

DIN ISO/IEC 27001

ICS 35.040

Ersatz für
DIN ISO/IEC 27001:2008-09

**Informationstechnik –
IT-Sicherheitsverfahren –
Informationssicherheits-Managementsysteme – Anforderungen
(ISO/IEC 27001:2013 + Cor. 1:2014)**

Information technology –
Security techniques –
Information security management systems – Requirements (ISO/IEC 27001:2013 +
Cor. 1:2014)

Technologies de l'information –
Techniques de sécurité –
Systèmes de gestion de sécurité de l'information – Exigences (ISO/CEI 27001:2013 +
Cor. 1:2014)

Gesamtumfang 31 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)



Inhalt

	Seite
Nationales Vorwort	3
Nationaler Anhang NA (informativ) Literaturhinweise	4
0 Einleitung	5
0.1 Allgemeines	5
0.2 Kompatibilität mit anderen Normen für Managementsysteme	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Kontext der Organisation	6
4.1 Verstehen der Organisation und ihres Kontextes	6
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien	6
4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems	7
4.4 Informationssicherheitsmanagementsystem	7
5 Führung	7
5.1 Führung und Verpflichtung	7
5.2 Politik	8
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	8
6 Planung	8
6.1 Maßnahmen zum Umgang mit Risiken und Chancen	8
6.2 Informationssicherheitsziele und Planung zu deren Erreichung	10
7 Unterstützung	11
7.1 Ressourcen	11
7.2 Kompetenz	11
7.3 Bewusstsein	11
7.4 Kommunikation	11
7.5 Dokumentierte Information	12
8 Betrieb	13
8.1 Betriebliche Planung und Steuerung	13
8.2 Informationssicherheitsrisikobeurteilung	13
8.3 Informationssicherheitsrisikobehandlung	13
9 Bewertung der Leistung	13
9.1 Überwachung, Messung, Analyse und Bewertung	13
9.2 Internes Audit	14
9.3 Managementbewertung	14
10 Verbesserung	15
10.1 Nichtkonformität und Korrekturmaßnahmen	15
10.2 Fortlaufende Verbesserung	15
Anhang A (normativ) Referenzmaßnahmenziele und -maßnahmen	16
Literaturhinweise	31



Nationales Vorwort

Dieses Dokument wurde vom DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) in Zusammenarbeit mit dem Austrian Standards Institute (ASI) und der Schweizerischen Normenvereinigung (SNV) erarbeitet.

Die Internationale Norm ISO/IEC 27001:2013 + Cor. 1:2014 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 DIN-Normenausschusses Informationstechnik und Anwendungen (NIA).

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.

Der Beginn und das Ende des vom Corrigendum 1 geänderten Textes werden durch die Markierungen   angezeigt.

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.

Frühere Ausgaben

DIN ISO/IEC 27001:2008-09

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN ISO/IEC 27000, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-
Managementsysteme — Überblick und Terminologie*

Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen

0 Einleitung

0.1 Allgemeines

Diese Internationale Norm wurde erarbeitet, um Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) festzulegen. Die Einführung eines Informationssicherheitsmanagementsystems stellt für eine Organisation eine strategische Entscheidung dar. Erstellung und Umsetzung 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.

Das Informationssicherheitsmanagementsystem wahrt die Vertraulichkeit, Integrität und Verfügbarkeit von Information unter Anwendung eines Risikomanagementprozesses und verleiht interessierten Parteien das Vertrauen in eine angemessene Steuerung von Risiken.

Es ist wichtig, dass das Informationssicherheitsmanagementsystem als Teil der Abläufe der Organisation in deren übergreifende Steuerungsstruktur integriert ist und die Informationssicherheit bereits bei der Konzeption von Prozessen, Informationssystemen und Maßnahmen berücksichtigt wird. Es wird erwartet, dass die Umsetzung eines Informationssicherheitsmanagementsystems entsprechend den Bedürfnissen der Organisation skaliert wird.

Diese Internationale Norm kann von internen und externen Parteien dazu eingesetzt werden, die Fähigkeit einer Organisation zur Einhaltung ihrer eigenen Informationssicherheitsanforderungen zu beurteilen.

Die Reihenfolge, in der die Anforderungen in dieser Internationalen Norm aufgeführt sind, spiegelt nicht deren Bedeutung wider noch die Abfolge, in der sie umzusetzen sind. Die Einträge sind lediglich zu Referenzierungszwecken nummeriert.

ISO/IEC 27000 liefert einen Überblick und die Begrifflichkeiten von Informationssicherheitsmanagementsystemen und verweist auf die Informationssicherheitsmanagementsystem-Normenfamilie (einschließlich ISO/IEC 27003 [2], ISO/IEC 27004 [3] und ISO/IEC 27005 [4]), einschließlich deren Begriffe.

0.2 Kompatibilität mit anderen Normen für Managementsysteme

Diese Internationale Norm wendet die Grundstrukturen, den einheitlichen Basistext, die gemeinsamen Benennungen und die Basisdefinitionen für den Gebrauch in Managementsystemnormen an, die jeweils im Anhang SL der ISO/IEC-Direktiven, Teil 1, „Consolidated ISO Supplement“ festgelegt sind, und stellt so die Übereinstimmung mit anderen Managementsystemnormen her, die ebenfalls den Anhang SL anwenden.

Die in Anhang SL festgelegte allgemeine Herangehensweise nützt jenen Organisationen, die sich für den Betrieb eines einzigen Managementsystems entscheiden, um die Anforderungen von zwei oder mehr Normen für Managementsysteme zu erfüllen.

1 Anwendungsbereich

Diese Internationale Norm legt die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems im Kontext der Organisation fest. Darüber hinaus beinhaltet diese Internationale Norm Anforderungen für die Beurteilung und Behandlung 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

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung des Dokuments erforderlich. 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 Verstehen der Organisation und ihres Kontextes

Die Organisation muss externe und interne Themen bestimmen, die für ihren Zweck relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse ihres Informationssicherheitsmanagementsystems zu erreichen.

ANMERKUNG Die Bestimmung dieser Themen bezieht sich auf die Festlegung des externen und internen Kontexts des Unternehmens, wie in ISO 31000:2009 [5], 5.3, beschrieben.

4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien

Die Organisation muss:

- a) die interessierten Parteien, die für ihr Informationssicherheitsmanagementsystem relevant sind; und
- b) die Anforderungen dieser interessierten Parteien mit Bezug zur Informationssicherheit bestimmen.

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

4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems

Die Organisation muss die Grenzen und die Anwendbarkeit des Informationssicherheitsmanagementsystems bestimmen, um dessen Anwendungsbereich festzulegen.

Bei der Festlegung des Anwendungsbereichs muss die Organisation:

- a) die unter 4.1 genannten externen und internen Themen;
- b) die unter 4.2 genannten Anforderungen; und
- c) Schnittstellen und Abhängigkeiten zwischen Tätigkeiten, die von der Organisation selbst durchgeführt werden, und Tätigkeiten, die von anderen Organisationen durchgeführt werden

berücksichtigen.

Der Anwendungsbereich muss als dokumentierte Information verfügbar sein.

4.4 Informationssicherheitsmanagementsystem

Die Organisation muss entsprechend den Anforderungen dieser Internationalen Norm ein Informationssicherheitsmanagementsystem aufbauen, verwirklichen, aufrechterhalten und fortlaufend verbessern.

5 Führung

5.1 Führung und Verpflichtung

Die oberste Leitung muss in Bezug auf das Informationssicherheitsmanagementsystem Führung und Verpflichtung zeigen, indem sie:

- a) sicherstellt, dass die Informationssicherheitspolitik und die Informationssicherheitsziele festgelegt und mit der strategischen Ausrichtung der Organisation vereinbar sind;
- b) sicherstellt, dass die Anforderungen des Informationssicherheitsmanagementsystems in die Geschäftsprozesse der Organisation integriert werden;
- c) sicherstellt, dass die für das Informationssicherheitsmanagementsystem erforderlichen Ressourcen zur Verfügung stehen;
- d) die Bedeutung eines wirksamen Informationssicherheitsmanagements sowie die Wichtigkeit der Erfüllung der Anforderungen des Informationssicherheitsmanagementsystems vermittelt;
- e) sicherstellt, dass das Informationssicherheitsmanagementsystem sein beabsichtigtes Ergebnis bzw. seine beabsichtigten Ergebnisse erzielt;
- f) Personen anleitet und unterstützt, damit diese zur Wirksamkeit des Informationssicherheitsmanagementsystems beitragen können;
- g) fortlaufende Verbesserung fördert; und
- h) andere relevante Führungskräfte unterstützt, um deren Führungsrolle in deren jeweiligen Verantwortungsbereichen deutlich zu machen.

