Bild: Pixabay

Ob Unternehmen, Behörden oder Organisationen – der Schutz sensibler Daten ist heute unerlässlich.

# ISO 27000er-Reihe: Ein Überblick

**Ob Unternehmen, Behörden oder Organisationen – der Schutz sensibler Daten ist heute unerlässlich. Doch es gibt inzwischen so viele Standards und Normen.**

Die ISO/IEC 27000er-Reihe bietet einen umfassenden Rahmen für das Management von Informationssicherheit, Risikobewertung und Datenschutz. Von grundlegenden Sicherheitsrichtlinien bis hin zu spezialisierten Normen für Cloud-Sicherheit, digitale Beweissicherung oder Datenschutz in Smart Cities – die Normenreihe deckt eine Vielzahl an Themen ab.

Doch welche dieser Standards sind besonders wichtig? In diesem Artikel geben wir eine kurze Übersicht über einige Normen der ISO 27000er-Reihe. Jede Norm wird kurz beschrieben, sodass Sie schnell einen Überblick über deren Inhalte erhalten. Hinweis: Das angegebene Jahr bezieht sich auf die aktuelle englische Ausgabe. Von einigen (wenigen) gibt es auch eine deutsche Veröffentlichung.

**ZUM AUTOR**

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

## ISO/IEC 27000:2018

Dieser Standard bietet einen Überblick und eine Einführung in die Normenreihe ISO/IEC 27000 für Informationssicherheitsmanagementsysteme (ISMS). Sie definiert zentrale Begriffe und Konzepte im Bereich der Informationssicherheit und stellt den Zusammenhang zwischen den verschiedenen ISO/IEC 27000-Normen dar.

Diese Norm dient als Grundlage für Organisationen, die ein ISMS implementieren, indem sie die Grundprinzipien, Terminologien und Anforderungen für ein effektives Informationssicherheitsmanagement beschreibt.

## ISO/IEC 27001:2022

Die Norm definiert die Anforderungen an ein ISMS sowie zur systematischen Absicherung von Informationen gegen Bedrohungen. Die Norm ist in mehrere Kapitel unterteilt, die Unternehmen dabei unterstützen, ihre Informationssicherheit effektiv zu verwalten und kontinuierlich zu verbessern.

Zu Beginn beschreiben die Kapitel 1 bis 3 den Anwendungsbereich, normative Verweise und Begriffe, die für das Verständnis und die Umsetzung der Norm erforderlich sind. Kapitel 4 legt den organisatorischen Kontext fest und verlangt von Unternehmen, interne und externe Faktoren zu analysieren, die ihre Informationssicherheit beeinflussen. Kapitel 5 behandelt die Führungsverantwortung und betont, dass das Management aktiv hinter der Informationssicherheitsstrategie stehen und diese unterstützen muss.

In Kapitel 6 werden die Anforderungen an das Risikomanagement beschrieben, darunter die Festlegung von Zielen und Massnahmen zur Risikobehandlung. Kapitel 7 befasst sich mit der Ressourcenplanung, einschliesslich Schulungen und Bewusstseinsbildung, um sicherzustellen, dass alle Beteiligten die ISMS-Anforderungen verstehen und umsetzen können. Kapitel 8 fordert eine operative Umsetzung der Sicherheitsmassnahmen, um Risiken proaktiv zu steuern.

Die Leistungsmessung ist ein wichtiger Bestandteil der Norm: Kapitel 9 beschreibt die Anforderungen an die Überwachung, Messung und Bewertung der ISMS-Prozesse, um deren Wirksamkeit sicherzustellen. Schliesslich verlangt Kapitel 10 eine kontinuierliche Verbesserung, um das ISMS regelmässig anzupassen und weiterzuentwickeln.

## ISO/IEC 27002:2022

Diese Norm ist ein Leitfaden für Informationssicherheitsmassnahmen, die als Ergänzung zur ISO/IEC 27001 dient. Während ISO 27001 die ISMS-Anforderungen definiert, bietet die ISO 27002 detaillierte Empfehlungen und Best Practices zur Implementierung von Sicherheitskontrollen. Die zentralen Sicherheitskontrollen sind in den Kapiteln 5 bis 8 beschrieben:

### Kapitel 5: Organisatorische Massnahmen

Enthält Richtlinien für das Risikomanagement, Sicherheitsrichtlinien, Rollen und Verantwortlichkeiten sowie die Schu-

lung und Sensibilisierung von Mitarbeitern.

### Kapitel 6: Massnahmen für Personen

Fokussiert sich auf die Sicherheitsaspekte des Personals, darunter der sichere Umgang mit Informationen, Verantwortlichkeiten, Disziplinarmassnahmen und die Sicherheit beim Beenden von Arbeitsverhältnissen.

### Kapitel 7: Physische Massnahmen

Deckt den Schutz physischer und umgebungsbezogener Sicherheit ab, einschliesslich Zutrittskontrollen, Schutz von IT-Räumen und Massnahmen zur Sicherung von Hardware und Geräten.

