ISO 27001: 2022

Was sich konkret geändert hat

Version: 1
Autor: Dr. Michael Wolfensberger und Joël Bühler

Dieser Artikel wendet sich an diejenigen, die sich konkret mit der 27001er Norm befassen und sich stundenlange Vergleiche mit der bisherigen Version von 2013 ersparen wollen. Der Artikel richtet sich also an Auditoren, ISMS-Verantwortliche, ISOs und alle, die die Details kennen müssen. Hier werden die Unterschiede im Normenteil und im Anhang der aktualisierten ISO 27001 aufgezeigt und kommentiert.

Die bisherige Norm der 27000er Serie ist 10 Jahre alt geworden. Jetzt gibt es eine neue Version, basierend auf der bereits überarbeiteten 27002 Guideline.

Auf den ersten Blick hat sich nicht so viel geändert. Aber auf den zweiten.

Der Normentext (Kapitel 4 – 10)

Was sofort auffällt: Die Norm ist derzeit nur auf Englisch erhältlich. Die Struktur des Normenteils entspricht aber nach wie vor der High Level Struktur der ISO-Normen. Man hat die Strategie also nicht geändert.

Was den Inhalt anbetrifft, so hält sich das Neue auch zuerst einmal zurück.

- Kapitel 1-3 (Anwendungsbereich, Normative Verweisungen und Begriffe) bleiben unverändert
- Kapitel 4 (Kontext der Organisation), 5 (Führung) und 7 (Unterstützung) bleiben unverändert

Ab dem Kapitel 6 (Planung) gibt es erste kleinere Änderungen bei den Inhalten und zum Teil eine neue Strukturierung, weil es weniger Untergruppen (a, b, c…) gibt, dafür mehr Unterkapitel, in denen die bisherigen Inhalte der Untergruppen einsortiert worden sind.

Planung (Kapitel 6)

- Abschnitt 6.2. wurde insoweit ergänzt, dass die Informationssicherheitsziele überwacht (monitored) und kommuniziert (communicated) werden müssen.

  Es genügt also nicht mehr, Ziele zu setzen, man muss auch deren Umsetzung nachweisen können.

- Neu wird klar gefordert, dass die Ziele der Informationssicherheit den entsprechenden Stakeholdern in angemessener Form mitgeteilt werden müssen. Ausserdem ist der Nachweis zu erbringen, dass die Zielerreichung nachverfolgt und kontrolliert wird (was die Bildung und Pflege entsprechender KPIs und damit die Operationalisierung der Ziele voraussetzt). Dies erscheint mir ein Schritt in Richtung Transparenz und Nachvollziehbarkeit zu sein, der vielen Unternehmungen guttun könnte.
- Abschnitt 6.3 fordert neu, dass Änderungen am ISMS geplant umgesetzt werden sollen. Daraus ist zu lesen, dass Veränderungen generell und die Anpassung von Inhalten des

ISMS grundsätzlich auch dem Change-Prozess unterzogen sein sollten. Ein zweiter Gedanke lässt aber auch vermuten, dass hier naheliegenderweise beim Audit der Transfer von der alten zur neuen Norm entsprechend unter die Lupe genommen wird.

Betrieb (Kapitel 8)

- Abschnitt 8.1 Betriebliche Planung und Steuerung (Operational Planning and Control). Es müssen die Prozesse zur Erbringung der Leistungen geplant, implementiert und kontrolliert werden und es müssen Kriterien für die Prozesse und die Kontrolle der Prozesse implementiert werden. Auch hier geht der Trend zur Nachvollziehbarkeit und damit zu einer stärkeren Einbindung von Kennzahlen. Die Erfahrung zeigt, dass hierzu gut implementierte Prozesse sehr hilfreich sind.

Bewertung der Leistung (Kapitel 9)

- Das Kapitel 9 hat eine neue Gliederung erfahren und zwei neue, verschärfende Aspekte.
- Abschnitt 9.1. b) war in der Version von 2013 noch eine Anmerkung und ist neu verbindlich. Auch hier geht die neue Norm in die Richtung, dass die Festlegung von Methoden für die Überwachung und Messungen von Sicherheitsprozessen und Kennzahlen vergleichbare und reproduzierbare Ergebnisse erzeugen sollen.
- Abschnitt 9.3.2. definiert die Inputs für den Management Review, aufgelistet von a) bis g). Hier ist ein inhaltlich neuer Unterabschnitt c) zu finden, der den Abschnitt 9.3.2.b) verstärkt. Der neue Abschnitt c) fordert, dass Veränderungen in Bedarf und Erwartung an das ISMS durch die interessierten Parteien berücksichtigt werden müssen. Die bisherige Berücksichtigung von internen und externen Themen ist also um die Bedürfnisse und Erwartungen der Stakeholder erweitert worden, die zusätzlich mit in den Management Review einfliessen müssen.

