Information Security Assessment

Herzlich Willkommen
im Information Security Assessment (ISA) des Verbandes der Automobilindustrie (VDA).

Der VDA ISA dient als Basis für
- ein Self-Assessment zur Bestimmung des Zustandes der Informationssicherheit in der Organisation (z. B. Unternehmen)
- Audits durch interne Fachabteilungen (z. B. Revision, Informationssicherheit)
- die Prüfung nach TISAX (Trusted Information Security Assessment Exchange, http://enx.com/tisax/)

Der VDA ISA besteht aus mehreren Tabellenblättern, deren Inhalt und Funktion nachfolgend erklärt wird:

Reifegrade:
Der VDA ISA sieht vor, dass die Umsetzung mittels eines Reifegrad-Modells bewertet wird, die in diesem Tabellenblatt definiert werden.
Vereinfacht sind die Reifegrade wie folgt abgestuft:
Level 0: Die Umsetzung der Anforderungen ist **unvollständig**. Es existiert kein Prozess bzw. der Prozess erreicht nicht die erforderlichen Ergebnisse.
Level 1: Die je nach Schutzbedarf der Informationen notwendigen Anforderungen sind **durchgeführt**. Ein Prozess existiert und lässt erkennen, dass er funktioniert. Er ist jedoch nicht vollständig dokumentiert. Es kann daher nicht sichergestellt werden, dass er immer funktioniert.
Level 2: Der Prozess zur Erreichung des Ziels ist **gesteuert**. Er ist dokumentiert und Nachweise (z. B. Dokumentationen) sind vorhanden.
Level 3: Der Prozess zur Erreichung des Ziels ist **etabliert**, die Prozesse sind verknüpft, um existierende Abhängigkeiten abzubilden. Die Dokumentation ist aktuell und wird gepflegt.
Level 4: Anforderungen aus Level 3, darüber hinaus finden Messungen der Ergebnisse (z. B. KPI) statt und machen den Prozess somit **vorhersagbar**.
Level 5: Anforderungen aus Level 4, darüber hinaus werden zusätzliche Ressourcen (z. B. Personal und Geld) **optimierend** eingesetzt. Es findet eine kontinuierliche Verbesserung des Prozesses statt.

Erläuterung:
Die Erläuterung enthält die Definition der Begriffe „muss“, „sollte“ und „kann“ als unterschiedliche Abstufungen innerhalb der Anforderungen in den folgenden Fragekatalogen.
Die Mindestanforderungen sind im Bereich „muss“ aufgelistet. Ohne deren Umsetzung kann das Ziel nicht erreicht werden.
In der Regel ist es notwendig, die unter „sollte“ definierten Anforderungen umzusetzen, um das Ziel zu erreichen.
Die Wahl adäquater Maßnahmen kann jedoch ebenfalls anerkannt werden, sofern das Ziel damit erreicht wird.
Je nach Unternehmensgröße und Anwendungsfall kann es nötig sein, die Anforderungen aus „kann“ umzusetzen, um das Ziel des Controls zu erreichen.
Eine weitere Besonderheit sind die Zusatzanforderungen je nach Schutzbedarf der Informationen. Grund hierfür ist die Tatsache, dass Informationen mit hohem / sehr hohem Schutzbedarf besondere Maßnahmen erfordern. Der

Deckblatt:
Das Deckblatt enthält Felder für Angaben zur anwendenden Organisation, dem Prüfbereich, dem Prüfer und dem Ansprechpartner der geprüften Organisation.
Ergebnisse:
Hier werden die Ergebnisse der einzelnen Tabellenblätter (Prüfkatalogseiten) zusammengefasst und für den Ausdruck formatiert dargestellt.
Das Spinnennetz-Diagramm dient der Übersichtsdarstellung aller Controls .
In der Auflistung aller Controls sind die anzustrebenden Zielreifegrade sichtbar.
Je nach Bedeutung der Controls variieren die Zielreifegrade zwischen Level 2 und Level 4.
Bei der Berechnung des Gesamtergebnisses werden die Ergebnisse von Controls, die den Zielreifegrad übererfüllen, gekürzt und der Durchschnitt ermittelt. Dies stellt sicher, dass die Anforderungen themenübergreifend erfüllt werden und kein Ausgleich von über- und untererfüllten Controls stattfindet.

