Kai Jendrian

Der Standard ISO/IEC 27001:2013

Nach acht Jahren wurde 2013 der ISMS-Standard ISO/IEC 27001 überarbeitet. In diese Überarbeitung sind viele Erfahrungen aus der Praxis eingeflossen, die ein Arbeiten nach dem neuen Standard vereinfachen sollen. In diesem Beitrag werden die wesentlichen Änderungen im Standard und im Anhang A vorgestellt. Um es vorweg zu nehmen: Die Änderungen sind weder belanglos noch revolutionär, sondern überwiegend praxisrelevante Verbesserungen.

Einführung

Gut acht Jahre nach der Veröffentlichung des Vorläufers wurde im Oktober 2013 der landläufig als ISO 27001 bekannte Informationssicherheitsstandard in der Version ISO/IEC 27001:2013 „*Information technology -- Security techniques -- Information security management systems -- Requirements*“ [ISO_27001_2013] veröffentlicht. Die optisch auffälligste Änderung ist die Anpassung der Gliederung an die inzwischen einheitlichen Vorgaben für ISO-Standards für Managementsysteme, die aus dem Annex SL der ISO/IEC Directives, Part1 [Annex_SL] abgeleitet wurden.[1] Der Annex SL beschreibt eine einheitliche Struktur für alle ISO-Standards, die Managementsysteme betreffen, um unterschiedliche Themen in einem Unternehmen, wie bspw. das Qualitäts- oder Umweltmanagement, besser miteinander zu verzahnen.

Die im Zusammenhang mit der ISO 27001[2] stehenden Standards ISO/IEC 27000:2014 „*Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*“ [ISO_27000_2014] und ISO/IEC 27002:2013 „*Information technology -- Security techniques -- Code of practice for information security controls*“ [ISO_27002_2013] wurden ebenfalls in einer überarbeiteten Form veröffentlicht. Ein Ziel dieser Überarbeitungen war die Verwendung von einheitlicheren und klareren Begriffen. Die Umbenennung des ISO 27002 ist ein Beispiel hierfür: Im neuen Titel wurde aus „*Code of practice for information security management*“ ein „*Code of practice for information security controls*“, was den eigentlichen Inhalt des Standards deutlich besser wiedergibt.

Die Kapitel zwei und drei des ISO/IEC 27001:2013 wurden gegenüber der Version 2005 signifikant gekürzt und bestehen nur noch aus Verweisen auf den ISO 27000 in der aktuellen Version. Der Verweis auf eine zentrale Quelle für die Definition relevanter Begriffe unterstützt die Bestrebungen nach Verwendung einer einheitlichen Nomenklatur.

Zum Zeitpunkt des Erscheinens dieses Beitrags sind weitere Standards der 270xx-Reihe noch nicht an den ISO 27001 angepasst. Besonders bedauerlich ist, dass gerade der ISO/IEC 27003:2010 *“Information technology -- Security techniques -- Information security management system implementation guidance*“ [ISO_27003_2010] noch nicht in einer aktualisierten Fassung vorliegt. Da bis Ende September 2015 alle bisherigen Zertifikate nach ISO 27001 auf die Version 2013 umgestellt sein müssen, wäre eine praktische Hilfestellung zur Umsetzung der neuen Version des Standards für alle Beteiligten sehr hilfreich gewesen. So kann es sein, dass sich einzelne Interpretationen der Vorgaben des ISO 27001 im Verlauf des kommenden Jahres noch ändern werden. Auch für Auditoren wäre es hilfreich gewesen, wenn der ISO/IEC 27007:2011 „*Information technology -- Security techniques -- Guidelines for information security management systems auditing*“ [ISO_27007_2011] zeitnah überarbeitet worden wäre.

Vom Asset zum Prozess

Die 2005er Version des ISO 27001 hat einen wesentlichen Schwerpunkt auf die Betrachtung der Risiken in Bezug auf Assets gelegt. Auch wenn der Begriff Assets im Sinne des ISO 27001 schon immer alle Unternehmenswerte inklusive der wesentlichen Informationen einer Organisation beinhaltet hat, wurde in der Praxis sehr häufig der Fokus auf die IT-Assets einer Organisation gelegt – besonders auf die sogenannten *supporting assets*, deren Definition sich im Annex B des ISO/IEC 27005:2011 „*Information technology – Security techniques – Information security risk management*“ [ISO_27005_2011] findet und zu denen alle IT-Systeme zählen, mit denen eine konkrete Informationsverarbeitung realisiert wird. Mit der Version 2013 des ISO 27001 wurde die Bedeutung von Informationen als *primary assets* einer Organisation klar in den Vordergrund gestellt – es soll unzweifelhaft deutlich werden, dass der ISO/IEC 27001:2013 ein Managementsystem-Standard und kein IT-Security-Standard ist. Letzte Zweifel werden in der Einleitung zum ISO 27001 ausgeräumt: Die Bedeu-

1 Siehe auch IRCA Briefing Note [IRCA_Briefing_Note].

2 Im Folgenden werden die umgangssprachlichen Namen der Standards verwendet, solange sich aus dem Kontext klar ergibt, welcher Standard genau gemeint ist.

Kai Jendrian

Security Consultant bei der Secorvo Security Consulting GmbH, lizenzierter Auditor und Mitglied im Board des deutschen OWASP Chapters. Beratungsschwerpunkte: Information Security Management und Anwendungssicherheit.
E-Mail: kai.jendrian@secorvo.de

tung von Informationssicherheit als Teil der Steuerung einer Organisation wird explizit beschrieben, genau wie die Erwartung der Integration der Informationssicherheit in die Aufbau- und Ablauforganisation einer Organisation.

Diese Schwerpunktsetzung erklärt auch, warum der ISO 27001 nicht mehr explizit auf den ISO 27005 verweist, sondern im Text direkt den Umgang mit Risiken nach ISO 31000:2009 *"Risk management -- Principles and guidelines"* [ISO_31000_2009] in den Vordergrund stellt. Eine neue Version des ISO 27005 sollte sich in das Zusammenspiel der Standards einpassen; zur Zeit referenziert der ISO 27005 allerdings sehr konkret auf den ISO/IEC 27001:2005 – eine uneingeschränkte Nutzung ohne Interpretation ist bis zur Veröffentlichung einer angepassten Version daher erst einmal nicht möglich.

Wer bin ich und was will ich?

An der Gliederung des ISO/IEC 27001:2013 sieht man deutlich, dass Erfahrungen aus acht Jahren Praxis in die Überarbeitung des Standards eingeflossen sind. Die wenig intuitive Gliederung des ISO/IEC 27001:2005 wurde komplett überarbeitet und Überschneidungen des damaligen Kapitel vier mit den Kapiteln fünf bis acht wurden eliminiert.

Kapitel vier des ISO/IEC 27001:2013 formuliert nun als Grundvoraussetzung an ein Information-Security-Managementsystem (ISMS), dass eine Organisation zunächst den Kontext verstehen muss, in dem das ISMS operiert. Für eine genauere Bestimmung des Begriffes Kontext (*context*) verweist der ISO 27001 auf den Abschnitt 5.3 im ISO 31000 mit dem Titel *„Establishing the context"*, in dem auf gut zwei Seiten beschrieben ist, welche Erwartungshaltung an die Bestimmung des Kontexts aus Sicht des Standards existiert. Weiter wird im ISO 27001 gefordert, die Anforderungen aller Beteiligten (*interested parties*) zu ermitteln; dabei kann es sich um Kunden, Lieferanten, Behörden und andere „Dritte" handeln.

Im Standard wird explizit erwähnt, dass unter die Bestimmung des Kontextes besonders auch die Ermittlung rechtlicher und vertraglicher Anforderungen fällt. Die ermittelten Ergebnisse sind zu verwenden, um den Geltungs- oder Anwendungsbereich (*scope*) des ISMS in der Organisation festzulegen.

Eine weitere wesentliche Einflussgröße für den Anwendungsbereich sind die Schnittstellen zwischen Aktivitäten, die innerhalb der Organisation ausgeführt und solchen, die außerhalb der Organisation umgesetzt werden. Ausgehend davon, dass der ISO 27001 auf die *primary assets* fokussiert, sind hier vor allem Informationsflüsse zu betrachten, die aus Geschäftsprozessen resultieren.

Scope ist, wo das ISMS lebt

Ein Informationssicherheitsmanagementsystem muss nicht immer für eine ganze Organisation gelten. Allerdings stellt gerade die Definition eines passenden Anwendungs- oder Geltungsbereiches (*scope*) eine große Herausforderung dar. Bei dieser Definition konnten bisher die Ausführungen des ISO 27003 herangezogen werden. Da dieser Standard in der derzeit gültigen Version sehr stark mit dem ISO/IEC 27001:2005 verknüpft ist, ist dies – wie beim ISO 27005 – derzeit nur eingeschränkt möglich.

Trotzdem ist es empfehlenswert, sich bis zur Veröffentlichung eines überarbeiteten ISO 27003 an die Empfehlungen aus der aktuellen Version des Standards zu halten und diese, ggf. interpretiert, anzuwenden. Konkret bedeutet das, dass auch für ein ISMS nach ISO/IEC 27001:2013 ein Anwendungsbereich festgelegt wird, der die organisatorischen Anwendungsbereiche und deren Grenzen (*organizational scope*), den IT-technischen Anwendungsbereich und dessen Grenzen (*ICT scope*) sowie die geografischen bzw. physischen Bereiche und deren Abgrenzungen berücksichtigt.

Für das ISMS einer Organisation spielen vor allem die Prozesse mit kritischen Informationsflüssen im Anwendungsbereich eine wesentliche Rolle, so dass deren Betrachtung zum Verständnis der Organisation und ihres Umfeldes unerlässlich ist. Eine weitere wichtige Eingangsgröße für die Bestimmung des Anwendungsbereichs sind relevante externe und interne Einflussfaktoren. Im ISO 31000 werden diese Einflussfaktoren etwas genauer bestimmt: Zu den externen Einflussfaktoren zählen bspw. rechtliche Vorgaben, der soziale Kontext, die Wettbewerbssituation, finanzielle Umstände aber auch Beziehungen zu Dritten.

Die internen Einflussfaktoren stehen im Zusammenhang damit, wie eine Organisation ihre Ziele erreichen will: Hier spielen die Aufbau- und Ablauforganisation, die Unternehmenskultur, die Unternehmensstrategie aber auch jeder weitere interne Faktor, der ein ISMS beeinflussen kann, eine Rolle.

Zur Bestimmung eines konkreten Scopes können die folgenden Fragestellungen eine gute Hilfestellung leisten:

- Welche (Teil-)Organisation oder Organisationseinheit soll vom ISMS abgedeckt werden?
- Was sind die (informationsverarbeitenden) Prozesse und die zugehörigen Datenflüsse?
- Welche Anforderungen stellen Dritte an die Organisation (besonders auch rechtlicher Natur)?
- Welche Dritte sind zu berücksichtigen (Kunden, Mitarbeiter, Lieferanten, Aufsichtsbehörden, ...)?
- Welche (impliziten) Erwartungen stellen Dritte an die Organisation?

Nach Ermittlung aller relevanten Einflussfaktoren ist der daraus abgeleitete Anwendungsbereich (*Scope*) des ISMS festzulegen und als dokumentierte Information (*documented information*) bereitzustellen.

Schon an dieser Stelle des Standards wird deutlich, dass eine Erfüllung der Anforderungen aus dem ISO 27001 nicht ein vorgegebenes Sicherheitsniveau bestätigt, sondern dass sichergestellt ist, dass eine Organisation alle Anforderungen erfüllt, um die sich selbst gesetzten Sicherheitszielvorgaben zu erfüllen und somit jedes Unternehmen sein individuelles Sicherheitsniveau festlegt.

Leadership – wer steuert?

Die Verantwortung zur Steuerung eine ISMS obliegt dem *Top Management* einer Organisation. In der Praxis hat sich häufig die Frage gestellt, wer denn genau das Top Management im konkreten Fall ist: Muss in einer AG der Vorstandsvorsitzende persönlich ins ISMS involviert sein? Mit Veröffentlichung des ISO/IEC 27000:2014 gibt es jetzt eine eindeutige Antwort auf die Frage, da dort der Begriff *top management* klar definiert ist: *top management* beschreibt den Personenkreis, der eine Organisation (oder bei eingeschränktem Anwendungsbereich eine Organisa-

tionseinheit) auf höchstem Level steuert. In der Praxis ist es also wichtig, das zum ISMS passende Management ins Boot zu holen.

Der ISO 27001 widmet der Führungsverantwortung (*leadership*) des Managements ein ganzes Kapitel, in dem einige wichtige Forderungen an die Leitungsebene formuliert sind, aus denen der Einsatz des Top Managements für das ISMS einer Organisation erkennbar ist. Hierunter fallen u. a. die Festlegung von Sicherheitszielen und Verabschiedung einer Sicherheitspolitik[3], die Integration des ISMS in die Prozesse der Organisation, die Bereitstellung angemessener Ressourcen sowie die kontinuierliche Verbesserung des ISMS.

Zielvorgaben für die Sicherheit

Eine weitere Neuerung im ISO 27001 ist die explizite Vorgabe einer Formulierung von Zielvorgaben zur Informationssicherheit (*information security objectives*). Es ist auffällig, dass hier bewusst nicht der unspezifischere Begriff *goal* verwendet wurde, der sich in diesem Zusammenhang eher mit Zielsetzung übersetzen lassen würde. Die Autoren der Norm setzen bewusst den Schwerpunkt auf die Formulierung von überprüfbaren konkreten Zielvorgaben (*objectives*).

