PERPETUUM
CAPITAL

ISO 27001 & Annex A

Version 2022

DEUTSCH

4 Kontext der Organisation

4.1 Verständnis der Organisation und ihres Kontexts: Die Organisation muss externe und interne Probleme bestimmen, die für ihren Zweck relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse ihres Informationssicherheitsmanagementsystems zu erreichen.

4.2 Verständnis der Bedürfnisse und Erwartungen interessierter Parteien:
Die Organisation bestimmt:

a) interessierte Parteien, die für das Informationssicherheitsmanagementsystem relevant sind; und
b) die Anforderungen dieser interessierten Kreise, die für die Informationssicherheit relevant sind**.**

4.3 Bestimmung des Umfangs des Informationssicherheitsmanagementsystems: Die Organisation muss die Grenzen und die Anwendbarkeit des Informationssicherheitsmanagementsystems bestimmen, um seinen Geltungsbereich festzulegen.

Bei der Festlegung dieses Umfangs hat die Organisation Folgendes zu berücksichtigen:
a) die in 4.1 genannten externen und internen Fragen;
b) die Anforderungen nach 4.2; und
c) Schnittstellen und Abhängigkeiten zwischen Aktivitäten, die von der Organisation durchgeführt werden, und solchen, die von anderen Organisationen durchgeführt werden.
Der Anwendungsbereich muss als dokumentierte Informationen verfügbar sein.

4.4 Informationssicherheitsmanagementsystem: Die Organisation muss ein Informationssicherheitsmanagementsystem in Übereinstimmung mit den Anforderungen dieser Internationalen Norm einrichten, implementieren, aufrechterhalten und kontinuierlich verbessern.

5 Führung

5.1 Führung und Engagement: Das Top-Management muss Führung und Engagement in Bezug auf das Informationssicherheitsmanagementsystem demonstrieren, indem es:

a) sicherstellt, dass die Informationssicherheitsrichtlinie und die Informationssicherheitsziele festgelegt sind und mit der strategischen Ausrichtung der Organisation vereinbar sind.
b) Sicherstellung der Integration der Anforderungen an das Informationssicherheitsmanagementsystem in die Prozesse der Organisation;
c) Sicherstellung, dass die für das Informationssicherheitsmanagementsystem erforderlichen Ressourcen zur Verfügung stehen;
d) Vermittlung der Bedeutung eines wirksamen Informationssicherheitsmanagements und der Einhaltung der Anforderungen an das Informationssicherheitsmanagementsystem;
e) Sicherstellung, dass das Informationssicherheitsmanagementsystem seine beabsichtigten Ergebnisse erreicht;
f) Leitung und Unterstützung von Personen, die zur Wirksamkeit des Informationssicherheitsmanagementsystems beitragen;
g) Förderung der kontinuierlichen Verbesserung; und

h) Unterstützung anderer relevanter Managementrollen, um ihre Führungsqualitäten in Bezug auf ihre Verantwortungsbereiche zu demonstrieren.

5.2 Richtlinie: Das Top-Management muss eine Informationssicherheitsrichtlinie festlegen, die:

a) dem Zweck der Organisation angemessen ist;
b) Informationssicherheitsziele enthält (siehe 6.2) oder den Rahmen für die Festlegung von

Informationssicherheitszielen vorgibt;
c) eine Verpflichtung zur Erfüllung der geltenden Anforderungen in Bezug auf die Informationssicherheit enthält; und
d) beinhaltet eine Verpflichtung zur kontinuierlichen Verbesserung des Informationssicherheitsmanagementsystems.
Die Informationssicherheitsrichtlinie muss:
e) als dokumentierte Informationen verfügbar sein;
f) innerhalb der Organisation kommuniziert werden; und
g) gegebenenfalls interessierten Parteien zur Verfügung stehen.

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

a) die Sicherstellung, dass das Informationssicherheitsmanagementsystem den Anforderungen dieser Internationalen Norm entspricht; und
b) Berichterstattung über die Leistung des Informationssicherheitsmanagementsystems an das Top-Management.

6 Planung

6.1 Maßnahmen zur Bewältigung von Risiken und Chancen:

6.1.1 Allgemeines: Bei der Planung des Informationssicherheitsmanagementsystems muss die Organisation die in 4.1 genannten Probleme und die in 4.2 genannten Anforderungen berücksichtigen und die Risiken und Chancen bestimmen, die angegangen werden müssen:

a) sicherstellen, dass das Informationssicherheitsmanagementsystem seine beabsichtigten Ergebnisse erreichen kann;
b) unerwünschte Wirkungen verhindern oder reduzieren; und
c) kontinuierliche Verbesserung zu erreichen.
Die Organisation plant:
d) Maßnahmen zur Bewältigung dieser Risiken und Chancen; und
e) wie man

1) die Maßnahmen in die Prozesse seines Informationssicherheitsmanagementsystems integriert und umsetzt; und
2) die Wirksamkeit dieser Maßnahmen zu bewerten.

