Die wichtigsten Änderungen der ISO/IEC 27001 und ISO/IEC 27002 auf einen Blick

UPDATE
ISO 27001

Aufgrund der wachsenden Herausforderungen im Bereich der Cyber Security erfordert die ISO/IEC 27001 (zusammen mit den ergänzenden optionalen Richtlinien der ISO/IEC 27002) die Implementierung neuer Anforderungen, um ein konformes Informationssicherheitsmanagement im Einklang mit digitalisierten Geschäftspraktiken und den daraus resultierenden Risiken zu gewährleisten.

Revision zur Sicherung einer wirksamen Informationssicherheit

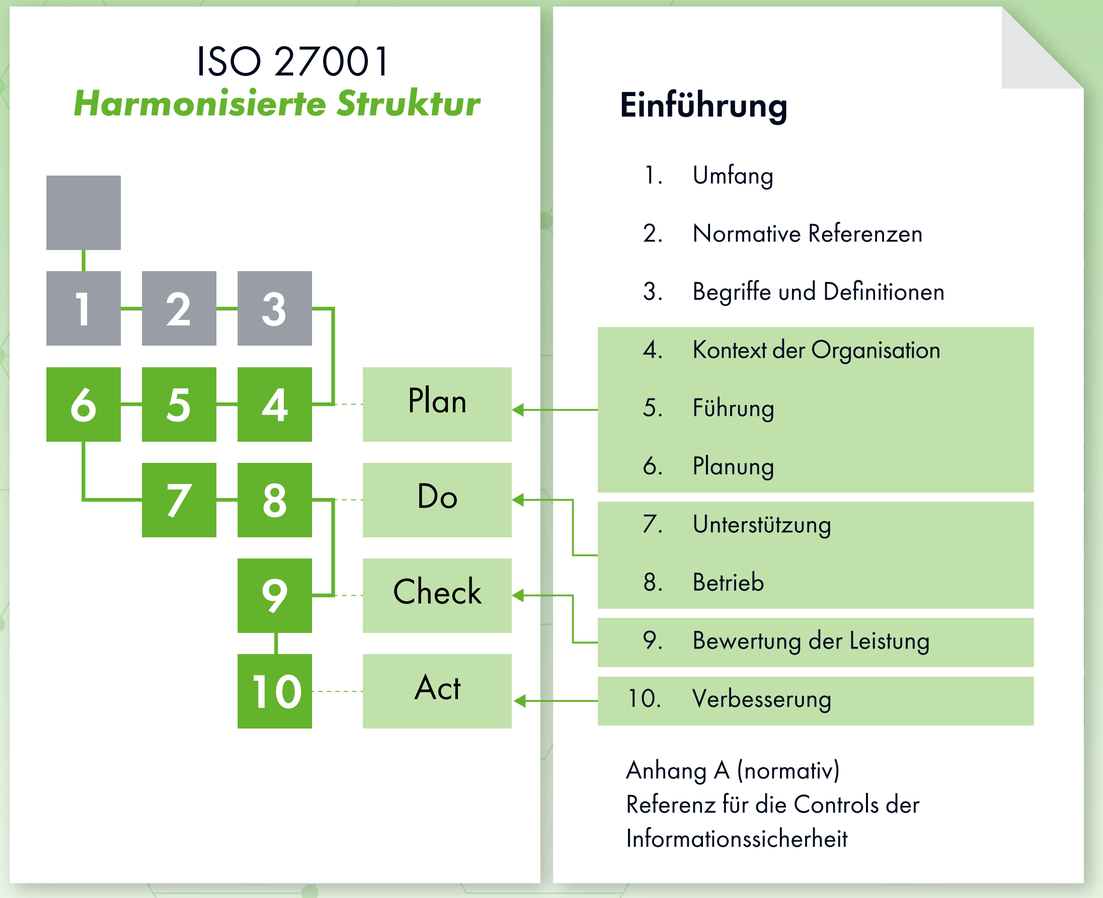
Unternehmen, die in der digitalen Geschäftswelt tätig sind, müssen belastbare Sicherheitsstrategien einführen und Informationssicherheitsmaßnahmen umsetzen, um Sicherheitsvorfälle zu reduzieren, geistiges Eigentum zu schützen und vertrauliche Informationen zu sichern. Nur so können sie ihr Engagement für den Aufbau einer vertrauenswürdigen und erfolgsorientierten Marke unter Beweis stellen. Ein flexibles und effektives Informationssicherheitsmanagement spielt eine entscheidende Rolle bei der Risikominimierung und der Abwehr von Cyberangriffen.