Es ist eine Leitungsaufgabe, neben der Informationssicherheitsleitlinie (*information security policy*) vor allem auch die Zielvorgaben zu etablieren und diese mit der strategischen Ausrichtung einer Organisation in Einklang zu bringen. Die Zielvorgaben sind explizit in der *information security policy* zu dokumentieren. Im Detail werden im ISO 27001 weitere konkrete Anforderungen an die Zielvorgaben formuliert: Sie müssen natürlich mit der *information security policy* im Einklang stehen und sollen auch überprüfbar (*measurable*) sein. Die Zielvorgaben müssen in dokumentierter Form vorliegen – in der Praxis wird es sich anbieten, sie im Zusammenspiel mit der *information security policy* zu erstellen und ggf. als Anhang zu dieser zu veröffentlichen, denn die Kommunikation sowie Überarbeitung der Zielvorgaben ist nach ISO 27001 ebenfalls Pflicht. Die Veröffentlichung in einem Dokument mag gewisse Herausforderungen mit sich bringen: Nach dem Standard sind die Ergebnisse des Risikoprozesses in den Zielvorgaben zu berücksichtigen, daher erscheint für die Zielvorgaben ein kürzerer Überarbeitungszyklus als der der *information security policy* angeraten.

Mit der Formulierung von Zielvorgaben ist es aber noch nicht getan: Die Erreichung der Zielvorgaben muss konkret geplant werden. Der ISO 27001 fordert allerdings nicht, dass diese Planung als *documented information* vorliegen muss. Es darf auch nicht bei der Planung alleine bleiben. Der ISO 27001 fordert auch die Umsetzung und das Vorhalten von dokumentierten Nachweisen für die Implementierung der Pläne.

Die explizite Betonung der Bedeutung von Zielvorgaben für Informationssicherheit ist neu im ISO/IEC 27001:2013. Die Ermittlung und Berücksichtigung dieser Zielvorgaben dürfte in der Praxis für Organisationen, die ihr ISMS nach ISO/IEC 27001:2005 aufgebaut haben ggf. eine Herausforderung werden.

3 Aus den vielen möglichen Übersetzungen von *policy* wird in diesem Artikel der Begriff *Politik* verwendet. In der Praxis finden sich auch häufig die Begriffe *Leitlinie* oder *Richtlinie*.

Wer schreibt, der bleibt – dokumentierte Informationen

Mit dem ISO/IEC 27000:2014 und damit auch mit der Überarbeitung des ISO 27001 bricht die ISO auch sprachlich mit der veralteten Vorstellung, dass alle Sachverhalte des ISMS in Dokumenten oder Aufzeichnungen festgehalten werden müssen.

In dem neuen ISO 27001 ist nicht mehr von *documents* und *records* die Rede, sondern von *documented information*, einem Begriff, der im ISO 27000 als ‚gelenkte Information' beschrieben ist. Dort wird auch klargestellt, dass es keine formalen Anforderungen an Format oder Speichermedium für die Dokumentation gibt und hierunter auch alle Informationen fallen, die in Vorgängerversionen als Dokumente oder Aufzeichnungen bezeichnet wurden.

Eine weitere Neuigkeit im ISO/IEC 27001:2013 ist der Wegfall des Abschnitts mit einer Auflistung der verbindlich geforderten Dokumente. Die geforderten Dokumente lassen sich aus dem Standard allerdings herauslesen:

- Scope des ISMS (4.3)
- Informationssicherheitspolitik (5.2.e)
- Methodik zur Beurteilung von Risiken (6.1.2)
- Statement of Applicability (6.1.3.d)
- Risikobehandlungsplan (6.1.3.e)
- Risikobehandlungsprozess (6.1.3)
- Sicherheitsziele (6.2)
- Nachweise zur Kompetenz (7.2.d)
- Nachweise über die korrekte Ausführung der Prozesse des ISMS (8.1)
- Nachweise über die Ergebnisse von Risikobeurteilungen (8.2)
- Nachweise zu Ergebnissen der Umsetzungen des Risikobehandlungsplans (8.3)
- Nachweise zur Kontrolle der Sicherheit und der Wirksamkeit des ISMS (9.1)
- Nachweise über die Durchführung von Audits und die Auditergebnisse (9.2.g)
- Nachweise über die Ergebnisse von Management-Reviews (9.3)
- Identifizierte Abweichungen und Aktivitäten zur Behebung (10.1.f)
- Ergebnisse von Korrekturen (10.1.g)

