DEUTSCHE NORM *Entwurf* **April 2023**

DIN EN ISO/IEC 27001

DIN

ICS 03.100.70; 35.030

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

Entwurf

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)

www.din.de
www.beuth.de

3420990

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 beigefügt. 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)*

– Leerseite –

– Entwurf –

März 2023

prEN ISO/IEC 27001

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.

7.4 Kommunikation

Die Organisation muss die Erfordernis einer internen und externen Kommunikation in Bezug auf das Informationssicherheitsmanagementsystem bestimmen, einschließlich:

a) worüber kommuniziert wird;

b) wann kommuniziert wird;

c) mit wem kommuniziert wird;

d) wie kommuniziert wird.

7.5 Dokumentierte Information

7.5.1 Allgemeines

Das Informationssicherheitsmanagementsystem der Organisation muss beinhalten:

a) die von diesem Dokument 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 Folgendes sicherstellen:

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.

7.5.3 Lenkung dokumentierter Information

Die für das Informationssicherheitsmanagementsystem erforderliche und von diesem Dokument 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 Anforderungen und zur Durchführung der in Abschnitt 6 bestimmten Maßnahmen planen, verwirklichen und steuern, indem sie

— Kriterien für die Prozesse festlegt,

— die Steuerung der Prozesse in Übereinstimmung mit den Kriterien durchführt.

Dokumentierte Information muss im notwendigen Umfang verfügbar sein, sodass darauf vertraut werden kann, dass die Prozesse wie geplant durchgeführt 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 extern bereitgestellte Prozesse, Produkte oder Dienstleistungen, die für das Informationssicherheitsmanagementsystem relevant sind, kontrolliert 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 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. 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;

f) wer diese Ergebnisse analysieren und bewerten muss.

Es müssen dokumentierte Informationen als Nachweis der Ergebnisse verfügbar sein.

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

9.2 Internes Audit

9.2.1 Allgemeines

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

a) folgende Anforderungen erfüllt:

   1) die Anforderungen der Organisation an ihr Informationssicherheitsmanagementsystem;

   2) die Anforderungen dieses Dokuments;

b) wirksam verwirklicht und aufrechterhalten wird.

9.2.2 Internes Auditprogramm

Die Organisation muss ein oder mehrere Auditprogramme planen, aufbauen, verwirklichen und aufrechterhalten, einschließlich der Häufigkeit von Audits, Methoden, Verantwortlichkeiten, Anforderungen an die Planung sowie Berichterstattung.

Beim Aufbauen der internen Auditprogramme muss die Organisation die Bedeutung der betroffenen Prozesse und die Ergebnisse vorheriger Audits berücksichtigen.

Die Organisation muss:

a) für jedes Audit die Auditkriterien sowie den Umfang festlegen;

b) Auditoren so auswählen und Audits so durchführen, dass die Objektivität und Unparteilichkeit des Auditprozesses sichergestellt sind;

c) sicherstellen, dass die Ergebnisse der Audits gegenüber der zuständigen Leitung berichtet werden.

Es müssen dokumentierte Informationen als Nachweis der Umsetzung der Auditprogramme und der Auditergebnisse verfügbar sein.

9.3 Managementbewertung

9.3.1 Allgemeines

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

9.3.2 Eingaben für die Managementbewertung

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) Veränderungen bei den Erfordernissen und Erwartungen von interessierten Parteien, die relevant für das Informationssicherheitsmanagementsystem sind;

d) Rückmeldung über die Informationssicherheitsleistung, einschließlich Entwicklungen bei:

   1) Nichtkonformitäten und Korrekturmaßnahmen;

   2) Ergebnissen von Überwachungen und Messungen;

   3) Auditergebnissen;

   4) Erreichung von Informationssicherheitszielen;

e) Rückmeldung von interessierten Parteien;

f) Ergebnissen der Risikobeurteilung und Status des Risikobehandlungsplans;

g) Möglichkeiten zur fortlaufenden Verbesserung.

9.3.3 Ergebnisse der Managementbewertung

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

Es müssen dokumentierte Informationen als Nachweis der Ergebnisse von Managementbewertungen verfügbar sein.

10 Verbesserung

10.1 Fortlaufende Verbesserung

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

10.2 Nichtkonformität und Korrekturmaßnahmen

Wenn eine Nichtkonformität auftritt, muss die Organisation:

a) darauf reagieren und falls zutreffend:

   1) Maßnahmen zur Überwachung und zur Korrektur ergreifen;

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.

Es müssen dokumentierte Informationen als Nachweis von Folgendem verfügbar sein:

f) der Art der Nichtkonformität sowie jeder daraufhin getroffenen Maßnahme;

g) der Ergebnisse jeder Korrekturmaßnahme.

Anhang A
(normativ)

Verweisung auf Informationssicherheitsmaßnahmen

Die in Tabelle A.1 aufgeführten Informationssicherheitsmaßnahmen sind aus denjenigen, die in ISO/IEC 27002:2022 [1], Abschnitt 5 bis Abschnitt 8, genannt sind, direkt abgeleitet, daran ausgerichtet und müssen im Kontext mit 6.1.3 angewendet werden.

