ISO 27099

Die ISO 27099 wurde im Dezember 2016 veröffentlicht. Sie ist aktuell nur in Englisch verfügbar und trägt den offiziellen Titel «Health informatics – Information security management in health using ISO/IEC 27002 (ISO 27799:2016)», auf Deutsch Medizinische Informatik - Informationsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002. Wie im Titel ersichtlich ist, basiert diese Norm auf der ISO 27002 (aus dem Jahr 2013). Doch warum schreibe ich in einer technischen Fachzeitschrift über eine Norm im Gesundheitswesen? Beim genauen Hinschauen verstecken sich einige interessante Punkte, die jedes Unternehmen prüfen sollte.

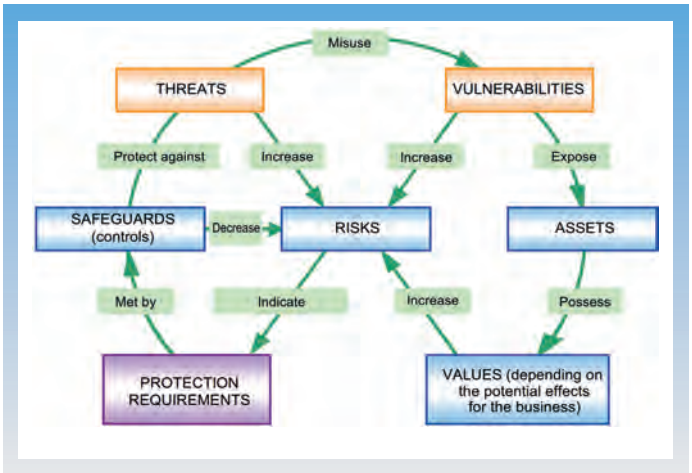


Bild 1: Risiken inklusive deren Quellen (Quelle: ISO 27799:2016, Seite 63).

Wie bereits aus dem Titel ersichtlich ist, bietet die Norm Organisationen des Gesundheitswesens eine Anleitung wie Gesundheitsdaten am besten geschützt werden können. Es handelt sich dabei beispielsweise um persönliche Gesundheitsinformationen, pseudonymisierte Daten, statistische Daten und Forschungsdaten oder klinisches/medizinisches Wissen. Anstelle Gesundheit könnte hier auch der Schutz von persönlichen Informationen und Firmenspezifisches Wissen stehen.

In Kapitel 3 werden neun zusätzliche Begriffe definiert. Es handelt sich um Gesundheitsinformatik, Gesundheitsinformationssystem, Gesundheitswesen, Gesundheitseinrichtung, Gesundheitsexperten, identifizierbare Person, Patient, persönliche Gesundheitsinformationen und Pflegethema (Hinweis: eigene Übersetzung).

Die Kapitel 5 bis 18 entsprechen eins zu eins der ISO 27002. Die jeweiligen Kapitel werden um Themen im Gesundheitswesen erweitert. Als Beispiel wird an dieser Stelle die 6.1.1 erwähnt. Eine zusätzliche Anforderung lautet: «Mindestens eine Person muss innerhalb der Organisation für die Sicherheit von Gesundheitsinformationen verantwortlich sein.» Auch dieser Punkt macht jedem Unternehmen Sinn. Jemand sollte verantwortlich für die Firmen-, Personen-, Fach- oder ähnliche Informationen sein.

Spannend sind die verschiedenen Anhänge

Die Norm definiert bei 68 von 114 Massnahmen zusätzliche Anforderungen, die in Unternehmen im Gesundheitswesen umzusetzen sind.

Drei Kapitel wurden mit zusätzlichen Kontrollen erweitert. Es handelt sich um folgende Themen:

- 14.1.1.1 Eindeutige Identifizierung von Pflegebedürftigen
- 14.1.1.2 Validierung der Ausgabedaten
- 14.1.3.1 Öffentlich zugängliche Gesundheitsinformationen

Der spannende Teil, welcher einen Mehrwert für alle Unternehmen, nicht nur im Gesundheitswesen, bietet, sind die verschiedenen Anhänge.

Der Anhang A listet 25 Bedrohungen auf und beschreibt diese ausführlich. Es handelt sich um:

- Maskerade durch Insider (einschliesslich Maskerade durch Angehörige und Hilfspersonal)
- Verschleierung durch Dienstleister (einschliesslich beauftragtem Wartungspersonal, wie Systemsoftware-Ingenieuren, Hardware-Reparaturpersonal und anderen, die pro forma einen legitimen Grund für den Zugriff auf Systeme und Daten haben)
- Maskerade durch Aussenstehende (einschliesslich Hacker)
- Unbefugte Nutzung einer Anwendung
- Einführung von schädlicher oder störender Software (einschliesslich Viren, Würmern und anderer «Malware»)
- Missbrauch von Systemressourcen
- Infiltration der Kommunikation
- Überwachung der Kommunikation
- Abstreitung (Repudition)
- Ausfall von Verbindungen
- Einbettung von bösartigem Code
- Unbeabsichtigte Fehlleitung
- Technisches Versagen des Hosts, der Speichereinrichtung oder der Netzinfrastruktur
- Ausfall der Umweltunterstützung (einschliesslich Stromausfälle und Unterbrechungen des Dienstes aufgrund von Naturkatastrophen oder vom Menschen verursachten Katastrophen).
- System- oder Netzwerksoftwarefehler
- Ausfall der Anwendungssoftware (zum Beispiel einer Anwendung für Gesundheitsinformationen)
- Betriebsfehler
- Wartungsfehler
- Benutzerfehler
- Personalmangel
- Diebstahl durch Insider (einschliesslich Diebstahl von Geräten oder Daten)
- Diebstahl durch Aussenstehende (einschliesslich Diebstahl von Geräten oder Daten)
- Vorsätzliche Schädigung durch Insider
- Mutwillige Beschädigung durch Aussenstehende
- Terrorismus