5.2 Politik

Die oberste Leitung muss eine Informationssicherheitspolitik festlegen, die:

- a) für den Zweck der Organisation angemessen ist;
- b) Informationssicherheitsziele (siehe 6.2) beinhaltet oder den Rahmen zum Festlegen von Informationssicherheitszielen bietet;
- c) eine Verpflichtung zur Erfüllung zutreffender Anforderungen mit Bezug zur Informationssicherheit enthält; und
- d) eine Verpflichtung zur fortlaufenden Verbesserung des Informationssicherheitsmanagementsystems enthält.

Die Informationssicherheitspolitik muss:

- e) als dokumentierte Information verfügbar sein;
- f) innerhalb der Organisation bekanntgemacht werden; und
- g) für interessierte Parteien verfügbar sein, soweit angemessen.

5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

Die oberste Leitung muss sicherstellen, dass die Verantwortlichkeiten und Befugnisse für Rollen mit Bezug zur Informationssicherheit zugewiesen und bekannt gemacht werden.

Die oberste Leitung muss die Verantwortlichkeit und Befugnis zuweisen für:

- a) das Sicherstellen, dass das Informationssicherheitsmanagementsystem die Anforderungen dieser Internationalen Norm erfüllt; und
- b) das Berichten an die oberste Leitung über die Leistung des Informationssicherheitsmanagementsystems.

ANMERKUNG Die oberste Leitung darf auch Verantwortlichkeiten und Befugnisse für das Berichten der Leistung des Informationssicherheitsmanagementsystems innerhalb der Organisation zuweisen.

6 Planung

6.1 Maßnahmen zum Umgang mit Risiken und Chancen

6.1.1 Allgemeines

Bei der Planung für das Informationssicherheitsmanagementsystem muss die Organisation die in 4.1 genannten Themen und die in 4.2 genannten Anforderungen berücksichtigen sowie die Risiken und Chancen bestimmen, die betrachtet werden müssen, um:

- a) sicherzustellen, dass das Informationssicherheitsmanagementsystem seine beabsichtigten Ergebnisse erzielen kann;
- b) unerwünschte Auswirkungen zu verhindern oder zu verringern; und
- c) fortlaufende Verbesserung zu erreichen.

Die Organisation muss planen:

- d) Maßnahmen zum Umgang mit diesen Risiken und Chancen; und
- e) wie
 - 1) die Maßnahmen in die Informationssicherheitsmanagementsystemprozesse der Organisation integriert und dort umgesetzt werden; und
 - 2) die Wirksamkeit dieser Maßnahmen bewertet wird.

6.1.2 Informationssicherheitsrisikobeurteilung

Die Organisation muss einen Prozess zur Informationssicherheitsrisikobeurteilung festlegen und anwenden, der:

- a) Informationssicherheitsrisikokriterien festlegt und aufrechterhält, welche:
 - 1) die Kriterien zur Risikoakzeptanz; und
 - 2) Kriterien für die Durchführung von Informationssicherheitsrisikobeurteilungen
 beinhalten;
- b) sicherstellt, dass wiederholte Informationssicherheitsrisikobeurteilungen zu konsistenten, gültigen und vergleichbaren Ergebnissen führen;
- c) die Informationssicherheitsrisiken identifiziert:
 - 1) den Prozess zur Informationssicherheitsrisikobeurteilung anwendet, um Risiken im Zusammenhang mit dem Verlust der Vertraulichkeit, Integrität und Verfügbarkeit von Information innerhalb des Anwendungsbereichs des ISMS zu ermitteln; und
 - 2) die Risikoeigentümer identifiziert;
- d) die Informationssicherheitsrisiken analysiert:
 - 1) die möglichen Folgen bei Eintritt der nach 6.1.2 c) 1) identifizierten Risiken abschätzt;
 - 2) die realistischen Eintrittswahrscheinlichkeiten der nach 6.1.2 c) 1) identifizierten Risiken abschätzt; und
 - 3) die Risikoniveaus bestimmt;
- e) die Informationssicherheitsrisiken bewertet:
 - 1) die Ergebnisse der Risikoanalyse mit den nach 6.1.2 a) festgelegten Risikokriterien vergleicht; und
 - 2) die analysierten Risiken für die Risikobehandlung priorisiert.

Die Organisation muss dokumentierte Information über den Informationssicherheitsrisikobeurteilungsprozess aufbewahren.

6.1.3 Informationssicherheitsrisikobehandlung

Die Organisation muss einen Prozess für die Informationssicherheitsrisikobehandlung festlegen und anwenden, um:

- a) angemessene Optionen für die Informationssicherheitsrisikobehandlung unter Berücksichtigung der Ergebnisse der Risikobeurteilung auszuwählen;
- b) alle Maßnahmen, die zur Umsetzung der gewählte(n) Option(en) für die Informationssicherheitsrisikobehandlung erforderlich sind, festzulegen;

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

- c) die nach 6.1.3 b) festgelegten Maßnahmen mit den Maßnahmen in Anhang A zu vergleichen und zu überprüfen, dass keine erforderlichen Maßnahmen ausgelassen wurden;

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

ANMERKUNG 2 In den ausgewählten Maßnahmen sind implizit Maßnahmenziele enthalten. Die Liste der Maßnahmenziele und Maßnahmen in Anhang A ist nicht erschöpfend und weitere Maßnahmenziele und Maßnahmen könnten erforderlich sein.

- d) eine Erklärung zur Anwendbarkeit zu erstellen, welche die erforderlichen Maßnahmen (siehe 6.1.3 b) und c)) und Gründe für deren Einbeziehung, unabhängig davon, ob sie nun umgesetzt sind oder nicht, sowie Gründe für die Nichteinbeziehung von Maßnahmen aus Anhang A enthält;
- e) einen Plan für die Informationssicherheitsrisikobehandlung zu formulieren; und
- f) bei den Risikoeigentümern eine Genehmigung des Plans für die Informationssicherheitsrisikobehandlung sowie ihre Akzeptanz der Informationssicherheitsrestrisiken einzuholen.

Die Organisation muss dokumentierte Information über den Informationssicherheitsrisikobehandlungsprozess aufbewahren.

ANMERKUNG Der in dieser Internationalen Norm genannte Prozess für die Informationssicherheitsrisikobeurteilung und -behandlung steht im Einklang mit den Grundsätzen und allgemeinen Leitlinien in ISO 31000 [5].

6.2 Informationssicherheitsziele und Planung zu deren Erreichung

Die Organisation muss Informationssicherheitsziele für relevante Funktionen und Ebenen festlegen.

Die Informationssicherheitsziele müssen:

- a) im Einklang mit der Informationssicherheitspolitik stehen;
- b) messbar sein (sofern machbar);
- c) anwendbare Informationssicherheitsanforderungen sowie die Ergebnisse, der Risikobeurteilung und Risikobehandlung berücksichtigen;
- d) vermittelt werden; und
- e) soweit erforderlich, aktualisiert werden.

Die Organisation muss dokumentierte Information zu den Informationssicherheitszielen aufbewahren.

Bei der Planung, zum Erreichen der Informationssicherheitsziele, muss die Organisation bestimmen:

- f) was getan wird;
- g) welche Ressourcen erforderlich sind;
- h) wer verantwortlich ist;
- i) wann es abgeschlossen wird; und
- j) wie die Ergebnisse bewertet werden.

7 Unterstützung

7.1 Ressourcen

Die Organisation muss die erforderlichen Ressourcen für den Aufbau, die Verwirklichung, die Aufrechterhaltung und die fortlaufende Verbesserung des Informationssicherheitsmanagementsystems bestimmen und bereitstellen.