Tabelle A.1 — Informationssicherheitsmaßnahmen

5	**Organisatorische Maßnahmen**	
5.1	Informationssicherheits-richtlinien	**Maßnahme** Informationssicherheitspolitik und themenspezifische Richtlinien müssen definiert, von der Geschäftsleitung genehmigt, veröffentlicht, dem zuständigen Personal und den interessierten Parteien mitgeteilt und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.
5.2	Informationssicherheitsrollen und -verantwortlichkeiten	**Maßnahme** Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen des Unternehmens definiert und zugewiesen werden.
5.3	Aufgabentrennung	**Maßnahme** Sich widersprechende Aufgaben und Verantwortungsbereiche müssen voneinander getrennt werden.
5.4	Verantwortlichkeiten der Leitung	**Maßnahme** Die Leitung muss von dem gesamten Personal verlangen, dass es die Informationssicherheit im Einklang mit der eingeführten Informationssicherheitspolitik und den themenspezifischen Richtlinien und Verfahren der Organisation umsetzt.
5.5	Kontakt mit Behörden	**Maßnahme** Die Organisation muss mit den zuständigen Behörden Kontakt aufnehmen und halten.
5.6	Kontakt mit speziellen Interessensgruppen	**Maßnahme** Die Organisation muss mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden Kontakt aufnehmen und halten.
5.7	Erkenntnisse über Bedrohungen	**Maßnahme** Informationen über Bedrohungen der Informationssicherheit müssen erhoben und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.
5.8	Informationssicherheit im Projektmanagement	**Maßnahme** Die Informationssicherheit muss in das Projektmanagement integriert werden.
5.9	Inventar der Informationen und anderen damit verbundenen Werten	**Maßnahme** Ein Inventar der Informationen und anderen damit verbundenen Werten, einschließlich der Eigentümer, muss erstellt und gepflegt werden.
5.10	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	**Maßnahme** Regeln für den zulässigen Gebrauch und Verfahren für den Umgang mit Informationen und anderen zugehörigen Vermögenswerten müssen aufgestellt, dokumentiert und angewendet werden.

Tabelle A.1 (*fortgesetzt*)

5.11	Rückgabe von Werten	**Maßnahme** Das Personal und gegebenenfalls andere interessierte Parteien müssen alle Werte der Organisation, die sich in ihrem Besitz befinden, bei Änderung oder Beendigung ihres Beschäftigungsverhältnisses, Vertrags oder ihrer Vereinbarung zurückgeben.
5.12	Klassifizierung von Information	**Maßnahme** Informationen müssen entsprechend den Informationssicherheitsanforderungen der Organisation auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen der interessierten Parteien klassifiziert werden.
5.13	Kennzeichnung von Information	**Maßnahme** Ein angemessener Satz von Verfahren zur Kennzeichnung von Information muss entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt werden.
5.14	Informationsübertragung	**Maßnahme** Für alle Arten von Übertragungseinrichtungen innerhalb der Organisation und zwischen der Organisation und anderen Parteien müssen Regeln, Verfahren oder Vereinbarungen zur Informationsübermittlung vorhanden sein.
5.15	Zugangssteuerung	**Maßnahme** Regeln zur Kontrolle des physischen und logischen Zugriffs auf Informationen und andere zugehörige Werte müssen auf der Grundlage von Geschäfts- und Informationssicherheitsanforderungen aufgestellt und umgesetzt werden.
5.16	Identitätsmanagement	**Maßnahme** Der gesamte Lebenszyklus von Identitäten muss verwaltet werden.
5.17	Informationen zur Authentifizierung	**Maßnahme** Die Zuweisung und Verwaltung von Authentifizierungsinformationen muss durch einen Managementprozess gesteuert werden, der auch die Beratung des Personals über den angemessenen Umgang mit Authentifizierungsinformationen umfasst.
5.18	Zugangsrechte	**Maßnahme** Zugangsrechte zu Informationen und anderen zugehörigen Werten müssen in Übereinstimmung mit den themenspezifischen Richtlinien und Regeln der Organisation für die Zugangssteuerung bereitgestellt, überprüft, geändert und entfernt werden.
5.19	Informationssicherheit in Lieferantenbeziehungen	**Maßnahme** Es müssen Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der Nutzung der Produkte oder Dienstleistungen des Lieferanten verbundenen Informationssicherheitsrisiken zu beherrschen.
5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen	**Maßnahme** Je nach Art der Lieferantenbeziehung müssen die entsprechenden Anforderungen an die Informationssicherheit festgelegt und mit jedem Lieferanten vereinbart werden.
5.21	Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)	**Maßnahme** Es müssen Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der IKT-Produkt- und Dienstleistungslieferkette verbundenen Informationssicherheitsrisiken zu beherrschen.
5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	**Maßnahme** Die Organisation muss regelmäßig die Informationssicherheitspraktiken der Lieferanten und die Erbringung von Dienstleistungen überwachen, überprüfen, bewerten und Änderungen steuern.