6.1.2 Risikobewertung der Informationssicherheit: Die Organisation muss einen Prozess zur Risikobewertung der Informationssicherheit definieren und anwenden, der:

a) Risikokriterien für die Informationssicherheit festlegt und aufrechterhält, darunter:

1) die Risikoakzeptanzkriterien; und
2) Kriterien für die Durchführung von Risikobewertungen für die Informationssicherheit;

b) stellt sicher, dass wiederholte Risikobewertungen der Informationssicherheit zu konsistenten, validen und vergleichbaren Ergebnissen führen;
c) identifiziert die Informationssicherheitsrisiken:

1) wendet den Prozess der Risikobewertung der Informationssicherheit an, um Risiken im Zusammenhang mit dem Verlust der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen im Rahmen des Informationssicherheitsmanagementsystems zu identifizieren; und
2) die Risikoverantwortlichen identifizieren;

d) analysiert die Risiken für die Informationssicherheit:

1) bewertet die möglichen Folgen, die sich ergeben würden, wenn die in 6.1.2 c) 1) genannten Risiken eintreten würden;
2) Bewertung der realistischen Wahrscheinlichkeit des Eintretens der in 6.1.2 c) 1) genannten Risiken; und
3) die Risikostufen bestimmen;

e) bewertet die Informationssicherheitsrisiken:

1) vergleicht die Ergebnisse der Risikoanalyse mit den in 6.1.2 a) festgelegten Risikokriterien; und
2) die analysierten Risiken für die Risikobehandlung priorisieren.
Die Organisation muss dokumentierte Informationen über den Prozess der Risikobewertung der Informationssicherheit aufbewahren.

6.1.3 Behandlung von Informationssicherheitsrisiken: Die Organisation muss einen Prozess zur Behandlung von Informationssicherheitsrisiken definieren und anwenden, um:

a) geeignete Optionen zur Behandlung von Informationssicherheitsrisiken unter Berücksichtigung der Ergebnisse der Risikobewertung auszuwählen;
b) alle Kontrollen zu bestimmen, die erforderlich sind, um die gewählte(n) Option(en) zur Behandlung von Informationssicherheitsrisiken zu implementieren;
c) die in Abschnitt 6.1.3 Buchstabe b) genannten Kontrollen mit denen in Anhang A vergleichen und überprüfen, ob keine erforderlichen Kontrollen ausgelassen wurden;
d) eine Erklärung über die Anwendbarkeit vorlegen, die die erforderlichen Kontrollen (siehe 6.1.3 b) und c)) und eine Begründung für die Aufnahme enthält, unabhängig davon, ob sie durchgeführt wird oder nicht, sowie die Begründung für den Ausschluss von Kontrollen aus Anhang A;
e) einen Plan zur Behandlung von Informationssicherheitsrisiken zu formulieren; und

f) die Genehmigung der Risikoverantwortlichen für den Behandlungsplan für Informationssicherheitsrisiken und die Akzeptanz der verbleibenden Informationssicherheitsrisiken einzuholen.
Die Organisation muss dokumentierte Informationen über den Prozess der Behandlung von Informationssicherheitsrisiken aufbewahren.

6.2 Informationssicherheitsziele und Planung zu deren Erreichung: Die Organisation muss Informationssicherheitsziele auf relevanten Funktionen und Ebenen festlegen.
Die Informationssicherheitsziele müssen:

a) mit der Informationssicherheitspolitik übereinstimmen;
b) messbar sein (falls praktikabel);
c) Berücksichtigung der geltenden Anforderungen an die Informationssicherheit und der Ergebnisse der Risikobewertung und Risikobehandlung;
d) mitgeteilt werden; und
e) gegebenenfalls aktualisiert werden.
Die Organisation muss dokumentierte Informationen über die Informationssicherheitsziele aufbewahren.

Bei der Planung, wie ihre Informationssicherheitsziele erreicht werden sollen, muss die Organisation festlegen:
f) was getan wird;
g) welche Ressourcen benötigt werden;
h) wer verantwortlich sein wird;
i) wann es abgeschlossen sein wird; und
j) wie die Ergebnisse bewertet werden.

7 Unterstützung

7.1 Ressourcen: Die Organisation bestimmt und stellt die Ressourcen zur Verfügung, die für die Einrichtung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung des Informationssicherheitsmanagementsystems erforderlich sind.

7.2 Kompetenz: Die Organisation muss:

a) die erforderliche Kompetenz der Person(en) bestimmen, die unter ihrer Kontrolle Arbeiten ausführen, die sich auf ihre Informationssicherheitsleistung auswirken;
b) sicherzustellen, dass diese Personen auf der Grundlage einer angemessenen Ausbildung, Ausbildung oder Erfahrung kompetent sind;
c) gegebenenfalls Maßnahmen ergreifen, um die erforderliche Kompetenz zu erwerben, und die Wirksamkeit der ergriffenen Maßnahmen bewerten; und
d) geeignete dokumentierte Informationen als Kompetenznachweis aufbewahren.

7.3 Bewusstsein: Personen, die unter der Kontrolle der Organisation arbeiten, müssen sich über Folgendes im Klaren sein:

a) die Informationssicherheitsrichtlinie;
b) ihren Beitrag zur Wirksamkeit des Informationssicherheitsmanagementsystems, einschließlich der Vorteile einer verbesserten Informationssicherheitsleistung; und
c) die Auswirkungen der Nichteinhaltung der Anforderungen an das Informationssicherheitsmanagementsystem.

