EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 27001

Juli 2023

ICS 03.100.70; 35.030

Ersetzt EN ISO/IEC 27001:2017

Deutsche Fassung

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)

Diese Europäische Norm wurde vom CEN am 23. Juli 2023 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Ref. Nr. EN ISO/IEC 27001:2023 D

Inhalt

Tabellen

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 EN ISO/IEC 27001:2023 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz" übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Januar 2024, und etwaige entgegenstehende nationale Normen müssen bis Januar 2024 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN-CENELEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument ersetzt EN ISO/IEC 27001:2017.

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 und CENELEC abrufbar.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 27001:2022 wurde von CEN-CENELEC als EN 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 die harmonisierte Struktur für Managementsystemnormen und an 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 Informationen 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 Listeneinträge 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 Managementsystemnormen

Dieses Dokument wendet die übergeordnete Struktur, die identischen Unterabschnittsnummern, den einheitlichen Basistext, die gemeinsamen Benennungen und die Basisdefinitionen an, die in Anhang SL der ISO/IEC Directives, Teil 1, „Consolidated ISO Supplement" festgelegt sind, und stellt so die Übereinstimmung mit anderen Managementsystemnormen her, die ebenfalls den Anhang SL anwenden.

Diese in Anhang SL festgelegte gemeinsame Herangehensweise nützt jenen Organisationen, die sich für den Betrieb eines einzigen Managementsystems entscheiden, das die Anforderungen von zwei oder mehr Normen für Managementsysteme erfüllt.

1 Anwendungsbereich

Dieses Dokument legt die Anforderungen an die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems im Kontext der Organisation fest. Darüber hinaus beinhaltet dieses Dokument Anforderungen an die Beurteilung und Behandlung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen der Organisation. Die in diesem Dokument festgelegten Anforderungen sind allgemein gehalten und dazu vorgesehen, auf alle Organisationen, ungeachtet ihrer Art und Größe, anwendbar zu 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 behandelt 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 genannten externen und internen Themen;

b) die unter 4.2 genannten 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 ihrer 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 Prozesse 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 Rollen unterstützt, um deren Führung in ihren 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 die Existenz der Organisation 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 bekanntgemacht werden;

g) soweit angemessen für interessierte Parteien verfügbar sein.

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 bekanntgemacht 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 über die 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 Informationen 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 gewählten 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 die erforderlichen Maßnahmen 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, wie die Informationssicherheitsziele erreicht werden, 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 die Notwendigkeit von Änderungen am Informationssicherheitsmanagementsystem ermittelt, müssen diese in geplanter Weise 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) sofern anwendbar, Maßnahmen einleiten, um die benötigte Kompetenz zu erwerben, und die Wirksamkeit der getroffenen Maßnahmen 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 des Folgenden 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 Steuerung dokumentierter Information

Die für das Informationssicherheitsmanagementsystem erforderliche und von diesem Dokument geforderte dokumentierte Information muss gesteuert 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 Steuerung 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 gesteuert 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 notwendigen 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 verwirklicht.

Dokumentierte Information muss im erforderlichen Umfang verfügbar sein, damit darauf vertraut werden kann, dass die Prozesse wie geplant durchgeführt wurden.

Die Organisation muss geplante Änderungen steuern sowie die Folgen unbeabsichtigter Änderungen überprüfen 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, gesteuert werden.

8.2 Informationssicherheitsrisikobeurteilung

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

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

8.3 Informationssicherheitsrisikobehandlung

Die Organisation muss den Plan für die Informationssicherheitsrisikobehandlung umsetzen.

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

9 Bewertung der Leistung

9.1 Überwachung, Messung, Analyse und Bewertung

Die Organisation muss 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, um als gültig betrachtet zu werden;

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.

Dokumentierte Information muss 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 zur Verfügung zu stellen, ob das Informationssicherheitsmanagementsystem:

a) folgende Anforderungen erfüllt:

   1) die eigenen 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 und Berichterstattung.

Beim Aufbau des/der internen Auditprogramms/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.

