Allgemeine Informationen zu Änderungen an der neuen Edition der ISO/IEC 27002

Stand: 13.07.2022

Die internationale Norm ISO/IEC 27001 stellt die Grundlage für ein Informationssicherheitsmanagementsystem (ISMS) dar. Die Norm definiert die Anforderungen an ein solches Managementsystem. Im Anhang A der Norm (englisch Annex A), sind die spezifischen Maßnahmenziele bzw. Kontrollen im Bereich der Informationssicherheit aufgeführt. Die Norm ISO/IEC 27002 ist eine dazu korrespondierende Orientierungshilfe, welche Hinweise gibt, wie diese Maßnahmenziele erreicht bzw. Kontrollen umgesetzt werden können.

In den vergangenen Jahren wurde die ISO/IEC 27002 umfassend überarbeitet und liegt seit Februar 2022 in der dritten Edition vor.

Die augenscheinlichste Änderung betrifft die Struktur der Maßnahmenziele (Controls). Diese wurden in neuen Gruppen organisiert, den sogenannten „Clauses“, und mit einer simplen Taxonomie inklusive zugehöriger Attribute versehen. Dazu wurden die Inhalte selbst stark modernisiert.

Die Änderungen im Detail:

- Neue Grundstruktur – 14 Clauses zu 4 Clauses restrukturiert
  - Kapitel 5, Clause „Organizational controls“ (Rollen und Verantwortlichkeiten, Berechtigungsmanagement, Umgang mit Informationen, etc.)
  - Kapitel 6, Clause „People controls“ (Personalprozesse – Einstieg, Stellenwechsel, Ausstieg; Sensibilisierung und Schulung, etc.)
  - Kapitel 7, Clause „Physical controls“ (Perimeter- und Objektschutz, Umgang mit Betriebsmitteln, etc.)
  - Kapitel 8, Clause „Technological controls“ (Absicherung von Endgeräten, Zugriffssteuerung, IT-Betrieb, Logging und Monitoring, Netzwerksegmentierung, etc.)

- Neue Controls - 11 Controls wurden neu aufgenommen, z. B.
  - Threat intelligence (Identifikation und Umgang mit Bedrohungen)
  - Information security for use of cloud services (Sicherheit von Cloud-Services)
  - Physical security monitoring (Überwachung der Sicherheit physischer Perimeter und Infrastrukturen)
  - Data leakage prevention (Vermeidung von Datenabfluss)
  - Monitoring activities (Überwachung und Anomalieerkennung in Netzwerken)
  - Secure coding (Anforderungen an die sichere Software-Entwicklung)

- Zusammenfassung von Controls – 56 Controls wurden zu 24 zusammengefasst, z. B. 12.4.1 Event logging, 12.4.2 Protection of log information, 12.4.3 Administrator and operator logs zu 8.15 Logging

- Neue Taxonomie[1] und Attribute zu jedem Control; der neue Standard gibt u.a. Hilfestellung zur Einordnung der Controls zu berührten Schutzzielen (Vertraulichkeit, Integrität, Verfügbarkeit) und ordnet die Controls in Bezug auf deren Wirkungsform ein (vorbeugend, erkennend, korrigierend)

Ziele der Neuordnung sowie Vor- und Nachteile

Sinn und Zweck der Aktualisierung bzw. der Neuordnung des ISO/IEC 27002 Standards war es, den Standard aktuell zu halten und zu vereinfachen.

Durch die Aktualisierung wurden bisher nicht oder nur ungenügend berücksichtigte Themen integriert und an den aktuellen Stand der Technik angepasst. Dazu zählen u. a. technische Anforderungen wie die Absicherung im Umgang mit Cloud-Systemen oder die Überwachung von Aktivitäten in der IT-Infrastruktur. Dies ist ebenfalls durch das IT-Sicherheitsgesetz 2.0 gefordert, so sollen Systeme zur Angriffserkennung etabliert und betrieben werden. Des Weiteren wurden auch die Empfehlungen zur Umsetzung (Guidance) zu bestehenden Controls aktualisiert.