7.4 Kommunikation: Die Organisation bestimmt den Bedarf an interner und externer Kommunikation, die für das Informationssicherheitsmanagementsystem relevant ist, einschließlich:

a) darüber, was kommuniziert werden soll;
b) wann kommuniziert werden soll;
c) mit wem kommuniziert werden soll;
d) wer kommuniziert; und
e) die Prozesse, durch die die Kommunikation beeinflusst werden soll.

7.5 Dokumentierte Informationen:
7.5.1 Allgemeines: Das Informationssicherheits-Managementsystem der Organisation muss Folgendes umfassen:

a) dokumentierte Informationen, die nach dieser Internationalen Norm erforderlich sind; und
b) dokumentierte Informationen, die von der Organisation als notwendig für die Wirksamkeit des Informationssicherheitsmanagementsystems erachtet werden.

1) die Größe der Organisation und ihre Art der Aktivitäten, Prozesse, Produkte und Dienstleistungen;
2) die Komplexität von Prozessen und deren Wechselwirkungen; und
3) die Kompetenz von Personen.

7.5.2 Erstellung und Aktualisierung: Bei der Erstellung und Aktualisierung dokumentierter Informationen muss die Organisation sicherstellen:

a) Identifizierung und Beschreibung (z. B. Titel, Datum, Autor oder Referenznummer);
b) Format (z. B. Sprache, Softwareversion, Grafik) und Medien (z. B. Papier, elektronisch); und
c) Überprüfung und Genehmigung auf Eignung und Angemessenheit.

7.5.3 Kontrolle dokumentierter Informationen: Dokumentierte Informationen, die vom Informationssicherheitsmanagementsystem und von dieser Internationalen Norm gefordert werden, müssen kontrolliert werden, um sicherzustellen:

a) sie sind verfügbar und geeignet für den Einsatz, wo und wann immer sie benötigt werden; und
b) sie angemessen geschützt sind (z. B. vor Verlust der Vertraulichkeit, unsachgemäßer Verwendung oder Verlust der Integrität).
Für die Kontrolle dokumentierter Informationen muss die Organisation die folgenden Aktivitäten berücksichtigen, sofern zutreffend:
c) Verteilung, Zugriff, Abruf und Verwendung;
d) Lagerung und Konservierung, einschließlich der Erhaltung der Lesbarkeit;
e) Überwachung von Änderungen (z. B. Versionskontrolle); und
f) Aufbewahrung und Veräußerung.

Dokumentierte Informationen externen Ursprungs, die von der Organisation für die Planung und den Betrieb des Informationssicherheitsmanagementsystems als notwendig erachtet werden, sind gegebenenfalls zu identifizieren und zu kontrollieren.

8 Betrieb

8.1 Operative Planung und Kontrolle: Die Organisation muss die Prozesse planen, implementieren und kontrollieren, die erforderlich sind, um die Anforderungen an die Informationssicherheit zu erfüllen und die in 6.1 festgelegten Maßnahmen umzusetzen.

Die Organisation muss auch Pläne zur Erreichung der in 6.2 festgelegten Informationssicherheitsziele umsetzen. Die Organisation muss dokumentierte Informationen in dem Umfang aufbewahren, der erforderlich ist, um darauf vertrauen zu können, dass die Prozesse wie geplant durchgeführt wurden. Die Organisation muss geplante Änderungen kontrollieren und die Folgen unbeabsichtigter Änderungen überprüfen und bei Bedarf Maßnahmen ergreifen, um nachteilige Auswirkungen zu mildern. Die Organisation muss sicherstellen, dass ausgelagerte Prozesse bestimmt und kontrolliert werden.

8.2 Risikobewertung der Informationssicherheit: Die Organisation muss Risikobewertungen der Informationssicherheit in geplanten Abständen oder wenn wesentliche Änderungen vorgeschlagen werden oder auftreten, unter Berücksichtigung der in 6.1.2 a) festgelegten Kriterien durchführen. Die Organisation muss dokumentierte Informationen über die Ergebnisse der Risikobewertungen für die Informationssicherheit aufbewahren.

8.3 Behandlung von Informationssicherheitsrisiken: Die Organisation muss den Plan zur Behandlung von Informationssicherheitsrisiken umsetzen.
Die Organisation muss dokumentierte Informationen über die Ergebnisse der Behandlung des Informationssicherheitsrisikos aufbewahren.

9 Leistungsbewertung

9.1 Überwachung, Messung, Analyse und Bewertung: Die Organisation muss die Informationssicherheitsleistung und die Wirksamkeit des Informationssicherheitsmanagementsystems bewerten.
Die Organisation muss festlegen:

a) was überwacht und gemessen werden muss, einschließlich Informationssicherheitsprozesse und -kontrollen;
b) gegebenenfalls die Methoden für die Überwachung, Messung, Analyse und Bewertung, um gültige Ergebnisse zu gewährleisten;
c) wann die Überwachung und Messung durchgeführt werden soll;
d) wer überwacht und misst;
e) wann die Ergebnisse der Überwachung und Messung analysiert und bewertet werden sollen; und
f) wer diese Ergebnisse analysiert und bewertet.