Informationssicherheit:
Das Tabellenblatt „Informationssicherheit“ enthält alle Basis-Controls basierend auf der Norm ISO/IEC27001. Die Controls selbst sind als Frage formuliert. Die Antwort kann im zusätzlichen Feld „Beschreibung der Umsetzung“ (sichtbar durch die Erweiterung der Tabelle mit „+“) dokumentiert werden. Weiter Felder („Referenz Dokumentation“, „Feststellungen“ und „Maßnahmen“) bieten die Möglichkeit zur erweiterten Dokumentation und werden üblicherweise zur Unterstützung des Auditors genutzt.
Das Ziel des jeweiligen Controls und die Anforderungen zur Erreichung des Ziels sind in den entsprechend benannten Feldern hinterlegt. Jedes Control muss hierbei immer anhand des Grades der Erreichung des Ziels bewertet werden.
Anbindung Dritter (23):
Die hier aufgeführten Controls enthalten Zusatzanforderungen für den Fall, dass Mitarbeiter in den Räumlichkeiten der Organisation über Netzwerkanbindungen auf IT-Systeme von Dritten/Auftraggeber zugreifen.
Prototypenschutz (25):
Das Tabellenblatt Prototypenschutz enthält physische und organisatorische Anforderungen zum Schutz von Fahrzeugprototypen und wird angewendet, sofern Fahrzeugprototypen durch die Organisation bearbeitet werden.
Datenschutz (24):
Dieses Tabellenblatt ist zusätzlich bei Auftragsdatenverarbeitung nach §11 BDSG zu bearbeiten und enthält Controls, die nur mit Ja / Nein zu beantworten sind.
KPIs:
Dieses Tabellenblatt zeigt Beispiele für Key Performance Indicators (KPI) zum Messen der Prozessergebnisse sowohl für Controls, bei denen der VDA ISA einen Zielreifegrad von Level 4 definiert hat als auch für weitere Controls, bei denen eine Messung sinnvoll erscheint. Der Inhalt des Tabellenblattes dient als Hilfestellung zur Identifizierung eigener, passender KPIs. Er stellt keine verbindlichen Vorgaben zum Erreichen des Reifegrads Level 4 vor. Bei Controls, die einen Zielreifegrad von Level 3 oder weniger haben, ist die Definition von KPIs nicht zwingend notwendig, kann aber für ein zentrales Management der Informationssicherheit vieler Standorte hilfreich
Hinweise:
Dieses Tabellenblatt enthält weitere Informationen und Definition zu den Themen „Sicherheitszonen“, „Optiken“, „Personal“, „Off-Premises Arbeitsplatz“ und Schutzklassen. Die in diesem Tabellenblatt aufgeführten Themen können als Best-practice-Beispiele angesehen werden.
Glossar:
Das Glossar beschreibt Abkürzungen und weitere Begriffe.
Lizenz:
Lizenzbedingungen, unter denen der VDA ISA veröffentlicht wird.

Wir empfehlen Ihnen, mit dem Tabellenblatt „Informationssicherheit“ zu starten und sich so einen Überblick über den Stand Ihrer Informationssicherheit zu verschaffen.

Viel Erfolg wünscht die AG Audit des Arbeitskreises Informationssicherheit des VDA.

Information Security Assessment - Reifegradmodell

Erläuterung des Reifegradmodells

Die Bewertung der Reifegrade erfolgt auf Basis eines generischen Prozess-Reifegradmodells. Das Reifegradmodell unterscheidet hierbei sechs verschiedene Stufen:

- Stufe 0: Unvollständig
- Stufe 1: Durchgeführt
- Stufe 2: Gesteuert
- Stufe 3: Etabliert
- Stufe 4: Vorhersagbar
- Stufe 5: Optimierend

Den einzelnen Stufen sind die Aktivitäten zugeordnet, die dazu führen, dass die Ergebnisse systematisch erarbeitet und am Ende des Prozesses in der definierten Qualität vorliegen.

Während der Bewertung muss objektiv nachgewiesen werden, dass die Anforderungen auf der entsprechenden Stufe erfüllt werden. Dieses erfolgt zum Beispiel anhand von Arbeitsprodukten, welche als Ergebnisse aus den Prozessen der Controls hervorgehen, oder durch Aussagen der Prozessausführenden in Interviews.

Level 0: Unvollständig

Ein Prozess ist nicht implementiert oder der Prozesszweck wird nicht erreicht. Es gibt nur geringe oder keine Anzeichen dafür, dass der Prozesszweck systematisch erreicht wird.

Level 1: Durchgeführt

- Der realisierte Prozess erfüllt seinen (Prozess-) Zweck.
- Nachweislich werden die beabsichten Basispraktiken durchgeführt.
- Arbeitsergebnisse werden erzeugt, die einen Nachweis zu Prozessergebnissen bieten.

Level 2: Gesteuert

Steuerung der Prozessdurchführung (PA 2.1):

- Die Leistungsziele des Prozesses sind identifiziert.
- Die Durchführung des Prozesses wird geplant und überwacht.
- Die Durchführung des Prozesses wird zur Erfüllung des Planungen angepasst.
- Verantwortlichkeiten und Befugnisse zur Durchführung des Prozesses sind definiert, zugewiesen und kommuniziert.
- Für die Durchführung des Prozesses notwendige Resourcen und Informationen sind ermittelt, bereitgestellt, zugewiesen und weden genutzt.
- Schnittstellen zwischen betroffenen Einheiten werden gemananged, um eine effektive Kommunikation und eine klare Zuweisung von Verantwortlichkeiten sicherzustellen.

Management der Arbeitsprodukte (PA 2.2):

- Anforderungen an die Arbeitsergebnisse des Prozesses sind definiert
- Anforderungen an die Dokumentation und die Steuerung der Arbeitsergebnisse sind definiert.
- Arbeitsergebnisse werden angemessen identifiziert, dokumentiert und gesteuert.
- Arbeitsergebnisse werden in Übereinstimmung mit geplanten Maßnahmen überprüft und nötigenfalls angepasst, um die Anforderungen zu erfüllen.