Im Anhang B ist ein Aktionsplan zur Umsetzung vorhanden. Er orientiert sich am PDCA (Plan-Do-Check-Act)-Kreislauf. Die vier Schritte werden ausführlich beschrieben. Spannend ist bei-

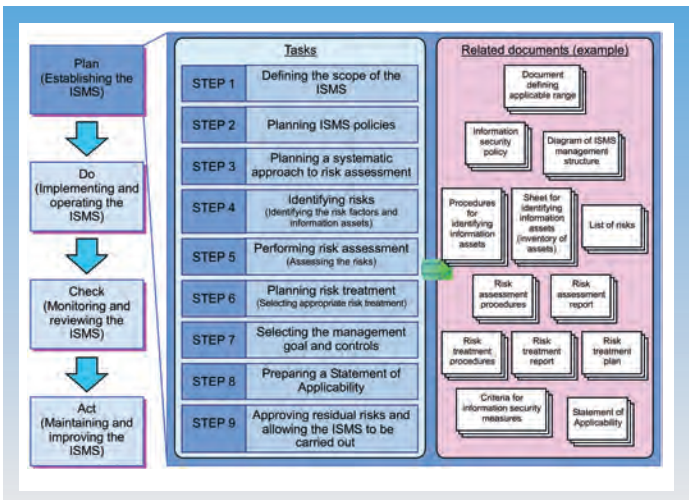
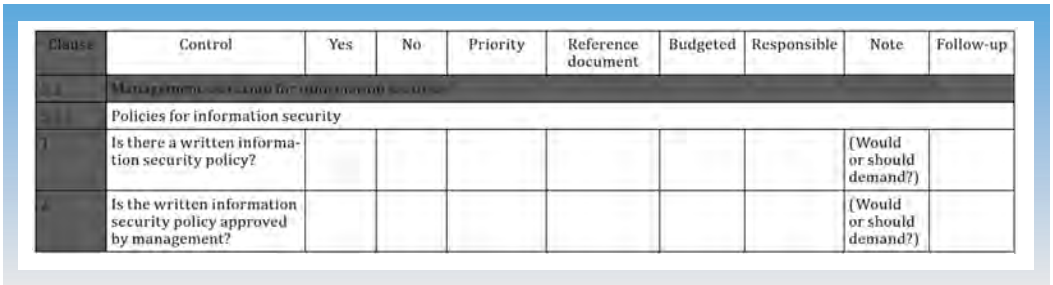


Bild 2: Aufgaben und zugehörige Dokumente zur Einrichtung des ISMS (Quelle: ISO 27799:2016, Seite 67).

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



Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
[illegible]	[illegible]								
[illegible]	Policies for information security								
7	Is there a written information security policy?							(Would or should demand?)	
[illegible]	Is the written information security policy approved by management?							(Would or should demand?)	

Bild 3: Checkliste zur Umsetzung (Quelle: ISO 27799:2016, Seite 72).

spielsweise die Beziehung zwischen Risiken und deren Quellen. Jeweils am Ende jedes der vier Themengebiete werden die einzelnen Teilschritte, inkl. deren Ergebnisse (Dokumente), aufgeführt.

In Bild 2 ist dasjenige des Schrittes «Plan» abgebildet. Im Anhang C ist eine Checkliste abgebildet. Sie listet die Kontrollen aus der ISO 27799 auf und enthält Spalten, in denen überprüft werden kann, ob die Kontrollen erfüllt wurden. Die Spalten enthalten:

- Klausel und Nummer der Massnahme
- Frage (zum Beispiel Gibt es eine schriftliche Informationssicherheitspolitik?)
- Implementierung (Ja/Nein)
- Priorität
- Referenzdokument (Name des Dokuments zu dieser Klausel)
- Budget (wurde ein entsprechendes Budget genehmigt)
- Verantwortlichkeit für die Umsetzung
- Hinweis
- Folgemassnahmen

Diese Tabelle (Bild 3) ist ideal für die Durchführung eines internen Audits.

Somit müssen keine eigenen Fragen «erfunden» werden, sondern können direkt von hier übernommen werden.

Fazit

Obschon die ISO 27799 sich an Unternehmen im Gesundheitswesen richtet, bietet sie für jedes Unternehmen einen Mehrwert. Vor allem die Anhänge sollten in jedes Informationssicherheitsmanagementsystem (ISMS) einfliessen. Bedrohungen werden ausführlich beschrieben und helfen, nicht eine eigene Definition erstellen zu müssen. Damit der PDCA-Kreislauf umgesetzt werden kann, sind alle Aufgaben pro Schritt erklärt und das notwendige Ergebnis festgehalten. Mit dem Fragenkatalog können interne Audits schnell und umfassend durchgeführt werden. Die Norm hilft mit klaren Schritten jedem Unternehmen viel Zeit zu sparen.