Tabelle A.1 (*fortgesetzt*)

5.23	Informationssicherheit für die Nutzung von Cloud-Diensten	**Maßnahme** Die Verfahren für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten müssen in Übereinstimmung mit den Informationssicherheitsanforderungen der Organisation festgelegt werden.
5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	**Maßnahme** Die Organisation muss die Handhabung von Informationssicherheitsvorfällen planen und vorbereiten, indem sie Prozesse, Rollen und Verantwortlichkeiten für die Handhabung von Informationssicherheitsvorfällen definiert, einführt und kommuniziert.
5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse	**Maßnahme** Die Organisation muss Ereignisse im Bereich der Informationssicherheit beurteilen und entscheiden, ob sie als Vorfälle im Bereich der Informationssicherheit eingestuft werden müssen.
5.26	Reaktion auf Informationssicherheitsvorfälle	**Maßnahme** Auf Informationssicherheitsvorfälle muss entsprechend den dokumentierten Verfahren reagiert werden.
5.27	Erkenntnisse aus Informationssicherheitsvorfällen	**Maßnahme** Aus Informationssicherheitsvorfällen gewonnene Erkenntnisse müssen zur Verstärkung und Verbesserung der Informationssicherheitsmaßnahmen genutzt werden.
5.28	Sammeln von Beweismaterial	**Maßnahme** Die Organisation muss Verfahren für die Identifizierung, Sammlung, Beschaffung und Aufbewahrung von Beweismaterial im Zusammenhang mit Informationssicherheitsvorfällen einführen und umsetzen.
5.29	Informationssicherheit bei Störungen	**Maßnahme** Die Organisation muss planen, wie die Informationssicherheit während einer Störung auf einem angemessenen Niveau gehalten werden kann.
5.30	IKT-Bereitschaft für Business Continuity	**Maßnahme** Die IKT-Bereitschaft muss auf der Grundlage von Business-Continuity-Zielen und IKT-Kontinuitätsanforderungen geplant, umgesetzt, aufrechterhalten und geprüft werden.
5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	**Maßnahme** Rechtliche, gesetzliche, behördliche und vertragliche Anforderungen, die für die Informationssicherheit relevant sind, und die Vorgehensweise der Organisation zur Erfüllung dieser Anforderungen müssen ermittelt, dokumentiert und auf dem neuesten Stand gehalten werden.
5.32	Geistige Eigentumsrechte	**Maßnahme** Die Organisation muss geeignete Verfahren zum Schutz der Rechte an geistigem Eigentum einführen.
5.33	Schutz von Aufzeichnungen	**Maßnahme** Aufzeichnungen müssen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt sein.
5.34	Privatsphäre und Schutz von personenbezogenen Daten (PbD)	**Maßnahme** Die Organisation muss die Anforderungen an die Wahrung der Privatsphäre und den Schutz personenbezogener Daten nach den geltenden Gesetzen und Vorschriften sowie den vertraglichen Anforderungen ermitteln und erfüllen.

Tabelle A.1 (*fortgesetzt*)

5.35	Unabhängige Überprüfung der Informationssicherheit	**Maßnahme** Die Vorgehensweise der Organisation für die Handhabung der Informationssicherheit und deren Umsetzung einschließlich der Mitarbeiter, Prozesse und Technologien, müssen auf unabhängige Weise in planmäßigen Abständen oder jeweils bei erheblichen Änderungen überprüft werden.
5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	**Maßnahme** Die Einhaltung der Informationssicherheitspolitik der Organisation, der themenspezifischen Richtlinien, Regeln und Normen muss regelmäßig überprüft werden.
5.37	Dokumentierte Bedienabläufe	**Maßnahme** Die Betriebsverfahren für Informationsverarbeitungsanlagen müssen dokumentiert und dem Personal, das sie benötigt, zur Verfügung gestellt werden.
6	**Personenbezogene Maßnahmen**	
6.1	Sicherheitsüberprüfung	**Maßnahme** Alle Personen, die in die Belegschaft aufgenommen werden, müssen vor dem Eintritt in die Organisation und fortlaufend unter Berücksichtigung geltender Gesetze, Vorschriften und ethischer Grundsätze einer Sicherheitsüberprüfung unterzogen werden und diese Überprüfung muss in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken stehen.
6.2	Beschäftigungs- und Vertragsbedingungen	**Maßnahme** In den arbeitsvertraglichen Vereinbarungen müssen die Verantwortlichkeiten des Personals und der Organisation für die Informationssicherheit festgelegt werden.
6.3	Informationssicherheits-bewusstsein, -ausbildung und -schulung	**Maßnahme** Das Personal der Organisation und relevante interessierte Parteien müssen ein angemessenes Bewusstsein für die Informationssicherheit, eine entsprechende Ausbildung und Schulung sowie regelmäßige Aktualisierungen der Informationssicherheitspolitik der Organisation, themenspezifischer Richtlinien und Verfahren erhalten, die für ihr berufliches Arbeitsgebiet relevant sind.
6.4	Maßregelungsprozess	**Maßnahme** Ein Maßregelungsprozess muss formalisiert und kommuniziert werden, um Maßnahmen gegen Mitarbeiter und andere interessierte Parteien zu ergreifen, die einen Verstoß gegen die Informationssicherheitspolitik begangen haben.
6.5	Verantwortlichkeiten nach Beendigung oder Änderung der Beschäftigung	**Maßnahme** Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, müssen festgelegt, durchgesetzt und den betreffenden Mitarbeitern und anderen interessierten Parteien mitgeteilt werden.
6.6	Vertraulichkeits- oder Geheim-haltungsvereinbarungen	**Maßnahme** Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, müssen identifiziert, dokumentiert, regelmäßig überprüft und von den Mitarbeitern und anderen interessierten Parteien unterzeichnet werden.