Aus dem Anhang A lassen sich weitere Forderungen nach dokumentierten Informationen extrahieren:

- Satz geeigneter Sicherheitsrichtlinien (A.5.1.1)
- Festlegung der Verantwortungen (A.6.1.1)
- Richtlinie für mobile Endgeräte (A.6.2.1)
- Richtlinie für die Telearbeit (A.6.2.2)
- Prozess zum Umgang mit Sicherheitsverstößen (A.7.2.3)
- Verantwortlichkeiten und Verpflichtungen mit Bezug zur Informationssicherheit, die nach Beendigung einer Beschäftigung bestehen bleiben (A.7.3.1)
- Inventar von Unternehmenswerten (A.8.1.1)
- Vorgaben zur Nutzung von Informationen und Unternehmenswerten (A.8.1.3)
- Richtlinie zur Zugriffskontrolle (A.9.1.1)
- Richtlinie zu kryptografischen Schutzmaßnahmen und zum Schlüsselmanagement (A.10.1.1, A.10.1.2)
- Angemessene Betriebsvorgaben (A.12.1.1)
- Richtlinie für die Datensicherung (A.12.3.1)
- Vorgaben zur Absicherung von Informationsaustausch (A.13.2.1)

- Vorgaben zu Vertraulichkeitsvereinbarungen (A.13.2.4)
- Anforderungen zur Informationssicherheit für neue oder geänderte Informationssysteme (A.14.1.1)
- Richtlinie zur Entwicklung sicherer Systeme und Anwendungen (A.14.2.1)
- Prinzipien zur Erstellung sicherer Systeme (A.14.2.5)
- Berücksichtigung der Informationssicherheitsrisiken in Vereinbarungen mit Zulieferern (A.15.1.3)
- Vorgaben zum Umgang mit Sicherheitsvorfällen (A.16.1.5)
- Vorgaben zur Gewährleistung der Verfügbarkeit aller notwendigen Ressourcen zur Sicherstellung der Informationssicherheit im Krisenfall (A.17.1.2)
- Alle relevanten rechtlichen Anforderungen mit Bezug auf Informationssicherheit und die Ansätze der Organisation, diese zu erfüllen (A.18.1.1)

Neben den expliziten Forderungen nach Dokumentation in den o. g. Maßnahmen erfordern auch andere Maßnahmen des Annex A in der Praxis ein entsprechendes Maß an Dokumentation.

Der Abschnitt 7.5 des Standards legt einige Anforderungen an den Umgang mit *documented information* fest, zu denen die explizit geforderten dokumentierten Informationen zählen sowie auch alle dokumentierten Informationen, die eine Organisation als notwendig für ihr eigenes ISMS identifiziert hat. Im Standard werden vor allem formale Anforderungen an die dokumentierten Informationen und die Prozesse zur Erstellung, Veröffentlichung, Speicherung, Änderung, Versionierung und Entsorgung formuliert. Die Freiheitsgrade hierbei sind so, dass in der Praxis vielfältige Ansätze zum Dokumentenmanagement realisiert werden können – im einfachsten Fall sollte ein diszipliniert genutztes Wiki die Anforderungen erfüllen können.

Sicherheitspolitik – die Verfassung des ISMS

Die in der Praxis recht künstliche Trennung zwischen IS- und ISMS-Policy, die im ISO/IEC 27001:2005 gefordert war, existiert in der Version 2013 nicht mehr. Die Forderung der aktuellen Version lautet, dass das Top Management eine Informationssicherheitspolitik (*policy*) verabschiedet, die für die Organisation angemessen ist. Der Standard fordert einige konkrete Inhalte dieser Politik:

- Nennung der Sicherheitsziele oder einer Methodik, um diese festzulegen,
- die Selbstverpflichtung zur Umsetzung von Informationssicherheit und
- die Selbstverpflichtung zur kontinuierlichen Verbesserung.

Es dürfte nicht überraschen, dass die Informationssicherheitspolitik als dokumentierte Information sowohl innerhalb der Organisation kommuniziert als auch – bei Bedarf – externen Dritten bereitgestellt wird. Gerade aufgrund des letzten Aspekts sollte die Informationssicherheitspolitik keine vertraulichen Details enthalten. Solche Details sollten in weitere Richtlinien des Sicherheitsregelwerks verlagert werden, damit durch eine geeignete Klassifizierung der Regelungen die Vertraulichkeit angemessen gewahrt bleiben kann. Dies ist ein Aspekt, der natürlich auch bei der Erfüllung der Anforderungen des Controls A.5.1.1 *Policies for information security* beachtet werden sollte.

Der PDCA ist tot – es lebe der PDCA!

Wer kennt ihn nicht, den PDCA-Zyklus nach William E. Deming? Jeder, der sich mit dem ISO/IEC 27001:2005 auseinandergesetzt hat, musste zwangsläufig auch den dort prominent beschriebenen PDCA-Zyklus zur Kenntnis nehmen. So mancher wird ihn auf den ersten Blick im ISO/IEC 27001:2013 vermissen: Der PDCA-Zyklus ist im Standard nicht mehr explizit erwähnt. Auf den zweiten Blick lässt sich erkennen, dass die Grundprinzipien des PDCA-Zyklus (*Nachdenken*, *Umsetzen*, *Erfolgskontrolle* und *Verbesserung*) nicht aus dem Standard verschwunden sind, sondern sich sogar in Reinform in der Gliederung wiederfinden: Die Kapitel vier bis sieben des Standards sind der Plan-Phase zuzuordnen, das Kapitel acht der Do-Phase, das Kapitel neun der Check-Phase und schlussendlich das Kapitel zehn der Act-Phase. Der Standard hat sich also nicht radikal geändert sondern verzichtet nur auf die prominente Erwähnung von eigentlich selbstverständlichen Handlungsprinzipien.

Kommunikation – wer darf was sagen?

Wurde dem Thema Kommunikation in der Version 2005 des ISO 27001 nur ein Satz gewidmet, gibt es in der Version 2013 inzwischen einen ganzen Absatz zu diesem Thema. Darin werden klare Anforderungen an die Kommunikation von Informationssicherheitsthemen formuliert. Nach der neuen Version sind für die Kommunikation die bekannten W-Fragen zu beantworten: Wer? Wann? Mit Wem? Worüber?

Wo sind die vorbeugenden Maßnahmen?

Wer in Kapitel 10 *Improvement* des ISO/IEC 27001:2013 genau hineinschaut, wird den Abschnitt zu *Preventive action* aus dem 2005er Standard vermissen. Wer noch genauer hinschaut, wird feststellen, dass die Forderung nach vorbeugenden Maßnahmen nicht aus dem Standard verschwunden ist, sondern an die Stelle gewandert ist, an die sie eigentlich auch hingehört: in den Abschnitt zur Planung des ISMS, auch wenn sich die Forderung etwas versteckt und nicht mehr so prominent formuliert ist.

Was tun mit dem Risiko?

Das Herzstück eines ISMS ist ein angemessener Umgang mit Risiken. Durch die Verschiebung weg von Assets, hin zu Informationen bei der Beurteilung von Risiken hat der neue ISO 27001 den Schwerpunkt des Risikomanagements verlagert: Der *risk owner*, dessen Rolle im ISO 31000 beschrieben ist als jemand mit Verantwortung und Kompetenz für die Behandlung eines Risikos, erhält nach ISO 27001 in der Organisation die Verantwortung für die Risiken.

Der Standard verlangt definierte Prozesse zur Identifikation, Beurteilung und Behandlung von Risiken. Bei der Behandlung der Risiken ist es nicht mehr zwingend erforderlich, den Annex A als Grundlage für die Auswahl risikoreduzierender Maßnahmen zu verwenden – mit der neuen Version kann jeder Maßnahmenkatalog, auch beispielsweise die IT-Grundschutz-Kata-

loge des BSI oder ein organisationseigener Maßnahmenkatalog, herangezogen werden. Allerdings existiert weiterhin die Forderung, die ausgewählten Maßnahmen gegen die Maßnahmen des Annex A abzugleichen.

Die Dokumentation der ausgewählten Maßnahmen samt ihres Umsetzungsstatus und einer Begründung für die Nicht-Anwendung von Maßnahmen des Annex A bildet das sogenannte *Statement of Applicability* oder kurz *SOA*.

Draußen ist auch wichtig

Mit der Version 2013 des ISO 27001 wurde die Bedeutung der Steuerung externer Ressourcen verstärkt. Zum einen werden im Abschnitt *Support* explizit Personen benannt, die durch die Organisation gesteuert werden (*doing work under its control*), zum anderen wurde der Annex A in Bezug auf *External parties* stark überarbeitet: Fand sich in der Vorgängerversion nur ein kleiner Abschnitt zu diesem Thema, zieht sich die Berücksichtigung von externen Ressourcen wie ein roter Faden durch den ISO/IEC 27001:2013. Beispiele hierfür sind

- die explizite Erwähnung ausgelagerter Prozesse im Abschnitt 8.1 zur Planung und Steuerung,
- die Forderung nach der Kontrolle und Steuerung ausgelagerter Entwicklungsaktivitäten (A.14.2.7) oder
- die explizite Berücksichtigung externer Ressourcen bei der Steuerung von Zugriffsberechtigungen (A 9.2.6).

