qualityaustria
Succeed with Quality

ISO 27001

Standard for Information Security Management Systems

MOTIVATION AND BENEFITS

With its inestimable value, information and data are the core of modern organizations. The need for protection goes far beyond technical IT security. Correspondingly, "IT service management" processes run like lifelines through the entire company and enable high-quality IT services at reduced costs.

The entire field of information security is developing with extreme dynamism. Security incidents, from global virus attacks to image-damaging data breaches, have raised awareness of the need for controllable information security management systems (ISMS).

The international standard ISO/IEC 27001 "Information technology - Security techniques - Information security management systems - Requirements" specifies the requirements for establishing, implementing, operating, monitoring, maintaining and improving a documented information security management system, taking into account the risks throughout the organization.

All types of organizations (e.g. commercial enterprises, government organizations, non-profit organizations) are considered.

OBJECTIVES

- Highest protection of data and information
- Protection of intangible assets: analog and digital information
- Implementation of technical and organizational measures with effectiveness checks and optimization loops
- Introduction of an information security management system from a single source
- Systematic assessment and minimization of security gaps

TARGET GROUP

This standard is suitable for organizations of any size and industry.

CRITERIA

ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

This document also includes requirements for the assessment and handling of information security risks tailored to the needs of the organization.

Information about transfer to the version ISO/IEC 27001:2022

The new version of ISO/IEC 27001 was published in October 2022. The following requirements must be observed in this regard:

- The transfer shall be completed before October 2025, any ISO/IEC 27001:2013 certificate will be withdrawn by 31 October 2025.
- The transition from ISO/IEC 27001:2013 to the version 2022 can take place in the course of a re-certification audit.
- If the transition takes place in the course of a surveillance audit or a special audit, at least 8 additional hours must be scheduled for this purpose (depending on complexity of the organization/ controls). If the transition takes place in the course of a recertification audit, there are 4 additional hours.
- The certificate ISO/IEC 27001:2022 will keep the original certification cycle.

With effect from 1 November 2023, initial certifications may only be carried out according to the new version ISO 27001:2022.

ISO/IEC 27001:2022 includes management system requirements specified in Clauses 4 to 10 and 93 information security controls in 4 Clauses (organizational controls, people controls, physical controls, technological controls) outlined in Annex A.

ISO 27001 is based on the ISO High Level Structure and can be combined efficiently with other standards such as ISO 9001 and ISO 14001 due to the same structure and format.

OTHER RELEVANT STANDARDS

While ISO/IEC 27001 offers guidance on a broad range of information security controls that are commonly applied in many different organizations, other documents in the **ISO/IEC 27000 family** provide complementary advice or requirements on other aspects of the overall process of managing information security.

Refer to **ISO/IEC 27000** for a general introduction to both ISMS and the range of documents. ISO/IEC 27000 provides a glossary, defining most of the terms used throughout the ISO/IEC 27000 family of documents, and describes the scope and objectives for each member of the norm family.

There are sector-specific standards that include additional controls which aim at addressing specific areas (e.g. **ISO/IEC 27017** for cloud services, **ISO/IEC 27701** for privacy, **ISO/IEC 27019** for energy, **ISO/IEC 27011** for telecommunications organizations and **ISO 27799** for health).

QUALITY AUSTRIA – WHO WE ARE

We are the leading Austrian contact for the Integrated Management System, based on quality, environmental and OH&S (occupational health and safety) management, and the topic of business excellence. Our main focuses are system and product certification, training and personal certification. We are accredited by Accreditation Austria for system, product as well as personal certification and have many international registrations and accreditations. Furthermore, we present the Austrian Excellence Award together with the BMWA (Federal Ministry for Economy and Work) and award the Austria Quality Seal.

Additionally, we organize several forums and conferences and have issued numerous publications. We participate actively in standardization bodies and international networks such as EOQ, IQNET and EFQM. We cooperate with some 50 partner and member organizations worldwide and thus ensure the facilitation of global know-how.

Having more than 1.000 auditors, trainers, assessors and technical experts all over the world, we ensure the successful implementation of standards and regulations within the organizations and provide sector and product specific knowledge with a very high focus on practical relevance. More than 10.000 customers in approx. 30 countries and over 6.000 annual participants in our trainings benefit from the long-standing expertise of our organization. We adapt our offer according to our clients' needs and support them in achieving their long-term goals!

Thomas Mertl
Head of IT,
Product expert ISO 27001
thomas.mertl@qualityaustria.com

qualityaustria
Succeed with Quality

Quality Austria
Trainings, Zertifizierungs und Begutachtungs GmbH

www.qualityaustria.com office@qualityaustria.com

Headquarters
Zelinkagasse 10/3
1010 Vienna, Austria
Tel.: +43 1 274 87 47
Fax: +43 1 274 87 47-100

Customer Service Center
Am Winterhafen 1
4020 Linz, Austria
Tel.: +43 732 34 23 22
Fax: +43 732 34 23 23

Dok. Nr.: RE 24_00_116_e, Edition: January 2023