Informationssicherheitsprozesse

Im März 2021 wurde die ISO 27022 veröffentlicht. Sie schliesst eine alte Lücke in der Normenreihe. Die neue Norm definiert Prozesse im Bereich der Informationssicherheit und hilft damit, die Normanforderungen aus der ISO 27001 zu schliessen. Zeit also, diese etwas genauer anzuschauen.

Die Norm trägt den offiziellen Titel «Information technology — Guidance on information security management system processes» und wurde als «Technical Specification» veröffentlicht. Sie ist keine verpflichtende Norm, wie diese selber in der Einleitung hinweist. Sie dient als Idee und die beschriebenen Prozesse dürfen, ja sollen sogar, angepasst werden.

Wie von ISO-Normen bekannt werden in Kapitel 3 die Grundbegriffe erläutert. Obwohl alle Begriffe seit einigen Jahren in der ISO 27000 zentral gesammelt werden, fehlen doch einige, beziehungsweise kommen mit neuen Normen dazu. Diesmal sind es sechs Begriffe: core process, integrated management system, key goal indicator, key performance indicator, management process und support process.

Prozesse

Das Dokument teilt die Prozesse in die drei Kategorien Management, Haupt (Core) und Support Prozesse ein. Insgesamt werden 17 Prozesse beschrieben. Es handelt sich dabei um die folgenden Prozesse:

- Information security governance/management interface
- Security policy management
- Requirements management
- Information security risk assessment
- Information security risk treatment
- Security implementation management
- Control outsourced services
- Assure necessary awareness and competence
- Information security incident management
- Information security change management
- Internal audit
- Performance evaluation
- Information security improvement
- Records control
- Resource management
- Communication
- Information security customer relationship management

Struktur

Bei der Struktur wurde darauf geachtet, die Anforderungen aus der ISO/IEC 33004 «Prozess Referenz Modell» einzuhalten. Im Annex A wird darauf eingegangen, warum die Norm diese Anforderungen erfüllt. Alle geforderten Punkte werden erfüllt, da alle Prozessbeschreibungen folgende Struktur enthalten:

- Prozess Kategorie
- Kurze Beschreibung
- Prozess-Grafik/Flussdiagramm
- Ziele/Zweck
- Eingabe und Ausgabe
- Aktivitäten/Funktionen
- Referenzen

Die Norm weist in der Übersicht nochmals darauf hin, dass diese Prozesse nicht «out of the box» verwendet werden sollten, ohne diese an die Ziele, Bedürfnisse und individuellen Anforderungen des eigenen Unternehmens anzupassen. Zusätzlich sollte für jeden ISMS-Prozess der notwendige Reifegrad ermittelt, implementiert und betrieben werden. Dabei kann es auch sein, dass ein vorgeschlagener Prozess im eigenen Unternehmen gar nicht zum Einsatz kommt und daher weggelassen werden kann.

Beispiel: Security Policy Management

Im Unternehmen fallen an verschiedenen Orten Richtlinien an. Diese gilt es in einen geordneten Ablauf zu bringen. An diesem Beispiel soll aufgezeigt werden, wie das Dokument die entsprechenden Prozesse beschreibt.

Zuerst wird angegeben, in welche Kategorie dieser Prozesse fällt. In unserem Beispiel ist dies «Core process», also ein Hauptprozess. Danach folgt eine kurze Beschreibung: «Der Prozess zur

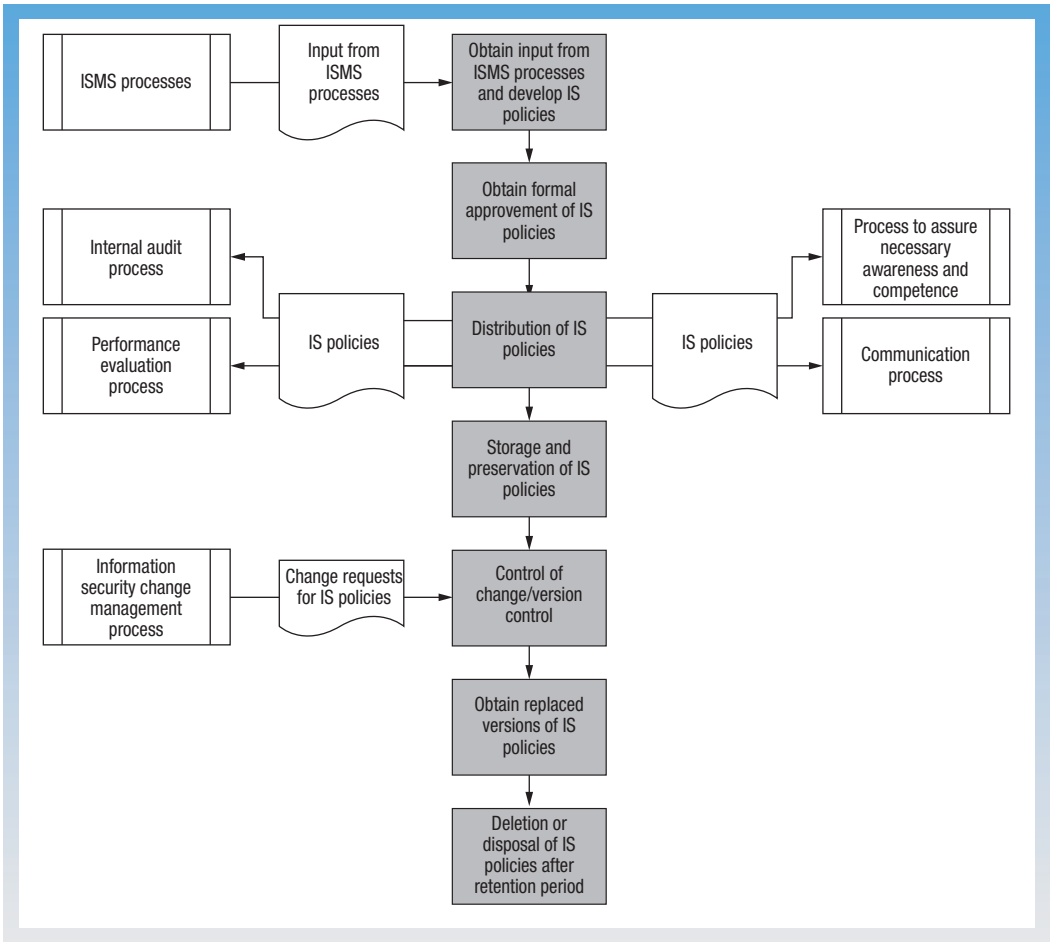

Bild: OutISO 27022:2021, Seite 10.

Prozess zur Sicherstellung des notwendigen Bewusstseins und Kompetenz.

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

Bild: Pixabay

Ein alte Lücke wurde durch die Norm ISO 27022 geschlossen.

Verwaltung der Sicherheitspolitik sollte ein Prozess zur Entwicklung, Pflege und Aufbewahrung von Informationssicherheitsrichtlinien, Standards, Verfahren und Leitlinien (als ‹IS-Richtlinien› bezeichnet) sein». Das Ziel ist dabei: «Sicherstellen, dass geeignete Strategien, Standards, Verfahren und Leitlinien (IS-Strategien) in Bezug auf die Informationssicherheit entwickelt, gepflegt, verfügbar und von der Zielgruppe verstanden werden.» Hier werden gleich verschiedene Anforderungen aus der ISO 27001 verpackt (zum Beispiel 5 Management Verantwortung, 7.5 Gelenkte Dokumente, A.5 Informationssicherheitsrichtlinien).

Die Prozessinputs sind hier fast selbstsprechend: von allen anderen Informationssicherheitsprozessen (als Grundlage für Richtlinien) und aus dem Änderungsmanagementprozess. Das Resultat sind dann geeignete Richtlinie für den Kommunikationsprozess, den internen Auditprozess, die Leistungsbewertung, Aufzeichnungskontrolle und den Prozess zur Sicherstellung des notwendigen Bewusstseins und Kompetenz.

Dieser Prozess umfasst dann die folgenden Schritte:

- Einholung von Informationen aus den ISMS-Prozessen und der Entwicklung von IS-Richtlinien
- Einholung der formellen Genehmigung
- Verteilung der IS-Richtlinien (über den Kommunikationsprozess)
- Speicherung und Aufbewahrung
- Kontrolle der Änderungen/Versionskontrolle
- Archivierung (inkl. Zugriff) ersetzter Versionen
- Löschung oder Entsorgung nach der Aufbewahrungsfrist

Als Referenzen werden die passenden Punkte angegeben. In unserem Beispiel sind es ISO/IEC 27001:2013, 5.2, 7.4, 7.5 sowie ISO/IEC 27003:2017, 5.2, 7.4, 7.5 und Annex A. In der Grafik auf Seite 22 wird der Prozess grafisch gezeigt. Alle weiteren, bereits erwähnten Prozesse, folgen dem identischen Aufbau.

Fazit

Gerade beim Aufbau eines Informationssicherheits-Mangementsystems steht jedes Unternehmen vor einem gewaltigen Berg von Anforderungen. Diese alle korrekt umzusetzen, ist alles andere als einfach. Die ISO 27022 hilft dabei, die notwendigen Prozesse auf einer guten Basis aufzubauen. Die Prozesse sind einfach und verständlich erklärt und können einfach an die eigenen Bedürfnisse angepasst werden. Damit lässt sich ein gutes Fundament bauen und gleichzeitig sehr viel Zeit sparen.