Die ISO/IEC 27001 wurde im Jahr 2022 überarbeitet, um den zuvor aktualisierten Leitfaden ISO/IEC 27002:2022 für die Maßnahmen/Controls der Informationssicherheit widerzuspiegeln. Die Änderungen der Norm ISO/IEC 27001 und des Leitfadens ISO/IEC 27002 sollen sicherstellen, dass die Maßnahmen zur Informationssicherheit mit den aktuellen technologischen Entwicklungen Schritt halten und die allgemeine Widerstandsfähigkeit von Unternehmen stärken.

Die wichtigsten Änderungen der ISO 27001

Die Überarbeitung der Norm ISO 27001 umfasst Änderungen an der Struktur (HLS), die vorschreibt, dass Prozesse und ihre Wechselwirkungen Teil des Informationssicherheitsmanagementsystems (ISMS) sein müssen, sowie Aktualisierungen des Katalogs der in Anhang A aufgeführten Sicherheitskategorien und -maßnahmen.

Aufbau der *ISO 27001-Norm (Harmonisierte Struktur)*



Änderungen der Abschnitte „Plan“, „Do“, „Check“ und „Act“ der Harmonisierten Struktur

Durch die Einbeziehung der harmonisierten Struktur in die Revision der ISO/IEC 27001:2022 mussten einige Abschnitte und deren Inhalte angepasst werden. Die Änderungen betreffen die Abschnitte „Plan, Do, Check, Act“ (PDCA) und beinhalten:

- **Abschnitt 4.4: Informationssicherheitsmanagementsystem**
  Erfordert die Bestimmung der notwendigen Prozesse und ihrer Wechselwirkungen im ISMS
- **Abschnitt 5.3: Rollen, Verantwortlichkeiten und Befugnisse in der Organisation**
  Verlangt die obligatorische Offenlegung der organisatorischen Zuständigkeiten und Befugnisse für Aufgaben im Zusammenhang mit Informationssicherheit
- **Abschnitt 6.1.3: Informationssicherheitsrisikobehandlung**
  Ermöglicht eine flexiblere Auswahl, Gestaltung und Erweiterung der in Anhang A aufgeführten Referenzmaßnahmen und betont die Öffnung des Managementsystemrahmens für organisationsspezifische Maßnahmen
- **Abschnitt 6.3: Planung von Änderungen**
  Erfordert die Beherrschung von ISMS-bezogenen Änderungsprozessen
- **Abschnitt 7.4: Kommunikation**
  Die bisherigen Abschnitte „worüber“, „wann“, „mit wem“ und „wer“ wurden um das „wie“ der Kommunikation erweitert
- **Abschnitt 8.1: Betriebliche Planung und Steuerung**
  Erfordert Prozesse im Rahmen der operativen Planung und Kontrolle, um die Maßnahmen zur Bewältigung der Informationssicherheitsrisiken umzusetzen (mit Prozesskriterien für die Prozesskontrolle)
- **Abschnitt 9.2 / 9.3: Internes Audit / Managementbewertung**
  Neu angepasst und weiter untergliedert in der überarbeiteten, harmonisierten Struktur
- **Abschnitt 10.1 / 10.2: Fortlaufende Verbesserung / Nichtkonformität und Korrekturmaßnahmen**
  Stellt die vorausschauende kontinuierliche Verbesserung vor die nachträgliche Behebung von Nichtkonformitäten und Korrekturmaßnahmen ohne inhaltliche Änderungen

Überarbeitung des Anhangs A der Norm ISO/IEC 27001

Im Gegensatz zu den 114 Maßnahmen zur Informationssicherheit, die in der Revision 2013 in 14 Kategorien unterteilt waren, enthält der Anhang A der Revision 2022 nur noch 93 Maßnahmen, die in vier Hauptkategorien – organisatorische, personenbezogene, physisch und technische Maßnahmen – unterteilt sind. Während einige Sicherheitsmaßnahmen gestrichen wurden, sind 11 neue Maßnahmen hinzugekommen:

- **Informationen über die Bedrohungslage (Threat Intelligence) –** Sammlung und Analyse von Informationen zur Festlegung von Schutzmaßnahmen
- **Informationssicherheit für die Nutzung von Cloud-Diensten (Cloud Services) –** Sichere Prozesse für die Einbindung, Nutzung, Verwaltung und den Ausstieg bei Cloud-Anbietern
- **IKT-Bereitschaft für Business Continuity (Business Continuity) –** Anforderungen an Wiederherstellungsmaßnahmen mit einem neuen Schwerpunkt auf technischen Maßnahmen
- **Physische Sicherheitsüberwachung (Physical Security Monitoring) –** Überwachungsmaßnahmen, Einbruchalarm usw. zur Abschreckung und zum Schutz vor unbefugtem Eindringen
- **Datenmaskierung (Data Masking) –** Einschränkung, Anonymisierung und Pseudonymisierung von Daten
- **Verhinderung von Datenlecks (Data Leakage Prevention) –** Erkennung und Überwachung von Datenverlust/-weitergabe/-lecks
- **Überwachungstätigkeiten (Monitoring) –** Proaktive Verfolgung von abweichenden Aktivitäten
- **Webfilterung (Web Filtering) –** Entfernen gefährlicher Webseiten, die Malware verbreiten oder nicht autorisierte Daten lesen
- **Sicheres Coding (Secure Coding) –** Beseitigung von Schwachstellen oder Anfälligkeit für Angriffe
- **Konfigurationsmanagement (Configuration Management) –** Korrekte Einstellung von Sicherheitsmaßnahmen und Sicherung der Konfiguration
- **Löschung von Informationen (Information Deletion) –** Anforderungen an die Datenspeicherung im Hinblick auf die DSGVO und GDPR

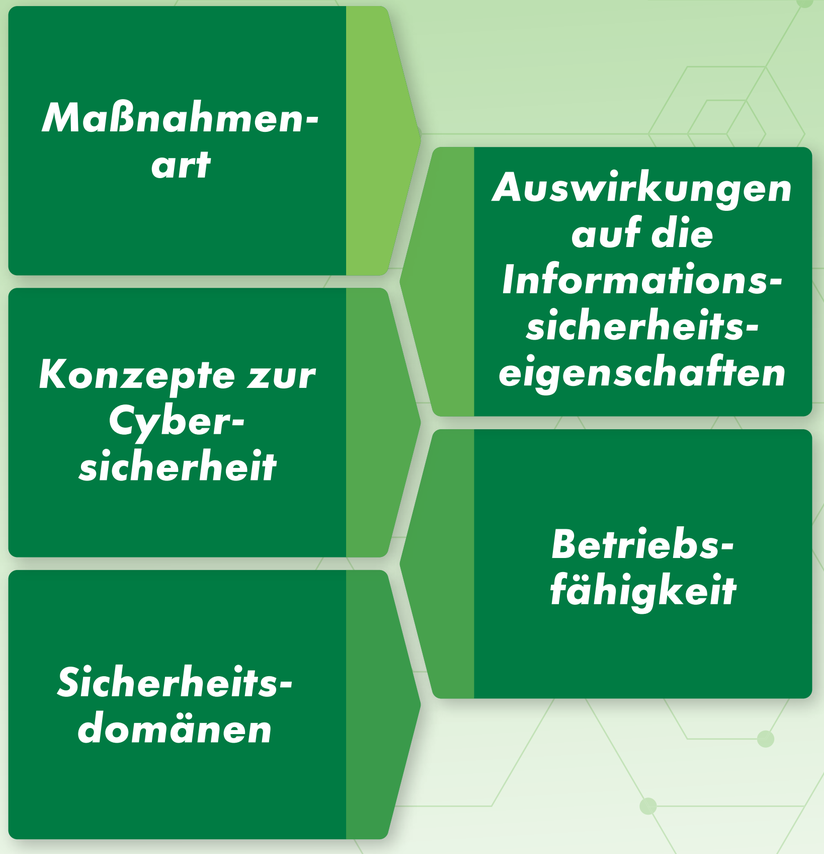
Aktualisierte ISO/IEC 27002-Leitlinien

Im Gegensatz zur Norm ISO/IEC 27001, die lediglich Sicherheitsmaßnahmen definiert, ist die ISO/IEC 27002 eine unterstützende Norm bzw. ein Praxisleitfaden. Obwohl der Anhang A der ISO/IEC 27001 beispielsweise Controls zur Sicherheit auflistet, bietet die neu benannte ISO/IEC 27002 „Information Security, Cybersecurity and Privacy Protection" konkrete Anleitungen für die Umsetzung dieser Controls.

Die Änderungen an der ISO/IEC 27002 beinhalten eine Namensänderung, die den Standard als eigenständigen Katalog von Informationssicherheitsmaßnahmen identifiziert, sowie die Einführung von fünf Attributen, die die Transparenz erhöhen und Fehlinterpretationen in der Anwendung reduzieren sollen. Diese Attribute umfassen:

- **Maßnahmenart (Control type)**
  Beschreibt Maßnahmen unter dem Gesichtspunkt, wann und wie sie das Risiko eines Informationssicherheitsvorfalles mindern
- **Auswirkungen auf die Informationssicherheitseigenschaften (Information security properties)**
  Betrachtet Maßnahmen unter dem Gesichtspunkt, welches Merkmal der Informationen durch die Maßnahme geschützt werden soll.
- **Konzepte zur Cybersicherheit (Cybersecurity concepts)**
  Kennzeichnet Maßnahmen aus Sicht der Cybersicherheit (vgl. Cybersecurity Framework gemäß ISO/IEC TS 27110)
- **Betriebsfähigkeit (Operational capabilities)**
  Dient dazu, die Maßnahmen aus der Perspektive der Informationssicherheitsfähigkeiten zu betrachten.
- **Sicherheitsdomänen (Security domains)**
  Betrachtet Maßnahmen aus der Perspektive von vier Informationssicherheitsdomänen „Governance und Ökosystem", „Schutz" , „Verteidigung" und „Resilienz".

Die 5 Attribute der
ISO/IEC 27002 Struktur
und ihre zugehörigen Bedeutungen



Vorteile der überarbeiteten Normen

Die neuen Normen ISO/IEC 27001 und ISO/IEC 27002 konzentrieren sich auf die Informationssicherheitstechnologien und befassen sich mit aktuellen Maßnahmen, die auf die heutigen Organisationsmethoden und Bedrohungen im Zusammenhang mit dem Informationssicherheitsmanagementsystem (ISMS) abgestimmt sind. Die ISO/IEC 27001 wurde vereinfacht und bietet nun mit Hilfe der ISO/IEC 27002 eine Reihe von Sicherheitsmaßnahmen mit den zugehörigen Merkmalen.

Die Kategorisierung wurde gestrafft und in Themenblöcke gegliedert. Besondere Aufmerksamkeit wurde der Prozessorientierung gewidmet, indem ihre Bedeutung hervorgehoben und ihre Kriterien und Wechselwirkungen veranschaulicht wurden. Die harmonisierte Struktur wurde überarbeitet, um den Status der Prozessorientierung im effektiven Management der Informationssicherheit widerzuspiegeln.

Empfehlungen für die Umstellung

Um die Umstellung auf die neue ISO/IEC 27001:2022 erfolgreich durchzuführen, empfehlen wir, so früh wie möglich mit den Vorbereitungen anzufangen sowie die entsprechenden Änderungen im Managementsystem zu integrieren.

Folgende Schritte sind besonders wichtig:

- Machen Sie sich genau mit den neuen Inhalten und Anforderungen vertraut
- Schulen Sie alle zuständigen Mitarbeitenden in Ihrem Unternehmen
- Finden Sie mögliche Lücken in Ihrem aktuellen ISMS
- Setzen Sie bereits frühzeitig neue Maßnahmen um und aktualisieren Sie Ihr Managementsystem

Zeitplan für den Übergang

Bis spätestens 12 Monate nach der Veröffentlichung der neuen ISO/IEC 27001:2022 (d. h. am 30. Oktober 2023) müsste die Umstellung der Akkreditierungen auf die neue Normgrundlage durch die DAkkS abgeschlossen sein. Erst nach erfolgreicher Akkreditierung sind Audits auf Basis der neuen Norm möglich.

Wie bei allen ISO-Revisionen gibt es Fristen für die Umstellung von der alten auf die neue Zertifizierungsnorm. Mit der Veröffentlichung im Oktober 2022 beginnt eine dreijährige Übergangsfrist, in der sich die Unternehmen auf die Zertifizierung bzw. Rezertifizierung nach der neuen Norm vorbereiten können. Ab dem 31. Oktober 2025 müssen alle bestehenden Zertifikate bereits auf die überarbeiteten Anforderungen der ISO/IEC 27001:2022 umgestellt sein. Bis dahin gilt, dass Erst- oder Rezertifizierungsaudit noch bis spätestens 18 Monate nach Veröffentlichung der neuen Norm (also bis zum 30.04.2024) noch nach der alten Norm DIN EN ISO/IEC 27001:2017 durchgeführt werden können, jedoch bis zum 31.10.2025 eine Umstellung auf die neue Normenrevision erfolgen muss. Diese kann entweder im Rahmen eines Überwachungsaudits oder als separates Umstellungsaudit durchgeführt werden. Der Zyklusverlauf bleibt dabei unverändert. Mit erfolgreichem Abschluss des Umstellungsaudits erhalten Sie dann ein neues Zertifikat für die ISO/IEC 27001:2022 mit einer Gültigkeit bis zum Ende des normalen, 36-Monats-Zyklus.

Sie haben Fragen zu den Änderungen der ISO/IEC 27001:2022 und ISO/IEC 27002:2022 oder möchten wissen, wie sich diese auf Ihr Unternehmen auswirken? Kontaktieren Sie unsere Sachverständigen!

→ Kontaktieren Sie uns!