Hierzu gehören u.a. folgende Dokumente (GWP):

+ Prozessdokumentation
+ Prozessplan
+ Qualitätsplan, -aufzeichnungen
+ Prozessdurchführungsaufzeichnungen

Level 3: Etabliert

Prozessdefinition (PA 3.1):
- Ein Standardprozess einschließlich in geeigneter Weise angepasste Vorgaben ist definiert, der die grundlegenenden Elemente beschreibt, die ein definerter Prozess enthalten muss.
- Die Reihenfolge und das Zusammenspiel des Standardprozesses mit anderen Prozessen sind bestimmt.
- Kompetenzen und Rollen, die zur Durchführung des Prozesses erforderlich sind, sind als Teil des Standardprozesses identifiziert.
- Infrastruktur und Arbeitsumgebung, die zur Durchführung eines Prozesses erforderlich sind, sind als Teil des Standardprozesses identifiziert.
- Geeignete Methoden sind bestimmt, um die Wirksamkeit und Angemessenheit des Prozesses zu überwachen.

Ausbringung/Verbreitung/Verteilung des Prozesses (PA 3.2):
- Ein definierter Prozess, der auf einem geeignet ausgewählten und/oder zugeschnittetnen Standardprozess basiert, ist ausgebracht/verbreitet.
- Benötigte Rollen, Verantwortlichkeiten und Befugnisse zur Durchführung des definierten Prozesses sind zugewiesen und kmmuniziert.
- Das Personal, welches den definierten Prozess durchführt, ist kompetent bzw. fachkundig, was auf einer geeigneten Ausbildung, Training und Erfahrung beruht.
- Erforderliche Ressourcen und Informationen, die zur Durchführung des definierten Prozesses erforderlich sind, sind verfügbar, zugewiesen und werden genutzt.
- Erforderliche Infrastruktur und eine Arbeitsumsumgebung, die zur Durchführung des definierten Prozesses erforderlich sind, sind verfügbar, werden gemaneged und gewartet.
- Geeignete Daten werden gesammelt und analysiert, um ein grundlegendes Verständnis für das Verhalten des Prozesses zu gewinnen, seine Angemessenheit und Wirksamkeit zu zeigen und zu bewerten, wo eine kontinuierliche Prozessverbesserung (KVP) gemacht werden kann.

Hierzu gehören u.a. folgende Dokumente (GWP):
+ Prozessdokumentation
+ Prozessplan
+ Qualitätsaufzeichnungen
+ Richtlinien und Standards
+ Prozessdurchführungsaufzeichnungen

Level 4: Vorhersagbar

Prozessmessung (PA 4.1):
- Anforderungen an Prozessinformationen zur Unterstützung von relevanten, definierten Geschäftszielen sind etabliert.
- Ziele zur Prozessmessung sind aus den Anforderungen an Prozessinformationen abgeleitet.
- Quantitative Ziele bzgl. der Prozessdurchführung zur Unterstützung von relevanten, definierten Geschäftszielen sind etabliert.
- Kennzahlen und die Häufigkeit von Messungen sind identifiziert und sind in Übereinstimmung mit den Zielen zur Prozessmessung und den quantitativen Zielen bzgl. der Prozessdurchführung definiert.
- Messergebnisse sind gesammelt, analysiert und werden berichtet, um den Grad der quantitativen Zielerreichung bzgl. der Prozessdurchführung zu überwachen.
- Messergebnisse werden dazu genutzt, die Durchführung des Prozesses zu charakterisieren.

Prozess-Steuerung (PA 4.2):
- Aanlyse- und Steuerungstechniken sind bestimmt und werden, wo zutreffend, angewendet.
- variable Steuerungsgrenzen sind zur gewöhnlichen Durchführung des Prozesses etabliert.
- Messdaten für spezielle Varianten werden analysiert
- korrigierende Maßnahmen werden durchgeführt, um spezielle Varianten zu adressieren.
- Steuerungsgrenzen werden erneut etabliert (falls erforderlich), um den korrigierenden Maßnahmen zu folgen.

Hierzu gehören u.a. folgende Dokumente (GWP):
+ Prozessdokumentation
+ Prozesssteuerungsplan
+ Prozessverbesserungsplan

Level 5: Optimierend
Prozessinnovation (PA 5.1):
- Ziele zur Prozessverbesserung sind für den jeweiligen Prozess definiert, welcher die relevanten Geschäftsziele unterstützt.
- Geeignete Daten werden analysiert, um die allgemeinen Gründe für Variantionen bei der Durchführung von Prozessen zu identifizieren.
- Geeignete Daten werden analysiert, um die Möglichkeiten für die Anwendung von Best Practices und Innovation zu identifizieren.
- Möglichkeiten zur Verbesserung, die aus neuen Technologien und neuen Prozesskonzepten abgeleitet werden, sind identifiziert.
- Eine Umsetzungsstrategie ist etabliert, um die Ziele einer Prozessverbesserung zu erreichen.

kontinuierliche Optimierung (PA 5.2):
- Die Auswirkung aller vorgeschlagenen Änderungen wird in Bezug auf die Ziele des definierten und des Standard-Prozesses bewertet.
- Die Umsetzung aller beschlossenen Änderungen wird gemanaged, um sicherzustellen, dass jegliche Unterbrechung der Durchführung eines Prozesses begriffen und darauf eingewrikt wird.
- Die Wirksamkeit einer Prozessänderung wird auf Grundlage seiner aktuellen Durchführung gegen definierte Prozessanforderungen und Prozessziele bewertet, um zu bestimmen, ob Ergebnisse mit allgemeinen oder speziellen Fällen übereinstimmen.