### Kapitel 8: Technologische Massnahmen

Beinhaltet technische Sicherheitskontrollen, wie Identitäts- und Zugriffsmanagement, Kryptografie, Netzwerksicherheit, System- und Anwendungsmanagement sowie Überwachungs- und Protokollierungsmechanismen.

Jede dieser Kategorien enthält spezifische Massnahmen mit detaillierten Anleitungen, wie Unternehmen diese effektiv umsetzen können.

## ISO/IEC 27003:2017

Die Norm beleuchtet erfolgsrelevante Aspekte beim Design und der Implementierung des ISMS. Der Aufbau entspricht 1:1 demjenigen der nicht mehr aktuellen ISO/IEC 27001:2013. Auf 41 Seiten werden zusätzliche Gedanken und Hilfestellungen zu den Schlüsselkomponenten Policy, Rollen und Verantwortlichkeiten, Risiko-Management, Awareness, dem PDCA-Zyklus sowie Verbesserungen und notwendiger Dokumentation gezeigt.

## ISO/IEC 27004:2016

Die Informationssicherheit zu messen, ist eine grosse Herausforderung. Welche Punkte gilt es zu messen? Wie kann sichergestellt werden, dass sich das ISMS wirklich weiterentwickelt und verbessert? Die ISO 27004 bietet eine Anleitung zur Beantwortung folgender Fragen:

- die Überwachung und Messung der Leistung der Informationssicherheit;
- die Überwachung und Messung der Wirksamkeit des ISMS einschliesslich seiner Prozesse und Kontrollen;
- die Analyse und Bewertung der Ergebnisse der Überwachung und Messung.

Die Norm ist in die Kapitel Gründe, Merkmale, Arten von Massnahmen und Abläufe unterteilt. Der Anhang B hilft bei der Suche nach sinnvollen Messungen. Damit stellt die Norm das notwendige Rüstzeug für das Messen und Auswerten von Sicherheitsmetriken dar.

## ISO/IEC 27005:2024

Dieser Standard geht auf das Thema Risikomanagement in der Informationssicherheit ein. Er bietet einen strukturierten Ansatz zur Identifikation, Bewertung und Behandlung von Risiken, die sich auf die Informationssicherheit auswirken können. Die Norm beschreibt bewährte Methoden zur Risikobewertung, Risikobehandlung, Risikokommunikation und Risikokontrolle, ohne eine spezifische Methodik vorzuschreiben. Ihr Ziel ist es, fundierte Sicherheitsentscheidungen zu treffen und Informationssicherheitsrisiken kontinuierlich zu überwachen und zu minimieren.

## ISO/IEC 27006:2024

Die Norm legt Anforderungen und allgemeine Prinzipien für die Kompetenz von Auditoren und deren Überwachung, die Anforderungen an Zertifizierungsstellen sowie den Auditierungs- und Zertifizierungsprozess fest.

## ISO 27017:2015

Diese Norm enthält Leitlinien für Informationssicherheitskontrollen, die für die Bereitstellung und Nutzung von Cloud-Diensten anwendbar sind. Sie bietet Kontrollen und Umsetzungsanleitungen sowohl für Anbieter von Cloud-Diensten als auch für Kunden von Cloud-Diensten.

## DIN SPEC 27076:2023

Die DIN SPEC 27076 ist eine Spezifikation, die speziell für die IT-Sicherheitsberatung von kleinen und Kleinstunternehmen (KMU) entwickelt wurde. Sie bietet externen Dienstleistern einen standardisierten Prozess, um die IT-Sicherheit in diesen Unternehmen zu bewerten und zu verbessern. Kernbestandteil ist der CyberRisikoCheck, bei dem in einem strukturierten Interview 27 Anforderungen aus sechs Themenbereichen geprüft werden, um den aktuellen Sicherheitsstatus des Unternehmens festzustellen. Anhand der Ergebnisse werden konkrete Handlungsempfehlungen zur Verbesserung der IT-Sicherheit gegeben. Die Norm zielt darauf ab, KMU eine praxisnahe und effiziente Methode zur Steigerung ihrer IT-Sicherheit bereitzustellen.

## ISO 27701:2019

Diese Norm bietet eine Anleitung für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Datenschutz-Informationsmanagementsystems (DSMS/Englisch: PIMS) in Form einer Erweiterung der ISO/IEC 27001 und ISO/IEC 27002. Die Norm legt Datenschutz-bezogene Anforderungen fest und bietet eine Anleitung für PII-Verantwortliche und PII-Verarbeiter, die für die Verarbeitung von PII verantwortlich und rechenschaftspflichtig sind (PII = Personally Identifiable Information, personenbezogene Informationen).

Dies war nur an der Oberfläche gekratzt. Inzwischen wurden von ISO über 77 Standards, die sich rund um die Informationssicherheit und den Datenschutz drehen, veröffentlicht. Nebst ISO gibt es weitere Gremien, die Sicherheitsstandards herausgegeben haben. Für ein Unternehmen ist es damit alles andere als einfach, die richtige Norm zu finden. Mit der ISO 27001, zusammen mit der ISO 27002, kann aber ein stabiles Fundament für die eigene Informationssicherheit erstellt werden. Die anderen Normen helfen, ein besseres Verständnis für die Informationssicherheit zu bekommen.