7.2 Kompetenz

Die Organisation muss:

- a) für Personen, die unter ihrer Aufsicht Tätigkeiten verrichten, welche die Informationssicherheitsleistung der Organisation beeinflussen, die erforderliche Kompetenz bestimmen;
- b) sicherstellen, dass diese Personen auf Grundlage angemessener Ausbildung, Schulung oder Erfahrung kompetent sind;
- c) wenn erforderlich, Maßnahmen einleiten, um die benötigte Kompetenz zu erwerben, und die Wirksamkeit der getroffenen Maßnahmen zu bewerten; und
- d) angemessene dokumentierte Information als Nachweis der Kompetenz aufbewahren.

ANMERKUNG Geeignete Maßnahmen können zum Beispiel sein: Schulung, Mentoring oder Versetzung von gegenwärtig angestellten Personen, oder Anstellung oder Beauftragung kompetenter Personen.

7.3 Bewusstsein

Personen, die unter Aufsicht der Organisation Tätigkeiten verrichten, müssen sich:

- a) der Informationssicherheitspolitik;
- b) ihres Beitrags zur Wirksamkeit des Informationssicherheitsmanagementsystems, einschließlich der Vorteile einer verbesserten Informationssicherheitsleistung; und
- c) der Folgen einer Nichterfüllung der Anforderungen des Informationssicherheitsmanagementsystems bewusst sein.

7.4 Kommunikation

Die Organisation muss die interne und externe Kommunikation in Bezug auf das Informationssicherheitsmanagementsystem bestimmen, einschließlich

- a) worüber kommuniziert wird;

- b) wann kommuniziert wird;
- c) mit wem kommuniziert wird;
- d) wer kommuniziert; und
- e) der Prozesse, mit welchen die Kommunikation bewerkstelligt wird.

7.5 Dokumentierte Information

7.5.1 Allgemeines

Das Informationssicherheitsmanagementsystem der Organisation muss beinhalten:

- a) die von dieser Internationalen Norm geforderte dokumentierte Information; und
- b) dokumentierte Information, welche die Organisation als notwendig für die Wirksamkeit des Managementsystems bestimmt hat.

ANMERKUNG Der Umfang dokumentierter Information für ein Informationssicherheitsmanagementsystem kann sich von Organisation zu Organisation unterscheiden, und zwar aufgrund:

- 1) der Größe der Organisation und der Art ihrer Tätigkeiten, Prozesse, Produkte und Dienstleistungen;
- 2) der Komplexität der Prozesse und deren Wechselwirkungen; und
- 3) der Kompetenz der Personen.

7.5.2 Erstellen und Aktualisieren

Beim Erstellen und Aktualisieren dokumentierter Information muss die Organisation:

- a) angemessene Kennzeichnung und Beschreibung (z. B. Titel, Datum, Autor oder Referenznummer);
- b) angemessenes Format (z. B. Sprache, Softwareversion, Graphiken) und Medium (z. B. Papier, elektronisches Medium); und
- c) angemessene Überprüfung und Genehmigung im Hinblick auf Eignung und Angemessenheit sicherstellen.

7.5.3 Lenkung dokumentierter Information

Die für das Informationssicherheitsmanagementsystem erforderliche und von dieser Internationalen Norm geforderte dokumentierte Information muss gelenkt werden, um sicherzustellen, dass sie

- a) verfügbar und für die Verwendung geeignet ist, wo und wann sie benötigt wird; und
- b) angemessen geschützt wird (z. B. vor Verlust der Vertraulichkeit, unsachgemäßem Gebrauch oder Verlust der Integrität).

Zur Lenkung dokumentierter Information muss die Organisation, falls zutreffend, folgende Tätigkeiten berücksichtigen:

- c) Verteilung, Zugriff, Auffindung und Verwendung;
- d) Ablage/Speicherung und Erhaltung, einschließlich Erhaltung der Lesbarkeit;

- e) Überwachung von Änderungen (z. B. Versionskontrolle); und
- f) Aufbewahrung und Verfügung über den weiteren Verbleib.

Dokumentierte Information externer Herkunft, die von der Organisation als notwendig für Planung und Betrieb des Informationssicherheitsmanagementsystems bestimmt wurde, muss angemessen gekennzeichnet und gelenkt werden.

ANMERKUNG Zugriff kann eine Entscheidung voraussetzen, mit der die Erlaubnis erteilt wird, dokumentierte Information lediglich zu lesen, oder die Erlaubnis und Befugnis zum Lesen und Ändern dokumentierter Information usw.

8 Betrieb

8.1 Betriebliche Planung und Steuerung

Die Organisation muss die Prozesse zur Erfüllung der Informationssicherheitsanforderungen und zur Durchführung der unter 6.1 bestimmten Maßnahmen planen, verwirklichen und steuern. Die Organisation muss darüber hinaus Pläne verwirklichen, um die in 6.2 bestimmten Informationssicherheitsziele zu erreichen.

Die Organisation muss dokumentierte Information im notwendigen Umfang aufbewahren, so dass darauf vertraut werden kann, dass die Prozesse wie geplant umgesetzt wurden.

Die Organisation muss geplante Änderungen überwachen sowie die Folgen unbeabsichtigter Änderungen beurteilen und, falls notwendig, Maßnahmen ergreifen, um jegliche negativen Auswirkungen zu vermindern.

Die Organisation muss sicherstellen, dass ausgegliederte Prozesse bestimmt und gesteuert werden.

8.2 Informationssicherheitsrisikobeurteilung

Die Organisation muss in geplanten Abständen Informationssicherheitsrisikobeurteilungen vornehmen oder immer dann, wenn erhebliche Änderungen vorgeschlagen werden oder auftreten. Dabei sind die in 6.1.2 a) festgelegten Kriterien zu berücksichtigen.

Die Organisation muss dokumentierte Information über die Ergebnisse der Informationssicherheitsrisikobeurteilungen aufbewahren.

8.3 Informationssicherheitsrisikobehandlung

Die Organisation muss den Plan für die Informationssicherheitsrisikobehandlung umsetzen.

Die Organisation muss dokumentierte Information über die Ergebnisse der Informationssicherheitsrisikobehandlung aufbewahren.

9 Bewertung der Leistung

9.1 Überwachung, Messung, Analyse und Bewertung

Die Organisation muss die Informationssicherheitsleistung und die Wirksamkeit des Informationssicherheitsmanagementsystems bewerten.

Die Organisation muss bestimmen:

- a) was überwacht und gemessen werden muss, einschließlich der Informationssicherheitsprozesse und Maßnahmen;
- b) die Methoden zur Überwachung, Messung, Analyse und Bewertung, sofern zutreffend, um gültige Ergebnisse sicherzustellen;

ANMERKUNG Die ausgewählten Methoden sollten zu vergleichbaren und reproduzierbaren Ergebnissen führen, damit sie als gültig zu betrachten sind.

- c) wann die Überwachung und Messung durchzuführen ist;
- d) wer überwachen und messen muss;
- e) wann die Ergebnisse der Überwachung und Messung zu analysieren und zu bewerten sind; und
- f) wer diese Ergebnisse analysieren und bewerten muss.

Die Organisation muss geeignete dokumentierte Information als Nachweis der Ergebnisse aufbewahren.

9.2 Internes Audit

Die Organisation muss in geplanten Abständen interne Audits durchführen, um Informationen darüber zu erhalten, ob das Informationssicherheitsmanagementsystem:

- a) die Anforderungen
 - 1) der Organisation an ihr Informationssicherheitsmanagementsystem; und
 - 2) dieser Internationalen Normerfüllt;

- b) wirksam verwirklicht und aufrechterhalten wird.