Hierzu gehören u.a. folgende Dokumente (GWP):

Information Security Assessment - Erläuterung der Anforderungen

Anforderungsstufen

Unterschiedlich hoher Schutzbedarf und spezielle Eigenschaften von Organisationen spiegeln sich in verschiedenen Anforderungen wieder. Bei der Beschreibung der Anforderungen zu den jeweiligen Controls werden die folgenden fünf Arten von Anforderungen unterschieden:

- Hierzu muss gehören
- Hierzu sollte gehören
- Hierzu kann gehören
- Zusätzlich bei hohem Schutzbedarf
- Zusätzlich bei sehr hohem Schutzbedarf

Die Interpretation der jeweiligen Anforderungskategorie ist wie folgt zu verstehen.

"Hierzu muss gehören"

Anforderungen der Kategorie "*Hierzu muss gehören*" sind eine strikte Anforderung, für die es keine Ausnahmen gibt.

"Hierzu sollte gehören"

Anforderungen der Kategorie "*Hierzu sollte gehören*" sind grundsätzlich durch die Organisation umzusetzen. Für Anforderungen der Kategorie "*Hierzu sollte gehören*" kann es jedoch unter bestimmten Umständen eine valide Begründung geben, diese nicht zu erfüllen. Die Auswirkungen einer Abweichung müssen durch die Organisation verstanden und eine Abweichung nachvollziehbar begründet werden.

"Hierzu kann gehören"

Anforderungen der Kategorie "*Hierzu kann gehören*" sind optional. Sie zeigen Beispiele und Möglichkeiten wie ein Control umgesetzt werden kann.

"Zusätzlich bei hohem Schutzbedarf"

Anforderungen der Kategorie "*Zusätzlich bei hohem Schutzbedarf*" müssen zusätzlich erfüllt sein, wenn der Assessment-Level einen hohen Schutzbedarf vorsieht.

"Zusätzlich bei sehr hohem Schutzbedarf"

Anforderungen der Kategorie "*Zusätzlich bei sehr hohem Schutzbedarf*" müssen zusätzlich erfüllt sein, wenn der Assessment-Level einen sehr hohen Schutzbedarf vorsieht.

Information Security Assessment - Ziele und Anforderungen

based on ISO 27001:2013

Level

Reifegrad Level: 0-5; na

Trifft eine Frage nicht zu, so ist na (not applicable) einzutragen.

1 General Aspects

1.1 **Inwieweit ist ein Information Security Management System durch die Organisationsleitung freigegeben und sein Umfang dokumentiert?**
(Referenz zu ISO 27001: 4 und 5.1)

Ziel:	Durch den Aufbau, Betrieb und die Weiterentwicklung eines Information Security Management Systems (ISMS) sowie der Benennung von Verantwortlichkeiten erfolgt eine systematische Steuerung und Kontrolle der Informationssicherheit innerhalb des festgelegten Anwendungsbereiches. Das ISMS definiert Prozesse und Verfahren, damit die Informationssicherheitsziele hinsichtlich einer angemessenen Vertraulichkeit, Verfügbarkeit und Integrität der Unternehmenswerte auf Basis der Sicherheitspolitik erreicht werden.
Anforderungen:	Hierzu muss gehören: + Die Anforderungen der Organisation an ein ISMS sind ermittelt. + Ein durch die Organisationsleitung freigegebenes ISMS ist etabliert. + Der Geltungsbereich (Scope) des ISMS ist festgelegt (z. B. gesamte Organisation, Teilbereiche). + Eine Anwendbarkeitserklärung (Statement of Applicability, SoA) ist vorhanden (z. B. ausgefüllter VDA ISA Katalog). Hierzu sollte gehören: + Kriterien (z. B. Kennzahlen oder -größen) zur Bewertung der Informationssicherheit sind festgelegt. Hierzu kann gehören: + Zertifizierung nach ISO27001:2013 (inklusive Scope Statement und SoA). Zusätzlich bei hohem Schutzbedarf: Keine. Zusätzlich bei sehr hohem Schutzbedarf: Keine.

1.2 **Inwieweit ist ein Prozess zur Identifikation, Bewertung und Behandlung von Informationssicherheits-Risiken definiert, dokumentiert und umgesetzt?**
(Referenz zu ISO 27001: 8.2 und 6.1.2)

Ziel:	Ziel eines auf die Organisation zugeschnittenen ISMS ist es, dass die Aufwände für die Informationssicherheit in einem angemessenen Verhältnis zu den zu schützenden Werten stehen. Um dies zu erreichen, müssen in einem Risikomanagement die Werte, deren Schutzbedarf und Bedrohungen identifiziert, analysiert, bewertet und dokumentiert werden. Bei einem fehlenden Informationssicherheits-Risikomanagement besteht die Gefahr, dass Informationssicherheitsrisiken unentdeckt bleiben und ein Schaden entstehen kann. Bei einem fehlenden Informationssicherheits-Risikomanagement besteht die Gefahr, dass Informationssicherheitsrisiken unentdeckt bleiben und ein Schaden entstehen kann.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Risikobeurteilungen werden sowohl regelmäßig als auch anlassbezogen durchgeführt.
+ Informationssicherheitsrisiken werden gemäß Schutzbedarf in die Stufen z.B. normal, hoch und sehr hoch eingeteilt.
+ Bei Änderung des Umfelds (z. B. Organisationsstruktur, Standort, Änderung von Regelwerken) erfolgt eine zeitnahe Neubewertung.