Operation – was ist genau zu tun?

Das Kapitel 8 *Operation* dient nach ISO Annex SL hauptsächlich dazu, die Umsetzung des betrachteten Managementsystems, in diesem Falle des ISMS und des Betriebs der Organisation in Bezug auf das ISMS zu beschreiben. Da das primäre Ziel eines ISMS die Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken ist, beschränkt sich das Kapitel 8 im ISO 27001 darauf, noch einmal die Umsetzung von Aktivitäten zur Erfüllung von Sicherheitsanforderungen und zur Erreichung der Sicherheitszielsetzungen zu fordern sowie die Durchführung von Risikobetrachtungen und Behandlung der identifizierten Risiken mit den gewählten Methoden festzuschreiben. Die Themen Umgang mit Änderungen und Reaktion auf *unintendet changes* (hierunter fallen bspw. Sicherheitsvorfälle) sind ebenfalls Bestandteil dieses Kapitels.

An dieser Stelle sei noch einmal darauf hingewiesen, dass der ISO 27001 auch in diesem Kapitel explizit die Berücksichtigung ausgelagerter Prozesse fordert.

Vertrauen ist gut – Kontrolle besser

Die Überprüfung des ISMS und der Informationssicherheit bleibt auch mit der Version 2013 ein wichtiger Bestandteil des Standards. Mit der neuen Version wurden die Freiheitsgrade für die Überprüfung stark erweitert. Sowohl die fix vorgeschriebene jährliche Frequenz für Management Reviews als auch die detaillierten Vorgaben des ISO/IEC 27001:2005 wurden aufgegeben und durch Anforderungen ersetzt, die einer Organisation mehr gestalterische Freiheit für die Umsetzung dieser Prozesse zugestehen, auch wenn weiterhin klare Mindestanforderungen formuliert bleiben.

Der ISO/IEC 27001:2013 dokumentiert auch die verschiedenen Aspekte zur Prüfung, die noch in der Vorgängerversion über den ganzen Standard verstreut waren, in einem Kapitel. Diese Zusammenfassung vereinfacht die praktische Umsetzung der Kontrolle von ISMS und Informationssicherheit.

Verbesserung

Der letzte Abschnitt des ISO 27001 beinhaltet die Verbesserung des ISMS und der Informationssicherheit. Auch hier wurden wieder Anforderungen, die in der Vorgängerversion noch verstreut waren, gebündelt in einem Kapitel dokumentiert.

Eine wesentliche Änderung ist der Wegfall von vorbeugenden Maßnahmen (*preventive action*), da diese jetzt implizit Bestandteil der Planungsphase sind.

Ansonsten wird in dem Standard festgelegt, wie mit Abweichungen umgegangen werden soll. Inhaltlich unterscheidet sich dieser Abschnitt nicht sonderlich von der Vorgängerversion. Auch die Festschreibung einer kontinuierlichen Verbesserung ist keine Änderung im Standard.

Annex A – Jetzt wird es ernst

Der Annex A behält weiterhin eine wichtige Bedeutung im ISO/IEC 27001:2013, auch wenn inzwischen andere Maßnahmenkataloge als Grundlage für die Auswahl von Sicherheitsmaßnahmen herangezogen werden können. Im Vergleich zum ISO/IEC 27001:2005 wurde der Annex A an einigen Stellen weitgehend überarbeitet und vor allem an aktuelle Sicherheitserfordernisse der Informationstechnologie angepasst. Im direkten Vergleich macht die Gliederung – bis auf wenige Ausnahmen – einen durchdachteren Eindruck. Hat sich die Anzahl der Gruppen von Sicherheitsmaßnahmen[4] (*controls*) von 11 auf 14 erhöht, ist die Gesamtzahl der Maßnahmen von 133 auf 114 gesunken. Geblieben ist auch bei der Überarbeitung die inhaltliche Deckungsgleichheit mit dem ISO/IEC 27002:2013.

Eine vollständige Gegenüberstellung der Annexe A der beiden Versionen des ISO 27001 würde den Umfang dieses Beitrags sprengen. Daher werden an dieser Stelle nur wesentliche Änderungen vorgestellt:

- Die Bedeutung von Lieferanten wurde verstärkt, dem Thema *Supplier relationships* wurde mit A.15 ein ganzer Abschnitt gewidmet.
- Die Inhalte des alten Abschnitts A.10 *Communications and operations management* wurden auf verschiedene Abschnitte verteilt.
- Mit der Umbenennung des Abschnitts A.16 wurde verdeutlicht, dass das ISMS nicht ein *Business Continuity* als Bestandteil hat, sondern nur die für seinen Fortbestand relevanten Aspekte betrachten muss. Für Business Continuity existiert mit dem ISO/IEC 22301:2012 [ISO_22301_2012] ein eigener ISO-Standard.

4 Der Begriff *control* sorgt immer wieder für Verwirrung. Ein Blick in den ISO/IEC 27000:2014 kann hier Klarheit schaffen: Dort ist der Begriff *control* als Maßnahme definiert, mit der ein Risiko verändert wird – hierzu zählen alle Arten von geeigneten organisatorischen und technischen Maßnahmen.

- Neue Anforderungen zu sicheren Anwendungsentwicklung (A.14.2.1), sicheren Entwicklungsprinzipien (A.14.2.5), sicheren Entwicklungsumgebungen (A.14.2.6) sowie Sicherheitstests der Anwendungen (A.14.2.8) zeigen die gewachsene Bedeutung von Anwendungssicherheit auch im Standard auf.

An vielen Stellen wurden die Inhalte von Maßnahmen umsortiert, an anderen Stellen wurden Maßnahmen entfernt. Die Umsortierung der Maßnahmen erfordert bei der Umstellung auf den neuen Standard einige Fleißarbeit in der Darstellung, inhaltliche Arbeiten fallen vor allem im Bereich der neuen Anforderungen an.

Fazit

Der ISO 27001 war noch nie ein Standard, der Vorgaben für ein konkretes Sicherheitsniveau gemacht hat. Schon immer war der Fokus des Standards der ordnungsgemäße Betrieb eines ISMS – das hat sich auch mit der aktuellen Version nicht geändert.

Der Standard wurde in der neuen Version an andere ISO-Managementstandards angeglichen, er wurde besser gegliedert und an aktuelle Erfordernisse der Informationssicherheit angepasst. Da die Freiheitsgrade der Umsetzung erhöht wurden, sollte eine Nutzung des Standards noch besser möglich sein als mit der letzten Version. Die Änderungen im Standard sind allerdings auch nicht so gravierend, dass ein Unternehmen, das nach dem ISO/IEC 27001:2005 zertifiziert ist, große Probleme bei der Umstellung auf den ISO/IEC 27001:2013 bis zur Deadline Ende September 2015 erwarten müsste.

Berater und Auditoren haben bis zur vollständigen Umstellung der Standards und Hilfestellungen eine Durststrecke vor sich. Sie sind bis dahin mit der Umsetzung oder Bewertung der neuen Anforderungen des Standards auf sich gestellt.

Referenzen

[ISO_22301_2012] *ISO/IEC 22301:2012 – Societal security – Business continuity management systems – Requirements* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50038

[ISO_27000_2014] *ISO/IEC 27000:2014 – Information technology – Security techniques – Information security management systems – Overview and vocabulary* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63411

[ISO_27001_2013] *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements* http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[ISO_27002_2013] *ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls* http://www.iso.org/iso/catalogue_detail?csnumber=54533

[ISO_27003_2010] *ISO/IEC 27003:2010 – Information technology – Security techniques – Information security management system implementation guidance* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42105

[ISO_27005_2011] *ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742

[ISO_27007_2011] *ISO/IEC 27007:2011 – Information technology – Security techniques – Guidelines for information security management systems auditing* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42506

[ISO_27008_2011] *ISO/IEC 27008:2011 – Information technology – Security techniques – Guidelines for auditors on information security controls* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45244

[ISO_31000_2009] *ISO 31000:2009 – Risk management – Principles and guidelines* http://www.iso.org/iso/catalogue_detail?csnumber=43170

[IEC_31010_2009] *IEC 31010:2009 – Risk management – Risk assessment techniques* http://www.iso.org/iso/catalogue_detail?csnumber=51073

[Annex_SL] *Annex SL* http://www.iso.org/iso/home/standards_development/resources-for-technical-work/iso_iec_directives_and_iso_supplement.htm

[IRCA_Briefing_Note] *IRCA Briefing Note – Annex SL* http://www.irca.org/en-gb/resources/INform/archive/issue35/Technical/Introducing-Annex-SL/