Die Organisation muss geeignete dokumentierte Informationen als Nachweis für die Überwachungs- und Messergebnisse aufbewahren

9.2 Interne Revision: Die Organisation führt in geplanten Abständen interne Audits durch, um Informationen darüber zu erhalten, ob das Informationssicherheitsmanagementsystem:
a) die Anforderungen

1) den eigenen Anforderungen der Organisation an ihr Informationssicherheitsmanagementsystem entspricht; und
2) die Anforderungen dieser Internationalen Norm;

b) wirksam umgesetzt und aufrechterhalten wird.

Die Organisation muss:
c) ein Auditprogramm planen, einrichten, umsetzen und aufrechterhalten, einschließlich der Häufigkeit, Methoden, Verantwortlichkeiten, Planungsanforderungen und Berichterstattung. Das/die Auditprogramm(e) trägt der Bedeutung der betreffenden Prozesse und den Ergebnissen früherer Audits Rechnung;
d) Festlegung der Prüfungskriterien und des Prüfungsumfangs für jede Prüfung;
e) Auswahl von Abschlussprüfern und Durchführung von Prüfungen, die Objektivität und Unparteilichkeit des Prüfungsprozesses gewährleisten;
f) sicherzustellen, dass die Ergebnisse der Audits dem zuständigen Management gemeldet werden; und
g) dokumentierte Informationen als Nachweis für das/die Auditprogramm(e) und die Auditergebnisse aufbewahren.

9.3 Management-Review: Das Top-Management überprüft das Informationssicherheits-Managementsystem der Organisation in geplanten Abständen, um seine anhaltende Eignung, Angemessenheit und Wirksamkeit sicherzustellen.
Die Managementbewertung umfasst die Berücksichtigung von:

a) dem Status von Maßnahmen aus früheren Managementbewertungen;
b) Änderungen externer und interner Themen, die für das Informationssicherheitsmanagementsystem relevant sind;
c) Feedback zur Informationssicherheitsleistung, einschließlich Trends bei:

1) Nichtkonformitäten und Korrekturmaßnahmen;
2) Überwachungs- und Messergebnisse;
3) Prüfungsergebnisse; und
4) Erfüllung der Informationssicherheitsziele;

d) Rückmeldungen von interessierten Parteien;
e) Ergebnisse der Risikobewertung und Status des Risikobehandlungsplans; und
f) Möglichkeiten zur kontinuierlichen Verbesserung.

Die Ergebnisse der Managementbewertung umfassen Entscheidungen in Bezug auf kontinuierliche Verbesserungsmöglichkeiten und den Bedarf an Änderungen am Informationssicherheitsmanagementsystem. Die Organisation muss dokumentierte Informationen als Nachweis für die Ergebnisse von Managementüberprüfungen aufbewahren.

10 Verbesserung

10.1 Nichtkonformität und Korrekturmaßnahmen: Wenn eine Nichtkonformität auftritt, muss die Organisation:

a) auf die Nichtkonformität reagieren und gegebenenfalls

1) Maßnahmen ergreifen, um sie zu kontrollieren und zu korrigieren; und
2) sich mit den Konsequenzen befassen;

b) den Handlungsbedarf zur Beseitigung der Ursachen der Nichtkonformität zu bewerten, damit sie nicht erneut auftritt oder an anderer Stelle auftritt, indem sie:

1) die Nichtkonformität überprüfen;
2) Ermittlung der Ursachen der Nichtkonformität; und
3) festzustellen, ob ähnliche Nichtkonformitäten bestehen oder möglicherweise auftreten könnten;

c) alle erforderlichen Maßnahmen zu ergreifen;
d) Überprüfung der Wirksamkeit der ergriffenen Korrekturmaßnahmen; und
e) erforderlichenfalls Änderungen am Informationssicherheitsmanagementsystem vorzunehmen.
Die Korrekturmaßnahmen müssen den Auswirkungen der festgestellten Nichtkonformitäten angemessen sein.

Die Organisation muss dokumentierte Informationen als Nachweis aufbewahren für:

f) die Art der Nichtkonformitäten und alle anschließend ergriffenen Maßnahmen und
g) die Ergebnisse von Korrekturmaßnahmen.

10.2 Kontinuierliche Verbesserung:
Die Organisation muss die Eignung, Angemessenheit und Wirksamkeit des Informationssicherheitsmanagementsystems kontinuierlich verbessern.

Erklärung zur Anwendbarkeit (SOA) ISO 27002:2022, Anhang A

A.5 Organisatorische Kontrollen

A.5.1 Richtlinien für die Informationssicherheit: Informationssicherheitsrichtlinien und themenspezifische Richtlinien sollten definiert, vom Management genehmigt, veröffentlicht, mitgeteilt und von relevanten Mitarbeitern und relevanten interessierten Parteien anerkannt und in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.

A.5.2 Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit: Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit müssen entsprechend den Bedürfnissen der Organisation definiert und zugewiesen werden.

A.5.3 Aufgabentrennung: Widersprüchliche Aufgaben und Verantwortungsbereiche sind zu trennen.