Hierzu sollte gehören:
+ Es existiert eine Prozessbeschreibung, wie Informationssicherheitsrisiken innerhalb der Organisation identifiziert, bewertet und beurteilt werden.
+ Kriterien für die Beurteilung und Behandlung sowie Akzeptanz von Informationssicherheitsrisiken sind vorhanden.
+ Die identifizierten Informationssicherheitsrisiken inklusive Ursache, Eintrittswahrscheinlichkeit, möglicher Auswirkungen und deren Bewertung sind dokumentiert.
+ Maßnahmen zur Risikobehandlung und deren Verantwortliche sind festgelegt und dokumentiert.
- Es existiert ein Maßnahmenplan bzw. Statusübersicht der Maßnahmenumsetzung.

Hierzu kann gehören:
+ Es existiert eine Übersicht über die fachlichen Ansprechpartner (Risikoeigentümer).

zusätzlich bei hohem Schutzbedarf:
Keine.

zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 1.3 **Inwieweit wird die Wirksamkeit des ISMS sichergestellt?**
(Referenz zu ISO 27001: 8.1, 9.1, 10.1 und 10.2)

Ziel:

Das ISMS ist in regelmäßigen Abständen (z.B. jährlich) hinsichtlich seiner Wirksamkeit zu überprüfen. Dies beinhaltet die Überprüfung der Zielerreichung und der Konformität hinsichtlich der gültigen Anforderungen.
Ein ISMS kann nur dann seinen Zweck erfüllen, wenn es auf die Anforderungen der Organisation zugeschnitten ist. Da sich Einflussfaktoren wie z. B. Organisationsstruktur oder Standortbedingungen ändern können, ist die Wirksamkeit des ISMS regelmäßig zu prüfen.

Anforderungen:

Hierzu muss gehören:
+ Es finden regelmäßig Wirksamkeitsprüfungen durch die Verantwortlichen für Informationssicherheit und das Management statt.
+ Die Ergebnisse der Wirksamkeitsprüfung sowie der festgelegten Maßnahmen sind dokumentiert.
+ Ein Maßnahmenplan bzw. eine Statusübersicht der Maßnahmenumsetzung (auch aus vorher durchgeführten Prüfungen) ist vorhanden, die Umsetzung der Maßnahmen wird überwacht.
+ Eventuell auftretende Sicherheitsereignisse werden analysiert.

Hierzu sollte gehören:
+ Es erfolgt eine regelmäßige Überprüfung des ISMS auf Angemessenheit und Zweckmäßigkeit.
+ Die Dokumentation wird regelmäßig auf ihre Aktualität hin geprüft und überarbeitet.

Hierzu kann gehören:
Keine.

zusätzlich bei hohem Schutzbedarf:
Keine.

zusätzlich bei sehr hohem Schutzbedarf:
Keine.

Information Security Assessment - Ziele und Anforderungen

5 Information Security Policies

☐ 5.1 **Inwieweit ist eine Richtlinie zur Informationssicherheit erstellt, veröffentlicht bzw. verteilt und wird sie in regelmäßigen Zeitabständen überprüft?**
(Referenz zu ISO 27001: Control A5.1.1 und A5.1.2)

Ziel:	Eine Organisation muss eine Richtlinie definieren, welche die Wichtigkeit und Bedeutung von Informationssicherheit für die Organisation widerspiegelt. Diese muss auf die Geschäftsstrategie, Vorschriften, Gesetze und potenzielle Bedrohungslagen der Informationssicherheit angepasst sein. Alle Beteiligten müssen erkennen können, dass Informationssicherheit von der Organisationsleitung unterstützt wird, jeden betrifft und es Vorgaben und Regeln gibt, die eingehalten werden müssen.
Anforderungen:	<u>Hierzu muss gehören:</u> + Die Anforderungen an die Informationssicherheit, angepasst an die Ziele des Unternehmens, im Hinblick auf den Schutz von Informationen sind in einer Richtlinie dokumentiert und von der Organisationsleitung freigegeben. + Die Richtlinie enthält Ziele und den Stellenwert der Informationssicherheit in der Organisation. <u>Hierzu sollte gehören:</u> + Die Anforderungen an die Informationssicherheit auf der Grundlage der Organisationsstrategie, Gesetzen und Verträgen sind in der Richtlinie berücksichtigt. + Verantwortlichkeiten für die Durchführung sind definiert. + Die Richtlinie weist auf Konsequenzen bei Nichtbeachtung hin. + Weitere Richtlinien/Regelungen/Informationssicherheitsstandards zur Informationssicherheit sind erstellt. + Ein Prozess zur regelmäßigen Prüfung und Überarbeitung der Richtlinien ist etabliert. + Die Richtlinien werden Mitarbeitern geeignet zur Verfügung gestellt. + Die Richtlinien werden fallbezogen (ggf. auch in Auszügen) an externe Geschäftspartner weitergegeben. <u>Hierzu kann gehören:</u> + Die Richtlinien sind im Intranet bereitgestellt. <u>Zusätzlich bei hohem Schutzbedarf:</u> Keine. <u>Zusätzlich bei sehr hohem Schutzbedarf:</u> Keine.