Im Hinblick auf die Vereinfachung des Standards wurde einerseits durch die Zusammenfassung von Controls die Gesamtzahl reduziert und andererseits die Komplexität der Struktur durch die Anpassung von 14 auf 4 Clauses verringert. Vorteilhaft an der neuen Struktur ist eine klare Trennung in organisatorische, physische, personelle und technische Maßnahmen, sodass für Organisationen klarer herausgestellt wird, dass Informationssicherheit über mehrere Ebenen realisiert werden muss und nicht nur durch die IT-Abteilung verantwortet wird.

Die Änderungen am Standard haben Auswirkungen auf bestehende, gelebte ISMS. Es ist notwendig bekannte Vorgehensweisen und Verfahren zu überprüfen und gegebenenfalls anzupassen. Das kann durch die jeweiligen Organisationen als nachteilig gesehen werden. Es benötigt Zeit und erfordert zu Anfang einen Mehraufwand. Des Weiteren wird es für verpflichtende Werke (insb. die ISO/IEC 27019, aber auch verschiedene branchenspezifische Standards), die auf die Norm ISO/IEC 27002 verweisen noch Zeit in Anspruch nehmen, bis diese die neue Struktur berücksichtigen. In der Zwischenzeit muss mit Mapping-Tabellen gearbeitet werden.

[1] Klassifikationsschema nach bestimmten Kriterien gemäß Anhang A der ISO/IEC27002:2022 Tabelle A.1

Aktivitäten beim Umstieg auf die neue ISO/IEC 27002

Organisationen, welche ein ISMS gemäß ISO/IEC 27001 etabliert haben, aber vor allem solche Organisationen, die gemäß der Norm zertifiziert sind, müssen die Aktualisierung der ISO/IEC 27002 berücksichtigen und die neuen bzw. veränderten Anforderungen umsetzen. Insbesondere muss im Rahmen der Risikobehandlung (gemäß ISO/IEC 27001 Kapitel 6.1.3 c) überprüft werden, ob die existierenden Maßnahmen der Organisation auch den Anforderungen aus den aktualisierten und neuen Controls gerecht werden. Dafür wird es notwendig sein, bestehende Lücken zu identifizieren und bei Bedarf ergänzende Maßnahmen zu ermitteln. Des Weiteren wird es gemäß ISO/IEC 27001 Kapitel 6.1.3 d) erforderlich sein, die Erklärung zur Anwendbarkeit (Statement of applicability – SoA) nach der neuen Struktur anzupassen und Prüfungen hinsichtlich der Anwendbarkeit der Controls vorzunehmen.

Abseits des Risikomanagements müssen im Rahmen der Auditvorbereitung das bestehende Auditprogramm überprüft und in Bezug auf die Aktualisierung der ISO27002 Anpassungen umgesetzt werden. Organisationen sollten sich des Weiteren auch darauf vorbereiten, dass die Auditplanung nach den bisherigen Annex A Abschnitten A.5 bis A.18 nicht weiter fortgeführt werden sollte. Selbstverständlich kann man die Struktur durch das Mapping weiterhin nutzen, es bietet sich allerdings an, hier die neu eingeführte Taxonomie1 zu verwenden.

Umsetzungsfrist

Für die Zertifizierung nach IT-Sicherheitskatalog auf Basis der aktualisierten Normen ist eine Übergangsfrist in den Konformitätsbewertungsprogrammen geregelt. So haben Audits spätestens nach Ablauf von zwei Jahren seit Veröffentlichung der aktualisierten Fassungen verpflichtend auf Basis dieser zu erfolgen. Bis zur Erscheinung der neuen ISO/IEC 27019 können Betreiber Anleitungen zur Abbildung der bestehenden ISO 27019 Struktur auf die neue ISO 27001/27002 nutzen.