ISACA Switzerland Chapter

Nr. 01 | März 2021 | www.isaca.ch

NEWSLETTER

ISO 27002
Nach acht Jahren ist der Nachfolger der ISO 27002:2013 als Draft veröffentlicht worden. **Seite 69**

CDPSE Zertifikat
Das neue ISACA Zertifikat 'Certified Data Privacy Solutions Engineer' hat es in sich. **Seite 72**

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder **Seite 73**

ISO 27002

Informationssicherheit in neuem Gewand

Am 28. Januar 2021 war es endlich soweit. Nach acht Jahren ist der Nachfolger der ISO 27002:2013 als Draft veröffentlicht worden. Noch läuft die 12-wöchige Eingabefrist für Kommentare, danach wird diese verbindlich. Unternehmen haben nach der finalen Veröffentlichung eine Übergangsfrist, um ihr ISMS auf den aktuellen Stand zu bringen. Wichtig also, sich bereits jetzt mit dieser Norm auseinander zu setzen.

Von Andreas Wisler

Bereits länger wurde diskutiert, wann der Nachfolger der in die Jahre gekommenen ISO 27002 «Information technology — Security techniques — Code of practice for information» endlich veröffentlicht wird. Normalerweise haben ISO-Normen einen Lebenszyklus von ca. fünf Jahren, hier sind es bereits acht Jahre. Doch das Warten hat sich gelohnt. Die neue Ausgabe macht einen aufgeräumten und umfassenden Eindruck. Dies beginnt bereits im Titel, dieser lautet neu «Information security, cybersecurity and privacy protection — Information security controls». Es ist ersichtlich, dass die Informationssicherheit in einem globalen Kontext angeschaut wird und alle Elemente berücksichtigen möchte (Cybersecurity) und dass auch hier der Datenschutz einen grösseren Stellenwert bekommt (Privacy Protection).

Struktur

Am Auffälligsten ist sicherlich, dass die Norm eine neue Struktur bekommen hat. Während in der alten Norm 14 Kapitel enthalten sind, sind es nun nur noch deren vier. Es handelt sich um die Themenblöcke 5 Organizational controls (37), 6 People controls (8), 7 Physical controls (14) und 8 Technological controls (34). In Klammern sind die Anzahl Massnahmen aufgeführt. Wer die Norm kennt, hat sicherlich bemerkt, dass es nun «nur» noch 93 Punkte sind, gegenüber den 114 bisherigen. Weiter ersichtlich ist, dass 11 neue Massnahmen dazu gekommen sind. Wer jetzt denkt, dass es hier tatsächlich zu einer Reduktion gekommen ist, irrt sich. Gestrichen wurde genau eine einzige Massnahme. Es handelt sich um die 11.2.5 (Removal of assets). Alle anderen Massnahmen wurden sinnvoll gruppiert. Damit erhöht sich der Aufwand zur Umsetzung für ein Unternehmen. Es wird auch schwieriger, entsprechende Massnahmen auszuklammern, wenn diese im

eigenen Unternehmen nicht passen. Dies könnte beispielsweise der Fall sein, wenn ein Unternehmen keine Software entwickelt. Auch die klassischen Punkte «Ladebereiche» oder «Export von Kryptografie» sind in andere Massnahmen integriert worden und können damit nicht mehr ausgeschlossen werden.

Normalerweise werden alle Begrifflichkeiten an einer zentralen Stelle in der ISO 27000 erläutert, damit diese in allen weiteren 27000er-Normen einheitlich verwendet werden. Die 2021er-Ausgabe führt 37 «neue Begriffe» ein. Teilweise werden diese aus anderen Normen angepasst übernommen (unter anderem aus ISO 9000, 15489, 22301, 27301, 27035, 27050, 29100, 29134, 30000, 31000). Zum ersten Mal werden auch diverse Abkürzungen aufgezeigt, insgesamt sind es deren 33.

Wie bereits erwähnt, sind nur noch vier Kapitel vorhanden. Folgende Definition wurde dabei getroffen:

- Kategorie «Menschen», wenn sie einzelne (oder mehrere) Menschen betreffen;
- Kategorie «Physisch», wenn sie physische Objekte betreffen;
- Kategorie «Technologie», wenn sie die Technik betreffen;
- ansonsten werden sie als «organisatorisch» eingestuft

Bewertung

Neu wird jede Massnahmen eingestuft. Dies sieht für die 5.1 Policies for information security wie folgt aus (siehe auch Bild 1):

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

Bild 1: 5.1 Policies for information security

Der **Kontrolltyp** ist ein Attribut zur Betrachtung von Kontrollen aus der Perspektive, wann und wie sich die Kontrolle auf das Risikoergebnis im Hinblick auf das Auftreten eines Informationssicherheitsvorfalls auswirkt. Die Attributwerte bestehen aus #Präventiv (die Kontrolle wirkt, bevor eine Bedrohung auftritt), #Detektiv (die Kontrolle wirkt, wenn eine Bedrohung auftritt) und #Korrektiv (die Kontrolle wirkt, nachdem eine Bedrohung aufgetreten ist).

Die **Informationssicherheitseigenschaften** sind die klassischen Schutzziele in der Informationssicherheit. Die Attributwerte bestehen aus #Vertraulichkeit, #Integrität und #Verfügbarkeit.

Cybersicherheitskonzepte ist ein Attribut zur Betrachtung von Kontrollen aus zeitlicher Abfolge. Sie leiten sich aus dem in der ISO/IEC TS 27101 beschriebenen Cybersicherheitsrahmenwerk ab. Die möglichen Attributwerte bestehen aus #Identify, #Protect, #Detect, #Respond und #Recover.

Operative Fähigkeiten ist das behandelte Themengebiet. Attributwerte bestehen aus #Governance, #Asset_management, #Information_protection, #Human_resource_security, #Physical_security, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Threat_and_vulnerability_management, #Continuity, #Supplier_relationships_security, #Legal_and_compliance, #Information_security_event_management und #Information_security_assurance.

Sicherheitsdomänen ist ein Attribut zur Betrachtung von Kontrollen aus der Perspektive von Informationssicherheitsbereichen, Fachwissen, Dienstleistungen und Produkten. Die Attributwerte bestehen aus #Governance_und_Ecosystem, #Protection, #Defence und #Resilience.

Aufbau der Massnahmen

Jede Massnahmen hat folgende Struktur:

- Control title: Kurzer Name des Controls
- Attribute table: Die Tabelle zeigt den/die Wert(e) jedes Attributs für das gegebene Control (siehe vorheriges Kapitel)
- Control: Beschreibung der Massnahme
- Purpose: Erläutert den Zweck des Controls
- Guidance: Implementierungsanleitung für das Control
- Other information: Erläuternder Text oder Verweise auf andere zugehörige Dokumente

Wie bereits erwähnt, haben die Massnahmen teilweise grössere Veränderungen erhalten. Dies ist bereits bei der ersten Massnahme ersichtlich (Neu 5.1 Policies for information security). In der 2013er Ausgabe lautete die Anforderung «A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties», neu lautet diese «Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur». Es ist ersichtlich, dass einige Unklarheiten aus der bisherigen Norm präzisiert wurden. Für ein Unternehmen gilt es damit, die vorhandenen Richtlinien über den gesamten Lebenslauf aktuell zu halten.

Neue Massnahmen

Die neue 27002er-Norm bringt 11 neue Massnahmen. Um welche es sich handelt, lesen Sie im Kasten rechts.

Anhang

Im Anhang A der Norm werden alle Steuerelemente und Attribute der Massnahmen nochmals aufgezeigt. Es wird ebenfalls aufgezeigt, wie die entsprechenden Massnahmen auszuwählen und zu bewerten sind.

Der Anhang B zeigt die Verknüpfung der neuen Massnahmen zu den Massnahmen aus ISO 27002:2013 sowie umgekehrt von der alten zur neuen ISO 27002:2021.

Fazit

Die ISO 27002 hat einen komplett neuen Anstrich bekommen. Die bisherigen Massnahmen wurden in vier Kategorien unterteilt und zusammengeführt, wo sinnvoll. 11 Massnahmen sind neu dazugekommen, jedoch nur eine einzige ge-

DER AUTOR

Andreas Wisler ist Inhaber der Firma goSecurity AG (https://goSecurity.ch). Er ist CISA, CDPSE, ISO 22301, 27001 sowie der erste Schweizer ISO 27701 Lead Auditor. Seit über 20 Jahren ist er im IT-Sicherheitsbereich tätig und unterstützt Firmen beim Aufbau eines ISMS und der Erlangung des ISO 27001 Zertifikats. Alle zwei Wochen veröffentlicht er den Podcast «Angriffslustig», zu abonnieren unter https://angriffslustig.ch.

strichen. In der Summe sind es nun 93 Massnahmen. Die Erweiterung mit Steuerelementen und Attributen zeigt, was mit einer Massnahme bezweckt wird.

Die Ausgabe 2021 hinterlässt einen sauberen und umfassenden Eindruck. Jedoch ist es nicht damit getan, nur die 11 neuen Massnahmen umzusetzen, denn in den bekannten Massnahmen «verstecken» sich neue bzw. erweiterte Anforderungen. Noch ist die Norm nicht final, doch schon jetzt sollten sich alle, die ein ISMS betreiben, mit dieser Norm auseinandersetzen und die ersten Schritte einleiten. Nach der Veröffentlichung bleibt nur eine kurze Übergangszeit, bis durch eine akkreditierte Stelle nach der ISO 27002:2021 geprüft wird.

NEUE MASSNAHMEN DER 27002ER-NORM

Kapitel	Titel	Anforderung
5.7	Threat intelligence	Information relating to information security threats should be collected and analysed to produce threat intelligence
5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.
5.30	ICT readiness for business continuity	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.
7.4	Physical security monitoring	Premises should be continuously monitored for unauthorized physical access.
8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.
8.10	Information deletion	Information stored in information systems and devices should be deleted when no longer required.
8.11	Data masking	Data masking should be used in accordance with the organization's topic-specific policy on access control and business requirement, taking legal requirements into consideration.
8.12	Data leakage prevention	Data leakage prevention measures should be applied to systems, networks and endpoint devices that process, store or transmit sensitive information.
8.16	Monitoring activities	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.
8.22	Web filtering	Access to external websites should be managed to reduce exposure to malicious content.
8.28	Secure coding	Secure coding principles should be applied to software development.