A.5.4 Verantwortlichkeiten des Managements: Das Management muss von allen Mitarbeitern verlangen, dass sie die Informationssicherheit in Übereinstimmung mit den festgelegten Informationssicherheitsrichtlinien, themenspezifischen Richtlinien und Verfahren der Organisation anwenden.

A.5.5 Kontakt mit Behörden: Die Organisation muss Kontakt zu den zuständigen Behörden herstellen und aufrechterhalten.

A.5.6 Kontakt zu speziellen Interessengruppen: Die Organisation muss Kontakte zu speziellen Interessengruppen oder anderen spezialisierten Sicherheitsforen und Berufsverbänden herstellen und pflegen.

A.5.7 Bedrohungsinformationen: Informationen zu Bedrohungen der Informationssicherheit müssen gesammelt und analysiert werden, um Bedrohungsinformationen zu erstellen.

A.5.8 Informationssicherheit im Projektmanagement: Die Informationssicherheit muss in das Projektmanagement integriert werden.

A.5.9 Inventar der Informationen und anderer zugehöriger Vermögenswerte: Ein Inventar der Informationen und anderer zugehöriger Vermögenswerte, einschließlich der Eigentümer, ist zu erstellen und zu pflegen.

A.5.10 Akzeptable Nutzung von Informationen und anderen zugehörigen Vermögenswerten: Regeln für die zulässige Verwendung und Verfahren für den Umgang mit Informationen und anderen zugehörigen Vermögenswerten müssen identifiziert, dokumentiert und umgesetzt werden.

A.5.11 Rückgabe von Vermögenswerten: Mitarbeiter und andere interessierte Parteien müssen bei Änderung oder Beendigung ihres Arbeitsverhältnisses, Vertrags oder ihrer Vereinbarung alle in ihrem Besitz befindlichen Vermögenswerte der Organisation zurückgeben.

A.5.12 Klassifizierung von Informationen: Informationen müssen gemäß den Informationssicherheitsanforderungen der Organisation auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen interessierter Parteien klassifiziert werden.

A.5.13 Kennzeichnung von Informationen: Ein geeigneter Satz von Verfahren für die Kennzeichnung von Informationen muss in Übereinstimmung mit dem von der Organisation angenommenen Informationsklassifizierungsschema entwickelt und umgesetzt werden.

A.5.14 Informationsübertragung: Regeln, Verfahren oder Vereinbarungen für die Informationsübertragung müssen für alle Arten von Übertragungseinrichtungen innerhalb der Organisation und zwischen der Organisation und anderen Parteien vorhanden sein.

A.5.15 Zugriffskontrolle: Regeln zur Kontrolle des physischen und logischen Zugriffs auf Informationen und andere zugehörige Vermögenswerte müssen auf der Grundlage von Geschäfts- und Informationssicherheitsanforderungen festgelegt und umgesetzt werden.

A.5.16 Identitätsmanagement: Der gesamte Lebenszyklus von Identitäten muss verwaltet werden.

A.5.17 Authentifizierungsinformationen: Die Zuweisung und Verwaltung von Authentifizierungsinformationen muss durch einen Verwaltungsprozess gesteuert werden, einschließlich der Beratung des Personals über den angemessenen Umgang mit Authentifizierungsinformationen.

A.5.18 Zugriffsrechte: Zugriffsrechte auf Informationen und andere zugehörige Ressourcen müssen in Übereinstimmung mit den themenspezifischen Richtlinien und Regeln der Organisation für die Zugriffskontrolle bereitgestellt, überprüft, geändert und entfernt werden.

A.5.19 Informationssicherheit in Lieferantenbeziehungen: Prozesse und Verfahren müssen definiert und implementiert werden, um die mit der Nutzung der Produkte oder Dienstleistungen des Lieferanten verbundenen Informationssicherheitsrisiken zu managen.

A.5.20 Berücksichtigung der Informationssicherheit in Lieferantenvereinbarungen: Relevante Anforderungen an die Informationssicherheit sind festzulegen und mit jedem Lieferanten auf der Grundlage der Art der Lieferantenbeziehung zu vereinbaren.

A.5.21 Management der Informationssicherheit in der IKT-Lieferkette: Es sind Prozesse und Verfahren zu definieren und umzusetzen, um die mit der Lieferkette von IKT-Produkten und -Dienstleistungen verbundenen Informationssicherheitsrisiken zu bewältigen.

A.5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen: Die Organisation muss Änderungen der Informationssicherheitspraktiken und der Servicebereitstellung von Lieferanten regelmäßig überwachen, überprüfen, bewerten und verwalten.

A.5.23 Informationssicherheit für die Nutzung von Cloud-Diensten: Prozesse für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten müssen in Übereinstimmung mit den Informationssicherheitsanforderungen der Organisation eingerichtet werden.

A.5.24 Planung und Vorbereitung des Managements von Informationssicherheitsvorfällen: Die Organisation muss das Management von Informationssicherheitsvorfällen planen und vorbereiten, indem sie Prozesse, Rollen und Verantwortlichkeiten für das Management von Informationssicherheitsvorfällen definiert, festlegt und kommuniziert.

A.5.25 Bewertung und Entscheidung über Informationssicherheitsereignisse: Die Organisation muss Informationssicherheitsereignisse bewerten und entscheiden, ob sie als Informationssicherheitsvorfälle einzustufen sind.