Verbesserung (Kapitel 10)

- Generell sind die Abschnitte 10.1 und 10.2 in ihrer Reihenfolge ausgetauscht worden.
- Abschnitt 10.2 Nonconformity and Corrective Action. Der Abschnitt c) lautet in der Norm von 2013 «erforderliche Massnahmen einleiten». Auch hier wird eine Nuance mehr eingefordert. Die Version von 2022 liest sich «implement any action needed» und geht damit über eine geforderte «Einleitung» von Massnahmen hinaus.

Anhang A

Hier hat die Norm eine deutliche Überarbeitung erfahren, denn die Kontrollen sind neu in die folgenden vier Gruppen strukturiert:

5. Organizational Controls
6. People Controls
7. Physical Controls
8. Technological Controls

Bei dieser Neuordnung wurden einige Kontrollen zusammengefasst und diskret umformuliert. Nimmt man es genau, steckt hinter den Neuformulierungen eine Konkretisierung der Norm, in Bezug auf die jeweilige Organisation.

Generell wird in den neuen Formulierungen oft gefordert, dass die Kontrollen passend zur Organisation definiert werden müssen. Das zieht nach sich, dass in den Policies und Richtlinien oft neu präzisiert werden muss, was die Organisation jeweils in ihrem Kontext als passend festlegt.

Ein Beispiel für diese feinen, aber wesentlichen Änderungen in den Kontrollen ist Control 8.15 (Logging). Hier heisst es “Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed”.

Im alten Text zum Logging (12.4.1) steht «Ereignisprotokolle, die Benutzertätigkeiten, Ausnahmen, Störungen und Informationssicherheitsvorfälle aufzeichnen, werden erzeugt, aufbewahrt und regelmässig überprüft.» Der Unterschied liegt in dem kleinen Wort «relevant».

Hier müsste jede individuelle Organisation ihre Policies und Richtlinien zum Logging dahingehend schärfen, was für sie eigentlich «relevant» ist, um das Logging korrekt umzusetzen und in einem Audit angemessen begründen zu können, welche Logs als Nachweise einzustufen sind.

Es sind aber auch noch einige Kontrollen hinzugekommen.

5.07 Threat Intelligence

Hier scheint es, als seien die Punkte 6.1.3 (neu 5.05) und 6.1.4 (neu 5.06) der alten Normen-Version in einer Kontrolle erweitert worden. Die Forderung nach Threat Intelligence geht über das Kontakthalten mit Behörden und Interessengruppen der alten Norm hinaus und fordert konkret eine fortlaufende Suche nach Erkenntnissen zu Bedrohungen, auch solche, technischen Charakters. Die Tendenz zum SIEM ist hier deutlich erkennbar.

5.23 Information Security for use of cloud services

Mit dieser Kontrolle wird versucht, der Nutzung von Cloud-Services generell zu begegnen. Cloud-Services sind eben nicht nur Share-Point und andere grosse und klar erkennbare Dienstleistungen, sondern auch z.B. Übersetzungsdienste im Internet, wo möglicherweise mit einfachen Webseiten-Zugriff klassifizierte Texte übersetzt - und natürlich von den Übersetzungs-Service-Betreibern gespeichert - werden.

5.30 ICT Readiness for Business Continuity

Die alten Kontrollen 7.11-7.13 sind in die neue 5.29 (Information Security during disruption) zusammengefasst worden. Zusätzlich dazu geht mit der Kontrolle 5.30 die explizite Anforderung an die ICT, sich technisch und organisatorisch vorzubereiten. Viele Organisationen werden dies unter BCM in einem BHB oder einem Notfallplan und -handbuch bereits festgelegt haben. Gleichwohl ist es noch einen Blick wert, Business Continuity und ICT-Readiness für den Notfall parat zu haben.

7.4 Physical Security Monitoring

Auch hier wurde der physischen und umgebungsbezogenen Sicherheit ein weiterer Punkt hinzugefügt. Die Forderung zur kontinuierlichen physischen Überwachung ist neu. Hier kommen Bewegungsmelder, CCTV oder gar ein Wachdienst als Optionen in Betracht. Der Einsatz elektronischer Kameras wird einen Rattenschwanz an weiteren Aspekten rechtlicher und technischer Natur nach sich ziehen.