Dokumentierte Information muss als Nachweis der Umsetzung des Auditprogramms/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 das Informationssicherheitsmanagementsystem betreffen;

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 jeglichen Änderungsbedarf am Informationssicherheitsmanagementsystem enthalten.

Dokumentierte Information muss als Nachweis der Ergebnisse von Managementbewertungen verfügbar sein.

10 Verbesserung

10.1 Fortlaufende Verbesserung

Die Organisation muss die Eignung, Angemessenheit und Wirksamkeit des 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 Ursachen 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.

Dokumentierte Information muss verfügbar sein als Nachweis:

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[N1] 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	Informationssicherheitspolitik und -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 vom 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	Informationen über die Bedrohungslage	**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 Werte	**Maßnahme** Ein Inventar der Informationen und anderen damit verbundenen Werte, einschließlich der Eigentümer, muss erstellt und gepflegt werden.

N1 Nationale Fußnote: Die hier im Zusammenhang genannten Maßnahmen können als Maßnahmen im Sinne der Steuerung des ISMS verstanden werden.

Tabelle A.1 (*fortgesetzt*)

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 damit verbundenen Werten müssen aufgestellt, dokumentiert und angewendet werden.
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 Informationen	**Maßnahme** Informationen müssen entsprechend den Informationssicherheitserfordernissen der Organisation auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen der interessierten Parteien klassifiziert werden.
5.13	Kennzeichnung von Informationen	**Maßnahme** Ein angemessener Satz von Verfahren zur Kennzeichnung von Informationen muss entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt werden.
5.14	Informationsübermittlung	**Maßnahme** Für alle Arten von Übermittlungseinrichtungen 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 Steuerung des physischen und logischen Zugriffs auf Informationen und andere damit verbundene 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	Authentisierungsinformationen	**Maßnahme** Die Zuweisung und Verwaltung von Authentisierungsinformationen muss durch einen Managementprozess gesteuert werden, der auch die Beratung des Personals über den angemessenen Umgang mit Authentisierungsinformationen umfasst.
5.18	Zugangsrechte	**Maßnahme** Zugangsrechte zu Informationen und anderen damit verbundenen Werten müssen in Übereinstimmung mit der themenspezifischen Richtlinie und den 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.

Tabelle A.1 (*fortgesetzt*)

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.
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 Informationssicherheitsereignisse beurteilen und entscheiden, ob sie als Informationssicherheitsvorfälle 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 Ermittlung, Sammlung, Beschaffung und Aufbewahrung von Beweismaterial im Zusammenhang mit Informationssicherheitsereignissen 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	Juristische, 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.

Tabelle A.1 (*fortgesetzt*)

5.34	Datenschutz 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.
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 und ihrer themenspezifischen Richtlinien, Regeln und Normen muss regelmäßig überprüft werden.
5.37	Dokumentierte Betriebsabläufe	**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 Informationen 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 Schritte gegen Mitarbeiter und andere interessierte Parteien zu ergreifen, die einen Verstoß gegen die Informationssicherheitspolitik begangen haben.
6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	**Maßnahme** Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung von Beschäftigungsverhältnissen bestehen bleiben, müssen festgelegt, durchgesetzt und den betreffenden Mitarbeitern und anderen interessierten Parteien mitgeteilt werden.

Tabelle A.1 (*fortgesetzt*)

6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	**Maßnahme** Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche den Bedarf der Organisation am Schutz von Informationen widerspiegeln, müssen identifiziert, dokumentiert, regelmäßig überprüft und von den Mitarbeitern und anderen interessierten Parteien unterzeichnet werden.
6.7	Remote-Arbeit	**Maßnahme** Es müssen Sicherheitsmaßnahmen ergriffen werden, wenn Mitarbeiter aus der Ferne arbeiten, um Informationen zu schützen, die außerhalb der Räumlichkeiten des Unternehmens abgerufen, verarbeitet oder gespeichert werden.
6.8	Meldung von Informationssicherheitsereignissen	**Maßnahme** Die Organisation muss einen Mechanismus bereitstellen, der es den Mitarbeitern ermöglicht, beobachtete oder vermutete Informationssicherheitsereignisse über geeignete Kanäle rechtzeitig zu melden.
7	**Physische Maßnahmen**	
7.1	Physische Sicherheitsperimeter	**Maßnahme** Zum Schutz von Bereichen, in denen sich Informationen und andere damit verbundene 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 von Büros, Räumen 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 geplant 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.