Tabelle A.1 (*fortgesetzt*)

6.7	Telearbeit	**Maßnahme** Es müssen Sicherheitsmaßnahmen ergriffen werden, wenn Mitarbeiter extern arbeiten, um Informationen zu schützen, die außerhalb der Räumlichkeiten des Unternehmens abgerufen, verarbeitet oder gespeichert werden.
6.8	Meldung von Informations-sicherheitsereignissen	**Maßnahme** Die Organisation muss einen Mechanismus bereitstellen, der es den Mitarbeitern ermöglicht, beobachtete oder vermutete Vorfälle im Bereich der Informationssicherheit über geeignete Kanäle rechtzeitig zu melden.
7	**Physische Maßnahmen**	
7.1	Physische Sicherheitsperimeter	**Maßnahme** Zum Schutz von Bereichen, in denen sich andere zugehörige Werte befinden, müssen Sicherheitsperimeter festgelegt und verwendet werden.
7.2	Physischer Zutritt	**Maßnahme** Sicherheitsbereiche müssen durch eine angemessene Zutrittssteuerung und Zutrittsstellen geschützt werden.
7.3	Sichern von Büros, Räumen und Einrichtungen	**Maßnahme** Die physische Sicherheit für Büros, Räume und Einrichtungen muss konzipiert und umgesetzt werden.
7.4	Physische Sicherheitsüberwachung	**Maßnahme** Die Räumlichkeiten müssen ständig auf unbefugten physischen Zugang überwacht werden.
7.5	Schutz vor physischen und umweltbedingten Bedrohungen	**Maßnahme** Der Schutz vor physischen und umweltbedingten Bedrohungen wie Naturkatastrophen und anderen absichtlichen oder unabsichtlichen physischen Bedrohungen der Infrastruktur muss konzipiert und umgesetzt werden.
7.6	Arbeiten in Sicherheitsbereichen	**Maßnahme** Es müssen Sicherheitsmaßnahmen für die Arbeit in Sicherheitsbereichen konzipiert und umgesetzt werden.
7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren	**Maßnahme** Es müssen klare Regeln für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und klare Regeln für Bildschirmsperren für informationsverarbeitende Einrichtungen festgelegt und angemessen durchgesetzt werden.
7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	**Maßnahme** Geräte und Betriebsmittel müssen sicher und geschützt aufgestellt werden.
7.9	Sicherheit von Werten außerhalb der Räumlichkeiten	**Maßnahme** Werte außerhalb des Standorts müssen geschützt werden.
7.10	Speichermedien	**Maßnahme** Speichermedien müssen während ihres gesamten Lebenszyklus – Erwerb, Verwendung, Transport und Entsorgung – in Übereinstimmung mit dem Klassifizierungsschema und den Handhabungsanforderungen der Organisation verwaltet werden.
7.11	Versorgungseinrichtungen	**Maßnahme** Informationsverarbeitungseinrichtungen müssen vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden, geschützt werden.

Tabelle A.1 (*fortgesetzt*)

7.12	Sicherheit der Verkabelung	**Maßnahme** Kabel, die Strom, Daten oder unterstützende Informationsdienste transportieren, müssen vor Unterbrechung, Störung oder Beschädigung geschützt werden.
7.13	Instandhalten von Geräten und Betriebsmitteln	**Maßnahme** Geräte und Betriebsmittel müssen ordnungsgemäß gewartet werden, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen sicherzustellen.
7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	**Maßnahme** Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, müssen überprüft werden, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind.
8	**Technologische Maßnahmen**	
8.1	Endpunktgeräte des Benutzers	**Maßnahme** Informationen, die auf Endpunktgeräten der Benutzer gespeichert sind, von ihnen verarbeitet werden oder über sie zugänglich sind, müssen geschützt werden.
8.2	Privilegierte Zugangsrechte	**Maßnahme** Zuteilung und Gebrauch von privilegierten Zugangsrechten müssen eingeschränkt und verwaltet werden.
8.3	Informationszugangs-beschränkung	**Maßnahme** Der Zugang zu Informationen und anderen zugehörigen Werten muss in Übereinstimmung mit der festgelegten themenspezifischen Richtlinie zur Zugangssteuerung eingeschränkt werden.
8.4	Zugriff auf den Quellcode	**Maßnahme** Der Lese- und Schreibzugriff auf den Quellcode, die Entwicklungswerkzeuge und die Softwarebibliotheken müssen angemessen verwaltet werden.
8.5	Sichere Authentifizierung	**Maßnahme** Sichere Authentifizierungstechnologien und -verfahren müssen auf der Grundlage von Informationszugangsbeschränkungen und der themenspezifischen Richtlinie zur Zugangssteuerung implementiert werden.
8.6	Kapazitätssteuerung	**Maßnahme** Die Nutzung von Ressourcen muss überwacht und entsprechend den aktuellen und erwarteten Kapazitätsanforderungen angepasst werden.
8.7	Schutz gegen Schadsoftware	**Maßnahme** Schutz gegen Schadsoftware muss umgesetzt und durch angemessene Sensibilisierung der Benutzer unterstützt werden.
8.8	Handhabung von technischen Schwachstellen	**Maßnahme** Es müssen Informationen über technische Schwachstellen verwendeter Informationssysteme eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen bewertet und angemessene Maßnahmen ergriffen werden.
8.9	Konfigurationsmanagement	**Maßnahme** Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken müssen festgelegt, dokumentiert, umgesetzt, überwacht und überprüft werden.