A.5.26 Reaktion auf Informationssicherheitsvorfälle: Auf Informationssicherheitsvorfälle muss gemäß den dokumentierten Verfahren reagiert werden.

A.5.27 Aus Informationssicherheitsvorfällen lernen: Die aus Informationssicherheitsvorfällen gewonnenen Erkenntnisse sind zur Stärkung und Verbesserung der Informations-sicherheitskontrollen zu nutzen.

A.5.28 Sammlung von Beweismitteln: Die Organisation muss Verfahren zur Identifizierung, Sammlung, Beschaffung und Sicherung von Beweismitteln im Zusammenhang mit Informationssicherheitsereignissen einrichten und umsetzen.

A.5.29 Informationssicherheit während der Störung: Die Organisation muss planen, wie die Informationssicherheit während der Störung auf einem angemessenen Niveau gehalten werden kann.

A.5.30 IKT-Bereitschaft für die Geschäftskontinuität: Die IKT-Bereitschaft muss auf der Grundlage der Ziele der Geschäftskontinuität und der IKT-Kontinuitätsanforderungen geplant, implementiert, aufrechterhalten und getestet werden.

A.5.31 Gesetzliche, gesetzliche, behördliche und vertragliche Anforderungen: Gesetzliche, gesetzliche, behördliche und vertragliche Anforderungen, die für die Informationssicherheit relevant sind, und der Ansatz der Organisation zur Erfüllung dieser Anforderungen müssen identifiziert, dokumentiert und auf dem neuesten Stand gehalten werden.

A.5.32 Rechte an geistigem Eigentum: Die Organisation muss geeignete Verfahren zum Schutz der Rechte an geistigem Eigentum einführen.

A.5.33 Schutz von Aufzeichnungen: Aufzeichnungen sind vor Verlust, Zerstörung, Verfälschung, unbefugtem Zugriff und unbefugter Freigabe zu schützen.

A.5.34 Privatsphäre und Schutz personenbezogener Daten: Die Organisation muss die Anforderungen an die Wahrung der Privatsphäre und den Schutz personenbezogener Daten gemäß den geltenden Gesetzen und Vorschriften sowie den vertraglichen Anforderungen identifizieren und erfüllen.

A.5.35 Unabhängige Überprüfung der Informationssicherheit: Der Ansatz der Organisation für das Management der Informationssicherheit und seine Implementierung, einschließlich Menschen, Prozesse und Technologien, muss in geplanten Abständen oder bei wesentlichen Änderungen unabhängig überprüft werden.

A.5.36 Einhaltung von Richtlinien, Regeln und Standards für die Informationssicherheit: Die Einhaltung der Informationssicherheitsrichtlinie der Organisation, themenspezifischer Richtlinien, Regeln und Standards muss regelmäßig überprüft werden.

A.5.37 Dokumentierte Betriebsverfahren: Betriebsverfahren für Informationsverarbeitungsanlagen müssen dokumentiert und dem Personal zur Verfügung gestellt werden, das sie benötigt.

A.6 Personenkontrollen

A.6.1 Screening: Hintergrundüberprüfungen aller Kandidaten, die zum Personal werden sollen, werden vor dem Eintritt in die Organisation und fortlaufend unter Berücksichtigung der geltenden Gesetze, Vorschriften und Ethik durchgeführt und sind proportional zu den Geschäftsanforderungen, der Klassifizierung der abzurufenden Informationen und den wahrgenommenen Risiken.

A.6.2 Beschäftigungsbedingungen: In den arbeitsvertraglichen Vereinbarungen sind die Verantwortlichkeiten des Personals und der Organisation für die Informationssicherheit festzulegen.

A.6.3 Sensibilisierung, Aus- und Weiterbildung für Informationssicherheit: Das Personal der Organisation und die relevanten interessierten Parteien müssen ein angemessenes Bewusstsein für Informationssicherheit, Aus- und Weiterbildung sowie regelmäßige Aktualisierungen der Informationssicherheitspolitik der Organisation, themenspezifischer Richtlinien und Verfahren erhalten, soweit dies für ihre berufliche Funktion relevant ist.

A.6.4 Disziplinarverfahren: Ein Disziplinarverfahren ist zu formalisieren und mitzuteilen, um Maßnahmen gegen Mitarbeiter und andere relevante interessierte Parteien zu ergreifen, die einen Verstoß gegen die Informationssicherheitsrichtlinie begangen haben.

A.6.5 Verantwortlichkeiten nach Beendigung oder Wechsel des Arbeitsverhältnisses: Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die nach Beendigung oder Wechsel des Arbeitsverhältnisses gültig bleiben, müssen definiert, durchgesetzt und dem zuständigen Personal und anderen interessierten Parteien mitgeteilt werden.

A.6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen: Vertraulichkeits- oder Geheimhaltungsvereinbarungen, die die Bedürfnisse der Organisation zum Schutz von Informationen widerspiegeln, müssen von Mitarbeitern und anderen relevanten interessierten Parteien identifiziert, dokumentiert, regelmäßig überprüft und unterzeichnet werden.