Die Organisation muss:

- c) ein oder mehrere Auditprogramme planen, aufbauen, verwirklichen und aufrechterhalten einschließlich der Häufigkeit von Audits, Methoden, Verantwortlichkeiten, Anforderungen an die Planung sowie Berichterstattung. Die Auditprogramme müssen die Bedeutung der betroffenen Prozesse und die Ergebnisse vorheriger Audits berücksichtigen;
- d) für jedes Audit die Auditkriterien sowie den Umfang festlegen;
- e) Auditoren so auswählen und Audits so durchführen, dass die Objektivität und Unparteilichkeit des Auditprozesses sichergestellt ist;
- f) sicherstellen, dass die Ergebnisse der Audits gegenüber der zuständigen Leitung berichtet werden; und
- g) dokumentierte Information als Nachweis des/der Auditprogramms(e) und der Ergebnisse der Audits aufbewahren.

9.3 Managementbewertung

Die oberste Leitung muss das Informationssicherheitsmanagementsystem der Organisation in geplanten Abständen bewerten, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen.

Die Managementbewertung muss folgende Aspekte behandeln:

- a) den Status von Maßnahmen vorheriger Managementbewertungen;
- b) Veränderungen bei externen und internen Themen, die das Informationssicherheitsmanagementsystem betreffen;

- c) Rückmeldung über die Informationssicherheitsleistung, einschließlich Entwicklungen bei:
 - 1) Nichtkonformitäten und Korrekturmaßnahmen;
 - 2) Ergebnissen von Überwachungen und Messungen;
 - 3) Auditergebnissen; und
 - 4) Erreichung von Informationssicherheitszielen;
- d) Rückmeldung von interessierten Parteien;
- e) Ergebnisse der Risikobeurteilung und Status des Plans für die Risikobehandlung; und
- f) Möglichkeiten zur fortlaufenden Verbesserung.

Die Ergebnisse der Managementbewertung müssen Entscheidungen zu Möglichkeiten der fortlaufenden Verbesserung sowie zu jeglichem Änderungsbedarf am Informationssicherheitsmanagementsystem enthalten.

Die Organisation muss dokumentierte Information als Nachweis der Ergebnisse der Managementbewertung aufbewahren.

10 Verbesserung

10.1 Nichtkonformität und Korrekturmaßnahmen

Wenn eine Nichtkonformität auftritt, muss die Organisation:

- a) darauf reagieren und falls zutreffend:
 - 1) Maßnahmen zur Überwachung und zur Korrektur ergreifen; und
 - 2) mit den Folgen umgehen;
- b) die Notwendigkeit von Maßnahmen zur Beseitigung der Ursache von Nichtkonformitäten bewerten, damit diese nicht erneut oder an anderer Stelle auftreten, und zwar durch:
 - 1) Überprüfen der Nichtkonformität;
 - 2) Bestimmen der Ursachen der Nichtkonformität; und
 - 3) Bestimmen, ob vergleichbare Nichtkonformitäten bestehen, oder möglicherweise auftreten könnten;
- c) jegliche erforderliche Maßnahme einleiten;
- d) die Wirksamkeit jeglicher ergriffener Korrekturmaßnahme überprüfen; und
- e) sofern erforderlich, das Informationssicherheitsmanagementsystem ändern.

Korrekturmaßnahmen müssen den Auswirkungen der aufgetretenen Nichtkonformitäten angemessen sein.

Die Organisation muss dokumentierte Information aufbewahren, als Nachweis:

- f) der Art der Nichtkonformität sowie jeder daraufhin getroffenen Maßnahme; und
- g) der Ergebnisse jeder Korrekturmaßnahme.

10.2 Fortlaufende Verbesserung

Die Organisation muss die Eignung, Angemessenheit und Wirksamkeit ihres Informationssicherheitsmanagementsystems fortlaufend verbessern.

Anhang A (normativ)

Referenzmaßnahmenziele und -maßnahmen

Die in Tabelle A.1 aufgeführten Maßnahmenziele und Maßnahmen sind aus denjenigen, die in ISO/IEC 27002, Abschnitte 5 bis 18, genannt sind, direkt abgeleitet, daran ausgerichtet und müssen im Kontext mit Abschnitt 6.1.3 angewendet werden.

Tabelle A.1 – Maßnahmenziele und Maßnahmen

A.5 Informationssicherheitsrichtlinien		
A.5.1 Vorgaben der Leitung für Informationssicherheit Ziel: Vorgaben und Unterstützung für die Informationssicherheit sind seitens der Leitung in Übereinstimmung mit geschäftlichen Anforderungen und den relevanten Gesetzen und Vorschriften bereitgestellt.		
A.5.1.1	Informationssicherheitsrichtlinien	<i>Maßnahme</i> Ein Satz Informationssicherheitsrichtlinien ist festgelegt, von der Leitung genehmigt, herausgegeben und den Beschäftigten sowie relevanten externen Parteien bekanntgemacht.
A.5.1.2	Überprüfung der Informationssicherheitsrichtlinien	<i>Maßnahme</i> Die Informationssicherheitsrichtlinien werden in geplanten Abständen oder jeweils nach erheblichen Änderungen überprüft, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.
A.6 Organisation der Informationssicherheit		
A.6.1 Interne Organisation Ziel: Ein Rahmenwerk für die Leitung, mit dem die Umsetzung der Informationssicherheit in der Organisation eingeleitet und gesteuert werden kann, ist eingerichtet.		
A.6.1.1	Informationssicherheitsrollen und -verantwortlichkeiten	<i>Maßnahme</i> Alle Informationssicherheitsverantwortlichkeiten sind festgelegt und zugeordnet.
A.6.1.2	Aufgabentrennung	<i>Maßnahme</i> Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sind getrennt, um die Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der Werte der Organisation zu reduzieren.
A.6.1.3	Kontakt mit Behörden	<i>Maßnahme</i> Angemessene Kontakte mit relevanten Behörden werden gepflegt.
A.6.1.4	Kontakt mit speziellen Interessensgruppen	<i>Maßnahme</i> Angemessene Kontakte mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden werden gepflegt.

A.6.1.5	Informationssicherheit im Projektmanagement	<i>Maßnahme</i> Informationssicherheit wird im Projektmanagement berücksichtigt, ungeachtet der Art des Projekts.
A.6.2 Mobilgeräte^{N1)} und Telearbeit Ziel: Die Informationssicherheit bei Telearbeit und der Nutzung von Mobilgeräten ist sichergestellt.		
A.6.2.1	Richtlinie zu Mobilgeräten	<i>Maßnahme</i> Eine Richtlinie und unterstützende Sicherheitsmaßnahmen sind umgesetzt, um die Risiken, welche durch die Nutzung von Mobilgeräten bedingt sind, zu handhaben.
A.6.2.2	Telearbeit	<i>Maßnahme</i> Eine Richtlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Information, auf die von Telearbeitsplätzen aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden, sind umgesetzt.
A.7 Personalsicherheit		
A.7.1 Vor der Beschäftigung Ziel: Es ist sichergestellt, dass Beschäftigte und Auftragnehmer ihre Verantwortlichkeiten verstehen und für die für sie vorgesehenen Rollen geeignet sind.		
A.7.1.1	Sicherheitsüberprüfung	<i>Maßnahme</i> Alle Personen, die sich um eine Beschäftigung bewerben, werden einer Sicherheitsüberprüfung unterzogen, die im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen sowie in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken ist.
A.7.1.2	Beschäftigungs- und Vertragsbedingungen	<i>Maßnahme</i> In den vertraglichen Vereinbarungen mit Beschäftigten und Auftragnehmern sind deren Verantwortlichkeiten und diejenigen der Organisation festgelegt.
A.7.2 Während der Beschäftigung Ziel: Es ist sichergestellt, dass Beschäftigte und Auftragnehmer sich ihrer Verantwortlichkeiten bezüglich der Informationssicherheit bewusst sind und diesen nachkommen.		
A.7.2.1	Verantwortlichkeiten der Leitung	<i>Maßnahme</i> Die Leitung verlangt von allen Beschäftigten und Auftragnehmern, dass sie die Informationssicherheit im Einklang mit den eingeführten Richtlinien und Verfahren der Organisation umsetzen.
A.7.2.2	Informationssicherheitsbewusstsein, -ausbildung und -schulung	<i>Maßnahme</i> Alle Beschäftigten der Organisation und, wenn relevant, Auftragnehmer, bekommen ein angemessenes Bewusstsein durch Ausbildung und Schulung sowie regelmäßige Aktualisierungen zu den Richtlinien und Verfahren der Organisation, die für ihr berufliches Arbeitsgebiet relevant sind.