Tabelle A.1 (*fortgesetzt*)

8.10	Löschung von Informationen	**Maßnahme** Informationen, die in Informationssystemen, Geräten oder auf anderen Speichermedien gespeichert sind, müssen gelöscht werden, wenn sie nicht mehr benötigt werden.
8.11	Datenmaskierung	**Maßnahme** Die Datenmaskierung muss in Übereinstimmung mit den themenspezifischen Richtlinien der Organisation zur Zugangssteuerung und anderen damit zusammenhängenden themenspezifischen Richtlinien sowie den geschäftlichen Anforderungen und unter Berücksichtigung der geltenden Rechtsvorschriften eingesetzt werden.
8.12	Verhinderung von Datenlecks	**Maßnahme** Maßnahmen zur Verhinderung von Datenlecks müssen auf Systeme, Netzwerke und alle anderen Geräte angewendet werden, die sensible Informationen verarbeiten, speichern oder übertragen.
8.13	Sicherung von Information	**Maßnahme** Sicherungskopien von Informationen, Software und Systemen müssen in Übereinstimmung mit den vereinbarten themenspezifischen Richtlinien für Datensicherungen aufbewahrt und regelmäßig geprüft werden.
8.14	Redundanz von informationsverarbeitenden Einrichtungen	**Maßnahme** Informationsverarbeitende Einrichtungen müssen mit ausreichender Redundanz zur Einhaltung der Verfügbarkeitsanforderungen realisiert werden.
8.15	Protokollierung	**Maßnahme** Protokolle, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen, müssen erstellt, gespeichert, geschützt und analysiert werden.
8.16	Überwachung von Aktivitäten	**Maßnahme** Netzwerke, Systeme und Anwendungen müssen auf unübliches Verhalten überwacht und geeignete Maßnahmen müssen ergriffen werden, um potentielle Informationssicherheitsvorfälle zu bewerten.
8.17	Uhrensynchronisation	**Maßnahme** Die Uhren der von der Organisation verwendeten Informationsverarbeitungssysteme müssen mit zugelassenen Zeitquellen synchronisiert werden.
8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	**Maßnahme** Der Gebrauch von Hilfsprogrammen, die fähig sein können, System- und Anwendungsschutzmaßnahmen zu umgehen, muss eingeschränkt und streng überwacht werden.
8.19	Installation von Software auf Systemen im Betrieb	**Maßnahme** Es müssen Verfahren und Maßnahmen umgesetzt werden, um die Installation von Software auf Betriebssystemen sicher zu verwalten.
8.20	Netzwerksicherheit	**Maßnahme** Netzwerke und Netzwerkgeräte müssen gesichert, verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen zu schützen.
8.21	Sicherheit von Netzwerkdiensten	**Maßnahme** Sicherheitsmechanismen, Dienstgüte und Dienstanforderungen für Netzwerkdienste müssen ermittelt, umgesetzt und überwacht werden.

Tabelle A.1 (*fortgesetzt*)

8.22	Trennung von Netzwerken	**Maßnahme** Informationsdienste, Benutzer und Informationssysteme müssen in Netzwerken der Organisation gruppenweise voneinander getrennt gehalten werden.
8.23	Webfilterung	**Maßnahme** Der Zugang zu externen Websites muss verwaltet werden, um die Gefährdung durch bösartige Inhalte zu verringern.
8.24	Verwendung von Kryptographie	**Maßnahme** Es müssen Regeln für den wirksamen Einsatz von Kryptographie, einschließlich der Verwaltung kryptographischer Schlüssel, festgelegt und umgesetzt werden.
8.25	Lebenszyklus einer sicheren Entwicklung	**Maßnahme** Regeln für die sichere Entwicklung von Software und Systemen müssen festgelegt und angewendet werden.
8.26	Anforderungen an die Anwendungssicherheit	**Maßnahme** Die Anforderungen an die Informationssicherheit müssen bei der Entwicklung oder Beschaffung von Anwendungen ermittelt, spezifiziert und genehmigt werden.
8.27	Sichere Systemarchitektur und technische Grundsätze	**Maßnahme** Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme müssen festgelegt, dokumentiert, aktuell gehalten und bei allen Entwicklungsaktivitäten eines Informationssystems angewendet werden.
8.28	Sichere Kodierung	**Maßnahme** Bei der Softwareentwicklung müssen die Grundsätze der sicheren Kodierung angewandt werden.
8.29	Sicherheitsprüfung in Entwicklung und Abnahme	**Maßnahme** Sicherheitsprüfverfahren müssen definiert und in den Entwicklungslebenszyklus integriert werden.
8.30	Ausgegliederte Entwicklung	**Maßnahme** Die Organisation muss die Aktivitäten im Zusammenhang mit der ausgegliederten Systementwicklung leiten, überwachen und überprüfen.
8.31	Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen	**Maßnahme** Entwicklungs-, Prüf- und Produktionsumgebungen müssen getrennt und gesichert werden.
8.32	Änderungssteuerung	**Maßnahme** Änderungen an Informationsverarbeitungseinrichtungen und Informationssystemen müssen Gegenstand von Änderungsmanagementverfahren sein.
8.33	Informationen zur Prüfung	**Maßnahme** Die Prüfinformationen müssen in geeigneter Weise ausgewählt, geschützt und verwaltet werden.
8.34	Schutz der Informationssysteme während der Überwachungsprüfung	**Maßnahme** Auditprüfungen und andere Sicherheitstätigkeiten, die eine Beurteilung der betrieblichen Systeme beinhalten, müssen zwischen dem Prüfer und dem zuständigen Management geplant und vereinbart werden.