6 Organization of Information Security

☐ 6.1 **Inwieweit sind die Verantwortlichkeiten für Informationssicherheit definiert und zugewiesen?**
(Referenz zu ISO 27001: Control A6.1.1)

Ziel:	Um ein ISMS erfolgreich umsetzen zu können, müssen die Verantwortlichkeiten für Informationssicherheit in geeigneter Weise geregelt sein. Hierfür sind Funktionen zu definieren, die die Aufgaben zur Erreichung der Schutzziele wahrnehmen. Für die Erfüllung der Aufgaben sind qualifizierte Mitarbeiter notwendig, die den Mitarbeitern der Organisation und ggf. auch Geschäftspartnern bekannt sind.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Verantwortlichkeiten für die Informationssicherheit in der Organisation sind definiert, dokumentiert und zugewiesen.
+ Die verantwortlichen Mitarbeiter sind definiert und für ihre Aufgabe qualifiziert.
+ Die Ansprechpartner sind innerhalb der Organisation und relevanten Geschäftspartnern bekannt.

Hierzu sollte gehören:
+ Es existiert eine Definition und Dokumentation einer geeigneten Informationssicherheitsstruktur in der Organisation.

Hierzu kann gehören:
+ Veröffentlichung der Verantwortlichkeiten und Ansprechpartner für Informationssicherheit an Mitarbeiter und externe Geschäftspartner, wenn dies zur Erfüllung der übertragenen Aufgabe(n) erforderlich ist.

Zusätzlich bei hohem Schutzbedarf:
+ Eine angemessene organisatorische Trennung von Verantwortlichkeiten sollte zur Vermeidung von Interessenskonflikten etabliert sein.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 6.2 **Inwieweit werden in Projekten, unabhängig von ihrer Art, Anforderungen an die Informationssicherheit berücksichtigt?**
(Referenz zu ISO 27001: Control A6.1.5)

Ziel: Die Anforderungen an die Informationssicherheit werden unabhängig von der Art des Projektes (auch Nicht IT-Projekte) berücksichtigt. Dies beinhaltet auch den Umgang mit Informationssicherheit und Informationssicherheitsrisiken in den Projektmanagementmethoden der Organisation.

Anforderungen:

Hierzu muss gehören:
+ Projekte sind unter Berücksichtigung ihrer Anforderungen an die Informationssicherheit zu klassifizieren.

Hierzu sollte gehören:
+ Die Vorgehensweise und Kriterien zur Klassifizierung von Projekten sind dokumentiert.
+ In frühen Projektphasen werden Risikobewertungen auf Basis der definierten Vorgehensweise durchgeführt.
+ Für identifizierte Informationssicherheitsrisiken (siehe Control 1.2) werden Maßnahmen abgeleitet und im Projekt berücksichtigt.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
+ Abgeleitete Maßnahmen werden im Projektverlauf regelmäßig überprüft und bei Änderungen der Bewertungskriterien neu bewertet.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 6.3 **Inwieweit gibt es eine Richtlinie zur Nutzung von mobilen Endgeräten und deren Remote Zugriff auf Daten der Organisation?**
(Referenz zu ISO 27001: Control A6.2.1 und A6.2.2)

Ziel: Der Umgang mit mobilen Endgeräten - insbesondere in ungeschützten Umgebungen - ist mit erhöhten Risiken verbunden (z. B. Verlust, Diebstahl, Infektion mit Malware). Damit die auf dem Gerät abgelegten Informationen geschützt sind, müssen technische Schutzmaßnahmen umgesetzt werden. Weiterhin sollten die Mitarbeiter auf die Gefahren im Umgang mit mobilen Endgeräten sensibilisiert werden.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Die Nutzung von mobilen Endgeräten (z. B. Smartphones, Notebooks) ist geregelt.

Hierzu sollte gehören:
+ Eine Richtlinie unter Berücksichtigung der folgenden Aspekte ist erstellt:
  - Registrierung mobiler Endgeräte
  - Anforderungen an den physischen Schutz (u. a. gegen Diebstahl, Ausspähen von Informationen)
  - Einschränkungen bei der Installation von Software
  - Anforderungen an die Versionierung von Software für mobile Endgeräte und das zugehörige Patch-Management
  - Zugangsbeschränkungen zu bestimmten Informationsdiensten
  - Verschlüsselungstechniken
  - Datensicherung (Backup)
  - Schutz vor Schadsoftware
  - Remote Löschverfahren
  - Nutzung von Web-Services und Web Apps
  - Verfahren bei Verlust des mobilen Endgeräts
+ Unterzeichnung einer Verpflichtungserklärung durch die Nutzer zum Umgang mit Besonderheiten bei der Arbeit mit mobilen Endgeräten in Abhängigkeit des Schutzbedarfs, wie z. B. Diebstahlschutz, Installation von Software, Verhinderung der Einsehbarkeit auf Informationen selbst (Sichtschutz), Verwendung einer geschützten Umgebung (z.B. geschlossener Raum, kein öffentlicher Ort), Umgang mit Authentifizierungsmitteln.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 6.4 **Inwieweit sind die gemeinsamen Rollen und Verantwortlichkeiten zwischen IT-Dienstanbietern (insbes. Cloud Providern) und der eigenen Organisation definiert?**
(Referenz zu ISO 27017: Control CLD.6.3.1)

Ziel:

Bei der Nutzung von IT-Diensten (insbesondere Cloud-Diensten) hat das Verhältnis zwischen Anbieter und eigener Organisation in Bezug auf die Informationssicherheit eine besondere Bedeutung, da die Umsetzungsverantwortung der Anforderungen geteilt wird. Die eigene Organisation muss Teile der Sicherheitsanforderungen weiterhin eigenverantwortlich umsetzen, während andere Anforderungen komplett oder in Teilen durch den Anbieter umgesetzt werden. Wie genau die Verantwortung geteilt ist, ist immer von dem genutzten Dienst abhängig und nicht pauschal zu beantworten.