^{N1)} Mobilgeräte umfassen mobile Endgeräte jeder Art (Smartphones, Tablets, Laptops, Netbooks, etc.)

A.7.2.3	Maßregelungsprozess	Maßnahme Ein formal festgelegter und bekanntgegebener Maßregelungsprozess ist eingerichtet, um Maßnahmen gegen Beschäftigte zu ergreifen, die einen Informationssicherheitsverstoß begangen haben.
A.7.3 Beendigung und Änderung der Beschäftigung Ziel: Der Schutz der Interessen der Organisation ist Teil des Prozesses der Änderung oder Beendigung einer Beschäftigung.		
A.7.3.1	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	Maßnahme Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, sind festgelegt, dem Beschäftigten oder Auftragnehmer mitgeteilt und durchgesetzt.
A.8 Verwaltung der Werte		
A.8.1 Verantwortlichkeit für Werte Ziel: Die Werte der Organisation sind identifiziert und angemessene Verantwortlichkeiten zu ihrem Schutz sind festgelegt.		
A.8.1.1	Inventarisierung der Werte	Maßnahme ^{AC} Information und andere ^{AC} Werte, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sind erfasst und ein Inventar dieser Werte ist erstellt und wird gepflegt.
A.8.1.2	Zuständigkeit für Werte	Maßnahme Für alle Werte, die im Inventar geführt werden, gibt es Zuständige.
A.8.1.3	Zulässiger Gebrauch von Werten	Maßnahme Regeln für den zulässigen Gebrauch von Information und Werten, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sind aufgestellt, dokumentiert und werden angewendet.
A.8.1.4	Rückgabe von Werten	Alle Beschäftigten und sonstige Benutzer, die zu externen Parteien gehören, geben bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung sämtliche in ihrem Besitz befindlichen Werte, die der Organisation gehören, zurück.
A.8.2 Informationsklassifizierung Ziel: Es ist sichergestellt, dass Information ein angemessenes Schutzniveau entsprechend ihrer Bedeutung für die Organisation erhält.		
A.8.2.1	Klassifizierung von Information	Maßnahme Information ist anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert.

A.8.2.2	Kennzeichnung von Information	<i>Maßnahme</i> Ein angemessener Satz von Verfahren zur Kennzeichnung von Information ist entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt.
A.8.2.3	Handhabung von Werten	<i>Maßnahme</i> Verfahren für die Handhabung von Werten sind entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt.
A.8.3 Handhabung von Datenträgern Ziel: Die unerlaubte Offenlegung, Veränderung, Entfernung oder Zerstörung von Information, die auf Datenträgern gespeichert ist, wird unterbunden.		
A.8.3.1	Handhabung von Wechseldatenträgern	<i>Maßnahme</i> Verfahren für die Handhabung von Wechseldatenträgern sind entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema umgesetzt.
A.8.3.2	Entsorgung von Datenträgern	<i>Maßnahme</i> Nicht mehr benötigte Datenträger werden sicher und unter Anwendung formaler Verfahren entsorgt.
A.8.3.3	Transport von Datenträgern	<i>Maßnahme</i> Datenträger, die Information enthalten, sind während des Transports vor unbefugtem Zugriff, Missbrauch oder Verfälschung geschützt.
A.9 Zugangssteuerung^{N2)}		
A.9.1 Geschäftsanforderungen an die Zugangssteuerung Ziel: Der Zugang zu Information und informationsverarbeitenden Einrichtungen ist eingeschränkt.		
A.9.1.1	Zugangssteuerungsrichtlinie	<i>Maßnahme</i> Eine Zugangssteuerungsrichtlinie ist auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen erstellt, dokumentiert und überprüft.
A.9.1.2	Zugang zu Netzwerken und Netzwerkdiensten	<i>Maßnahme</i> Benutzer haben ausschließlich Zugang zu denjenigen Netzwerken und Netzwerkdiensten, zu deren Nutzung sie ausdrücklich befugt sind.
A.9.2 Benutzerzugangssverwaltung Ziel: Es ist sichergestellt, dass befugte Benutzer Zugang zu Systemen und Diensten haben und unbefugter Zugang unterbunden wird.		
A.9.2.1	Registrierung und Deregistrierung von Benutzern	<i>Maßnahme</i> Ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern ist umgesetzt, um die Zuordnung von Zugangsrechten zu ermöglichen.

N2) Der Zugang kann sowohl physisch als auch logisch erfolgen.

A.9.2.2	Zuteilung von Benutzerzugängen	<i>Maßnahme</i> Ein formaler Prozess zur Zuteilung von Benutzerzugängen ist umgesetzt, um die Zugangsrechte für alle Benutzerarten zu allen Systemen und Diensten zuzuweisen oder zu entziehen.
A.9.2.3	Verwaltung privilegierter Zugangsrechte	<i>Maßnahme</i> Zuteilung und Gebrauch von privilegierten Zugangsrechten ist eingeschränkt und wird gesteuert.
A.9.2.4	Verwaltung geheimer Authentisierungsinformation von Benutzern	<i>Maßnahme</i> Die Zuordnung von geheimer Authentisierungsinformation wird über einen formalen Verwaltungsprozess gesteuert.
A.9.2.5	Überprüfung von Benutzerzugangsrechten	<i>Maßnahme</i> Die für Werte Zuständigen überprüfen in regelmäßigen Abständen die Benutzerzugangsrechte.
A.9.2.6	Entzug oder Anpassung von Zugangsrechten	<i>Maßnahme</i> Die Zugangsrechte aller Beschäftigten und Benutzer, die zu externen Parteien gehören, auf Information und informationsverarbeitende Einrichtungen werden bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung entzogen oder bei einer Änderung angepasst.
A.9.3 Benutzerverantwortlichkeiten Ziel: Benutzer sind für den Schutz ihrer Authentisierungsinformation verantwortlich gemacht.		
A.9.3.1	Gebrauch geheimer Authentisierungsinformation	<i>Maßnahme</i> Benutzer sind verpflichtet, die Regeln der Organisation zur Verwendung geheimer Authentisierungsinformation zu befolgen.
A.9.4 Zugangssteuerung für Systeme und Anwendungen Ziel: Unbefugter Zugang zu Systemen und Anwendungen ist unterbunden.		
A.9.4.1	Informationszugangssbeschränkung	<i>Maßnahme</i> Zugang zu Information und Anwendungssystemfunktionen ist entsprechend der Zugangssteuerungsrichtlinie eingeschränkt.
A.9.4.2	Sichere Anmeldeverfahren	<i>Maßnahme</i> Soweit es die Zugangssteuerungsrichtlinie erfordert, wird der Zugang zu Systemen und Anwendungen durch ein sicheres Anmeldeverfahren gesteuert.
A.9.4.3	System zur Verwaltung von Kennwörtern	<i>Maßnahme</i> Systeme zur Verwaltung von Kennwörtern sind interaktiv und stellen starke Kennwörter sicher.
A.9.4.4	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	<i>Maßnahme</i> Der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, ist eingeschränkt und streng überwacht.
A.9.4.5	Zugangssteuerung für Quellcode von Programmen	<i>Maßnahme</i> Zugang zu Quellcode von Programmen ist eingeschränkt.

