

DIN EN ISO/IEC 27001



ICS 03.100.70; 35.030

Entwurf

Einsprüche bis 2023-05-17
Vorgesehen als Ersatz für
DIN EN ISO/IEC 27001:2017-06

**Informationssicherheit, Cybersicherheit und Datenschutz –
Informationssicherheitsmanagementsysteme –
Anforderungen (ISO/IEC 27001:2022);
Deutsche und Englische Fassung prEN ISO/IEC 27001:2023**

Information security, cybersecurity and privacy protection –
Information security management systems –
Requirements (ISO/IEC 27001:2022);
German and English version prEN ISO/IEC 27001:2023

Sécurité de l'information, cybersécurité et protection de la vie privée –
Systèmes de management de la sécurité de l'information –
Exigences (ISO/IEC 27001:2022);
Version allemande et anglaise prEN ISO/IEC 27001:2023

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2023-03-17 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe 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/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, 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 53 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 27001:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 27001:2023 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 27000	siehe	DIN EN ISO/IEC 27000
ISO/IEC 27002:2022	siehe	DIN EN ISO/IEC 27002:2023-XX (Veröffentlichung in Vorbereitung)
ISO 31000:2018	siehe	DIN ISO 31000:2018-10

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Änderungen

Gegenüber DIN EN ISO/IEC 27001:2017-06 wurden folgende Änderungen vorgenommen:

- a) der Text wurde an die harmonisierte Struktur für Managementsystemnormen und ISO/IEC 27002:2022 angepasst.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 27000, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Überblick und Terminologie*

DIN EN ISO/IEC 27002:2023-XX, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022); Deutsche Fassung EN ISO/IEC 27002:2022*

DIN ISO 31000:2018-10, *Risikomanagement — Leitlinien (ISO 31000:2018)*

– *Entwurf* –

E DIN EN ISO/IEC 27001:2023-04

– Leerseite –

**Informationssicherheit, Cybersicherheit und Datenschutz –
Informationssicherheitsmanagementsysteme – Anforderungen
(ISO/IEC 27001:2022)**

Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée – Systèmes de management de la sécurité de l'information – Exigences (ISO/IEC 27001:2022)

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Kontext der Organisation	7
4.1 Verstehen der Organisation und ihres Kontextes	7
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien	7
4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems	8
4.4 Informationssicherheitsmanagementsystem	8
5 Führung	8
5.1 Führung und Verpflichtung	8
5.2 Politik	9
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	9
6 Planung	9
6.1 Maßnahmen zum Umgang mit Risiken und Chancen	9
6.1.1 Allgemeines	9
6.1.2 Informationssicherheitsrisikobeurteilung	10
6.1.3 Informationssicherheitsrisikobehandlung	10
6.2 Informationssicherheitsziele und Planung zu deren Erreichung	11
6.3 Planung von Änderungen	12
7 Unterstützung	12
7.1 Ressourcen	12
7.2 Kompetenz	12
7.3 Bewusstsein	12
7.4 Kommunikation	13
7.5 Dokumentierte Information	13
7.5.1 Allgemeines	13
7.5.2 Erstellen und Aktualisieren	13
7.5.3 Lenkung dokumentierter Information	13
8 Betrieb	14
8.1 Betriebliche Planung und Steuerung	14
8.2 Informationssicherheitsrisikobeurteilung	14
8.3 Informationssicherheitsrisikobehandlung	14
9 Bewertung der Leistung	14
9.1 Überwachung, Messung, Analyse und Bewertung	14
9.2 Internes Audit	15
9.2.1 Allgemeines	15
9.2.2 Internes Auditprogramm	15
9.3 Managementbewertung	16
9.3.1 Allgemeines	16
9.3.2 Eingaben für die Managementbewertung	16
9.3.3 Ergebnisse der Managementbewertung	16
10 Verbesserung	16
10.1 Fortlaufende Verbesserung	16
10.2 Nichtkonformität und Korrekturmaßnahmen	16
Anhang A (normativ) Verweisung auf Informationssicherheitsmaßnahmen	18
Literaturhinweise	26

Tabellen

Tabelle A.1 — Informationssicherheitsmaßnahmen	18
---	-----------

Europäisches Vorwort

Der Text von ISO/IEC 27001:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 27001:2023 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wird EN ISO/IEC 27001:2017 ersetzen.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Anerkennungsnotiz

Der Text von ISO/IEC 27001:2022 wurde von CEN als prEN ISO/IEC 27001:2023 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Directives, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Directives, Teil 2 erarbeitet (siehe www.iso.org/directives oder www.iec.ch/members_experts/refdocs).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents) oder in der IEC-Liste der erhaltenen Patenterklärungen (siehe <https://patents.iec.ch>).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html. Diesbezügliche Informationen der IEC sind unter www.iec.ch/understanding-standards verfügbar.

Dieses Dokument wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection*, erarbeitet.

Diese dritte Ausgabe ersetzt die zweite Ausgabe (ISO/IEC 27001:2013), die technisch überarbeitet wurde. Sie enthält auch die Technischen Berichtigungen ISO/IEC 27001:2013/Cor 1:2014 und ISO/IEC 27001:2013/Cor 2:2015.

Die wesentlichen Änderungen sind folgende:

- der Text wurde an den harmonisierten Aufbau für Managementsystemnormen und ISO/IEC 27002:2022 angepasst.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html und www.iec.ch/national-committees zu finden.

Einleitung

0.1 Allgemeines

Dieses Dokument 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.