Wenn kein gemeinsames Verständnis bei allen beteiligten Parteien über die Verantwortungsteilung existiert, kann das Sicherheitssystem geschwächt oder ganz ausgehebelt werden. Der Nutzer von Diensten muss daher zu jeder Zeit sicherstellen, dass ein gemeinsames Verständnis der Verantwortungsverteilung existiert und für jede Anforderung geklärt ist, das und von wem diese umgesetzt wird.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Die für den Dienst relevanten Sicherheitsanforderungen sind erhoben und dokumentiert:
 - Mindestens die Anwendbarkeit der Controls des VDA ISA wurde geprüft und dokumentiert.
+ Für jede Anforderung ist dokumentiert, wer für die Umsetzung in wie weit verantwortlich ist.
 - Für die anwendbaren Controls des VDA ISA wurde dokumentiert, wer die Verantwortung für die Umsetzung trägt bzw. wie sie aufgeteilt ist.
+ Die eigene Organisation wird ihren Verantwortlichkeiten gerecht.
+ Es liegen Nachweise vor, dass der Dienstanbieter seiner Verantwortlichkeit gerecht wird.

Hierzu sollte gehören:
+ Die Dienstkonfiguration wurde anhand der notwendigen Sicherheitsanforderungen konzipiert, umgesetzt und dokumentiert.
+ Die Dienstkonfiguration ist in die regelmäßigen Sicherheitsprüfungen einbezogen.
+ Integration in lokale Schutzmaßnahmen (wie z.B. sichere Authentisierungsmechanismen) ist etabliert und dokumentiert.
+ Das Personal ist (z.B. in Hinsicht auf sicheren Betrieb und Konfiguration, sicheren Umgang mit Daten anhand ihrer Klassifikation, Bewusstsein über Gefahren, Umgang mit Incidents) geschult.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

7 Human Resources Security

☐ 7.1 **Inwieweit werden Mitarbeiter vertraglich zur Einhaltung der Richtlinien zur Informationssicherheit verpflichtet?**
(Referenz zu ISO 27001: Control A7.1.2 und A7.3.1)

Ziel: Für Organisationen gelten Gesetze, Vorschriften und interne Regelungen. Bereits bei der Einstellung von Mitarbeitern muss sichergestellt werden, dass sich sowohl interne als auch externe Mitarbeiter zur Einhaltung der Richtlinien verpflichten und die Konsequenzen eines Fehlverhaltens bekannt sind.

Anforderungen:

Hierzu muss gehören:
+ Es besteht eine Verpflichtung zur Geheimhaltung - auch über das Arbeitsverhältnis bzw. den Auftrag hinaus.
+ Es besteht eine Verpflichtung zur Einhaltung der Richtlinien zur Informationssicherheit (siehe 5.1)

Hierzu sollte gehören:
+ Aspekte der Informationssicherheit sind in den Arbeitsverträgen der Mitarbeiter berücksichtigt.
+ Die Verantwortlichkeiten und Pflichten für den Umgang mit sensiblen Informationen sind im Arbeitsvertrag verankert.
+ Eine Vorgehensweise bei Verstößen gegen vertragliche Inhalte mit Informationssicherheitsrelevanz ist beschrieben.
+ Mitarbeiter werden über Änderungen von Richtlinien informiert.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

Information Security Assessment - Ziele und Anforderungen

7.2 **Inwieweit werden Mitarbeiter über die Risiken beim Umgang mit Informationen und deren Verarbeitung geschult und sensibilisiert?**
(Referenz zu ISO 27002: Control 7.2.1 und 7.2.2)

Ziel: Informationssicherheit muss von allen Mitarbeitern als selbstverständlicher Teil ihrer Arbeitsumgebung verinnerlicht und gelebt werden. Durch Schulungen zur Informationssicherheit müssen die Mitarbeiter die notwendigen Kenntnisse und Kompetenzen für sicherheitsbewusstes Verhalten erwerben. Insbesondere muss ihnen bekannt sein, was von ihnen im Hinblick auf Informationssicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollten.

Anforderungen:

Hierzu muss gehören:
+ Mitarbeiter sind geschult und sensibilisiert.

Hierzu sollte gehören:
+ Ein Konzept zur Sensibilisierung und Schulung der Mitarbeiter ist erstellt.
- Zielgruppen für Schulungs- und Sensibilisierungsmaßnahmen (z. B. neue Mitarbeiter, Administratoren) sind definiert und im Schulungskonzept berücksichtigt.
+ Das Konzept wurde vom verantwortlichen Management freigegeben
- Für die Durchführung notwendige Ressourcen sind freigegeben
+ Schulungs- und Sensibilisierungsmaßnahmen werden sowohl regelmäßig als auch anlassbezogen durchgeführt.
+ Die Teilnahme an Schulungs- und Sensibilisierungsmaßnahmen wird dokumentiert.
+ Mitarbeitern sind die Ansprechpartner zur Informationssicherheit bekannt.
+ Geeignete KPIs zur Sensibilisierung- und Schulung sind definiert und werden ausgewertet.

