Unterschiede zwischen ISO 27001:2017 und ISO 27001:2022

Was hat sich geändert? Was ist weggefallen? Was ist dazugekommen?

In der **ISO 27001:2022** haben sich eine ganze Reihe von Dingen geändert gegenüber ihrer Vorgängerin, der **ISO 27001:2017**. Wir gehen die größeren (und vermutlich arbeitsintensiven) Änderungen hier einmal für Sie durch.

Zunächst einmal die gute Nachricht: Im Hauptteil der Norm hat sich so gut wie gar nichts geändert. Zwei Änderungen sollen hier erwähnt werden:

1. **Interessierte Parteien:** Schon in der ISO 27001:2017 war es erforderlich (Kapitel 4.2), die Interessierten Parteien und ihre Wünsche zu bestimmen. In der Version 2022 können Sie jetzt aber entscheiden, welche der Ihnen bekannten Interessierten Parteien Sie ernst nehmen – und welche nicht.

2. **Betriebliche Planung und Steuerung:** Kapitel 8.1 ist etwas strenger geworden. Die Anforderungen an die Prozesse, die Sie in Ihrer Organisation benötigen, um Informationssicherheit zu verfolgen, sind deutlicher: Zwar fordert die ISO 27001:2022 nicht direkt, dass alle Prozesse beschrieben sein müssen – aber die Kriterien an eine Verschriftlichung sind genauer. Und es ist zu erwarten, dass Auditoren gewissenhafter hinschauen werden.

Aber jetzt zum **Anhang A der ISO 27001:2022**. Dieser ist **komplett überarbeitet** worden, es ist kein Stein auf dem anderen geblieben. Während es in der ISO 27001:2017 genau 119 einzelne Maßnahmen gab, gibt es in der neuen Version **nur noch 93**. Allerdings sind meist nur Maßnahmen zusammengelegt worden. Und – einige Dinge hinzugekommen, die Arbeit machen:

1. **Threat Intelligence:** Sowohl auf strategischer (Geschäftsführung) als auch auf operativer und taktischer (bspw. IT) Ebene werden aufkommende Bedrohungen aktiv gesammelt, damit frühzeitig darauf reagiert werden kann.

2. **Information Asset Management:** Die ISO 27001 verlangt jetzt auch explizit, dass Informationswerte (primary assets) denselben Regeln unterliegen wie Informationsträger (supporting assets). D.h. die Eigentümerschaft muss geregelt werden, die Zugänge zu den Informationswerten, Rückgabe der Zugänge u.v.m. – in der ISO 27001:2017 konnte man sich hier noch recht gut auf die Informationsträger beschränken. Das geht nun nicht mehr.

3. **Web Filtering:** Zugang zu externen Webseiten muss ab sofort gemanagt werden, damit Mitarbeiter der Organisation nicht unabsichtlich Malware herunterladen oder Zugang zu Ressourcen haben, den sie nicht haben sollen.

4. **Identity Management:** wird ganzheitlicher verlangt – über den gesamten Lebenszyklus von Identitäten, die Zugang zu Informationswerten und Informationsträgern haben sollen (menschliche sowie auch maschinelle Identitäten).

5. **Information Security bei Nutzung von Clouddiensten:** Seit 2017 hat sich die Welt weitegedreht – alle Welt nutzt Clouddienste! Prinzipiell war das Thema bereits in der ISO 27001:2017 abgedeckt, im Bereich des Lieferantenmanagements. Jetzt gibt es hier aber einige konkrete Anforderungen. Beispielsweise: Wie stellt die Organisation sicher, dass sie ihre Daten aus dem Cloudsystem wieder in weiter verarbeitbarer Form herausbekommt, wenn zu einem anderen System gewechselt werden soll (Stichwort „lock in prevention")?

6. **Informationssicherheit während Ausfällen:** Ausfälle können immer passieren. Aber welchen Grad an Informationssicherheit (meist Verfügbarkeit) möchte die Organisation denn bei dem Ausfall welches Dienstes oder welches Geräts noch aufrechterhalten? Auch dieses Thema war (etwas versteckt) im Thema Business Continuity in der ISO 27001:2017 bereits enthalten – bzw. konnte man es dort abdecken. Jetzt ist es explizit gefordert.

7. **Sicherheit im Home-Office:** Auch die ISO 27001:2022 kennt Corona und weiß, dass Mitarbeiter im Home-Office in aller Regel eine deutlich unsicherere Infrastruktur zur Verfügung haben als im Büro. Dies ist ab sofort zu regeln.

8. **Event Reporting:** Hiermit ist keine automatisierte Suche in Logfiles gemeint – Mitarbeiter sollen Möglichkeiten kennen, mit denen sie einfach und schnell mögliche Informationssicherheitsvorfälle melden oder weiterleiten können.

9. **Zugangsbeschränkungen gem. Policy:** Wer auf welche Informationen Zugriff haben kann, darf und soll, muss sich aus einer Policy ergeben, die sich aus der Informationssicherheitsstrategie ableitet (und nicht im Gutdünken eines Entscheiders liegen). Dies gab es so explizit in der ISO 27001:2017 noch nicht. Hier war nur ein „formeller Prozess" gefordert.

10. **Configuration Management:** Für die Sicherheit wichtige Konfigurationen von Systemen (Hardware, Software, Dienste, Netzwerke, ...) müssen etabliert, dokumentiert und aufrechterhalten werden. Diese Forderung gab es so in der Vorgängerversion der Norm noch nicht.

11. **Data Masking:** Daten werden nach bestimmten Regeln pseudonymisiert oder anonymisiert, damit die schützenswerten Bestandteile nicht zu unberechtigten Personen gelangen.

12. **Löschkonzept (und zwar nicht nur für personenbezogene Daten):** Ab sofort muss es ein Löschkonzept geben (das natürlich auch umgesetzt wird) für die Datenarten, die in der Organisation gespeichert werden. Für die DSGVO war das bereits gesetzliche Pflicht. Die ISO 27001:2022 macht dies nun verpflichtend für alle schützenswerten Informationsarten.

13. **Data Leakage Prevention:** Dies ist wohl eine der „härtesten Nüsse", die uns die neue ISO 27001:2022 mitgibt. Die Anforderung ist hier, dass eine Organisation sich überlegen muss, auf welchen Wegen geschützte Informationen unabsichtlich „abhanden" kommen

können (Meetings, Emails, Uploads auf Server, unverschlüsselte abhanden gekommene Laptops oder Mobiltelefone, Ablage auf den falschen – weil allen Mitarbeitern zugänglichen – internen Fileservern u.v.m.) und dies durch geeignete technische und möglicherweise auch organisatorische Maßnahmen durchsetzt.

Das waren sie nun – die (vermutlich) größten Baustellen, die uns die ISO 27001:2022 mitgibt. Zugegeben, alles sinnvolle Anforderungen, die Tücke liegt in einer schlanken, aber dennoch wirksamen Umsetzung.

Sind noch Fragen offengeblieben? Möchten Sie wissen, wie die ein oder andere Neuerung bei Ihnen sinnvollerweise umgesetzt werden könnte? Kein Problem. Kontaktieren Sie uns gerne per E-Mail an info@einfachiso.de oder natürlich in unserem Chat.

Wir freuen uns!

Joachim Reinke
Certified Information Security
Lead Auditor ISO 27001

einfachISO GmbH