A.10 Kryptographie		
A.10.1 Kryptographische Maßnahmen		
Ziel: Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information ist sichergestellt.		
A.10.1.1	Richtlinie zum Gebrauch von kryptographischen Maßnahmen	<i>Maßnahme</i> Eine Richtlinie für den Gebrauch von kryptographischen Maßnahmen zum Schutz von Information ist entwickelt und umgesetzt.
A.10.1.2	Schlüsselverwaltung	<i>Maßnahme</i> Eine Richtlinie zum Gebrauch, zum Schutz und zur Lebensdauer von kryptographischen Schlüsseln ist entwickelt und wird über deren gesamten Lebenszyklus umgesetzt.
A.11 Physische und umgebungsbezogene Sicherheit		
A.11.1 Sicherheitsbereiche		
Ziel: Unbefugter Zutritt, die Beschädigung und die Beeinträchtigung von Information und informationsverarbeitenden Einrichtungen der Organisation sind verhindert.		
A.11.1.1	Physischer Sicherheitsperimeter	<i>Maßnahme</i> Zum Schutz von Bereichen, in denen sich entweder sensible oder kritische Information oder informationsverarbeitende Einrichtungen befinden, sind Sicherheitsperimeter festgelegt und werden verwendet.
A.11.1.2	Physische Zutrittssteuerung	<i>Maßnahme</i> Sicherheitsbereiche sind durch eine angemessene Zutrittssteuerung geschützt, um sicherzustellen, dass nur berechtigtes Personal Zugang hat.
A.11.1.3	Sichern von Büros, Räumen und Einrichtungen	<i>Maßnahme</i> Die physische Sicherheit für Büros, Räume und Einrichtungen ist konzipiert und wird angewendet.
A.11.1.4	Schutz vor externen und umweltbedingten Bedrohungen	<i>Maßnahme</i> Physischer Schutz vor Naturkatastrophen, bösartigen Angriffen oder Unfällen ist konzipiert und wird angewendet.
A.11.1.5	Arbeiten in Sicherheitsbereichen	<i>Maßnahme</i> Verfahren für das Arbeiten in Sicherheitsbereichen sind konzipiert und werden angewendet.
A.11.1.6	Anlieferungs- und Ladebereiche	<i>Maßnahme</i> Zutrittsstellen wie Anlieferungs- und Ladebereiche sowie andere Stellen, über die unbefugte Personen die Räumlichkeiten betreten könnten, werden überwacht und sind, falls möglich, von informationsverarbeitenden Einrichtungen getrennt, um unbefugten Zutritt zu verhindern.

A.11.2 Geräte und Betriebsmittel		
Ziel: Verlust, Beschädigung, Diebstahl oder Gefährdung von Werten und die Unterbrechung von Organisationstätigkeiten sind unterbunden.		
A.11.2.1	Platzierung und Schutz von Geräten und Betriebsmitteln	<i>Maßnahme</i> Geräte und Betriebsmittel sind so platziert und geschützt, dass Risiken durch umweltbedingte Bedrohungen und Gefahren sowie Möglichkeiten des unbefugten Zugangs verringert sind.
A.11.2.2	Versorgungseinrichtungen ^{N3)}	<i>Maßnahme</i> Geräte und Betriebsmittel sind vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden, geschützt.
A.11.2.3	Sicherheit der Verkabelung	<i>Maßnahme</i> Telekommunikationsverkabelung, welche Daten trägt oder Informationsdienste unterstützt, und die Stromverkabelung sind vor Unterbrechung, Störung oder Beschädigung geschützt.
A.11.2.4	Instandhalten von Geräten und Betriebsmitteln	<i>Maßnahme</i> Geräte und Betriebsmittel werden Instand gehalten, um ihre fortgesetzte Verfügbarkeit und Integrität sicherzustellen.
A.11.2.5	Entfernen von Werten	<i>Maßnahme</i> Geräte, Betriebsmittel, Information oder Software werden nicht ohne vorherige Genehmigung vom Betriebsgelände entfernt.
A.11.2.6	Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten	<i>Maßnahme</i> Werte außerhalb des Standorts werden gesichert, um die verschiedenen Risiken beim Betrieb außerhalb der Räumlichkeiten der Organisation zu berücksichtigen.
A.11.2.7	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	<i>Maßnahme</i> Alle Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, werden überprüft, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind.
A.11.2.8	Unbeaufsichtigte Benutzergeräte	<i>Maßnahme</i> Benutzer stellen sicher, dass unbeaufsichtigte Geräte und Betriebsmittel angemessen geschützt sind.
A.11.2.9	Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren	<i>Maßnahme</i> Richtlinien für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und für Bildschirmsperren für informationsverarbeitende Einrichtungen werden angewendet.

N3) Unter Versorgungseinrichtungen werden auch Entsorgungseinrichtungen verstanden.

A.12 Betriebssicherheit		
A.12.1 Betriebsabläufe und -verantwortlichkeiten		
Ziel: Der ordnungsgemäße und sichere Betrieb von informationsverarbeitenden Einrichtungen ist sichergestellt.		
A.12.1.1	Dokumentierte Bedienabläufe	<i>Maßnahme</i> Die Bedienabläufe sind dokumentiert und allen Benutzern, die sie benötigen, zugänglich.
A.12.1.2	Änderungssteuerung	<i>Maßnahme</i> Änderungen der Organisation, der Geschäftsprozesse, an den informationsverarbeitenden Einrichtungen und an den Systemen werden gesteuert.
A.12.1.3	Kapazitätssteuerung	<i>Maßnahme</i> Die Ressourcennutzung/Benutzung von Ressourcen wird überwacht und abgestimmt, und es werden Prognosen zu zukünftigen Kapazitätsanforderungen erstellt, um die erforderliche Systemleistung sicherzustellen.
A.12.1.4	Trennung von Entwicklungs-, Test- und Betriebsumgebungen	<i>Maßnahme</i> Entwicklungs-, Test- und Betriebsumgebungen sind voneinander getrennt, um das Risiko unbefugter Zugriffe auf oder Änderungen an der Betriebsumgebung zu verringern.
A.12.2 Schutz vor Schadsoftware		
Ziel: Information und informationsverarbeitende Einrichtungen sind vor Schadsoftware geschützt.		
A.12.2.1	Maßnahmen gegen Schadsoftware	<i>Maßnahme</i> Erkennungs-, Vorbeugungs- und Wiederherstellungsmaßnahmen zum Schutz vor Schadsoftware in Verbindung mit einer angemessenen Sensibilisierung der Benutzer sind umgesetzt.
A.12.3 Datensicherung		
Ziel: Daten sind vor Verlust geschützt.		
A.12.3.1	Sicherung von Information	<i>Maßnahme</i> Sicherheitskopien von Information, Software und Systemabbildern werden entsprechend einer vereinbarten Sicherungsrichtlinie angefertigt und regelmäßig getestet.
A.12.4 Protokollierung und Überwachung		
Ziel: Ereignisse sind aufgezeichnet und Nachweise sind erzeugt.		
A.12.4.1	Ereignisprotokollierung	<i>Maßnahme</i> Ereignisprotokolle, die Benutzertätigkeiten, Ausnahmen, Störungen und Informationssicherheitsvorfälle aufzeichnen, werden erzeugt, aufbewahrt und regelmäßig überprüft.
A.12.4.2	Schutz der Protokollinformation	<i>Maßnahme</i> Protokollierungseinrichtungen und Protokollinformation sind vor Manipulation und unbefugtem Zugriff geschützt.

A.12.4.3	Administratoren- und Bedienerprotokolle	<i>Maßnahme</i> Tätigkeiten von Systemadministratoren und Systembedienern werden aufgezeichnet und die Protokolle sind geschützt und werden regelmäßig überprüft.
A.12.4.4	Uhrensynchronisation	<i>Maßnahme</i> Die Uhren aller relevanten informationsverarbeitenden Systeme innerhalb einer Organisation oder einem Sicherheitsbereich werden mit einer einzigen Referenzzeitquelle synchronisiert.
A.12.5 Steuerung von Software im Betrieb Ziel: Die Integrität von Systemen im Betrieb ist sichergestellt.		
A.12.5.1	Installation von Software auf Systemen im Betrieb	<i>Maßnahme</i> Verfahren zur Steuerung der Installation von Software auf Systemen im Betrieb sind umgesetzt.
A.12.6 Handhabung technischer Schwachstellen Ziel: Die Ausnutzung technischer Schwachstellen ist verhindert.		
A.12.6.1	Handhabung von technischen Schwachstellen	<i>Maßnahme</i> Information über technische Schwachstellen verwendeter Informationssysteme wird rechtzeitig eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen wird bewertet und angemessene Maßnahmen werden ergriffen, um das dazugehörige Risiko zu behandeln.
A.12.6.2	Einschränkung von Softwareinstallation	<i>Maßnahme</i> Regeln für die Softwareinstallation durch Benutzer sind festgelegt und umgesetzt.
A.12.7 Audit von Informationssystemen Ziel: Die Auswirkung von Audittätigkeiten auf Systeme im Betrieb ist minimiert.		
A.12.7.1	Maßnahmen für Audits von Informationssystemen	<i>Maßnahme</i> Auditanforderungen und -tätigkeiten, welche eine Überprüfung betrieblicher Systeme beinhalten, werden sorgfältig geplant und vereinbart, um Störungen der Geschäftsprozesse zu minimieren.
A.13 Kommunikationssicherheit		
A.13.1 Netzwerksicherheitsmanagement Ziel: Der Schutz von Information in Netzwerken und den unterstützenden informationsverarbeitenden Einrichtungen ist sichergestellt.		
A.13.1.1	Netzwerksteuerungsmaßnahmen	<i>Maßnahme</i> Netzwerke werden verwaltet und gesteuert, um Information in Systemen und Anwendungen zu schützen.
A.13.1.2	Sicherheit von Netzwerkdiensten	<i>Maßnahme</i> Sicherheitsmechanismen, Dienstgüte und Anforderungen an die Verwaltung aller Netzwerkdienste sind bestimmt und werden sowohl für interne als auch für ausgegliederte Netzwerkdienste in Vereinbarungen aufgenommen.