A.6.7 Remote-Arbeit: Sicherheitsmaßnahmen müssen implementiert werden, wenn Mitarbeiter aus der Ferne arbeiten, um Informationen zu schützen, auf die außerhalb der Räumlichkeiten der Organisation zugegriffen, diese verarbeitet oder gespeichert werden.

A.6.8 Meldung von Informationssicherheitsereignissen: Die Organisation muss dem Personal einen Mechanismus zur Verfügung stellen, mit dem beobachtete oder vermutete Informationssicherheitsereignisse rechtzeitig über geeignete Kanäle gemeldet werden können.

A.7 Physische Kontrollen

A.7.1 Physische Sicherheitsabgrenzungen: Sicherheitsperimeter müssen definiert und verwendet werden, um Bereiche zu schützen, die Informationen und andere zugehörige Vermögenswerte enthalten.

A.7.2 Physischer Eintritt: Sichere Bereiche müssen durch geeignete Zugangskontrollen und Zugangspunkte geschützt werden.

A.7.3 Sicherung von Büros, Räumen und Anlagen: Die physische Sicherheit von Büros, Räumen und Einrichtungen muss konzipiert und umgesetzt werden.

A.7.4 Überwachung der physischen Sicherheit: Räumlichkeiten müssen kontinuierlich auf unbefugten physischen Zugang überwacht werden.

A.7.5 Schutz vor physischen und ökologischen Bedrohungen: Der Schutz vor physischen und ökologischen Bedrohungen wie Naturkatastrophen und anderen absichtlichen oder unbeabsichtigten physischen Bedrohungen der Infrastruktur muss konzipiert und umgesetzt werden.

A.7.6 Arbeiten in Sicherheitsbereichen:
Sicherheitsmaßnahmen für die Arbeit in sicheren Bereichen müssen entworfen und umgesetzt werden.

A.7.7 Clear Desk und Clear Screen:
Klare Schreibtischregeln für Papiere und Wechselmedien sowie klare Bildschirmregeln für Informationsverarbeitungseinrichtungen sind festzulegen und in geeigneter Weise durchzusetzen.

A.7.8 Standortwahl und Schutz der Geräte: Die Ausrüstung muss sicher aufgestellt und geschützt sein.

A.7.9 Sicherheit von Vermögenswerten außerhalb von Geschäftsräumen: Ausserhalb des Standorts befindliche Vermögenswerte sind zu schützen.

A.7.10 Speichermedien: Speichermedien müssen während ihres gesamten Lebenszyklus von Erwerb, Verwendung, Transport und Entsorgung in Übereinstimmung mit dem Klassifizierungsschema und den Handhabungsanforderungen der Organisation verwaltet werden.

A.7.11 Unterstützende Dienstprogramme: Informationsverarbeitungsanlagen müssen vor Stromausfällen und anderen Störungen geschützt sein, die durch Ausfälle in unterstützenden Versorgungseinrichtungen verursacht werden.

A.7.12 Sicherheit der Verkabelung: Kabel, die Strom, Daten oder unterstützende Informationsdienste übertragen, müssen vor Abfangen, Störungen oder Beschädigungen geschützt sein.

A.7.13 Wartung der Ausrüstung: Die Ausrüstung muss korrekt gewartet werden, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen zu gewährleisten.

A.7.14 Sichere Entsorgung oder Wiederverwendung von Geräten: Geräte, die Speichermedien enthalten, müssen überprüft werden, um sicherzustellen, dass sensible Daten und lizenzierte Software vor der Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben wurden.

A.8 Technologische Kontrollen

A.8.1 Benutzer-Endgeräte: Informationen, die auf Benutzerendgeräten gespeichert, von diesen verarbeitet werden oder über Benutzerendgeräte zugänglich sind, sind zu schützen.

A.8.2 Privilegierte Zugriffsrechte: Die Zuweisung und Nutzung privilegierter Zugriffsrechte wird eingeschränkt und verwaltet.

A.8.3 Beschränkung des Informationszugangs: Der Zugang zu Informationen und anderen damit verbundenen Vermögenswerten wird im Einklang mit der festgelegten themenspezifischen Richtlinie zur Zugangskontrolle eingeschränkt.

A.8.4 Zugang zum Quellcode: Der Lese- und Schreibzugriff auf Quellcode, Entwicklungswerkzeuge und Softwarebibliotheken muss angemessen verwaltet werden.

A.8.5 Sichere Authentifizierung: Sichere Authentifizierungstechnologien und -verfahren müssen auf der Grundlage von Informationszugriffsbeschränkungen und der themenspezifischen Richtlinie zur Zugriffskontrolle implementiert werden.

A.8.6 Verwaltung der Kapazitäten: Der Ressourceneinsatz wird überwacht und entsprechend dem aktuellen und dem erwarteten Kapazitätsbedarf angepasst.

A.8.7 Schutz vor Malware: Der Schutz vor Malware muss durch ein angemessenes Bewusstsein der Benutzer implementiert und unterstützt werden.

A.8.8 Management von technischen Schwachstellen: Es müssen Informationen über technische Schwachstellen von verwendeten Informationssystemen eingeholt, die Gefährdung der Organisation durch solche Schwachstellen bewertet und geeignete Maßnahmen ergriffen werden.

