Bild: Pixabay

ISO 27001:2022 veröffentlicht

Ende Oktober war es nach einigen Verzögerungen so weit, die neue ISO 27001:2022 wurde veröffentlicht. Vorneweg, es hat sich inhaltlich nicht sehr viel geändert. Eine grosse Tragweite haben lediglich die Controls in Anhang A. Trotzdem ist es Zeit, genauer auf die Änderungen und das weitere Vorgehen einzugehen.

Lange mussten wir auf die neue Ausgabe warten, nach neun Jahren wurde Ende Oktober die neue Ausgabe herausgegeben. Bislang ist diese nur in Englisch verfügbar. Mit der deutschen Übersetzung ist frühestens in einem Jahr zu rechnen. Der Aufbau entspricht nun dem aus anderen ISO-Normen gewohnten Bild. Sei es ISO 9001 (Qualitätsmanagement), ISO 22301 (Business Continuity) oder weiteren, die Struktur ist nun identisch. Die Kapitel 9.2 (Internal Audit) und 9.3 (Management Review) haben Unterkapitel erhalten. Die Kapitel 10.1 (Neu: Continual improvement) und 10.2 (Neu: Nonconformity and corrective action) haben ihre Positionen gewechselt.

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

Aufgefallen ist, dass durchgängig «International Standard» durch «document» ersetzt wurde. Die Definitionen von Begriffen sind schon länger in ISO 27000 enthalten und können kostenlos unter www.iso.org/obp aufgerufen werden.

Änderungen

Nachfolgend wird auf die geänderten Text-Passagen eingegangen (Hinweis: Deutsche Übersetzungen sind vom Autor. Diese können von der zukünftigen offiziellen Version abweichen):

Im Kapitel 4.2 (Understanding the needs and expectations of interested parties/Verstehen der Erfordernisse und Erwartungen interessierter Parteien) wurde ein weiterer Punkt ergänzt: Die Organisation muss festlegen, welche dieser Anforderungen durch das Informationssicherheits-Managementsystem (ISMS) erfüllt werden sollen.

Im Kapitel 4.4 (ISMS) wurde der bestehende Satz mit dem fetten Teil ergänzt: «Die Organisation muss in Übereinstimmung mit den Anforderungen dieses Dokuments ein ISMS einrichten, umsetzen, aufrechterhalten und kontinuierlich verbessern, einschliesslich der erforderlichen Prozesse und ihrer Wechselwirkungen.»

In Kapitel 5.1 (Leadership and commitment/Führung und Verpflichtung) kam eine Fussnote dazu, die erläutert, dass der Begriff «Business» weit ausgelegt werden kann, um Aktivitäten zu bezeichnen, die die für den Zweck der Organisation von zentraler Bedeutung sind.

Viele Berater und Auditoren sind über die Fussnote 2 in Kapitel 6.1.3 (Information security risk treatment/Informationssicherheitsrisikobehandlung) froh. «Anhang A enthält eine Liste der möglichen Informationssicherheitskontrollen.» In vielen Audits gab es Diskussionen, ob nun alle Kontrollen umgesetzt werden müssen oder nicht. Diese sind zwar mit dem zusätzlichen Wort «möglichen» noch nicht ganz vom Tisch, aber es zeigt, dass hier Spielraum vorhanden ist.

Das Erstellen einer SoA (Statement of Applicability/Erklärung zur Anwendbarkeit) wurde bereits mit dem Technical Corrigendium 2 im Dezember 2015 korrigiert und nun nochmals bestätigt.

Im Kapitel 6.2 (Information security objectives and planning to achieve them/Informationssicherheitsziele und Planung zu deren Erreichung) wurde zu den Informationssicherheitszielen «überwacht» und «als dokumentierte Informationen verfügbar sein» ergänzt.

Ein neues Kapitel ist die 6.3: «Planung von Änderungen». Darin wird verlangt: «Wenn die Organisation feststellt, dass Änderungen am ISMS notwendig sind, müssen die Änderungen geplant durchgeführt werden.» Eigentlich selbstverständlich, aber nun auch als Muss-Anforderung enthalten.

Das Kapitel 7.4 (Communication/Kommunikation) wurden die Punkte d) und e) als «wie kommuniziert wird» zusammengefasst.

Einige Modifikationen hat das Kapitel 8.1 (Operational planning and control/Betriebliche Planung und Steuerung) erfahren. Es wird verlangt, dass zur Steuerung Kriterien für die Prozesse festgelegt und Kontrollen in Übereinstimmung mit diesen durchgeführt werden. Weiter müssen Dokumentationen so verfügbar sein, dass damit ein Nachweis über die korrekte Funktionsweise der Prozesse möglich ist. Auch wird auf extern bezogene Prozesse hingewiesen: «Extern bereitgestellte Prozesse, Produkte oder Dienstleistungen müssen kontrolliert werden.»