8.9 Configuration Management

Diese Neuerung wird am ehesten für gehobene Augenbrauen sorgen. Die Forderung ist ebenso einfach wie umfassend. Das Asset Management wird durch das Configuration Management ergänzt, wo die Zusammenstellung und das Zusammenwirken der in der IT und zu ihrer Sicherheit eingesetzten Assets beschrieben und dargelegt werden muss. Daraus folgt natürlich, dass alle Dokumente über die Konfiguration der IT und speziell die der Sicherheitsmassnahmen wiederum höchst schützenswert sind.

8.10 Information Deletion

Dieser Abschnitt fordert «good housekeeping» mit Daten und Informationen, die nicht mehr benötigt werden, um sie vor versehentlicher oder absichtlicher Bekanntgabe oder Entwendung zu schützen. Auch hier müsste folgerichtig in den Policies eine Regelung hinterlegt werden, wann dies für welche Daten und Informationen in der betreffenden Organisation der Fall wäre. Hier spielen auch noch regulatorisch vorgegebene Retentionszeiten mit hinein.

8.11 Data Masking

Auch diese neue Kontrolle hat es in sich. Datenmaskierung gemäss den Bedürfnissen der Organisation, ihrer Stakeholder und des Gesetzes. Dazu muss wiederum in den Policies festgelegt werden, welche Daten und Informationen zu welcher Maskierungskategorie gehören, wer sie unter welchen Umständen einsehen darf und welche Maskierungsmittel in welcher Stärke und in welchen Stufen eingesetzt werden sollen. Besonders sticht hier hervor, dass erwähnt wird, dass trotz anonymisierter Personendaten (Name, Geburtsdatum etc.) bei hinreichender Metadatendichte die Daten oft wieder einer Person zugeordnet werden können.

8.12 Data Leakage Prevention

Obwohl die Norm keine Tools fordert, legt diese Kontrolle in der Praxis den vermehrten Einsatz von DLP-Tools nahe, um technisch zu unterbinden, dass Daten und Informationen ungewollt abfliessen. Auch hier bedarf es wiederum der tiefgreifenden Dokumentation und der Definition in den Policies, wie und für welche Daten und Geschäftsfälle das DLP eingesetzt werden soll. Es ist auch noch nicht klar, ob technische Auditoren die Einrichtung von speziellen Vorkehrungen z.B. im Mail Transport Hub im Exchange o.ä. ebenso akzeptieren wie dedizierte zusätzliche DLP-Systeme der einschlägigen Hersteller.

8.16 Monitoring Activities

Obwohl lobenswert und sinnvoll ist der hier geforderte Umfang an Messungen und Analyse für Einzelfirmen oder KMUs möglicherweise nur schwer zu leisten. Neben der erneuten Einführung von Definitionen in den Policies und Richtlinien, was genau alles wie genau überwacht werden soll, und dem Nachführen der Konfigurationsdokumente, deutet die Kontrolle hier auf den Einsatz eines SIEMs und damit für viele auf ein Outsourcing, das wiederum Risiken und Kosten mit sich bringt.

8.23 Web Filtering

Diese Kontrolle ist dem Netzwerk-Teil beigefügt worden. Auch hier werden allfällig noch Definitionen und Listen zur weiteren Dokumentation anfallen. Das Filtern und der generelle Umgang mit dem Web werden sicher auch Gegenstand der Nutzerschulung sein und sicher auch einige unter 5.23 (Information Security for use of cloud services) anfallende Themen beinhalten.

8.28 Secure Coding

Hier wird die Norm ebenfalls spezifischer als bisher. Es werden u.a. «unternehmensspezifische Erwartungen und anerkannte Grundsätze für sichere Kodierung» erwartet, «die sowohl für interne als auch für ausgelagerte Code-Entwicklungen verwendet werden können». Es werden Vorgaben für die Vorbereitung und Durchführung der Kodierung, Testing und Review und Wartung von Code gemacht.

Fazit

Insgesamt wird die Norm technischer und in ihrer inneren Konsistenz verbindlicher, indem sie mehr Kennzahleneinsatz fordert und geschärfte konkretere Vorgaben macht und einfordert, dass tiefergehende individuelle sicherheitsrelevante Definitionen und Festlegungen der Organisation gemacht werden. Es scheint ausserdem, dass es weniger einfach wird, Kontrollen auszuschliessen.

Sie ist da. Setzen wir sie um!