TÜVNORD

Inspired by
Knowledge

ISO/IEC 27001 certification

Overview: Information Security in the current regulatory enviroment
Information is now a key production and success factor for modern organizations. Digitization, cloud services, mobile working, networked supply chains, and increasing regulatory requirements mean that companies are increasingly dependent on the secure processing and availability of information. At the same time, the risks posed by cyber-attacks, data breaches, system failures, and compliance violations are on the rise.

Against this backdrop, the protection objectives of confidentiality, integrity, and availability are becoming increasingly important. Information is a valuable organizational asset, and its loss, manipulation, or unauthorized disclosure can cause considerable economic, legal, and reputational damage. In addition to operational risks, violations of legal and regulatory requirements, for example, from data protection, IT security, or supervisory law, are becoming increasingly relevant.

An effective information security management system (ISMS) is the basis for addressing these challenges in a structured manner. An ISMS enables the systematic identification, assessment, and treatment of information security risks. It also ensures that information security is sustainably, transparently, and verifiably embedded within the organization. Technical, organizational, personnel, and physical aspects are taken into account equally.

The internationally recognized ISO/IEC 27001 standard defines the requirements for establishing, implementing, operating, monitoring, and continuously improving a documented information security management system (ISMS). It consistently follows a risk-based approach and is designed to be both technology- and industry-neutral.

ISO/IEC 27001 certification by TÜV NORD CERT confirms that these requirements have been effectively implemented and that information security is an integral part of corporate management.

Key features of ISO/IEC 27001 certification:

- Internationally recognized standard for information security management systems
- Risk-based, holistic approach to managing information security risks
- Clear governance structures with defined roles and responsibilities
- Continuous improvement process through audits, reviews, and action control
- Structure based on the Harmonized Structure (HS), as applied in almost all modern management system standards, enabling extensive synergies with other standards (e.g., integrated documentation, joint programs for internal audits and management reviews, and, in particular, integrated certification programs and audits)

Classification in the context of laws and compliance:

- Support in complying with legal and regulatory requirements
- Structured proof of information security for customers, partners, supervisory authorities, and auditors
- Fulfillment of contractual security requirements in national and international supply and value chains

Target groups for certification

The certification is aimed at organizations of all sizes and in all industries.

Typical target groups are organizations:

- that process sensitive or business-critical information (e.g., personal data, research and development data, intellectual property)
- that are subject to legal and regulatory requirements (e.g., critical infrastructures, data protection, IT security, supervisory requirements)
- that are required by customers or partners to have ISO/IEC 27001 certification as a prerequisite for cooperation or for tenders
- that seek to strengthen their cyber resilience, reliability, and business continuity in the long term
- that want to build and demonstrate trust among customers, investors, and other stakeholders

The standard is suitable for organizations with existing management systems as well as for companies that want to establish information security in a holistic and structured manner for the first time.

Your route to ISO 27001 certification in 5 steps

1 Preparation

2 Internal audit

3 Stage 1 audit, including approval process

4 Stage 2 audit, including approval process

5 Monitoring, including approval process

Our know-how for your success

TÜV NORD CERT is an internationally recognized and reliable partner for testing and certification services. Our experts and auditors have in-depth knowledge and generally have a permanent position at TÜV NORD. This ensures independence and neutrality as well as continuity in serving our customers. The benefit to you is clear: our auditors accompany and support the development of your company and provide you with objective feedback.

Contact

TÜV NORD CERT
ISMS Sales &
Projectmanagement

sales.isms@tuev-nord.de
tuev-nord-cert.de

Further information
and contact form: