DEUTSCHE NORM **Entwurf** **Februar 2014**

DIN ISO/IEC 27001

DIN

ICS 35.040

Einsprüche bis 2014-03-10
Vorgesehen als Ersatz für
DIN ISO/IEC 27001:2008-09

Entwurf

Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC DIS 27001:2013)

Information technology –
Security techniques –
Information security management systems – Requirements (ISO/IEC DIS 27001:2013)

Technologies de l'information –
Techniques de sécurité –
Systèmes de gestion de sécurité de l'information – Exigences (ISO/CEI DIS 27001:2013)

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2014-01-10 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 32 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Preisgruppe 14
www.din.de
www.beuth.de

2073161

Inhalt

Nationales Vorwort

Die Internationale Norm ISO/IEC DIS 27001:2013 wurde in deutscher Sprachfassung unverändert in das Deutsche Normenwerk übernommen. Fachlich zuständig ist für diese Deutsche Norm der Arbeitsausschuss NA 043-01-27 AA „IT-Sicherheitsverfahren“ des Normenausschusses Informationstechnik und Anwendungen (NIA) im DIN.

Die dieser Norm zugrunde liegende Internationale Norm ISO/IEC 27001 wurde von ISO/IEC JTC 1/SC 27 (International Organization for Standardization/International Electrotechnical Commission – Joint Technical Committee 1 „Information Technology“ / Subcommittee 27 „Security techniques“) erarbeitet.

DIN ISO/IEC 27001 beinhaltet Anforderungen an ein ISMS, das mittelbar zur Informationssicherheit beiträgt. Da das Dokument sehr generisch gehalten ist, um auf alle Organisationen unabhängig von Typ, Größe und Geschäftsfeld anwendbar zu sein, haben diese Anforderungen einen niedrigen technischen Detaillierungsgrad, wobei die Anforderungen an die Prozesse wohl definiert sind.

Für die in diesem Dokument zitierte internationale Norm wird im Folgenden auf die entsprechende deutsche Norm hingewiesen:

ISO/IEC 27000 siehe DIN ISO/IEC 27000

Änderungen

Gegenüber DIN ISO/IEC 27001:2008-09 wurden folgende Änderungen vorgenommen:

a) Anpassung an die neue Struktur für ISO Management System Standards, vorgegeben im Anhang SL der ISO/IEC Direktiven.

b) Folgende Abschnitte wurden neu aufgenommen:

   4.2(a), 4.3(c), 5.1(b), 6.1.1(a), 6.1.1(b), 6.1.1(c), 6.1.2(a), 6.2, 7.3(a), 7.4(a), 7.4(b), 7.4(c), 7.4(d), 7.4(e), 7.5.1(b), 8.1, 9.1(c), 9.1(d), 9.1(f), 9.3(4), 10.1(a), 10.1(1), 10.1(2), 10.1(e), 10.1(f)

c) Folgende Abschnitte wurden gestrichen:

   4.2.1, 4.2.1(i), 4.2.3(1), 4.2.3(2), 4.2.3(4), 4.2.3(5), 4.2.3(h), 4.3.1, 4.3.1(c), 4.3.2, 4.3.3, 5.2.1(b), 5.2.1(d), 8.3(d), 8.3(e), 8.3

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN ISO/IEC 27000, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Mangamentsysteme — Überblick und Terminolgie*

Informationstechnologie — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen

0 Einleitung

0.1 Allgemeines

Diese Internationale Norm wurde erarbeitet, um Anforderung für die Einrichtung, Implementierung, Wartung und laufende Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) festzulegen. Die Einführung eines Informationssicherheitsmanagementsystems stellt für eine Organisation eine strategische Entscheidung dar. Erstellung und Implementierung eines Informationssicherheitsmanagementsystems innerhalb einer Organisation richten sich nach deren Bedürfnissen und Zielen, den Sicherheitsanforderungen, den organisatorischen Abläufen sowie nach Größe und Struktur der Organisation. Es ist davon auszugehen, dass sich alle diese Einflussgrößen im Laufe der Zeit ändern werden.

Das Informationssicherheitsmanagementsystem schützt die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Informationen durch Anwendung eines Risikomanagement-Prozesses und verleiht dadurch interessierten Parteien das Vertrauen darauf, dass mit Risiken angemessen umgegangen wird.

Hierfür ist es wichtig, dass das Informationssicherheitsmanagementsystem in die Abläufe und die gesamte Verwaltungsstruktur der Organisation integriert ist und einen untrennbaren Bestandteil davon darstellt. Außerdem muss die Informationssicherheit bereits bei der Konzeption von Prozessen, Informationssystemen und Maßnahmen berücksichtigt werden. Es ist davon auszugehen, dass die Implementierung eines Informationssicherheitsmanagementsystems entsprechend den Bedürfnissen der Organisation skaliert wird.

Diese Internationale Norm kann von internen und externen Parteien – darunter Zertifizierungsstellen – dazu eingesetzt werden, die Fähigkeit einer Organisation zur Einhaltung ihrer eigenen Informationssicherheits-anforderungen zu bewerten.

Die Anforderungen werden in dieser Internationalen Norm weder in der Reihenfolge ihrer Wichtigkeit aufgeführt noch in der zeitlichen Abfolge, in der sie umgesetzt werden sollten. Die Listeneinträge werden lediglich zu Referenzzwecken aufgeführt.

Mit ISO/IEC 27000 wird ein Überblick über Informationssicherheitsmanagementsysteme gegeben und das entsprechende Vokabular für Systeme vorgegeben, auf welche die ISMS-Normenfamilie (einschließlich ISO/IEC 27003, ISO/IEC 27004 und ISO/IEC 27005) anwendbar ist. Außerdem beinhaltet die Norm Festlegungen zu den dazugehörigen Begriffen und Definitionen.

0.2 Kompatibilität mit anderen Normen für Managementsysteme

In dieser Internationalen Norm werden die grobe Struktur, die gleichen Titel von Unterabschnitten, identischer Text, häufige Begriffe und wichtige Definitionen angewandt wie in Anhang SL von ISO/IEC-Richtlinien, Teil 1. Dadurch wird die Kompatibilität mit anderen Normen für Managementsysteme gewahrt, die ebenfalls Anhang SL übernommen haben.

Diese gemeinsame Herangehensweise nach den Definitionen in Anhang SL ist für diejenigen Organisationen nützlich, die sich für den Einsatz eines einzelnen Managementsystems zur Erfüllung der Anforderungen von zwei oder mehr Normen für Managementsysteme entscheiden.

1 Anwendungsbereich

Diese Norm legt die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und laufende Verbesserung eines Informationssicherheitsmanagementsystems im Kontext der Organisation fest. Darüber hinaus beinhaltet diese Internationale Norm Anforderungen für die Einschätzung und Handhabung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen der Organisation. Die in dieser Internationalen Norm festgelegten Anforderungen sind allgemein gehalten und sollen auf alle Organisationen ungeachtet ihrer Art und Größe anwendbar sein. Wenn eine Organisation Konformität mit dieser Internationalen Norm für sich beansprucht, darf sie keine der Anforderungen in den Abschnitten 4 bis 10 ausschließen.

2 Normative Verweisungen

Das folgende zitierte Dokument ist für die Anwendung dieses Dokuments unverzichtbar. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 27000, *Information technology — Security Techniques — Information security management systems — Overview and vocabulary*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die in ISO/IEC 27000 angegebenen Begriffe.

4 Kontext der Organisation

4.1 Verständnis der Organisation und ihres Kontexts

Die Organisation muss festlegen, welche externen und internen Angelegenheiten für ihren Zweck relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse ihres Informationssicherheitsmanagement-systems zu erreichen.

ANMERKUNG Die Ermittlung dieser Angelegenheiten bezieht sich auf die Festlegung des externen und internen Kontexts des Unternehmens, wie in ISO 31000:2009, 5.3.1 geschildert.

4.2 Verständnis der Bedürfnisse und Erwartungen interessierter Parteien

Die Organisation muss Folgendes festlegen:

a) interessierte Parteien, die im Hinblick auf das Informationssicherheitsmanagementsystem relevant sind; und

b) die Anforderungen dieser interessierten Parteien in Bezug auf die Informationssicherheit.

ANMERKUNG Die Anforderungen interessierter Parteien können gesetzliche und amtliche Vorgaben sowie vertragliche Verpflichtungen beinhalten.

4.3 Festlegung des Geltungsbereichs des Informationssicherheitsmanagementsystems

Die Organisation muss die Grenzen und die Anwendbarkeit des Informationssicherheitsmanagementsystems festlegen und damit seinen Geltungsbereich festlegen.

Bei der Festlegung des Geltungsbereichs muss die Organisation Folgendes berücksichtigen:

a) die in 4.1 genannten externen und internen Angelegenheiten;

b) die in 4.2 genannten Anforderungen; und

c) Schnittstellen und Abhängigkeitsverhältnisse zwischen Tätigkeiten, die von der Organisation selbst durchgeführt werden, und Tätigkeiten anderer Organisationen.

Der Geltungsbereich muss als dokumentierte Information verfügbar sein.

4.4 Informationssicherheitsmanagementsystem

Die Organisation muss ein Informationssicherheitsmanagementsystem nach den Anforderungen dieser Internationalen Norm einrichten, implementieren, aufrechterhalten und laufend verbessern.

5 Führung

5.1 Führung und Engagement

Die Leitung muss durch folgende Maßnahmen ihre Führung und ihr Engagement in Bezug auf das Informationssicherheitsmanagementsystem demonstrieren:

a) Sicherstellen, dass eine Informationssicherheitsleitlinie und Informationssicherheitsziele vorgegeben werden und mit der strategischen Ausrichtung der Organisation vereinbar sind;

b) Sicherstellen, dass die Anforderungen im Rahmen des Informationssicherheitsmanagementsystem in die Prozesse der Organisation integriert werden;

c) Sicherstellung, dass die für das Informationssicherheitsmanagementsystem erforderlichen Ressourcen bereitstehen;

d) Kommunikation der Bedeutung eines effektiven Informationssicherheitsmanagements sowie der Einhaltung der Anforderungen im Rahmen des Informationssicherheitsmanagementsystems;

e) Sicherstellen, dass mit dem Informationssicherheitsmanagementsystem die beabsichtigten Ergebnisse erzielt werden;

f) Führen und Unterstützen von Personen, damit diese einen Beitrag zur Wirksamkeit des Informationssicherheitsmanagementsystems leisten;

g) Fördern der laufenden Verbesserung; und

h) Unterstützen anderer relevanter Führungskräfte bei der Demonstration ihrer Führung im jeweiligen Zuständigkeitsbereich.

5.2 Leitlinie

Die Leitung muss eine Informationssicherheitsleitlinie vorgeben, die folgende Eigenschaften aufweist:

a) Eignung für den Zweck der Organisation;

b) Einbeziehung von Informationssicherheitszielen (siehe 6.2) oder Bereitstellung eines Frameworks zur Vorgabe von Sicherheitszielen;

c) Einbeziehung einer Verpflichtung zur Einhaltung der Anforderungen in Bezug auf die Informationssicherheit; und

d) Einbeziehung einer Verpflichtung zur laufenden Verbesserung des Informationssicherheitsmanagementsystems.

Die Informationssicherheitsleitlinie muss:

e) als dokumentierte Information verfügbar sein;

f) innerhalb der Organisation bekannt gemacht werden; und

g) ggf. interessierten Parteien zur Verfügung stehen.

5.3 Organisatorische Aufgaben, Zuständigkeiten und Befugnisse

Die Leitung muss sicherstellen, dass die Zuständigkeiten und Befugnisse von Aufgaben, die für die Informationssicherheit relevant sind, zugewiesen und kommuniziert werden.

Die Leitung muss Zuständigkeiten und Befugnisse für folgende Aspekte zuweisen:

a) Sicherstellen, dass das Informationssicherheitsmanagementsystem den Anforderungen dieser Internationalen Norm entspricht; und

b) Berichterstatten zur Leistung des Informationssicherheitsmanagementsystems gegenüber der Leitung.

ANMERKUNG Die Leitung weist u. U. auch Zuständigkeiten und Befugnisse für die Berichterstattung zur Leistung des Informationssicherheitsmanagementsystems innerhalb der Organisation zu.

6 Planung

6.1 Maßnahmen zum Umgang mit Risiken und Chancen

6.1.1 Allgemeines

Beim Planen des Informationssicherheitsmanagementsystems muss die Organisation die unter 4.1 genannten Angelegenheiten sowie die unter 4.2 genannten Anforderungen berücksichtigen und ermitteln, auf welche Risiken und Chancen zu achten sein wird, um Folgendes zu erreichen:

a) Sicherstellen, dass mit dem Informationssicherheitsmanagementsystem die beabsichtigten Ergebnisse erzielt werden können;

b) Vorbeugen oder Abschwächen unerwünschter Auswirkungen; und

c) laufende Verbesserung.

Die Organisation muss Folgendes planen:

d) Maßnahmen zum Umgang mit Risiken und Chancen; und

e) Möglichkeiten zur

   1) Integration und Einbeziehung dieser Maßnahmen in die eigenen Informationssicherheits-managementprozesse; und

   2) Auswertung der Wirksamkeit dieser Maßnahmen.

6.1.2 Informationssicherheitsrisikoeinschätzung

Die Organisation muss einen Prozess zur Informationssicherheitsrisikoeinschätzung festlegen, der Folgendes bewirkt:

a) Einrichten und Aufrechterhalten von Informationssicherheitsrisikokriterien einschließlich Risiko-akzeptanzkriterien;

b) Festlegen der Kriterien für eine Durchführung von Informationssicherheitrisikoeinschätzungen; und

c) Sicherstellen, dass wiederholte Informationssicherheitsrisikoeinschätzungen zu konsistenten, aussage-kräftigen und vergleichbaren Ergebnisse führen.

Die Organisation muss Folgendes leisten:

d) Ermitteln der Informationssicherheitsrisiken.

   1) Anwenden des Informationssicherheitsrisikoeinschätzungsprozesses zur Ermittlung von Risiken im Zusammenhang mit Mängeln bei Vertraulichkeit, Integrität und Verfügbarkeit von Informationen innerhalb des Geltungsbereichs des ISMS.

   2) Ermittlen der Risikoeigentümer.

e) Analyse der Informationssicherheitsrisiken.

   1) Bewerten der potenziellen Auswirkungen bei Eintritt der nach 6.1.1 e) 1) ermittelten Risiken.

   2) Bewerten der realistischen Eintretenswahrscheinlichkeiten der nach 6.1.1 e) 1) ermittelten Risiken.

   3) Festlegen der Risikostufen.

f) Auswertung der Informationssicherheitsrisiken.

   1) Vergleich der analysierten Risiken mit den nach 6.1.2 a) festgelegten Risikokriterien und Festlegen von Prioritäten bezüglich des Umgangs mit diesen Risiken.

Die Organisation muss dokumentierte Informationen über den Informationssicherheitsrisikoeinschätzungs-prozess aufbewahren.

6.1.3 Informationssicherheitsrisikobehandlung

Die Organisation muss einen Prozess für die Informationssicherheitsrisikobehandlung festlegen, der Folgendes bewirkt:

a) Auswahl angemessener Optionen für die Sicherheitsrisikobehandlung unter Berücksichtigung der Ergebnisse der Risikoeinschätzung;

b) Festlegen aller Maßnahmen, die zur Implementierung der gewählten Optionen für die Sicherheitsrisikobehandlung erforderlich sind;

ANMERKUNG Organisationen können Maßnahmen nach Bedarf gestalten oder vorgefertigte Maßnahmen aus einer beliebigen Quelle wählen.

c) Vergleich der nach 6.1.3 b) festgelegten Maßnahmen mit den Maßnahmen in Anhang A und Vergewisserung, dass keine erforderlichen Kontrollmaßnahmen ausgelassen wurden;

ANMERKUNG 1 Anhang A enthält eine umfassende Liste von Maßnahmenzielen und Maßnahmen. Anwender dieser Internationalen Norm werden für die Sicherstellung, dass keine wichtigen Maßnahmen übersehen wurden, auf Anhang A verwiesen.

ANMERKUNG 2 Maßnahmenziele sind implizit in den gewählten Maßnahmen enthalten. Die Liste der Maßnahmenziele und Maßnahmen in Anhang A ist nicht erschöpfend; u. U. sind weitere Maßnahmenziele und Maßnahmen erforderlich.

d) Erstellen einer Erklärung zur Anwendung, die die erforderlichen Maßnahmen (siehe 6.1.3 a), b) und c)) und Gründe für deren Einbeziehung enthält (egal, ob sie implementiert werden oder nicht) sowie Gründe für die Nichteinbeziehung von Maßnahmen in Anhang A.

e) Formulieren eines Plans für die Informationssicherheitsrisikobehandlung;

f) Einholen einer Genehmigung des Plans für die Informationssicherheitsrisikobehandlung seitens der Risikoeigentümer sowie deren Akzeptanz der verbleibenden Informationssicherheitsrisiken.

Die Organisation muss dokumentierte Informationen über den Prozess zur Informationssicherheitsrisikobehandlung aufbewahren.

ANMERKUNG Die in dieser Internationalen Norm genannten Prozesse für die Informationssicherheitsrisikoeinschätzung und den Umgang damit entsprechen den Grundsätzen und allgemeinen Richtlinien in ISO 31000.

6.2 Informationssicherheitsziele und Pläne für deren Erreichung

Die Organisation muss in relevanten Funktionen und auf relevanten Ebenen Informationssicherheitsziele festlegen.

Diese Informationssicherheitsziele müssen:

a) mit der Informationssicherheitsleitlinie konsistent sein;

b) messbar sein (falls praktikabel);

c) unter Berücksichtigung der anwendbaren Informationssicherheitsanforderungen, der Risikoeinschätzung und der Ergebnisse des Umgangs mit diesen Risiken festgelegt werden;

d) kommuniziert werden, und

e) ggf. aktualisiert werden.

Die Organisation muss dokumentierte Informationen über die Informationssicherheitsziele aufbewahren.

Beim Planen, wie die Informationssicherheitsziele erreicht werden sollen, muss die Organisation Folgendes ermitteln:

f) zu ergreifende Maßnahmen;

g) erforderliche Ressourcen;

h) zuständige Personen;

i) Frist bis zum Abschluss; und

j) Verfahren zur Auswertung der Ergebnisse.

7 Unterstützung

7.1 Ressourcen

Die Organisation muss die zur Einrichtung, Implementierung, Aufrechterhaltung und laufenden Verbesserung des Informationssicherheitsmanagementsystems erforderlichen Ressourcen ermitteln und bereitstellen.

7.2 Kompetenz

Die Organisation muss Folgendes leisten:

a) Ermitteln der erforderlichen Kompetenzen von Personen, die Arbeiten unter ihrer Kontrolle verrichten, die sich auf die Leistung im Bereich der Informationssicherheit auswirken;

b) Sicherstellen, dass diese Personen durch angemessene Ausbildung, Schulung oder Erfahrung über die erforderlichen Kompetenzen verfügen;

c) ggf. Einleiten von Maßnahmen zur Aneignung der erforderlichen Kompetenzen und Auswertung der Wirksamkeit dieser Maßnahmen; und

d) Aufbewahren entsprechender dokumentierter Informationen als Kompetenznachweis.

ANMERKUNG Zu den erforderlichen Maßnahmen kann beispielsweise Folgendes zählen: Schulung, Betreuung oder Versetzung der aktuellen Mitarbeiter oder die Einstellung oder Beauftragung kompetenter Personen.

7.3 Bewusstsein

Bei den Personen, die Arbeiten unter der Kontrolle der Organisation verrichten, muss Bewusstsein hinsichtlich der folgenden Punkte herrschen:

a) der Informationssicherheitsleitlinie;

b) des eigenen Beitrags zur Wirksamkeit des Informationssicherheitsmanagementsystems einschließlich der Vorteile einer besseren Leistung im Bereich der Informationssicherheit; und

c) der Auswirkungen eines Verstoßes gegen die Anforderungen des Informationssicherheitsmanagement-systems.

7.4 Kommunikation

Die Organisation muss ermitteln, welcher Bedarf an interner und externer Kommunikation zum Informationssicherheitsmanagement besteht. Hierbei muss Folgendes berücksichtigt werden:

a) Inhalt der Kommunikation;

b) Zeitpunkt der Kommunikation;

c) Adressaten der Kommunikation;

d) Kommunikationsverantwortliche; und

e) Kommunikationsprozesse.

7.5 Dokumentierte Informationen

7.5.1 Allgemeines

Das Informationssicherheitsmanagementsystem der Organisation muss Folgendes umfassen:

a) nach dieser Internationalen Norm erforderliche dokumentierte Informationen; und

b) von der Organisation als für die Wirksamkeit des Informationssicherheitsmanagementsystems erforderlich befundene dokumentierte Informationen.

ANMERKUNG Der Umfang der dokumentierten Informationen für ein Informationssicherheitsmanagementsystem kann aus folgenden Gründen je nach Organisation unterschiedlich sein:

1) Größe der Organisation und Art ihrer Tätigkeiten, Prozesse, Produkte und Dienstleistungen;

2) Komplexität der Prozesse und deren Wechselwirkungen; und

3) Kompetenz der Personen.

7.5.2 Erstellen und Aktualisieren

Beim Erstellen und Aktualisieren der dokumentierten Informationen muss die Organisation Folgendes sicherstellen:

a) angemessenes Kennzeichnen und Beschreiben (z. B. Titel, Datum, Autor oder Referenznummer);

b) angemessenes Format (z. B. Sprache, Software-Version, Grafik) und Medium (z. B. Papier, elektronisches Medium); und

c) angemessene Eignungs- und Tauglichkeitsprüfung sowie Genehmigung.

7.5.3 Kontrolle der dokumentierten Informationen

Die nach dem Informationssicherheitsmanagementsystem und dieser Internationalen Norm erforderlichen dokumentierten Informationen müssen kontrolliert werden, damit Folgendes sichergestellt ist:

a) Verfügbarkeit und Eignung für die Verwendung unabhängig von Ort und Zeitpunkt; und

b) angemessener Schutz (z. B. vor Verlust der Vertraulichkeit, unsachnache Verwendung oder Verlust der Integrität).

Zur Kontrolle der dokumentierten Informationen müssen die Organisationen je nach Bedarf die folgenden Tätigkeiten berücksichtigen:

c) Verteilung, Zugriff, Abruf und Verwendung;

d) Lagern und Erhalten, einschließlich Erhalten der Lesbarkeit;

e) Änderungskontrolle (z. B. Versionskontrolle); und

f) Aufbewahren und Entsorgen.

Dokumentierte Informationen aus externer Quelle, die von der Organisation als für das Planen und den Einsatz des Informationssicherheitsmanagementsystems für erforderlich befunden wurde, müssen entsprechend gekennzeichnet und kontrolliert werden.

ANMERKUNG Der Zugriff impliziert eine Entscheidung hinsichtlich einer Erlaubnis, die dokumentierten Informationen ausschließlich einsehen zu dürfen, oder die Erlaubnis und Befugnis zur Einsicht und Änderung der dokumentierten Informationen usw.

8 Einsatz

8.1 Einsatzplanung und -kontrolle

Die Organisation muss die für die Einhaltung der Informationssicherheit sowie für die Implementierung der nach 6.1 festgelegten Maßnahmen erforderlichen Prozesse planen, implementieren und kontrollieren. Darüber hinaus muss die Organisation Pläne für das Erreichen der nach 6.2 festgelegten Informationssicherheitsziele implementieren.

Die Organisation muss die dokumentierten Informationen so weit wie erforderlich aufbewahren, damit Gewissheit herrscht, dass die Prozesse wie geplant umgesetzt wurden.

Die Organisation muss planmäßige Änderungen kontrollieren und die Auswirkungen ungeplanter Änderungen prüfen sowie ggf. Maßnahmen zur Minimierung eventueller negativer Auswirkungen ergreifen.

Die Organisation muss sicherstellen, dass ausgelagerte Prozesse festgelegt und kontrolliert werden.

8.2 Informationssicherheitsrisikoeinschätzung

Die Organisation muss in geplanten Abständen eine Informationssicherheitsrisikoeinschätzung vornehmen oder immer dann, wenn erhebliche Änderungen vorgeschlagen oder umgesetzt werden. Dabei sind die unter 6.1.2 festgelegten Kriterien zu berücksichtigen.

Die Organisation muss die dokumentierten Informationen zu den Ergebnissen von Informationssicherheitsrisikoeinschätzungen aufbewahren.

8.3 Informationssicherheitsrisikobehandlung

Die Organisation muss den Plan für die Informationssicherheitsrisikobehandlung implementieren.

Die Organisation muss die dokumentierten Informationen zu den Ergebnissen der Informationssicherheitsrisikobehandlung aufbewahren.

9 Leistungsauswertung

9.1 Überwachung, Messung, Analyse und Auswertung

Die Organisation muss die Leistung des Informationssicherheitssystems und die Wirksamkeit des Informationssicherheitsmanagementsystems auswerten.

Die Organisation muss Folgendes ermitteln:

a) zu überwachende und zu messende Aspekte einschließlich der Informationssicherheitsprozesse und Maßnahmen;

b) die Verfahren zur Überwachung, Messung, Analyse und Auswertung (je nach Bedarf) zur Sicherstellung aussagekräftiger Ergebnisse;

ANMERKUNG Die ausgewählten Verfahren sollten zu vergleichbaren und reproduzierbaren Ergebnissen führen, die als aussagekräftig zu betrachten sind.

c) den Zeitpunkt der Überwachung und Messung;

d) die für die Überwachung und Messung zuständigen Personen;

e) den Zeitpunkt für die Analyse und Auswertung der Ergebnisse aus Überwachung und Messung; und

f) die für Analyse und Auswertung zuständigen Personen.

Die Organisation muss angemessene dokumentierte Informationen zum Nachweis der Überwachungs- und Messergebnisse aufbewahren.

9.2 Internes Audit

Die Organisation muss in geplanten Abständen interne Audits abhalten, um Informationen über folgende Eigenschaften des Informationssicherheitsmanagementsystems zu erhalten:

a) Übereinstimmung mit

   1) den eigenen Anforderungen der Organisation in Bezug auf ihr Informationssicherheitsmanagement-system; und

   2) den Anforderungen dieser Internationalen Norm;

b) Effektive Implementierung und Aufrechterhaltung.

Die Organisation muss Folgendes leisten:

c) Planen, Festlegen, Einführen und Aufrechterhalten eines Auditprogramms, das Aspekte wie Häufigkeit, Verfahren, Zuständigkeiten, Planungsanforderungen und Berichterstattung beinhaltet. Im Auditprogramm muss die Bedeutung der betroffenen Prozesse und der Ergebnisse vorangegangener Audits berücksichtigt werden;

d) Festlegen der Auditkriterien und des Umfangs jedes Audits;

e) Auswahl der Auditoren und Leitung von Audits zur Sicherstellung der Objektivität und Unparteilichkeit im Auditprozess;

f) Sicherstellen, dass Audit-Ergebnisse der relevanten Leitung gemeldet werden; und

g) Aufbewahren dokumentierter Informationen als Nachweis des Auditprogramms und der Ergebnisse.

9.3 Prüfung durch die Leitung

Die Leitung muss das Informationssicherheitsmanagementsystem der Organisation in planmäßigen Abständen prüfen, um sicherzustellen, dass es nach wie vor geeignet, angemessen und wirksam ist.

Bei dieser Prüfung durch die Leitung müssen folgende Aspekte berücksichtigt werden:

a) der Stand von Maßnahmen aus vorangegangenen Prüfungen durch die Leitung;

b) Änderungen in externen und internen Angelegenheiten, die für das Informationssicherheitsmanagement-system relevant sind;

c) Rückmeldung zur Leistung in Bezug auf die Informationssicherheit einschließlich Angaben zu Tendenzen bei:

   1) Fehlern und Korrekturmaßnahmen;

   2) Überwachungs- und Messergebnissen;

   3) Auditergebnissen; und

   4) erreichten Informationssicherheitszielen;

d) Rückmeldung von interessierten Parteien;

e) Ergebnisse der Risikoeinschätzung und Status des Plans für die Risikobehandlung; und

f) Möglichkeiten für die laufende Verbesserung.

Das Ergebnis der Prüfung durch die Leitung muss Entscheidungen zu Möglichkeiten für die laufende Verbesserung sowie eventuell erforderliche Änderungen am Informationssicherheitsmanagementsystem beinhalten.

Die Organisation muss dokumentierte Informationen zum Nachweis der Ergebnisse der Prüfung durch die Leitung aufbewahren.

10 Verbesserung

10.1 Fehler und Korrekturmaßnahmen

Bei Auftreten eines Fehlers muss das Unternehmen:

a) auf den Fehler reagieren und ggf.:

   1) Maßnahmen ergreifen, um den Fehler unter Kontrolle zu bekommen und ihn zu korrigieren; und

   2) sich mit den Auswirkungen auseinandersetzen;

b) ermitteln, ob Bedarf an Maßnahmen zur Beseitigung der Fehlerursachen entsteht, damit der Fehler nicht erneut oder an anderer Stelle auftritt, und zwar durch:

   1) Prüfen des Fehlers;

   2) Ermitteln der Fehlerursache; und

   3) Ermitteln, ob ähnliche Fehler existieren oder u. U. auftreten könnten;

c) Einführen erforderlicher Maßnahmen;

d) Prüfen der Wirksamkeit von Korrekturmaßnahmen; und

e) Umsetzen von Änderungen am Informationssicherheitsmanagementsystem, falls erforderlich.

Die Korrekturmaßnahmen müssen in einem angemessenen Verhältnis zu den Auswirkungen der aufgetretenen Fehler stehen.

Die Organisation muss dokumentierte Informationen zum Nachweis der folgenden Aspekte aufbewahren:

f) Art der Fehler und ggf. ergriffene Folgemaßnahmen; und

g) Ergebnisse eventueller Korrekturmaßnahmen.

10.2 Laufende Verbesserung

Die Organisation muss die Eignung, Angemessenheit und Wirksamkeit des Informationssicherheits-managementsystems laufend verbessern.

Anhang A
(normativ)

Referenz-Maßnahmenziele und Maßnahmen

Die in Tabelle A.1 aufgeführten Maßnahmenziele und Maßnahmen sind direkt aus den unter Abschnitt 5–18 in ISO IEC DIS 27002 genannten Zielen und Maßnahmen abgeleitet und danach ausgerichtet. Die Maßnahmenziele und Maßnahmen in diesen Tabellen sind nicht erschöpfend, und eine Organisation kann u. U. zu dem Schluss kommen, dass weitere Ziele und Maßnahmen erforderlich sind. Die Auswahl von Maßnahmenzielen und Maßnahmen aus diesen Tabellen stellt einen Teil des Informationssicherheitsmanagementprozesses nach Abschnitt 6.1.3 dar.

Den Abschnitten 5–18 von ISO/IEC DIS 27002 sind Ratschläge zur Implementierung und Anleitungen bezüglich der besten Vorgehensweise zur Unterstützung der in A.5 bis A.18 genannten Maßnahmen zu entnehmen (A.0 bis A.4 werden nicht verwendet; dies ermöglicht die Anpassung des Referenzindexes für Maßnahmen an die Anleitungsabschnitte ISO/IEC DIS 27002).

Tabelle A.1 – Maßnahmenziele und Maßnahmen

A.5 Sicherheitsleitlinien		
A.5.1 Vorgaben der Leitung zur Informationssicherheit Ziel: Bereitstellung von Vorgaben und Unterstützung seitens der Leitung für die Informationssicherheit nach geschäftlichen Anforderungen und den geltenden Gesetzen und Vorschriften.		
A.5.1.1	Informations-sicherheitsleitlinien	*Maßnahme* Ein Satz Informationssicherheitsleitlinien ist festzulegen, von der Leitung zu genehmigen, zu veröffentlichen und den Mitarbeitern sowie relevanten externen Parteien bekanntzumachen.
A.5.1.2	Prüfung der Informations-sicherheitsleitlinien	*Maßnahme* Die Informationssicherheitsleitlinien müssen in planmäßigen Abständen oder jeweils nach erheblichen Änderungen geprüft werden, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.
A.6 Organisation der Informationssicherheit		
A.6.1 Interne Organisation Ziel: Festlegung eines Frameworks für die Leitung, mit dem die Implementierung der Informationssicherheit in der Organisation eingeleitet und kontrolliert werden kann.		
A.6.1.1	Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit	*Maßnahme* Alle Zuständigkeiten im Bereich der Informationssicherheit müssen festgelegt und zugeordnet werden.
A.6.1.2	Kontakt zu Behörden	*Maßnahme* Es sind angemessene Kontakte zu relevanten Behörden zu pflegen.
A.6.1.3	Kontakt mit Interessen-vertretungen	*Maßnahme* Es sind angemessene Kontakte zu Interessenvertretungen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden zu pflegen.

A.6.1.4	Informationssicherheit im Projektmanagement	*Maßnahme* Die Informationssicherheit muss ungeachtet der Art des Projekts auch im Projektmanagement berücksichtigt werden.
A.6.1.5	Aufgabentrennung	*Maßnahme* Miteinander in Konflikt stehende Aufgaben und Zuständigkeitsbereiche müssen getrennt werden, um das Risiko unautorisierter oder versehentlicher Änderung oder missbräuchlicher Anwendung der Werte der Organisation zu verringern.
A.6.2 Mobilgeräte und Telearbeit Ziel: Sicherstellung der Informationssicherheit bei Telearbeit und der Nutzung von Mobilgeräten		
A.6.2.1	Leitlinie zu Mobilgeräten	*Maßnahme* Es müssen eine Leitlinie und unterstützende Sicherheitsmaßnahmen zum Schutz vor den Risiken durch die Nutzung von Mobilgeräten eingesetzt werden.
A.6.2.2	Telearbeit	*Maßnahme* Es müssen eine Leitlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Informationen festgelegt werden, auf die von Telearbeitsplätzen aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden.
A.7 Sicherheit des Personals		
A.7.1 Vor der Einstellung Ziel: Festlegung eines Frameworks für die Leitung, mit dem die Implementierung der Informationssicherheit in der Organisation eingeleitet und kontrolliert werden kann		
A.7.1.1	Überprüfung	*Maßnahme* Prüfungen des Hintergrunds von Bewerbern müssen im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen sowie in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Informationen und den wahrgenommenen Risiken stehen.
A.7.1.2	Arbeitsvertragsklauseln	*Maßnahme* Im Rahmen ihrer vertraglichen Verpflichtung müssen Mitarbeiter den Arbeitsvertragsklauseln in ihrem Arbeitsvertrag, mit denen ihre eigenen Pflichten und die Pflichten der Organisation im Bereich der Informationssicherheit festgelegt werden, zustimmen und sie unterzeichnen.
A.7.2 Während der Anstellung Ziel: Sicherstellung, dass Mitarbeiter und externe Benutzer ihre Pflichten bezüglich der Informationssicherheit kennen und ihnen nachkommen.		
A.7.2.1	Verantwortung des Managements	*Maßnahme* Das Management muss alle Mitarbeiter und externen Benutzer dazu anhalten, Sicherheitsmaßnahmen entsprechend den festgelegten Leitlinien und Verfahren der Organisation anzuwenden.

A.7.2.2	Bewusstsein, Ausbildung und Schulung für Informations-sicherheit	*Maßnahme* Alle Mitarbeiter der Organisation sowie, falls relevant, externe Benutzer müssen ein Programm zur Sensibilisierung für Informationssicherheit sowie entsprechende Aus- und Weiterbildung und Schulungen durchlaufen und regelmäßig bezüglich der Leitlinien und Verfahren der Organisation, die für ihre berufliche Funktion relevant sind, auf dem neuesten Stand gehalten werden.
A.7.2.3	Disziplinarverfahren	*Maßnahme* Es muss ein formales und offiziell bekanntgegebenes Disziplinarverfahren eingeleitet werden, in dessen Rahmen Maßnahmen gegen Mitarbeiter verhängt werden können, die gegen Informationssicherheitsvorschriften verstoßen haben.
A.7.3 Beendigung und Wechsel der Anstellung Ziel: Schutz der Interessen der Organisation bei einem Wechsel oder der Beendigung der Anstellung		
A.7.3.1	Zuständigkeiten bei Beendigung oder Wechsel der Anstellung	*Maßnahme* Zuständigkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Wechsel der Anstellung gültig bleiben, müssen definiert, dem Mitarbeiter oder externen Benutzer mitgeteilt und durchgesetzt werden.
A.8 Wertemanagement		
A.8.1 Verantwortung für Werte Ziel: Erreichen und Erhaltung eines angemessenen Schutzes der Werte der Organisation		
A.8.1.1	Inventar der Werte	*Maßnahme* Werte, die mit Informationen und Einrichtungen zur Verarbeitung von Informationen in Zusammenhang stehen, müssen ermittelt werden, und von diesen Anlagen ist ein Inventar zu erstellen und zu pflegen.
A.8.1.2	Eigentum von Werten	*Maßnahme* Für im Inventar geführte Werte muss es Eigentümer geben.
A.8.1.3	Zulässiger Gebrauch von Werten	*Maßnahme* Es müssen Regeln für den zulässigen gebrauch von Informationen und Werten, die mit Informationen und Einrichtungen zur Verarbeitung von Informationen in Zusammenhang stehen, aufgestellt, dokumentiert und implementiert werden.
A.8.2 Klassifizierung von Informationen Ziel: Sicherstellung, dass Informationen eine angemessene Schutzstufe entsprechend ihrer Bedeutung für die Organisation zugeteilt bekommen.		
A.8.2.1	Klassifizierung von Informationen	*Maßnahme* Informationen sind nach ihrem Wert, gesetzlichen Anforderungen, Vertraulichkeit und Betriebswichtigkeit zu klassifizieren.

A.8.2.2	Kennzeichnung von Informationen	*Maßnahme* Ein angemessener Satz Verfahren zur Kennzeichnung von Informationen ist entsprechend dem von der Organisation eingesetzten Plan zur Einstufung von Informationen zu entwickeln und zu implementieren.
A.8.2.3	Umgang mit Werten	*Maßnahme* Verfahren für den Umgang mit Werten sind entsprechend dem von der Organisation eingesetzten Plan zur Einstufung von Informationen zu entwickeln und zu implementieren.
A.8.2.4	Rückgabe von Werten	*Maßnahme* Alle Mitarbeiter und externen Benutzer müssen sämtliche Werte der Organisation zurückgeben, die sich bei Auslauf ihrer Anstellung oder ihres Vertrags noch in Ihrem Besitz befinden.
A.8.3 Umgang mit Medien Ziel: Verhinderung von unerlaubter Veröffentlichung, Veränderung, Entnahme oder Zerstörung von Informationen, die auf Medien gespeichert sind		
A.8.3.1	Verwaltung von Wechselmedien	*Maßnahme* Es sind Verfahren für die Verwaltung von Wechselmedien entsprechend dem von der Organisation eingesetzten Plan zur Klassifizierung von Informationen zu implementieren.
A.8.3.2	Entsorgung von Medien	*Maßnahme* Medien müssen sicher und unter Anwendung formaler Verfahrensanweisungen entsorgt werden, wenn sie nicht mehr benötigt werden.
A.8.3.3	Physische Weitergabe von Medien	*Maßnahme* Medien, auf denen Informationen gespeichert sind, müssen vor unautorisiertem Zugriff, missbräuchlicher Verwendung oder Verfälschung während des Transports geschützt werden.
A.9 Zugriffskontrolle		
A.9.1 Geschäftliche Anforderungen in Bezug auf die Zugriffskontrolle Ziel: Beschränkung des Zugriffs auf Informationen und informationsverarbeitenden Einrichtungen		
A.9.1.1	Zugriffskontrollleitlinie	*Maßnahme* Eine Zugriffskontrollleitlinie ist auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen zu erstellen, zu dokumentieren und zu prüfen.
A.9.1.2	Leitlinie zur Nutzung von Netzwerkdiensten	*Maßnahme* Benutzer dürfen ausschließlich auf denjenigen Netzwerken und Netzwerkdiensten Zugriff erhalten, zu deren Nutzung sie ausdrücklich autorisiert wurden.
A.9.2 Benutzerverwaltung Ziel: Sicherstellung des Zugriffs ausschließlich für autorisierte Benutzer und Verhinderung von nicht autorisierten Zugriffen auf Systeme und Dienste.		
A.9.2.1	An- und Abmeldung von Benutzern	*Maßnahme* Es muss ein formales Verfahren für die An- und Abmeldung von Benutzern implementiert werden, mit dem allen Arten von Benutzern der Zugriff auf Systeme und Dienste gewährt und wieder entzogen werden kann.

A.9.2.2	Verwaltung von Sonderrechten	*Maßnahme* Die Zuteilung und Nutzung von Sonderzugriffsrechten muss eingeschränkt und kontrolliert werden.
A.9.2.3	Verwaltung geheimer Authentisierungs-informationen von Benutzern	*Maßnahme* Die Zuordnung von geheimen Authentisierungsinformationen muss über einen formalen Verwaltungsprozess kontrolliert werden.
A.9.2.4	Prüfung von Zugriffs-berechtigungen der Benutzer	*Maßnahme* Werteeigentümer müssen die Zugriffsberechtigungen der Benutzer in regelmäßigen Abständen prüfen.
A.9.2.5	Entzug oder Anpassung von Zugriffsberechtigungen	*Maßnahme* Die Zugriffsberechtigungen aller Mitarbeiter und externen Benutzer zu Informationen und informationsverarbeitenden Einrichtungen müssen nach Auslauf der Anstellung oder des Vertrags entzogen bzw. bei einem Wechsel der Anstellung entsprechend angepasst werden.
A.9.3 Benutzerverantwortung Ziel: Übertragung der Verantwortung für den Schutz der Authentisierungsinformationen auf die Benutzer		
A.9.3.1	Verwendung von geheimen Authentisierungs-informationen	*Maßnahme* Von den Benutzern muss verlangt werden, die sicherheitsrelevanten Praktiken der Organisation zur Verwendung von geheimen Authentisierungsinformationen zu befolgen.
A.9.4 Kontrolle des Zugriffs auf Systeme und Anwendungen Ziel: Verhinderung des unautorisierten Zugriffs auf Systeme und Anwendungen		
A.9.4.1	Beschränkung des Zugriffs auf Informationen	*Maßnahme* Der Zugriff auf Funktionen von Informations- und Anwendungssystemen muss entsprechend der Zugriffskontrollleitlinie beschränkt werden.
A.9.4.2	Sichere Anmeldeverfahren	*Maßnahme* Der Zugriff auf Systeme und Anwendungen muss über ein sicheres Anmeldeverfahren kontrolliert werden, wenn dies nach der Zugriffskontrollleitlinie erforderlich ist.
A.9.4.3	Kennwortmanagementsystem	*Maßnahme* Kennwortmanagementsysteme müssen interaktiv sein und starke Kennwörter erfordern.
A.9.4.4	Verwendung von Dienstprogrammen mit Sonderberechtigungen	*Maßnahme* Die Verwendung von Dienstprogrammen, mit denen sich u. U. System- und Anwendungskontrollen umgehen lassen, muss beschränkt und streng kontrolliert werden.
A.9.4.5	Kontrolle des Zugriffs auf Software-Quellcode	*Maßnahme* Der Zugriff auf den Software-Quellcode muss beschränkt werden.

A.10	**Kryptographie**	
A.10.1	**Kryptographische Maßnahmen**	
Ziel: Sicherstellung der ordnungsnachen und wirksamen Verwendung von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen		
A.10.1.1	Leitlinie zur Nutzung von kryptographischen Maßnahmen	*Maßnahme* Eine Leitlinie zur Verwendung von kryptographischen Maßnahmen für den Schutz von Informationen ist zu entwickeln und zu implementieren.
A.10.1.2	Verwaltung von Schlüsseln	*Maßnahme* Eine Leitlinie zur Verwendung, zum Schutz und zur Gültigkeitsdauer von kryptographischen Schlüsseln ist zu entwickeln und über deren gesamten Nutzungsdauer hinweg umzusetzen.
A.11	**Schutz vor physischem Zugang und Umwelteinflüssen**	
A.11.1	**Sicherheitsbereiche**	
Ziel: Verhinderung des unautorisierten physischen Zugriffs auf die Informationen und informationsverarbeitende Einrichtungen der Organisation sowie deren Beschädigung und Beeinträchtigung.		
A.11.1.1	Physische Sicherheitszone	*Maßnahme* Zum Schutz von Bereichen, in denen sich entweder vertrauliche oder betriebswichtige Informationen oder informationsverarbeitende Einrichtungen befinden, sind Sicherheitszonen festzulegen und zu verwenden.
A.11.1.2	Physische Zugangskontrolle	*Maßnahme* Sicherheitsbereiche müssen durch angemessene Zugriffskontrollen geschützt werden, durch die sichergestellt ist, dass nur autorisiertes Personal Zugriff hat.
A.11.1.3	Sicherung von Zweigstellen, Räumen und Anlagen	*Maßnahme* Es sind physische Sicherungsvorkehrungen für Niederlassungen, Räume und Anlagen zu konzipieren und anzuwenden.
A.11.1.4	Schutz vor externen und umweltbedingten Bedrohungen	*Maßnahme* Es sind physische Schutzvorkehrungen gegen Naturkatastrophen, vorsätzliche Angriffe oder Unfälle zu konzipieren und anzuwenden.
A.11.1.5	Arbeit in Sicherheitsbereichen	*Maßnahme* Es sind physische Schutzvorkehrungen und Richtlinien für die Arbeit in Sicherheitsbereichen zu konzipieren und anzuwenden.
A.11.1.6	Anlieferungs- und Ladezonen	*Maßnahme* Zugangspunkte wie Anlieferungs- und Ladezonen sowie andere Punkte, über die sich unautorisierte Personen Zugang zu den Betriebsgebäuden verschaffen könnten, müssen kontrolliert und nach Möglichkeit von informationsverarbeitenden Einrichtungen isoliert werden, um unautorisierten Zugriff zu verhindern.

A.11.2 Betriebsmittel Ziel: Vorbeugung von Verlust, Beschädigung, Diebstahl oder Beeinträchtigung von Werten und Unterbrechungen der Betriebstätigkeit der Organisation		
A.11.2.1	Platzierung und Schutz von Betriebsmitteln	*Maßnahme* Betriebsmittel sind so zu platzieren und zu schützen, dass Risiken durch Umweltbedrohungen und Gefährdungen sowie Möglichkeiten für den unautorisierten Zugriff verringert werden.
A.11.2.2	Versorgungseinrichtungen	*Maßnahme* Betriebsmittel müssen vor Stromausfällen und anderen Betriebsunterbrechungen durch Ausfälle von Versorgungseinrichtungen geschützt werden.
A.11.2.3	Sicherheit der Verkabelung	*Maßnahme* Stromversorgungs- und Telekommunikationskabel, die zur Übertragung von Daten oder zur Unterstützung von Informationsdiensten verwendet werden, sind vor dem Abfangen der Daten sowie vor Beeinträchtigung oder Beschädigung zu schützen.
A.11.2.4	Instandhaltung von Gerätschaften	*Maßnahme* Gerätschaften müssen ordnungsnach instand gehalten und gepflegt werden, um ihre Verfügbarkeit und Integrität sicherzustellen.
A.11.2.5	Entfernung von Werten	*Maßnahme* Ausstattung, Informationen oder Software dürfen nicht ohne vorherige Autorisierung vom Standort entfernt werden.
A.11.2.6	Sicherheit von Betriebsmitteln und Werten außerhalb der Betriebsgebäude	*Maßnahme* Sicherheitsvorkehrungen werden unter Berücksichtigung der diversen Risiken bei Arbeiten außerhalb der Betriebsgebäude der Organisation auch auf Werte außerhalb des Standorts angewandt.
A.11.2.7	Sichere Entsorgung oder Wiederverwendung von Betriebsmitteln	*Maßnahme* Alle Geräte, die Speichermedien enthalten, müssen vor ihrer Entsorgung oder Wiederverwendung überprüft werden, um sicherzustellen, dass vertrauliche Daten und lizenzierte Software entfernt oder sicher überschrieben wurden.
A.11.2.8	Unbeaufsichtigte Benutzerausstattung	*Maßnahme* Benutzer müssen sicherstellen, dass unbeaufsichtigte Ausstattung angemessen geschützt ist.
A.11.2.9	Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms	*Maßnahme* Der Grundsatz des aufgeräumten Schreibtisches für Papiere und Wechselmedien sowie des leeren Bildschirms für informationsverarbeitende Einrichtungen muss Anwendung finden.
A.12 Betriebssicherheit		
A.12.1 Betriebsverfahren und Zuständigkeiten Ziel: Sicherstellung des ordnungsnahen und sicheren Betriebs von Vorrichtungen zur Verarbeitung von Informationen		
A.12.1.1	Dokumentierte Betriebsverfahren	*Maßnahme* Die Betriebsverfahren müssen dokumentiert und allen Benutzern zugänglich gemacht werden, die sie benötigen.

A.12.1.2	Änderungsmanagement	*Maßnahme* Änderungen an der Organisation, an Geschäftsprozessen, an Datenverarbeitungseinrichtungen und an Systemen sind zu kontrollieren.
A.12.1.3	Kapazitätsmanagement	*Maßnahme* Die Ressourcennutzung muss überwacht und abgestimmt werden, und es sind Prognosen zu zukünftigen Kapazitätsanforderungen zu erstellen, um ausreichende Systemleistung sicherzustellen.
A.12.1.4	Trennung von Entwicklungs-, Test- und Betriebs-umgebungen	*Maßnahme* Entwicklungs-, Test- und Betriebsumgebungen sind zu trennen, um das Risiko unautorisierter Zugriffe oder unautorisierter Änderungen an der Betriebsumgebung zu verringern.
A.12.2 Schutz vor Malware Ziel: Sicherstellung, dass Daten und Datenverarbeitungseinrichtungen vor Malware geschützt sind		
A.12.2.1	Kontrollmaßnahmen gegen Malware	*Maßnahme* Es sind Erkennungs-, Präventions- und Wiederherstellungs-maßnahmen zum Schutz vor Malware in Verbindung mit einer angemessenen Sensibilisierung der Benutzer zu implementieren.
A.12.3 Datensicherungen Ziel: Schutz vor Datenverlust		
A.12.3.1	Datensicherungen	*Maßnahme* Es sind Sicherungskopien von Daten und Software sowie System-Images anzufertigen und regelmäßig entsprechend der vereinbarten Sicherungsleitlinie zu prüfen.
A.12.4 Protokollierung und Überwachung Ziel: Aufzeichnung von Ereignissen und Generierung von Beweismaterial		
A.12.4.1	Ereignisprotokollierung	*Maßnahme* Es sind Ereignisprotokolle anzufertigen, aufzubewahren und regelmäßig zu prüfen, in denen Aktivitäten der Benutzer, Ausnahmen, Fehler und Informationssicherheitsereignisse aufgezeichnet werden.
A.12.4.2	Schutz von Protokoll-informationen	*Maßnahme* Protokollierungseinrichtungen und Protokollinformationen müssen vor Manipulation und unbefugtem Zugriff geschützt werden.
A.12.4.3	Administrator- und Betreiberprotokolle	*Maßnahme* Es sind Protokolle der Aktivitäten von Systemadministratoren und Systembetreibern anzufertigen, zu schützen und regelmäßig zu prüfen.
A.12.4.4	Zeitsynchronisation	*Maßnahme* Die Uhren aller relevanten Datenverarbeitungssysteme innerhalb einer Organisation oder einer Sicherheitsdomäne müssen auf eine einzelne Referenz-Zeitquelle synchronisiert werden.

A.12.5 Kontrolle von Software im Betrieb Ziel: Sicherstellung der Integrität von Systemen im Betrieb		
A.12.5.1	Installation von Software auf Systemen im Betrieb	*Maßnahme* Es sind Verfahren zur Kontrolle der Installation von Software auf betriebsrelevanten Systemen zu implementieren.
A.12.6 Management technischer Schwachstellen Ziel: Verhinderung einer Ausnutzung technischer Schwachstellen		
A.12.6.1	Management technischer Schwachstellen	*Maßnahme* Informationen über technische Schwachstellen von verwendeten Informationssystemen müssen rechtzeitig eingeholt werden, die Anfälligkeit der Organisation für eine Ausnutzung solcher Schwachstellen ist zu bewerten, und es müssen angemessene Maßnahmen für den Umgang mit dem damit einhergehenden Risiko ergriffen werden.
A.12.6.2	Beschränkungen der Software-Installation	*Maßnahme* Für Software-Installationen durch Benutzer müssen Regeln festgelegt und implementiert werden.
A.12.7 Auswirkungen von Audits auf Informationssysteme Ziel: Minimierung der Auswirkungen von Audit-Aktivitäten auf Systeme im Betrieb		
A.12.7.1	Kontrollen für Audits von Informationssystemen	*Maßnahme* Audit-Anforderungen und -Aktivitäten im Zusammenhang mit betriebsrelevanten Systemen müssen sorgfältig geplant und vereinbart werden, um Unterbrechungen der Geschäftsabläufe zu minimieren.
A.13 Sicherheit in der Kommunikation		
A.13.1 Netzwerksicherheitsmanagement Ziel: Sicherstellung des Schutzes von Informationen in Netzwerken und den unterstützenden informationsverarbeitenden Einrichtungen		
A.13.1.1	Netzwerkkontrollen	*Maßnahme* Netzwerke müssen verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen zu schützen.
A.13.1.2	Sicherheit von Netzwerkdiensten	*Maßnahme* Es müssen Sicherheitsmechanismen, Service-Level und Anforderungen für die Verwaltung aller Netzwerkdienste ermittelt und in Verträge über Netzwerkdienste aufgenommen werden, und zwar unabhängig davon, ob diese Dienste intern erbracht oder ausgelagert werden.
A.13.1.3	Trennung in Netzwerken	*Maßnahme* Gruppen von Informationsdiensten, Benutzern und Informationssystemen müssen in Netzwerken voneinander getrennt gehalten werden.

A.13.2 Informationsübertragung Ziel: Wahrung der Sicherheit von Informationen, die innerhalb einer Organisation oder im Austausch mit einer externen Stelle übertragen werden.		
A.13.2.1	Leitlinien und Verfahren für die Informationsübertragung	*Maßnahme* Es müssen formale Leitlinien, Verfahren und Kontrollmaßnahmen in Kraft sein, mit denen die Informationsübertragung über alle Arten von Kommunikationseinrichtungen geschützt wird.
A.13.2.2	Vereinbarungen zur Informationsübertragung	*Maßnahme* Es muss Vereinbarungen für die sichere Übertragung von geschäftlichen Informationen zwischen der Organisation und externen Parteien geben.
A.13.2.3	Elektronische Nachrichtenübermittlung	*Maßnahme* Informationen in elektronischen Nachrichten müssen angemessen geschützt werden.
A.13.2.4	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	*Maßnahme* Entsprechend den Bedürfnissen der Organisation in Bezug auf den Schutz von Informationen müssen Anforderungen für Vertraulichkeits- oder Geheimhaltungsvereinbarungen ermittelt, regelmäßig geprüft und dokumentiert werden.
A.14 Anschaffung, Entwicklung und Instandhaltung von Systemen		
A.14.1 Sicherheitsanforderungen für Informationssysteme Ziel: Sicherstellung, dass Sicherheit über den gesamten Lebenszyklus von Informationssystemen hinweg fester Bestandteil dieser Systeme ist. Dies beinhaltet insbesondere spezifische Sicherheitsanforderungen für Informationssysteme, mit denen Dienste über öffentliche Netze bereitgestellt werden.		
A.14.1.1	Analyse und Spezifikation von Sicherheitsanforderungen	*Maßnahme* Die Anforderungen für Kontrollen der Informationssicherheit müssen in den Angaben zu den geschäftlichen und technischen Anforderungen für neue Informationssysteme oder Verbesserungen an bestehenden Informationssystemen enthalten sein, und darin müssen alle relevanten Kriterien wie die gesamte Nutzungsdauer oder ggf. die Verfügbarkeit der Anwendung über öffentliche Netze berücksichtigt sein.
A.14.1.2	Sicherung von Anwendungsdiensten in öffentlichen Netzen	*Maßnahme* Informationen im Zusammenhang mit Anwendungsdiensten, die über öffentliche Netze übertragen werden, müssen gegen betrügerische Aktivitäten, Vertragsstreitigkeiten, unberechtigte Veröffentlichung oder Veränderung geschützt werden.
A.14.1.3	Schutz von Transaktionen im Zusammenhang mit Anwendungsdiensten	*Maßnahme* Informationen, die im Zuge von Transaktionen im Zusammenhang mit Anwendungsdiensten übertragen werden, müssen geschützt werden, um unvollständigen Übertragungen und Fehlleitungen sowie unautorisierten Offenlegungen, Vervielfältigungen oder wiederholten Wiedergaben von Nachrichten vorzubeugen.

A.14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen Ziel: Sicherstellung, dass Informationssicherheit im Rahmen des Entwicklungszyklus von Informationssystemen konzipiert und implementiert wird		
A.14.2.1	Leitlinie für sichere Entwicklung	*Maßnahme* Es müssen Regeln für die Entwicklung von Software und Systemen festgelegt und bei Entwicklungen innerhalb der Organisation angewandt werden.
A.14.2.2	Änderungskontrollverfahren	*Maßnahme* Die Umsetzung von Änderungen muss einem formalen Änderungskontrollverfahren unterliegen.
A.14.2.3	Technische Prüfung von Anwendungen nach Wechseln der Betriebsplattform	*Maßnahme* Bei einem Wechsel der Betriebsplattform müssen geschäftskritische Anwendungen geprüft und getestet werden, um sicherzustellen, dass keine negativen Auswirkungen auf die Betriebstätigkeit oder die Sicherheit der Organisation gibt.
A.14.2.4	Beschränkung von Änderungen an Software-Paketen	*Maßnahme* Von Änderungen an Software-Paketen ist abzuraten. Falls doch Änderungen vorgenommen werden, müssen diese auf das Notwendige beschränkt sein und in jedem Fall streng kontrolliert werden.
A.14.2.5	Systementwicklungsverfahren	*Maßnahme* Es sind Grundsätze für die Entwicklung sicherer Systeme festzulegen, zu dokumentieren, aufrechtzuerhalten und bei jedem Systementwicklungsvorhaben anzuwenden.
A.14.2.6	Sichere Entwicklungs-umgebung	*Maßnahme* Organisationen müssen eine sichere Entwicklungsumgebung für Systementwicklungen und Integrationsvorhaben, die den gesamten Zyklus der Systementwicklung abdeckt, herstellen und angemessen schützen.
A.14.2.7	Ausgelagerte Entwicklung	*Maßnahme* Die Organisation muss ausgelagerte Systementwicklungs-tätigkeiten beaufsichtigen und überwachen.
A.14.2.8	Systemsicherheitsprüfungen	*Maßnahme* Während der Entwicklung müssen die Sicherheits-vorkehrungen auf Funktion geprüft werden.
A.14.2.9	Systemabnahmeprüfung	*Maßnahme* Für neue Informationssysteme, Upgrades und neue Versionen sind Abnahmeprüfungsprogramme und dazugehörige Kriterien festzulegen.
A.14.3 Prüfdaten Ziel: Sicherstellung des Schutzes von zu Prüfzwecken verwendeten Daten		
A.14.3.1	Schutz von Prüfdaten	*Maßnahme* Prüfdaten müssen sorgfältig ausgewählt, geschützt und kontrolliert werden.