Tabelle A.1 (*fortgesetzt*)

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 unterstützenden Versorgungseinrichtungen verursacht werden, geschützt werden.
7.12	Sicherheit der Verkabelung	**Maßnahme** Kabel, die Strom, Daten oder unterstützende Informationsdienste transportieren, müssen vor Abhören, Störung oder Beschädigung geschützt werden.
7.13	Instandhaltung 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 damit verbundenen Werten muss in Übereinstimmung mit der festgelegten themenspezifischen Richtlinie zur Zugangssteuerung eingeschränkt werden.
8.4	Zugriff auf den Quellcode	**Maßnahme** Lese- und Schreibzugriff auf den Quellcode, die Entwicklungswerkzeuge und die Softwarebibliotheken müssen angemessen verwaltet werden.
8.5	Sichere Authentisierung	**Maßnahme** Sichere Authentisierungstechnologien 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.

Tabelle A.1 (*fortgesetzt*)

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.
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 übermitteln.
8.13	Sicherung von Informationen	**Maßnahme** Sicherungskopien von Informationen, Software und Systemen müssen in Übereinstimmung mit der vereinbarten themenspezifischen Richtlinie zu Datensicherungen aufbewahrt und regelmäßig geprüft werden.
8.14	Redundanz von informationsverarbeitenden Einrichtungen	**Maßnahme** Informationsverarbeitende Einrichtungen müssen mit ausreichender Redundanz für die 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 anormales 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 in Betrieb befindlichen Systemen sicher zu verwalten.

Tabelle A.1 (*fortgesetzt*)

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.
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 Entwicklungsgrundsätze	**Maßnahme** Grundsätze für die Entwicklung sicherer Systeme müssen festgelegt, dokumentiert, aufrechterhalten und bei allen Aktivitäten der Informationssystemsentwicklung angewendet werden.
8.28	Sichere Codierung	**Maßnahme** Bei der Softwareentwicklung müssen die Grundsätze der sicheren Codierung angewandt werden.
8.29	Sicherheitsprüfung bei 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-, Test- und Produktionsumgebungen	**Maßnahme** Entwicklungs-, Test- und Produktionsumgebungen müssen getrennt und gesichert werden.
8.32	Änderungssteuerung	**Maßnahme** Änderungen an Informationsverarbeitungseinrichtungen und Informationssystemen müssen Gegenstand von Änderungsmanagementverfahren sein.

Tabelle A.1 (*fortgesetzt*)

8.33	Testdaten	**Maßnahme** Die Testdaten müssen in geeigneter Weise ausgewählt, geschützt und verwaltet werden.
8.34	Schutz der Informationssysteme während Tests im Rahmen von Audits	**Maßnahme** Tests im Rahmen von Audits und andere Sicherheitstätigkeiten, die eine Beurteilung der in Betrieb befindlichen 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*

[redacted]

ISMS Processes

5.0, 05.01.2024

Type	Process / Activity	ISO 27001:2022
Project	0.1. ISMS Designing and Planning (project)	6.2, 6.3, 8.1, A.5.8
Core ISMS processes	1.1 Requirements management	4.2, A.5.5, A.5.6, A.5.31, A.5.32, A.5.34
	1.2 ISMS Communication	4.2, 7.4, A.5.5, A.5.6
	1.3 ISMS document management	5.2, 7.5, A.5.1, A.5.37
	1.4 Information security risk management	6.1, 8.2, 8.3, A.5.7
	1.5 ISMS resource management	5.1, 7.1
	1.6 Information security awareness, trainings and education	7.2, 7.3, A.6.3
	1.7 Internal information security audits and assessments	9.2, A.5.36, A.8.34
	1.8 Preparation for external audits and assessments	A.5.35, A.5.36, A.8.34
	1.9 ISMS monitoring and measurement	6.2, 9.1
	1.10 ISMS management review	9.3
	1.11 Nonconformity management	10.2
	1.12 Planning and Continual Improvement (inc. IS Committee Meetings)	5.1, 5.3, 6.3, 8.1, 8.3, 10.1, A.5.2, A.5.4
IT and IS operations	2.1. Inventory of assets	4.3, A.5.9
	2.2. Access management (+review)	A.5.15-18, A.8.1-5
	2.3. Incident management and notification	A.5.5, A.5.24-29, A.6.8
	2.4. Configuration and change management	A.8.9, A.8.19, A.8.32
	2.5. Vulnerability and patch management	A.8.8
	2.6. Capacity management	A.8.6
	2.7. Backup and recovery (+testing)	A.8.13
	2.8. Business continuity management (+testing)	A.5.29, A.5.30
	2.9. Release and deployment management	A.8.25-34
	2.10. Logging and monitoring	A.8.15-16, A.8.21, A.8.23
	2.11. Information transfer management	A.5.14
	2.12. Configuring and managing information security tools	A.8.7, A.8.12, A.8.20-23, A.8.24
Supporting Processes	3.1. Document management (+classification and labeling)	7.5, A.5.12, A.5.13, A.5.33, A.5.37
	3.2. Physical security management	A.7.1-14, A.5.10, A.5.11
	3.3. Human resources management	A.6.1-8
	3.4. Supplier management	A.5.19-21, A.5.23
	3.5. Monitoring and review of supplier services	8.1, A.5.22, A.5.23

[redacted]

ISMS Processes

1.0, 05.01.2024

ISO/IEC TS 27022:2021	ISO/IEC TS 33052:2016	Tesis Doctoral by Knut Haufe
Guidance on ISMS processes	Process reference model (PRM) for information security management	Maturity based approach for ISMS governance
Management 1. Information security governance / management interface process **Core Processes** 2. Security policy management process 3. Requirements management process 4. Information security risk assessment process 5. Information security risk treatment process 6. Security implementation management process 7. Process to control outsourced services 8. Process to assure necessary awareness and competence 9. Information security incident management process 10. Information security change management process 11. Internal audit process 12. Performance evaluation process 13. Information security improvement process **Support processes** 14. Records control process 15. Resource management process 16. Communication process 17. Information security customer relationship management process	**Common Integrated Management Processes** COM.01 Communication management COM.02 Documentation management COM.03 Human resource management COM.04 Improvement COM.05 Internal audit COM.06 Management review COM.07 Non-conformity management COM.08 Operational planning COM.09 Operational implementation and control COM.10 Performance evaluation COM.11 Risk and opportunity management **Organisational Processes** ORG.01 Asset management ORG.02 Equipment management ORG.03 Human resource employment management ORG.04 Infrastructure and work environment ORG.05 Supplier management **Technical Processes** TEC.01 Capacity management TEC.02 Change management TEC.03 Configuration management TEC.04 Incident management TEC.05 Product/service release TEC.06 Service availability management TEC.07 Service continuity management TEC.08 Service requirements TEC.09 Technical data preservation and recovery	**Management** 1. Information security governance process **Core Processes:** 2. Information security risk assessment process 3. Information security risk treatment process 4. Resource management process 5. Process to assure necessary awareness and competence 6. Communication process 7. Documentation and record control process 8. Requirements management process 9. Information security change management process 10. Process to control outsourced services 11. Performance evaluation process 12. Internal audit process 13. Information security improvement process 14. Information security incident management process **Operation and Support** 15. Service level management process 16. Service reporting process 17. Service continuity and availability management process 18. Budgeting and accounting for services process 19. Capacity management process 20. Business relationship management process 21. Supplier management process 22. Incident and service request management process 23. Problem management process 24. Configuration management process 25. Change management process 26. Release and deployment management process 27. Information security customer relationship management process **Other** 28. Controlling process 29. Human resources management process 30. Facility management process