qualityaustria
Erfolg mit Qualität

ISO 27001

Standard für Informationssicherheitsmanagementsysteme

MOTIVATION UND NUTZEN

Informationen und Daten bilden mit ihrem unschätzbaren Wert das Herzstück moderner Organisationen. Ihr Schutzbedarf geht weit über technische IT-Sicherheit hinaus. Korrespondierend dazu ziehen sich „IT Service Management"-Prozesse wie Lebensadern durch das ganze Unternehmen und ermöglichen hochwertige IT-Leistungen zu reduzierten Kosten.

Der gesamte Bereich Informationssicherheit entwickelt sich mit äußerster Dynamik. Sicherheitsvorfälle – von globalen Virusattacken bis hin zu imageschädigenden Datenverlusten – haben die Notwendigkeit von steuerbaren Informationssicherheitsmanagementsystemen (ISMS) verdeutlicht.

Die internationale Norm ISO/IEC 27001 „Informationstechnologie – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen" spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation.

Hierbei werden sämtliche Arten von Organisationen (z. B. Handelsunternehmen, staatliche Organisationen, Non-Profit Organisationen) berücksichtigt.

ZIELE

- Höchster Schutz von Daten und Informationen
- Schutz von immateriellem Vermögen: analoge und digitale Informationen
- Implementierung technischer und organisatorischer Maßnahmen mit Wirksamkeitskontrollen und Optimierungsschleifen
- Einführung eines Informationssicherheitsmanagementsystems aus einem Guss
- Systematische Bewertung und Minimierung von Sicherheitslücken

ZIELGRUPPE

Dieser Standard ist für Organisationen jeglicher Größe und Branche geeignet.

KRITERIEN

ISO/IEC 27001 spezifiziert die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems im Rahmen der Organisation. Der Standard enthält auch Anforderungen für die Bewertung und Behandlung von Informationssicherheitsrisiken, die auf die Bedürfnisse der Organisation zugeschnitten sind.

Information zum Umstieg auf die Version ISO/IEC 27001:2022

Die neue Version der ISO/IEC 27001 wurde im Oktober 2022 veröffentlicht. Folgende Vorgaben sind diesbezüglich zu beachten:

- Der Transfer auf die neue Version muss vor Oktober 2025 erfolgen, ISO/IEC 27001:2013 Zertifikate werden ab 31. Oktober 2025 entzogen.

- Der Umstieg von einer Zertifizierung nach ISO/IEC 27001 Version 2013 auf die Version 2022 kann im Zuge eines Verlängerungsaudits erfolgen.
- Bei Umstieg im Zuge eines Überwachungsaudits bzw. eines Special Audits sind mindestens 8 zusätzliche Stunden (je nach Komplexität der Organisation bzw. der Controls) dafür vorzusehen. Bei Umstieg im Zuge eines Rezertifizierungsaudits sind weitere 4 Stunden vorzusehen.
- Das Zertifikat ISO/IEC 27001:2022 behält den ursprünglichen Zertifizierungszyklus.

Erstzertifizierungen können ab 1. November 2023 nur mehr nachder neuen Version erfolgen.

ISO/IEC 27001:2022 enthält Anforderungen an das Managementsystem, die in den Abschnitten 4 bis 10 spezifiziert sind, und 93 Informationssicherheitscontrols in 4 Abschnitten (organisatorisch, personell, physisch und technologisch), die im Annex A aufgeführt sind.

Die ISO 27001 basiert auf der ISO High Level Structure und lässt sich mit den Standards ISO 9001, ISO 14001, usw. aufgrund der gleichen Struktur und dem gleichen Aufbau sehr effizient kombinieren.

ANDERE RELEVANTE NORMEN

Während die ISO/IEC 27001 einen Leitfaden für eine breite Palette von Informationssicherheitskontrollen bietet, die in vielen verschiedenen Organisationen üblicherweise angewendet werden, bieten andere Dokumente der **ISO/IEC 27000-Familie** ergänzende Ratschläge oder Anforderungen zu anderen Aspekten des Gesamtprozesses des Informationssicherheitsmanagements.

In der **ISO/IEC 27000** finden Sie eine allgemeine Einführung in das ISMS und die Dokumentenfamilie. ISO/IEC 27000 enthält ein Glossar, in dem die meisten der in der ISO/IEC 27000-Dokumentenfamilie verwendeten Begriffe definiert sind, und beschreibt den Anwendungsbereich und die Ziele für jedes Mitglied der Normfamilie.

Darüber hinaus gibt es sektorspezifische Normen mit zusätzlichen Schwerpunkten, die auf bestimmte Bereiche abzielen (z. B. **ISO/IEC 27017** für Cloud-Dienste, **ISO/IEC 27701** für Datenschutz, **ISO/IEC 27019** für Energie, **ISO/IEC 27011** für Telekommunikationsunternehmen und **ISO 27799** für das Gesundheitswesen).

QUALITY AUSTRIA STELLT SICH VOR

Wir sind die führende österreichische Instanz für das Integrierte Managementsystem – aufbauend auf Qualitäts-, Umwelt-, Sicherheits- und Gesundheitsschutzmanagement sowie zum Thema Unternehmensqualität. Unsere Kernbereiche sind System- und Produktzertifizierung sowie Trainings und Personenzertifizierung. Wir sind von Akkreditierung Austria sowohl für die System-, Produkt- als auch für die Personenzertifizierung akkreditiert und verfügen über zahlreiche internationale Zulassungen. Außerdem vergeben wir gemeinsam mit dem BMAW (Bundesministerium für Arbeit und Wirtschaft) den Staatspreis Unternehmensqualität und verleihen das Austria Gütezeichen.

Neben der Veranstaltung diverser Fachforen (z. B. zum Thema Nachhaltigkeit, Lebensmittel und Gesundheit) und Konferenzen geben wir auch zahlreiche Publikationen heraus und arbeiten aktiv in Normungsgremien und internationalen Netzwerken (EOQ, IQNET, EFQM etc.) mit. Weltweit kooperieren wir mit rund 50 Organisationen und sichern so die Vermittlung von globalem Know-how.

Mit über 1.000 Auditor*innen, Trainer*innen, Assessor*innen und Fachexpert*innen stellen wir die erfolgreiche Umsetzung von Normen, inkl. branchen- und produktspezifischem Wissen mit hohem Praxisbezug, in den Organisationen sicher. Über 10.000 Kund*innen in knapp 30 Ländern und mehr als 6.000 Trainingsteilnehmende im Jahr profitieren von der langjährigen Expertise unseres Unternehmens. Wir passen das Angebot an unsere Kund*innen an und unterstützen bei der konzentrierten Ausrichtung auf langfristige Ziele!

DI (FH) Thomas Mertl
Head of IT,
Produktexperte ISO 27001
thomas.mertl@qualityaustria.com

qualityaustria
Erfolg mit Qualität

Quality Austria
Trainings, Zertifizierungs und Begutachtungs GmbH

www.qualityaustria.com office@qualityaustria.com

Headquarters
Zelinkagasse 10/3
1010 Wien, 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, Ausgabe: Jänner 2023