Literaturhinweise

[1] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

[2] ISO/IEC 27003, *Information technology — Security techniques — Information security management systems — Guidance*

[3] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[4] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[5] ISO 31000:2018, *Risk management — Guidelines*

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Context of the organization ... **1**
4.1 Understanding the organization and its context ... 1
4.2 Understanding the needs and expectations of interested parties ... 1
4.3 Determining the scope of the information security management system ... 2
4.4 Information security management system ... 2
5 Leadership ... **2**
5.1 Leadership and commitment ... 2
5.2 Policy ... 3
5.3 Organizational roles, responsibilities and authorities ... 3
6 Planning ... **3**
6.1 Actions to address risks and opportunities ... 3
6.1.1 General ... 3
6.1.2 Information security risk assessment ... 4
6.1.3 Information security risk treatment ... 4
6.2 Information security objectives and planning to achieve them ... 5
7 Support ... **6**
7.1 Resources ... 6
7.2 Competence ... 6
7.3 Awareness ... 6
7.4 Communication ... 6
7.5 Documented information ... 6
7.5.1 General ... 6
7.5.2 Creating and updating ... 7
7.5.3 Control of documented information ... 7
8 Operation ... **7**
8.1 Operational planning and control ... 7
8.2 Information security risk assessment ... 8
8.3 Information security risk treatment ... 8
9 Performance evaluation ... **8**
9.1 Monitoring, measurement, analysis and evaluation ... 8
9.2 Internal audit ... 8
9.2.1 General ... 8
9.2.2 Internal audit programme ... 9
9.3 Management review ... 9
9.3.1 General ... 9
9.3.2 Management review inputs ... 9
9.3.3 Management review results ... 9
10 Improvement ... **10**
10.1 Continual improvement ... 10
10.2 Nonconformity and corrective action ... 10
Annex A (normative) **Information security controls reference** ... **11**
Bibliography ... **19**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information Technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 27001:2013), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 27001:2013/Cor 1:2014 and ISO/IEC 27001:2013/Cor 2:2015.

The main changes are as follows:

— the text has been aligned with the harmonized structure for management system standards and ISO/IEC 27002:2022.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

0.1 General

This document has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This document can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this document does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This document applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

1 Scope

This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.4.1 of ISO 31000:2018[5].

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system;

b) the relevant requirements of these interested parties;

c) which of these requirements will be addressed through the information security management system.

NOTE The requirements of interested parties can include legal and regulatory requirements and contractual obligations.

4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;

b) the requirements referred to in 4.2;

c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.

4.4 Information security management system

The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information security management system requirements into the organization's processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

e) ensuring that the information security management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.2 Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security;

d) includes a commitment to continual improvement of the information security management system.

The information security policy shall:

e) be available as documented information;

f) be communicated within the organization;

g) be available to interested parties, as appropriate.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the information security management system conforms to the requirements of this document;

b) reporting on the performance of the information security management system to top management.

NOTE Top management can also assign responsibilities and authorities for reporting performance of the information security management system within the organization.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects;

c) achieve continual improvement.

The organization shall plan:

d) actions to address these risks and opportunities; and

e) how to

1) integrate and implement the actions into its information security management system processes; and

2) evaluate the effectiveness of these actions.

6.1.2 Information security risk assessment

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:

   1) the risk acceptance criteria; and

   2) criteria for performing information security risk assessments;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

c) identifies the information security risks:

   1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and

   2) identify the risk owners;

d) analyses the information security risks:

   1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;

   2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

   3) determine the levels of risk;

e) evaluates the information security risks:

   1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and

   2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the information security risk assessment process.

6.1.3 Information security risk treatment

The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

   NOTE 1 Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

   NOTE 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked.