Dieses Dokument 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 diesem Dokument 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

Dieses Dokument 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

Dieses Dokument legt die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems im Kontext der Organisation fest. Darüber hinaus beinhaltet dieses Dokument Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen der Organisation. Die in diesem Dokument festgelegten Anforderungen sind allgemein gehalten und sollen auf alle Organisationen, ungeachtet ihrer Art und Größe, anwendbar sein. Wenn eine Organisation Konformität mit diesem Dokument für sich beansprucht, darf sie keine der Anforderungen in Abschnitt 4 bis Abschnitt 10 ausschließen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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 Begriffe nach ISO/IEC 27000.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <https://www.electropedia.org/>

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 31000:2018 [5], 5.4.1, beschrieben.

4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien

Die Organisation muss Folgendes bestimmen:

- a) die interessierten Parteien, die für ihr Informationssicherheitsmanagementsystem relevant sind;
- b) die relevanten Anforderungen dieser interessierten Parteien;
- c) welche dieser Anforderungen durch das Informationssicherheitsmanagementsystem erfüllt werden.

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 Folgendes berücksichtigen:

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

Der Anwendungsbereich muss als dokumentierte Information verfügbar sein.

4.4 Informationssicherheitsmanagementsystem

Die Organisation muss entsprechend den Anforderungen dieses Dokuments ein Informationssicherheitsmanagementsystem aufbauen, verwirklichen, aufrechterhalten und fortlaufend verbessern, einschließlich der benötigten Prozesse und ihren Wechselwirkungen.

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.

ANMERKUNG Wenn in diesem Dokument das Wort „Geschäft“ (en: business) verwendet wird, kann dieses im weiteren Sinne verstanden werden und bezieht sich auf Tätigkeiten, die für den Zweck der Organisation bzw. deren Existenz entscheidend sind.

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,
- d) eine Verpflichtung zur fortlaufenden Verbesserung des Informationssicherheitsmanagementsystems enthält.

Die Informationssicherheitspolitik muss

- e) als dokumentierte Information verfügbar sein,
- f) innerhalb der Organisation bekannt gemacht werden,
- 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 innerhalb der Organisation bekannt gemacht werden.

Die oberste Leitung muss die Verantwortlichkeit und Befugnis zuweisen für:

- a) das Sicherstellen, dass das Informationssicherheitsmanagementsystem die Anforderungen dieses Dokuments erfüllt;
- b) das Berichten an die oberste Leitung über die Leistung des Informationssicherheitsmanagementsystems.

ANMERKUNG Die oberste Leitung kann 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 Planungen 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 behandelt werden müssen, um

- a) sicherzustellen, dass das Informationssicherheitsmanagementsystem seine beabsichtigten Ergebnisse erzielen kann,
- b) unerwünschte Auswirkungen zu verhindern oder zu verringern,
- 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, die Folgendes beinhalten:
 - 1) die Kriterien zur Risikoakzeptanz; und
 - 2) Kriterien für die Durchführung von Informationssicherheitsrisikobeurteilungen;
- b) sicherstellt, dass wiederholte Informationssicherheitsrisikobeurteilungen zu konsistenten, gültigen und vergleichbaren Ergebnissen führen;
- c) die Informationssicherheitsrisiken identifiziert:
 - 1) Anwendung des Prozesses zur Informationssicherheitsrisikobeurteilung, um Risiken im Zusammenhang mit dem Verlust der Vertraulichkeit, Integrität und Verfügbarkeit von Information innerhalb des Anwendungsbereichs des ISMS zu ermitteln; und
 - 2) Identifizierung der Risikoeigentümer;
- d) die Informationssicherheitsrisiken analysiert:
 - 1) Abschätzung der möglichen Folgen bei Eintritt der nach 6.1.2 c) 1) identifizierten Risiken;
 - 2) Abschätzung der realistischen Eintrittswahrscheinlichkeiten der nach 6.1.2 c) 1) identifizierten Risiken; und
 - 3) Bestimmung der Risikoniveaus;
- e) die Informationssicherheitsrisiken bewertet:
 - 1) Vergleich der Ergebnisse der Risikoanalyse mit den nach 6.1.2 a) festgelegten Risikokriterien; und
 - 2) Priorisierung der analysierten Risiken für die Risikobehandlung.

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 1 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 2 Anhang A enthält eine Liste von möglichen Informationssicherheitsmaßnahmen. Anwender dieses Dokuments werden auf Anhang A verwiesen, um sicherzustellen, dass keine wichtigen Informationssicherheitsmaßnahmen übersehen wurden.

ANMERKUNG 3 Die in Anhang A aufgeführten Informationssicherheitsmaßnahmen sind nicht erschöpfend und können bei Bedarf durch zusätzliche Informationssicherheitsmaßnahmen ergänzt werden.

- d) eine Erklärung zur Anwendbarkeit zu erstellen, die Folgendes enthält:

- die erforderlichen Maßnahmen [siehe 6.1.3 b) und c)];
- Gründe für deren Einbeziehung;
- ob sie umgesetzt sind oder nicht; sowie
- Gründe für die Nichteinbeziehung von Maßnahmen aus Anhang A.

- 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 4 Der in diesem Dokument 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) überwacht werden;
- e) vermittelt werden;
- f) soweit erforderlich, aktualisiert werden;
- g) als dokumentierte Information verfügbar sein.

Die Organisation muss dokumentierte Information zu den Informationssicherheitszielen aufbewahren.

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

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

6.3 Planung von Änderungen

Wenn die Organisation feststellt, dass Änderungen am Informationssicherheitsmanagementsystem erforderlich sind, müssen diese Änderungen geplant durchgeführt 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 Folgendem bewusst sein:

- 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.