Im Kapitel 9.1 (Monitoring, measurement, analysis and evaluation/Überwachung, Messung, Analyse und Bewertung) wurden die Sätze umgestellt, um den Lesefluss zu verbessern. Neu dazu gekommen ist, dass zum Nachweis der Ergebnisse dokumentierte Informationen verfügbar sein müssen.

Das Kapitel 9.2 (Internal audit/Internes Audit) wurde komplett neu unterteilt. Es hat nun die Kapitel 9.2.1 (General/Allgemein) und 9.2.2 (Internal audit programme/Internes Auditprogramm). Inhaltlich hat sich aber nichts geändert.

Analoges gilt auch für das Kapitel 9.3 (Management review/Managementbewertung). Es ist unterteilt in 9.3.1 (General/Allgemein), 9.3.2 (Management review inputs/Inhalte Managementbewertung) und 9.3.3 (Ma-

nagement review results/Resultate Managementbericht). Dazu gekommen ist in 9.3.2, dass auch Änderungen der Bedürfnisse und Erwartungen der interessierten Parteien, die für das ISMS relevant sind, behandelt werden.

Wie bereits erwähnt, haben die Kapitel 10.1 und 10.2 ihre Positionen gewechselt. Inhaltlich hat sich aber nichts geändert.

Kontrollen

Die grosse Änderung ist im Anhang A zu finden: Information security controls reference, in der deutschen Ausgabe «Referenzmassnahmenziele und -massnahmen» genannt. Die Struktur wurde komplett neu aufgebaut. Anstelle von 114 sind es «nur» noch 93. Und dies, obschon elf neue dazu gekommen sind und nur eines gestrichen wurde. Einige der Massnahmen wurden sinnvollerweise zusammengefasst. Die dazu gehörende ISO 27002 wurde bereits Mitte Februar 2022 veröffentlicht. Details dazu finden Sie in der Ausgabe «Maschinenbau 2022/04: ISO 27002:2022 – Informationssicherheit neu organisiert».

Die Kontrollen gliedern sich in die vier Themenbereiche 5 Organizational controls (37), 6 People controls (8), 7 Physical controls (14) und 8 Technological controls (34). In Klammern sind die Anzahl Kontrollen aufgeführt. Zu den neuen Kontrollen gehören:

- 5.7 Threat intelligence/Informationen über Bedrohungen
- 5.23 Information security for use of cloud services/Informationssicherheit bei der Nutzung von Cloud-Diensten
- 5.30 ICT readiness for business continuity/IKT-Bereitschaft für die Geschäftsweiterführung
- 7.4 Physical security monitoring/Überwachung der physischen Sicherheit
- 8.9 Configuration management/(IT-)Konfigurationsmanagement
- 8.10 Information deletion/Löschung von Informationen
- 8.11 Data masking/Datenmaskierung
- 8.12 Data leakage prevention/Verhinderung von Datenverlusten
- 8.16 Monitoring activities/Überwachung von Aktivitäten
- 8.22 Web filtering/Web-Filterung
- 8.28 Secure coding/Sichere Programmierung

Wie geht es nun weiter?

Eine erste Zertifizierung nach der neuen ISO 27001:2022 soll bereits für den November möglich sein. Fraglich ist, ob die akkreditierten Zertifizierungsstellen auch schon bereit sind.

Die letzte Möglichkeit für eine Erst- oder Rezertifizierung nach der alten ISO 27001:2013 (englische Ausgabe)/2017 (deutsche Ausgabe) ist 18 Monate, beziehungsweise April 2024. Hinweis: damit sind nicht die Aufrechterhaltungs-Audits gemeint.

Bestehende Zertifizierungen haben noch eine Gültigkeit von 3 Jahren, das heisst maximal bis Oktober 2025. Bis dahin müssen alle ISMS auf die neue Norm angepasst sein.

Fazit

Die neue Ausgabe der ISO 27001:2022 hat vor allem kosmetische Änderungen erfahren. Einige Klarstellungen sind vorhanden, aber ein Wechsel benötigt keinen riesigen Aufwand. Dieser versteckt sich in den angepassten Kontrollen. Auf diese wird im nächsten Artikel genauer eingegangen. Weiter benötigen die elf zusätzlichen Kontrollen Zeit. Auch wenn noch drei Jahre Zeit bis zum Wechsel bleiben, sollte sich jedes bereits zertifizierte Unternehmen damit auseinandersetzen und einen Projektplan zur Migration erstellen, damit nicht am Ende doch noch ein (unnötiger) Zeitdruck entsteht.