   NOTE 3 The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed.

d) produce a Statement of Applicability that contains:

   — the necessary controls (see 6.1.3 b) and c));

— justification for their inclusion;

— whether the necessary controls are implemented or not; and

— the justification for excluding any of the Annex A controls.

e) formulate an information security risk treatment plan; and

f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

The organization shall retain documented information about the information security risk treatment process.

NOTE 4 The information security risk assessment and treatment process in this document aligns with the principles and generic guidelines provided in ISO 31000[5].

6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable (if practicable);

c) take into account applicable information security requirements, and results from risk assessment and risk treatment;

d) be monitored;

e) be communicated;

f) be updated as appropriate;

g) be available as documented information.

The organization shall retain documented information on the information security objectives.

When planning how to achieve its information security objectives, the organization shall determine:

h) what will be done;

i) what resources will be required;

j) who will be responsible;

k) when it will be completed; and

l) how the results will be evaluated.

6.3 Planning of changes

When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and

d) retain appropriate documented information as evidence of competence.

NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the re-assignment of current employees; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

a) the information security policy;

b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and

c) the implications of not conforming with the information security management system requirements.

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) how to communicate.

7.5 Documented information

7.5.1 General

The organization's information security management system shall include:

a) documented information required by this document; and

b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

NOTE The extent of documented information for an information security management system can differ from one organization to another due to:

1) the size of organization and its type of activities, processes, products and services;

2) the complexity of processes and their interactions; and

3) the competence of persons.

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the information security management system and by this document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;

d) storage and preservation, including the preservation of legibility;

e) control of changes (e.g. version control); and

f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

— establishing criteria for the processes;

— implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.

8.2 Information security risk assessment

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).

The organization shall retain documented information of the results of the information security risk assessments.

8.3 Information security risk treatment

The organization shall implement the information security risk treatment plan.

The organization shall retain documented information of the results of the information security risk treatment.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid;

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analysed and evaluated;

f) who shall analyse and evaluate these results.

Documented information shall be available as evidence of the results.

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

9.2 Internal audit

9.2.1 General

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to

   1) the organization's own requirements for its information security management system;

2) the requirements of this document;

b) is effectively implemented and maintained.

9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

a) define the audit criteria and scope for each audit;

b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant management;

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

9.3 Management review

9.3.1 General

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

9.3.2 Management review inputs

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information security management system;

c) changes in needs and expectations of interested parties that are relevant to the information security management system;

d) feedback on the information security performance, including trends in:

1) nonconformities and corrective actions;

2) monitoring and measurement results;

3) audit results;

4) fulfilment of information security objectives;

e) feedback from interested parties;

f) results of risk assessment and status of risk treatment plan;

g) opportunities for continual improvement.

9.3.3 Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

Documented information shall be available as evidence of the results of management reviews.

10 Improvement

10.1 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

10.2 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

   1) take action to control and correct it;

   2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

   1) reviewing the nonconformity;

   2) determining the causes of the nonconformity; and

   3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

Documented information shall be available as evidence of:

f) the nature of the nonconformities and any subsequent actions taken,

g) the results of any corrective action.

Annex A
(normative)

Information security controls reference

The information security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2022[1], Clauses 5 to 8, and shall be used in context with 6.1.3.

Table A.1 — Information security controls

5	**Organizational controls**	
5.1	Policies for information security	**Control** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
5.2	Information security roles and responsibilities	**Control** Information security roles and responsibilities shall be defined and allocated according to the organization needs.
5.3	Segregation of duties	**Control** Conflicting duties and conflicting areas of responsibility shall be segregated.
5.4	Management responsibilities	**Control** Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.
5.5	Contact with authorities	**Control** The organization shall establish and maintain contact with relevant authorities.
5.6	Contact with special interest groups	**Control** The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.
5.7	Threat intelligence	**Control** Information relating to information security threats shall be collected and analysed to produce threat intelligence.
5.8	Information security in project management	**Control** Information security shall be integrated into project management.
5.9	Inventory of information and other associated assets	**Control** An inventory of information and other associated assets, including owners, shall be developed and maintained.
5.10	Acceptable use of information and other associated assets	**Control** Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.
5.11	Return of assets	**Control** Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.

Table A.1 *(continued)*

5.12	Classification of information	**Control** Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.
5.13	Labelling of information	**Control** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
5.14	Information transfer	**Control** Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.
5.15	Access control	**Control** Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.
5.16	Identity management	**Control** The full life cycle of identities shall be managed.
5.17	Authentication information	**Control** Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.
5.18	Access rights	**Control** Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.
5.19	Information security in supplier relationships	**Control** Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.
5.20	Addressing information security within supplier agreements	**Control** Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.
5.21	Managing information security in the information and communication technology (ICT) supply chain	**Control** Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.
5.22	Monitoring, review and change management of supplier services	**Control** The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.
5.23	Information security for use of cloud services	**Control** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.
5.24	Information security incident management planning and preparation	**Control** The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

Table A.1 *(continued)*

5.25	Assessment and decision on information security events	**Control** The organization shall assess information security events and decide if they are to be categorized as information security incidents.
5.26	Response to information security incidents	**Control** Information security incidents shall be responded to in accordance with the documented procedures.
5.27	Learning from information security incidents	**Control** Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.
5.28	Collection of evidence	**Control** The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.
5.29	Information security during disruption	**Control** The organization shall plan how to maintain information security at an appropriate level during disruption.
5.30	ICT readiness for business continuity	**Control** ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.
5.31	Legal, statutory, regulatory and contractual requirements	**Control** Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.
5.32	Intellectual property rights	**Control** The organization shall implement appropriate procedures to protect intellectual property rights.
5.33	Protection of records	**Control** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.
5.34	Privacy and protection of personal identifiable information (PII)	**Control** The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.
5.35	Independent review of information security	**Control** The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.
5.36	Compliance with policies, rules and standards for information security	**Control** Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.
5.37	Documented operating procedures	**Control** Operating procedures for information processing facilities shall be documented and made available to personnel who need them.

