ISO 27001: Führung

Das Kapitel 7 der ISO 27001 befasst sich mit den Themen Ressourcen, Kompetenz, Bewusstsein, Kommunikation und Dokumentation.

Die Norm verlangt, dass die notwendigen Ressourcen auch zur Verfügung stehen. Es darf nicht nur ein Lippenbekenntnis sein, «wir betreiben ein ISMS», aber die notwendigen Ressourcen, die es dazu benötigt, werden nicht zur Verfügung gestellt. Oft reicht es zwar für den Aufbau des ISMS. Da sind alle noch begeistert. Sobald aber die Zertifizierung bestanden ist, wird es vernachlässigt. «Es läuft ja, wir müssen nun nicht mehr ständig etwas machen.»

Kurz vor dem Aufrechterhaltungsaudit werden nochmals grosse Anstrengungen unternommen und alles auf Vordermann gebracht. Doch einem erfahrenen Auditor fällt dies sofort auf. Ein ISMS verlangt stetige Tätigkeiten und nicht nur einmal im Jahr. Dazu sind die Themen zu vielfältig, als dass dies in einer Nachtübung nachgeholt werden kann. Daher verlangt das Kapitel 7.1 auch die Aufrechterhaltung und fortlaufende Verbesserung des ISMS.

Weiter ist die notwendige Kompetenz, sprich die Ausbildung und das Wissen, nachzuweisen (7.2). Dazu gilt es für alle involvierten Personen (oder auch Rollen) einen entsprechenden Anforderungskatalog zu erstellen: Welche Erfahrungen muss diese Person mitbringen? Welche Schulungen/Ausbildungen sind notwendig? Wie kann die regelmässige Aktualisierung des Wissens sichergestellt werden? Wenn etwas fehlt, ist dies nicht tragisch, es muss aber sichergestellt sein, dass dieses Wissen erarbeitet wird. Dazu gibt es verschiedene Kurse und Schulungen von diversen Anbietern.

Die Norm verlangt weiter, dass ein entsprechender Nachweis vorhanden ist. Bewahren Sie daher unbedingt die Kursbestätigungen und Zertifikate auf.

Gerade kleinere und mittlere Unternehmen müssen sich überlegen, ob sie diese Funktion wirklich intern besetzen möchten. Eine Person zu bestimmen, welche dies neben ihren normalen Aufgaben auch noch bewältigt, bringt oft nicht das notwendige Resultat. Die Norm erwähnt in einer Anmerkung, dass dies auch durch Beauftragung einer kompetenten Person erfolgen kann.

Für einen CISO könnte folgendes Pflichtenheft erstellt werden:

- Identifikation sicherheitsrelevanter Unternehmensprozesse
- Erarbeitung und Definition der sicherheitsrelevanten Objekte, der Bedrohungen und Risiken und den daraus abgeleiteten Sicherheitszielen
- Aufbau und Betrieb einer Organisationseinheit zur Umsetzung der Sicherheitsziele
- Ausarbeitung, Anpassung von Sicherheitsrichtlinien und IT-Sicherheitszielen, inklusive Definition von KPIs
- Aufbau und Betrieb eines Managementsystems zur Informationssicherheit (ISMS)
- Aufsicht über die Einhaltung von Vorschriften
- Auditierung der Funktionseinheiten zum Stand der Umsetzung und Weiterentwicklung der Sicherheitsvorschriften
- Beaufsichtigung des Identity- und Access-Managements
- Bewusstsein der Mitarbeitenden durch Trainings und Awareness-Kampagnen schaffen

Informationssicherheitspolitik

Der Normpunkt 7.3 verlangt, dass alle Personen im Anwendungsbereich des ISMS die Informationssicherheitspolitik (oft auch Informationssicherheitsrichtlinie genannt) kennen müssen. Zudem wird verlangt, dass alle einen Beitrag zur Wirksamkeit des ISMS leisten sowie die Folgen bei Zuwiderhandlung kennen. Idealerweise wird dies bereits im Arbeitsvertrag oder einem Anhang zum Arbeitsvertrag geregelt und durch Unterschrift bestätigt.

Folgendes Beispiel könnte in einen Arbeitsvertrag aufgenommen werden: Hiermit erkläre ich, dass mir die Informationssicherheitsleitlinie der Firma Firmenname vollständig bekannt ist, ebenso wie die weiteren Dokumente, die als Teil des Informationssicherheits-Managementsystems (ISMS) veröffentlicht wurden:

- Auflistung aller veröffentlichten Dokumente

Ich erkläre hiermit, dass ich die Vorgaben der Richtlinie und aller weiteren Dokumente befolgen werde. Mir ist bewusst, dass Nichtbefolgung jeglichen Teils dieser Erklärung eine Verletzung meiner Pflichten darstellt und mit disziplinarischen Massnahmen geahndet werden kann.

