to ISO 27001? Then contact us now!

DEKRA Certification

Active. Diligent. Visionary. Whether you are focusing on efficient business processes, product and system reliability for your international market success or qualified experts: With more than 1,000 specialists worldwide, DEKRA Certification offers you a comprehensive service on all aspects of quality and performance, safety and health, sustainability and responsibility. Around 30,000 companies in more than 50 countries are already using our certifications, tests and inspections to turn their individual goals into reality, quickly and without complication.

The DEKRA seal

Offer your customers reliability and quality – with our DEKRA seal!
The DEKRA seal stands for highest reliability – across different industries and internationally. It will create trust and give your customers the certainty of being on the safe side. Our seal will be your strength. Use it as an image bearer and marketing tool. We will be pleased to help you.

DEKRA Business Assurance
System Certification
Telefonl +1 800 768-5362
Mail sales.us@dekra.com
Web www.dekra-certification.us