A.8.9 Konfigurationsmanagement: Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken müssen eingerichtet, dokumentiert, implementiert, überwacht und überprüft werden.

A.8.10 Löschung von Informationen: Informationen, die in Informationssystemen, Geräten oder anderen Speichermedien gespeichert sind, werden gelöscht, wenn sie nicht mehr benötigt werden.

A.8.11 Maskierung von Daten: Die Datenmaskierung muss in Übereinstimmung mit der themenspezifischen Richtlinie der Organisation zur Zugriffskontrolle und anderen damit verbundenen themenspezifischen und geschäftlichen Anforderungen unter Berücksichtigung der geltenden Gesetze verwendet werden.

A.8.12 Verhinderung von Datenverlusten: Maßnahmen zur Verhinderung von Datenlecks müssen auf Systeme, Netzwerke und andere Geräte angewendet werden, die sensible Informationen verarbeiten, speichern oder übertragen.

A.8.13 Sicherung von Informationen: Sicherungskopien von Informationen, Software und Systemen sind gemäß der vereinbarten themenspezifischen Sicherungsrichtlinie zu pflegen und regelmäßig zu testen.

A.8.14 Redundanz von Informationsverarbeitungsanlagen: Informationsverarbeitungsanlagen müssen mit ausreichender Redundanz implementiert werden, um die Verfügbarkeitsanforderungen zu erfüllen.

A.8.15 Protokollierung: Protokolle, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen, müssen erstellt, gespeichert, geschützt und analysiert werden.

A.8.16 Überwachung der Aktivitäten: Netzwerke, Systeme und Anwendungen müssen auf anomales Verhalten überwacht und geeignete Maßnahmen zur Bewertung potenzieller Informationssicherheitsvorfälle ergriffen werden.

A.8.17 Synchronisierung der Uhr: Die Uhren der von der Organisation verwendeten Informationsverarbeitungssysteme müssen mit genehmigten Zeitquellen synchronisiert werden.

A.8.18 Verwendung privilegierten Dienstprogrammen: Die Verwendung von Hilfsprogrammen, die in der Lage sein können, System- und Anwendungskontrollen außer Kraft zu setzen, muss eingeschränkt und streng kontrolliert werden.

A.8.19 Installation von Software auf operativen Systemen: Es müssen Verfahren und Maßnahmen implementiert werden, um die Softwareinstallation auf Betriebssystemen sicher zu verwalten.

A.8.20 Netzwerksicherheit: Netzwerke und Netzwerkgeräte müssen gesichert, verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen zu schützen.

A.8.21 Sicherheit der Netzdienste: Sicherheitsmechanismen, Dienstniveaus und Dienstanforderungen der Netzdienste sind zu ermitteln, umzusetzen und zu überwachen.

A.8.22 Abtrennung von Netzen: Gruppen von Informationsdiensten, Benutzern und Informationssystemen sind in den Netzen der Organisation zu trennen.

A.8.23 Webfilterung: Der Zugriff auf externe Websites muss so gesteuert werden, dass die Gefährdung durch schädliche Inhalte verringert wird.

A.8.24 Einsatz der Kryptographie: Regeln für die effektive Nutzung der Kryptographie, einschliesslich der kryptografischen Schlüsselverwaltung, sind zu definieren und umzusetzen.

A.8.25 Sicherer Entwicklungslebenszyklus: Es werden Regeln für die sichere Entwicklung von Software und Systemen festgelegt und angewendet.

A.8.26 Anforderungen an die Anwendungssicherheit: Die Anforderungen an die Informationssicherheit müssen bei der Entwicklung oder dem Erwerb von Anwendungen identifiziert, spezifiziert und genehmigt werden.

A.8.27 Sichere Systemarchitektur und technische Grundsätze:
Grundsätze für die Entwicklung sicherer Systeme müssen festgelegt, dokumentiert, gepflegt und auf alle Aktivitäten zur Entwicklung von Informationssystemen angewendet werden.

A.8.28 Sichere Codierung: Die Prinzipien der sicheren Codierung müssen auf die Softwareentwicklung angewendet werden.

A.8.29 Sicherheitstests in Entwicklung und Abnahme: Sicherheitstestprozesse müssen im Entwicklungslebenszyklus definiert und implementiert werden.

A.8.30 Ausgelagerte Entwicklung: Die Organisation muss die Aktivitäten im Zusammenhang mit der ausgelagerten Systementwicklung leiten, überwachen und überprüfen.

A.8.31 Trennung von Entwicklungs-, Test- und Produktionsumgebungen: Entwicklungs-, Test- und Produktionsumgebungen müssen getrennt und gesichert sein.

A.8.32 Management von Veränderungen: Änderungen an Informationsverarbeitungseinrichtungen und Informationssystemen unterliegen Änderungsmanagementverfahren.

A.8.33 Informationen zum Test: Die Prüfinformationen sind in geeigneter Weise auszuwählen, zu schützen und zu verwalten.

A.8.34 Schutz von Informationssystemen während der Prüfung:
Auditprüfungen und andere Prüfungstätigkeiten, die eine Bewertung der operativen Systeme umfassen, sind zwischen dem Tester und der zuständigen Geschäftsleitung zu planen und zu vereinbaren.