A.13.1.3	Trennung in Netzwerken	<i>Maßnahme</i> Informationsdienste, Benutzer und Informationssysteme werden in Netzwerken gruppenweise voneinander getrennt gehalten.
A.13.2 Informationsübertragung Ziel: Die Sicherheit von übertragener Information, sowohl innerhalb einer Organisation als auch mit jeglicher externen Stelle, ist aufrechterhalten.		
A.13.2.1	Richtlinien und Verfahren zur Informationsübertragung	<i>Maßnahme</i> Formale Übertragungsrichtlinien, -verfahren und -maßnahmen sind vorhanden, um die Übertragung von Information für alle Arten von Kommunikationseinrichtungen zu schützen.
A.13.2.2	Vereinbarungen zur Informationsübertragung	<i>Maßnahme</i> Vereinbarungen behandeln die sichere Übertragung von Geschäftsinformation zwischen der Organisation und externen Parteien.
A.13.2.3	Elektronische Nachrichtenübermittlung	<i>Maßnahme</i> Information in der elektronischen Nachrichtenübermittlung ist angemessen geschützt.
A.13.2.4	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	<i>Maßnahme</i> Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, werden identifiziert, regelmäßig überprüft und sind dokumentiert.
A.14 Anschaffung, Entwicklung und Instandhalten von Systemen		
A.14.1 Sicherheitsanforderungen an Informationssysteme Ziel: Es ist sichergestellt, dass Informationssicherheit ein fester Bestandteil über den gesamten Lebenszyklus von Informationssystemen ist. Dies beinhaltet auch die Anforderungen an Informationssysteme, die Dienste über öffentliche Netze bereitstellen.		
A.14.1.1	Analyse und Spezifikation von Informationssicherheitsanforderungen	<i>Maßnahme</i> Die Anforderungen, die sich auf Informationssicherheit beziehen, sind in die Anforderungen an neue Informationssysteme oder die Verbesserungen bestehender Informationssysteme aufgenommen.
A.14.1.2	Sicherung von Anwendungsdiensten in öffentlichen Netzwerken	<i>Maßnahme</i> Information, die durch Anwendungsdiensten über öffentliche Netzwerke übertragen wird, ist vor betrügerischer Tätigkeit, Vertragsstreitigkeiten und unbefugter Offenlegung sowie Veränderung geschützt.
A.14.1.3	Schutz der Transaktionen bei Anwendungsdiensten	<i>Maßnahme</i> Information, die an Transaktionen bei Anwendungsdiensten beteiligt ist, ist so geschützt, dass unvollständige Übertragung, Fehlleitung, unbefugte Offenlegung, unbefugte Vervielfältigung oder unbefugte Wiederholung von Nachrichten verhindert ist.

A.14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen

Ziel: Es ist sichergestellt, dass Informationssicherheit im Entwicklungszyklus von Informationssystemen geplant und umgesetzt ist.

A.14.2.1	Richtlinie für sichere Entwicklung	<i>Maßnahme</i> Regeln für die Entwicklung von Software und Systemen sind festgelegt und werden bei Entwicklungen innerhalb der Organisation angewendet.
A.14.2.2	Verfahren zur Verwaltung von Systemänderungen	<i>Maßnahme</i> Änderungen an Systemen innerhalb des Entwicklungszyklus werden durch formale Verfahren zur Verwaltung von Änderungen gesteuert.
A.14.2.3	Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform	<i>Maßnahme</i> Bei Änderungen an Betriebsplattformen, werden geschäftskritische Anwendungen überprüft und getestet, um sicherzustellen, dass es keine negativen Auswirkungen auf die Organisationstätigkeiten oder Organisationssicherheit gibt.
A.14.2.4	Beschränkung von Änderungen an Softwarepaketen	<i>Maßnahme</i> Änderungen an Softwarepaketen werden nicht gefördert, sind auf das Erforderliche beschränkt und alle Änderungen unterliegen einer strikten Steuerung.
A.14.2.5	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme	<i>Maßnahme</i> Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme sind festgelegt, dokumentiert, werden aktuell gehalten und bei jedem Umsetzungsvorhaben eines Informationssystems angewendet.
A.14.2.6	Sichere Entwicklungsumgebung	<i>Maßnahme</i> Organisationen schaffen sichere Entwicklungsumgebungen für Systementwicklungs- und Systemintegrationsvorhaben über den gesamten Entwicklungszyklus und schützen diese angemessen.
A.14.2.7	Ausgegliederte Entwicklung	<i>Maßnahme</i> Die Organisation beaufsichtigt und überwacht die Tätigkeit ausgegliederter Systementwicklung.
A.14.2.8	Testen der Systemsicherheit	<i>Maßnahme</i> Die Sicherheitsfunktionalität wird während der Entwicklung getestet.
A.14.2.9	Systemabnahmetest	<i>Maßnahme</i> Für neue Informationssysteme, Aktualisierungen und neue Versionen sind Abnahmetestprogramme und dazugehörige Kriterien festgelegt.

A.14.3 Testdaten

Ziel: Der Schutz von Daten, die für das Testen verwendet werden, ist sichergestellt.

A.14.3.1	Schutz von Testdaten	<i>Maßnahme</i> Testdaten werden sorgfältig ausgewählt, geschützt und gesteuert.
----------	----------------------	---

A.15 Lieferantenbeziehungen^{N4)}		
A.15.1 Informationssicherheit in Lieferantenbeziehungen		
Ziel: Für Lieferanten zugängliche Werte des Unternehmens sind geschützt.		
A.15.1.1	Informationssicherheitsrichtlinie für Lieferantenbeziehungen	<i>Maßnahme</i> Die Informationssicherheitsanforderungen zur Verringerung von Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf Werte der Organisation werden mit dem Zulieferer vereinbart und sind dokumentiert.
A.15.1.2	Behandlung von Sicherheit in Lieferantenvereinbarungen	<i>Maßnahme</i> Alle relevanten Informationssicherheitsanforderungen werden mit jedem Lieferanten festgelegt, der Zugang zu Information der Organisation haben könnte, diese verarbeiten, speichern, weitergeben könnte oder IT-Infrastrukturkomponenten dafür bereitstellt und sind vereinbart.
A.15.1.3	Lieferkette für Informations- und Kommunikationstechnologie	<i>Maßnahme</i> Anforderungen für den Umgang mit Informationssicherheitsrisiken, die mit Informations- und Kommunikationsdienstleistungen und der Produktlieferkette verbunden sind, werden in Vereinbarungen mit Lieferanten aufgenommen.
A.15.2 Steuerung der Dienstleistungserbringung von Lieferanten		
Ziel: Ein vereinbartes Niveau der Informationssicherheit und der Dienstleistungserbringung ist im Einklang mit Lieferantenverträgen aufrechterhalten.		
A.15.2.1	Überwachung und Überprüfung von Lieferantendienstleistungen	<i>Maßnahme</i> Organisationen überwachen, überprüfen und auditieren die Dienstleistungserbringung durch Lieferanten regelmäßig.
A.15.2.2	Handhabung der Änderungen von Lieferantendienstleistungen	<i>Maßnahme</i> Änderungen bei der Bereitstellung von Dienstleistungen durch Lieferanten werden gesteuert. Solche Änderungen umfassen auch die Pflege und Verbesserung bestehender Informationssicherheitsrichtlinien, -verfahren und -maßnahmen. Dabei werden die Kritikalität der betroffenen Geschäftsinformation, -systeme und -prozesse und eine erneute Risikobeurteilung beachtet.
A.16 Handhabung von Informationssicherheitsvorfällen		
A.16.1 Handhabung von Informationssicherheitsvorfällen und Verbesserungen		
Ziel: Eine konsistente und wirksame Herangehensweise für die Handhabung von Informationssicherheitsvorfällen einschließlich der Benachrichtigung über Sicherheitsereignisse und Schwächen ist sichergestellt.		
A.16.1.1	Verantwortlichkeiten und Verfahren	<i>Maßnahme</i> Handhabungsverantwortlichkeiten und -verfahren sind festgelegt, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sicherzustellen.