Table A.1 *(continued)*

6	**People controls**	
6.1	Screening	**Control** Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
6.2	Terms and conditions of employment	**Control** The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.
6.3	Information security awareness, education and training	**Control** Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.
6.4	Disciplinary process	**Control** A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.
6.5	Responsibilities after termination or change of employment	**Control** Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.
6.6	Confidentiality or non-disclosure agreements	**Control** Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.
6.7	Remote working	**Control** Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.
6.8	Information security event reporting	**Control** The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.
7	**Physical controls**	
7.1	Physical security perimeters	**Control** Security perimeters shall be defined and used to protect areas that contain information and other associated assets.
7.2	Physical entry	**Control** Secure areas shall be protected by appropriate entry controls and access points.
7.3	Securing offices, rooms and facilities	**Control** Physical security for offices, rooms and facilities shall be designed and implemented.
7.4	Physical security monitoring	**Control** Premises shall be continuously monitored for unauthorized physical access.

Table A.1 *(continued)*

7.5	Protecting against physical and environmental threats	**Control** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.
7.6	Working in secure areas	**Control** Security measures for working in secure areas shall be designed and implemented.
7.7	Clear desk and clear screen	**Control** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.
7.8	Equipment siting and protection	**Control** Equipment shall be sited securely and protected.
7.9	Security of assets off-premises	**Control** Off-site assets shall be protected.
7.10	Storage media	**Control** Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.
7.11	Supporting utilities	**Control** Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.
7.12	Cabling security	**Control** Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.
7.13	Equipment maintenance	**Control** Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.
7.14	Secure disposal or re-use of equipment	**Control** Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
8	**Technological controls**	
8.1	User end point devices	**Control** Information stored on, processed by or accessible via user end point devices shall be protected.
8.2	Privileged access rights	**Control** The allocation and use of privileged access rights shall be restricted and managed.
8.3	Information access restriction	**Control** Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.
8.4	Access to source code	**Control** Read and write access to source code, development tools and software libraries shall be appropriately managed.

Table A.1 *(continued)*

8.5	Secure authentication	**Control** Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.
8.6	Capacity management	**Control** The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.
8.7	Protection against malware	**Control** Protection against malware shall be implemented and supported by appropriate user awareness.
8.8	Management of technical vulnerabilities	**Control** Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.
8.9	Configuration management	**Control** Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.
8.10	Information deletion	**Control** Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.
8.11	Data masking	**Control** Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.
8.12	Data leakage prevention	**Control** Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.
8.13	Information backup	**Control** Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.
8.14	Redundancy of information processing facilities	**Control** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
8.15	Logging	**Control** Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.
8.16	Monitoring activities	**Control** Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.
8.17	Clock synchronization	**Control** The clocks of information processing systems used by the organization shall be synchronized to approved time sources.

Table A.1 *(continued)*

8.18	Use of privileged utility programs	**Control** The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.
8.19	Installation of software on operational systems	**Control** Procedures and measures shall be implemented to securely manage software installation on operational systems.
8.20	Networks security	**Control** Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.
8.21	Security of network services	**Control** Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.
8.22	Segregation of networks	**Control** Groups of information services, users and information systems shall be segregated in the organization's networks.
8.23	Web filtering	**Control** Access to external websites shall be managed to reduce exposure to malicious content.
8.24	Use of cryptography	**Control** Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.
8.25	Secure development life cycle	**Control** Rules for the secure development of software and systems shall be established and applied.
8.26	Application security requirements	**Control** Information security requirements shall be identified, specified and approved when developing or acquiring applications.
8.27	Secure system architecture and engineering principles	**Control** Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.
8.28	Secure coding	**Control** Secure coding principles shall be applied to software development.
8.29	Security testing in development and acceptance	**Control** Security testing processes shall be defined and implemented in the development life cycle.
8.30	Outsourced development	**Control** The organization shall direct, monitor and review the activities related to outsourced system development.
8.31	Separation of development, test and production environments	**Control** Development, testing and production environments shall be separated and secured.
8.32	Change management	**Control** Changes to information processing facilities and information systems shall be subject to change management procedures.
8.33	Test information	**Control** Test information shall be appropriately selected, protected and managed.

Table A.1 *(continued)*

8.34	Protection of information systems during audit testing	**Control** Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.

Bibliography

[1] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

[2] ISO/IEC 27003, *Information technology — Security techniques — Information security management systems — Guidance*

[3] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[4] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[5] ISO 31000:2018, *Risk management — Guidelines*