A.15 Lieferantenbeziehungen		
A.15.1 Sicherheit in Lieferantenbeziehungen Ziel: Sicherstellung des Schutzes der für Lieferanten zugänglichen Informationen des Unternehmens		
A.15.1.1	Informationssicherheitsleitlinie für Lieferantenbeziehungen	*Maßnahme* Die Informationssicherheitsanforderungen zurr Verringerung von Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf Informationen oder informationsverarbeitende Einrichtungen der Organisation sind zu dokumentieren.
A.15.1.2	Sicherheitsthemen in Lieferantenverträgen	*Maßnahme* Mit jedem Lieferanten, der u. U. Zugriff auf Informationen der Organisation hat, sie verarbeitet, speichert, weitergibt oder IT-Infrastrukturkomponenten dafür bereitstellt, müssen jeweils alle relevanten Informationssicherheitsanforderungen festgelegt und vereinbart werden.
A.15.1.3	IKT-Lieferkette	*Maßnahme* Vereinbarungen mit Lieferanten müssen Anforderungen für den Umgang mit Informationssicherheitsrisiken im Zusammenhang mit der Dienstleistungs- und Produktlieferkette im Bereich der Informations- und Kommunikationstechnologie enthalten.
A.15.2 Management der Dienstleistungserbringung durch Lieferanten Ziel: Aufrechterhaltung einer vereinbarten Informationssicherheitsstufe und Dienstleistungserbringung im Einklang mit Lieferantenverträgen		
A.15.2.1	Überwachung und Prüfung von Lieferantendienstleistungen	*Maßnahme* Organisationen müssen die Dienstleistungserbringung durch Lieferanten regelmäßig überwachen, prüfen und auditieren.
A.15.2.2	Management von Änderungen an Lieferantendienstleistungen	*Maßnahme* Änderungen an der Erbringung von Dienstleistungen durch Lieferanten einschließlich der Pflege und Verbesserung bestehender Informationssicherheitsleitlinien, -verfahren und -kontrollen müssen unter Berücksichtigung der Betriebswichtigkeit der betroffenen geschäftlichen Informationen, Systeme und Prozesse sowie einer erneuten Risikobewertung verwaltet werden.
A.16 Management von Informationssicherheitsvorfällen		
A.16.1 Management von Informationssicherheitsvorfällen und Verbesserungen Ziel: Sicherstellung einer konsistenten und wirksamen Strategie für das Management von Informationssicherheitsvorfällen einschließlich Benachrichtigung über Sicherheitsvorfälle und Schwachstellen		
A.16.1.1	Zuständigkeiten und Verfahren	*Maßnahme* Zuständigkeiten und Verfahren für das Management sind festzulegen, damit schnell, effektiv und koordiniert auf Informationssicherheitsvorfälle reagiert werden kann.
A.16.1.2	Meldung von Informationssicherheitsereignissen	*Maßnahme* Informationssicherheitsereignisse müssen so schnell wie möglich über geeignete Management-Kanäle gemeldet werden.

A.16.1.3	Meldung von Informations-sicherheitsschwachstellen	*Maßnahme* Mitarbeiter und externe Parteien, die die Informationssysteme und -dienste der Organisation nutzen, müssen dazu aufgefordert werden, jegliche beobachteten oder vermuteten Informationssicherheitsschwachstellen in Systemen oder Diensten festzuhalten und zu melden.
A.16.1.4	Bewertung und Einstufung von Informations-sicherheitsereignissen	*Maßnahme* Informationssicherheitsereignisse sind zu bewerten, und es muss darüber entschieden werden, ob sie als Informationssicherheitsvorfälle eingestuft werden.
A.16.1.5	Reaktion auf Informationssicherheitsvorfälle	*Maßnahme* Auf Informationssicherheitsvorfälle muss entsprechend den dokumentierten Verfahren reagiert werden.
A.16.1.6	Erkenntnisse aus Informations-sicherheitsvorfällen	*Maßnahme* Aus der Analyse und Lösung von Informationssicherheits-vorfällen gewonnene Erkenntnisse müssen dazu genutzt werden, die Auftretenswahrscheinlichkeit oder die Auswirkungen zukünftiger Vorfälle zu verringern.
A.16.1.7	Sammeln von Beweismaterial	*Maßnahme* Die Organisation muss Verfahren für die Ermittlung, Sammlung, Aneignung und Aufbewahrung von Informationen, die als Beweismaterial dienen können, festlegen und anwenden.
A.17 Informationssicherheitsaspekte des Business Continuity Management		
A.17.1 Kontinuität der Informationssicherheit Ziel: Die Kontinuität der Informationssicherheit muss Teil des Business Continuity Management (BCM) der Organisation sein, so dass sichergestellt ist, dass Informationen jederzeit geschützt sind und die Organisation auf negative Ereignisse vorbereitet ist.		
A.17.1.1	Planung der Kontinuität der Informationssicherheit	*Maßnahme* Die Organisation muss ihre Anforderungen für die Informationssicherheit und für die Aufrechterhaltung des Informationssicherheitsmanagements auch in schwierigen Situationen wie z. B. während einer Krise oder Katastrophe festlegen.
A.17.1.2	Implementierung der Kontinuität der Informations-sicherheit	*Maßnahme* Die Organisation muss Prozesse, Verfahren und Kontroll-maßnahmen festlegen, dokumentieren, implementieren und aufrechterhalten, um das erforderliche Maß an Kontinuität der Informationssicherheit in einer schwierigen Situation sicherstellen zu können.
A.17.1.3	Überprüfung, Überarbeitung und Auswertung der Kontinuität der Informations-sicherheit	*Maßnahme* Die Organisation muss die festgelegten und implementierten Kontrollmaßnahmen für die Kontinuität der Informations-sicherheit in regelmäßigen Abständen überprüfen, um sicherzustellen, dass sie gültig und auch in schwierigen Situationen wirksam sind.

A.17.2 Redundanzen Ziel: Sicherstellung der Verfügbarkeit von informationsverarbeitenden Einrichtungen		
A.17.2.1	Verfügbarkeit von informationsverarbeitenden Einrichtungen	*Maßnahme* Informationsverarbeitende Einrichtungen müssen mit ausreichender Redundanz für die Einhaltung der Verfügbarkeitsanforderungen implementiert werden.
A.18 Richtlinienkonformität		
A.18.1 Informationssicherheitsprüfungen Ziel: Sicherstellung, dass Informationssicherheitsvorkehrungen entsprechend den Leitlinien und Verfahren der Organisation implementiert und angewandt werden.		
A.18.1.1	Unabhängige Prüfung der Informationssicherheit	*Maßnahme* Die Strategie der Organisation für das Management der Informationssicherheit und deren Implementierung (d. h. Kontrollziele und -maßnahmen, Leitlinien, Prozesse und Verfahren zur Informationssicherheit) müssen in planmäßigen Abständen oder jeweils bei erheblichen Änderungen an der Implementierung von Sicherheitsvorkehrungen durch eine unabhängige Stelle geprüft werden.
A.18.1.2	Einhaltung der Sicherheitsleitlinien und -normen	*Maßnahme* Vorgesetzte müssen regelmäßig die Konformität der Informationsverarbeitung und der Verfahren in ihrem Zuständigkeitsbereich mit den jeweils anwendbaren Sicherheitsleitlinien, Normen und jeglichen sonstigen Sicherheitsanforderungen prüfen.
A.18.1.3	Inspektion der Technik auf Richtlinienkonformität	*Maßnahme* Informationssysteme müssen regelmäßig auf Konformität mit den Informationssicherheitsleitlinien und -normen der Organisation geprüft werden.
A.18.2 Einhaltung gesetzlicher und vertraglicher Anforderungen Ziel: Vermeidung von Verstößen gegen gesetzliche, amtliche oder vertragliche Verpflichtungen im Zusammenhang mit Informationssicherheit sowie gegen jegliche Sicherheitsanforderungen		
A.18.2.1	Ermittlung anwendbarer gesetzlicher und vertraglicher Anforderungen	*Maßnahme* Alle relevanten gesetzlichen, amtlichen und vertraglichen Anforderungen sowie die Strategie der Organisation zur Erfüllung dieser Anforderungen müssen für jedes Informationssystem sowie für die Organisation ausdrücklich ermittelt, dokumentiert und auf dem neuesten Stand gehalten werden.
A.18.2.2	Rechte an geistigem Eigentum	*Maßnahme* Es sind angemessene Verfahren zu implementieren, mit denen die Einhaltung gesetzlicher, amtlicher und vertraglicher Anforderungen zur Verwendung von Material, an dem möglicherweise Schutzrechte bestehen, sowie von urheberrechtlich geschützten Software-Produkten sichergestellt wird.
A.18.2.3	Schutz dokumentierter Informationen	*Maßnahme* Aufzeichnungen sind nach gesetzlichen, amtlichen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung, Fälschung, unautorisiertem Zugriff und unautorisierter Freigabe zu schützen.

A.18.2.4	Privatsphäre und Schutz von personenbezogenen Informationen	*Maßnahme* Die Privatsphäre sowie der Schutz von personenbezogenen Informationen müssen entsprechend den Anforderungen der relevanten Gesetze, Vorschriften und ggf. Vertragsbestimmungen sichergestellt werden.
A.18.2.5	Regulierung kryptographischer Kontrollmaßnahmen	*Maßnahme* Kryptographische Kontrollmaßnahmen müssen unter Einhaltung aller relevanten Vereinbarungen, Gesetze und Vorschriften angewandt werden.

Literaturhinweise

[1] ISO/IEC 27002:2005, *Information technology — Security Techniques — Code of practice for information security management*

[2] ISO/IEC 27003:2010, *Information technology — Security Techniques — Information security management system implementation guidance*

[3] ISO/IEC 27004:2009, *Information technology — Security Techniques — Information security management — Measurement*

[4] ISO/IEC 27005:2011, *Information technology — Security Techniques — Information security risk management*

[5] ISO 19011:2011, *Guidelines for auditing management systems*

[6] ISO 31000:2009, *Risk Management — Principles and guidelines*

[7] ISO/IEC Directives, *Part 1 Consolidated ISO Supplement — Procedures specific to ISO:2012*

[8] ISO/IEC 27007:2011 *Information technology — Security Techniques — Guidelines for Information security management systems auditing*