N4) Dienstleister werden hier ebenfalls als Lieferanten betrachtet.

A.16.1.2	Meldung von Informationssicherheitsereignissen	<i>Maßnahme</i> Informationssicherheitsereignisse werden so schnell wie möglich über geeignete Kanäle zu deren Handhabung gemeldet.
A.16.1.3	Meldung von Schwächen in der Informationssicherheit	<i>Maßnahme</i> Beschäftigte und Auftragnehmer, welche die Informationssysteme und -dienste der Organisation nutzen, werden angehalten, jegliche beobachteten oder vermuteten Schwächen in der Informationssicherheit in Systemen oder Diensten festzuhalten und zu melden.
A.16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse	<i>Maßnahme</i> Informationssicherheitsereignisse werden beurteilt, und es wird darüber entschieden, ob sie als Informationssicherheitsvorfälle einzustufen sind.
A.16.1.5	Reaktion auf Informationssicherheitsvorfälle	<i>Maßnahme</i> Auf Informationssicherheitsvorfälle wird entsprechend den dokumentierten Verfahren reagiert.
A.16.1.6	Erkenntnisse aus Informationssicherheitsvorfällen	<i>Maßnahme</i> Aus der Analyse und Lösung von Informationssicherheitsvorfällen gewonnene Erkenntnisse werden dazu genutzt, die Eintrittswahrscheinlichkeit oder die Auswirkungen zukünftiger Vorfälle zu verringern.
A.16.1.7	Sammeln von Beweismaterial	<i>Maßnahme</i> Die Organisation legt Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Information, die als Beweismaterial dienen kann, fest und wendet diese an.
A.17 Informationssicherheitsaspekte beim Business Continuity Management		
A.17.1 Aufrechterhalten der Informationssicherheit		
Ziel: Die Aufrechterhaltung der Informationssicherheit ist in das Business Continuity Managementsystem der Organisation eingebettet.		
A.17.1.1	Planung zur Aufrechterhaltung der Informationssicherheit	<i>Maßnahme</i> Die Organisation bestimmt ihre Anforderungen an die Informationssicherheit und zur Aufrechterhaltung des Informationssicherheitsmanagements bei widrigen Situationen, z. B. Krise oder Katastrophe.
A.17.1.2	Umsetzen der Aufrechterhaltung der Informationssicherheit	<i>Maßnahme</i> Die Organisation legt Prozesse, Verfahren und Maßnahmen fest, dokumentiert, setzt sie um und erhält diese aufrecht, um das erforderliche Niveau an Informationssicherheit in einer widrigen Situation aufrechterhalten zu können.
A.17.1.3	Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit	<i>Maßnahme</i> Die Organisation überprüft in regelmäßigen Abständen die festgelegten und umgesetzten Maßnahmen zur Aufrechterhaltung der Informationssicherheit, um sicherzustellen dass diese gültig und in widrigen Situationen wirksam sind.

A.17.2 Redundanzen

Ziel: Die Verfügbarkeit von informationsverarbeitenden Einrichtungen ist sichergestellt.

A.17.2.1	Verfügbarkeit von informationsverarbeitenden Einrichtungen	<i>Maßnahme</i> Informationsverarbeitende Einrichtungen werden mit ausreichender Redundanz zur Einhaltung der Verfügbarkeitsanforderungen realisiert.
----------	--	--

A.18 Compliance**A.18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen**

Ziel: Verstöße gegen gesetzliche, regulatorische, selbstaufgelegte oder vertragliche Verpflichtungen mit Bezug auf Informationssicherheit und gegen jegliche Sicherheitsanforderungen sind vermieden.

A.18.1.1	Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen	<i>Maßnahme</i> Alle relevanten gesetzlichen, regulatorischen, selbstaufgelegten oder vertraglichen Anforderungen sowie das Vorgehen der Organisation zur Einhaltung dieser Anforderungen sind für jedes Informationssystem und die Organisation ausdrücklich bestimmt und dokumentiert und werden auf dem neuesten Stand gehalten.
A.18.1.2	Geistige Eigentumsrechte	<i>Maßnahme</i> Es sind angemessene Verfahren umgesetzt, mit denen die Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen mit Bezug auf geistige Eigentumsrechte und der Verwendung von urheberrechtlich geschützten Softwareprodukten sichergestellt ist.
A.18.1.3	Schutz von Aufzeichnungen	<i>Maßnahme</i> Aufzeichnungen sind gemäß gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt.
A.18.1.4	Privatsphäre und Schutz von personenbezogener Information	<i>Maßnahme</i> Die Privatsphäre und der Schutz von personenbezogener Information sind, soweit anwendbar, entsprechend den Anforderungen der relevanten Gesetze und Vorschriften sichergestellt.
A.18.1.5	Regelungen bezüglich kryptographischer Maßnahmen	<i>Maßnahme</i> Kryptographische Maßnahmen werden unter Einhaltung aller relevanten Vereinbarungen, Gesetze und Vorschriften angewandt.

A.18.2 Überprüfungen der Informationssicherheit

Ziel: Informationssicherheit ist in Übereinstimmung mit den Richtlinien und Verfahren der Organisation umgesetzt und wird entsprechend angewendet.

A.18.2.1	Unabhängige Überprüfung der Informationssicherheit	<i>Maßnahme</i> Die Vorgehensweise der Organisation für die Handhabung der Informationssicherheit und deren Umsetzung (d. h. Maßnahmenziele, Maßnahmen, Richtlinien, Prozesse und Verfahren zur Informationssicherheit) werden auf unabhängige Weise in planmäßigen Abständen oder jeweils bei erheblichen Änderungen überprüft.
----------	--	---

A.18.2.2	Einhaltung von Sicherheitsrichtlinien -standards und	<i>Maßnahme</i> Leitende Angestellte überprüfen regelmäßig die Einhaltung der jeweils anzuwendenden Sicherheitsrichtlinien, Standards und jeglicher sonstiger Sicherheitsanforderungen bei der Informationsverarbeitung und den Verfahren in ihrem Verantwortungsbereich.
A.18.2.3	Überprüfung der Einhaltung von technischen Vorgaben	<i>Maßnahme</i> Informationssysteme werden regelmäßig auf Einhaltung der Informationssicherheitsrichtlinien und -standards der Organisation überprüft.

Literaturhinweise

- [1] ISO/IEC 27002:2013, *Information technology — Security Techniques — Code of practice for information security management*
- [2] ISO/IEC 27003, *Information technology — Security Techniques — Information security management system implementation guidance*
- [3] ISO/IEC 27004, *Information technology — Security Techniques — Information security management — Measurement*
- [4] ISO/IEC 27005, *Information technology — Security Techniques — Information security risk management*
- [5] ISO 31000:2009, *Risk Management — Principles and guidelines*
- [6] ISO/IEC Directives, *Part 1 Consolidated ISO Supplement — Procedures specific to ISO:2012*