Kommunikation gegen innen und aussen

Ein weiterer wichtiger Punkt spricht der Normpunkt 7.4 an: die Kommunikation gegen innen und aussen. Im Vorfeld muss definiert werden, was, wann, mit wem und durch wen kommuniziert wird. Entsprechende Schritte sollten in den jeweiligen Prozessen definiert sein. Beispielsweise bei einer Sicherheitsverletzung, bei einem Hackerangriff, einem Datenverlust oder sonst einem wichtigen Ereignis. Wie in einem Notfallplan gewohnt, gilt es dies auch für die verschiedenen Schritte im Bereich des ISMS zu definieren. Nur was gut vorbereitet ist, kann bei Eintreten eines Ereignisses auch entsprechend

Pflichtdokumente

Nachfolgende Dokumente müssen mindestens erstellt werden:

- Lenkung von Dokumenten und Aufzeichnungen
- Identifikation der Anforderungen (Liste gesetzlicher, amtlicher, vertraglicher und anderer Anforderungen)
- ISMS-Anwendungsbereich
- Informationssicherheitsleitlinie
- Risiko-Bewertung und -Behandlung
- Erklärung zur Anwendbarkeit (SOA)
- Plan für Training und Awareness
- Verfahren für interne Audits
- Protokoll zur Management-Bewertung
- Verfahren zu Korrekturmassnahmen

Weitere Dokumente aus ISO 27002:

- Zulässiger Gebrauch von:
  - Bring Your Own Device (BYOD) Richtlinie
  - Mobilgeräten und Telearbeit
  - Kennwörtern
  - Aufgeräumter Arbeitsplatz und leerer Bildschirm (Clear Desk, Clear Screen)
  - Entsorgung und Vernichtung
- Vertraulichkeitserklärung
- Akzeptanz von ISMS-Dokumenten
- Klassifizierung von Informationen
- Zugangskontrollrichtlinie
- Anwendung von kryptografischen Massnahmen
- IT-Konzept (Informations- und Kommunikationstechnik, IKT)
- Change-Management
- Backup-Richtlinie
- Informationsübertragung
- Sicherheitsrichtlinie für Lieferanten
- Incident-Management
- BCM Vorsorgeplan

funktionieren. Der letzte Punkt, der Normpunkt 7.5, definiert Anforderungen an die Dokumentation. An verschiedenen Stellen quer durch die Normen 27001 und 27001 werden schriftliche Nachweise verlangt. Jedes Unternehmen kann weitere Dokumente definieren, die notwendig sind, zum Beispiel ein Firewall-Konzept oder ein Serverraum-Reglement.

Angemessene Kennzeichnung und Beschreibung erwünscht

Die Norm selber stellt keine Anforderungen an die Art der Dokumentation. Theoretisch könnte dies von Hand auf Papier erfolgen. Die Nachvollziehbarkeit wäre dann aber eine grosse Herausforderung. Ob nun Word und Excel, ein Dokumentenmanagementsystem wie SharePoint oder ein Wiki wie Confluence/JIRA zum Einsatz kommen, spielt keine Rolle. Erfahrungsgemäss ist es am Einfachsten, das zu verwenden, was bereits im Unternehmen etabliert ist. Der Auditor hat beispielsweise gute Erfahrungen mit Confluence als Wiki und JIRA als erweitertes Tickettool (für Incidents, Risiken, Asset-Management …) gemacht.

Verlangt wird jedoch eine angemessene Kennzeichnung und Beschreibung (zum Beispiel Autor, Titel, Metadaten) sowie ein angemessenes Format. Weiter gilt es sicherzustellen, wer das Dokument überprüft sowie schlussendlich genehmigt und freigibt.

Alle Dokumente, die im ISMS anfallen, sind entsprechend zu schützen. Je nach Kritikalität kann es sein, dass Dokumente für einen Teil der Mitarbeitenden nur lesend oder gar nicht zugreifbar sind. Andere Dokumente müssen allen involvierten Personen bekannt sein. Hier gilt es sicherzustellen, dass alle Zugriff haben und auch informiert werden, wenn neue Dokumente dazu kommen oder Dokumente verändert wurden.

Idealerweise wird im Header jeder Datei angegeben, um welche Version es sich handelt (fortlaufende Nummer, Datum oder ähnliches), wer die Anwender sind, welche Kritikalität das Dokument hat, wer der Autor (oder Inhaber) ist, wer es wann freigegeben hat, wo es abgespeichert und wann es zu überprüfen ist. Eventuell wird auch eine Versionskontrolle inklusive gemachten Änderungen geführt. Von Vorteil wird eine alte Version des Dokuments aufbewahrt. Bei ersetzten Dokumenten ist es wichtig, alle alten (ausgedruckten) Versionen wieder einzuziehen und entsprechend den Vorgaben zu vernichten. Mit der Erfüllung dieses Kapitels kann das notwendige Wissen auf- und ausgebaut, die Kommunikation gegen innen und aussen sichergestellt sowie die Dokumentation sauber und nachvollziehbar geführt werden. Es bildet somit das Fundament für ein funktionierendes ISMS.