Hierzu kann gehören:
+ Es erfolgt eine regelmäßige Lernzielkontrolle über durchgeführte Sensibilisierungen und Schulungen von Teilnehmern.
+ Der Lernerfolg von Sensibilisierungs- und Schulungsprogrammen wird quantitativ und qualitativ überprüft.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

8 Asset Management

8.1 **Inwieweit gibt es Verzeichnisse für Werte (Assets), die Informationen in verschiedenen Ausprägungen enthalten?**
(Referenz zu ISO 27001: Control A8.1.1, A8.1.2, A8.1.3 und A8.1.4)

Ziel: Neben der klassischen Inventarisierung von physischen Gegenständen ist es wichtig, eine Übersicht über die innerhalb der Organisation verarbeiteten Informationen zu erhalten. Information-Assets sind hierbei Elemente mit Informationscharakter, wie z. B. Dokumente, Bilder, Dateien, Programme, Server, Netze, Einrichtungen, Fahrzeug-Prototypen, Werkzeuge und Vorrichtungen. Ein Informationseigentümer übernimmt die Rolle des Verantwortlichen für einzelne Information-Assets.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Jedem Information-Asset ist ein Verantwortlicher (Einzelperson oder organisatorische Einheit) zugeordnet.
+ Information-Assets sind klassifiziert. (siehe hierzu auch Control 8.2)

Hierzu sollte gehören:
+ Verzeichnisse über die Information-Assets sind erstellt und werden regelmäßig aktualisiert.
+ Der Lebenszyklus der Information-Assets über die Phasen der Erstellung, Verarbeitung, Speicherung oder Lagerung, Übertragung und Löschung bzw. Vernichtung ist definiert.
+ Regelungen für die Rückgabe von Information-Assets bei Verlassen der Organisation oder Auslauf eines Vertrags sind vorhanden.

Hierzu kann gehören:
+ Regeln für eine zulässige Nutzung von Information-Assets ("acceptable use policy") liegen vor.
+ Information-Assets können ggf. in Gruppen (z.B. Arbeitsplatzrechner) zusammengefasst werden.

Zusätzlich bei hohem Schutzbedarf:
+ Eine Festlegung zur expliziten Genehmigung der Nutzung eines Information-Assets ist definiert.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 8.2 **Inwieweit werden Informationen hinsichtlich ihres Schutzbedarfs eingestuft und gibt es Regeln für Kennzeichnung, Handhabung, Transport, Speicherung, Lagerung, Löschung und Entsorgung?**

(Referenz zu ISO 27001: Control A8.2.1, A8.2.2 und A8.2.3)

Ziel: Informationen sind in Abhängigkeit ihres Wertes für eine Organisation einzustufen. Bei dieser Bewertung muss der Wert der Informationen für die Organisation auf Basis von Faktoren wie Vertraulichkeit, Integrität und Verfügbarkeit bewertet werden. Der Umgang mit Informationen in Abhängigkeit von ihrer Klassifizierung muss definiert sein und von den Mitarbeitern angewendet werden.

Anforderungen:

Hierzu muss gehören:
+ Ein einheitliches Schema zur Klassifizierung von Unterlagen/Informationen ist vorhanden und wird angewendet.

Hierzu sollte gehören:
+ Die Einstufung von Informationen erfolgt nach definierten Kriteren, z.B. Wert, gesetzlicher Anforderungen, Vertraulichkeit, Integrität und Verfügbarkeit.
+ Eine Richtlinie mit Vorgaben für die Klassifizierung von Informationen und den jeweiligen Schutzmaßnahmen zur Kennzeichnung, Handhabung, Transport, Speicherung, Lagerung, Löschung und Entsorgung ist vorhanden und wird angewendet.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 8.3 **Inwieweit ist ein angemessener Umgang mit gespeicherten Informationen auf mobilen Datenträgern geregelt?**
(Referenz zu ISO 27001: Control A8.3.1, A8.3.2 und A8.3.3)

Ziel: Informationen auf mobilen Datenträgern sind in der Regel erhöhten Risiken ausgesetzt. Damit Informationen nicht durch Verlust oder Diebstahl eines Datenträgers verloren gehen, müssen Regelungen zur Reduzierung dieser Risiken definiert und Maßnahmen getroffen werden.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
Keine.

Hierzu sollte gehören:
+ Definition von Regeln zum Umgang mit Informationen auf mobilen Datenträgern unter Berücksichtigung ihrer Klassifizierung. Hierzu zählen die Punkte: Löschung, Weitergabe, Entsorgung sowie Schutzmaßnahmen.
+ Daten auf mobilen Datenträgern sind gemäß definierter Regeln unter Berücksichtigung der Klassifizierung zu schützen.

Hierzu kann gehören:
+ Hilfsmitteln für den Mitarbeiter zur Einhaltung der Regeln werden durch die Organisation bereitgestellt.

Zusätzlich bei hohem Schutzbedarf:
+ Es muss ein Verfahren etabliert sein, wie Mitarbeiter im Fall eines Verlustes vorzugehen haben.
+ Regelungen für den Umgang auf (Dienst-) Reisen im In- und Ausland, z. B. bei Einsichtnahme durch Behörden sind definiert.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 8.4 **Inwieweit wird das sichere Entfernen von Information-Assets aus den IT-Diensten (insbes. Cloud) gewährleistet?**
(Referenz zu ISO 27017: Control CLD.8.1.5)

Ziel: Es muss sichergestellt werden, dass bekannt ist, wie die Nutzung eines Dienstes geregelt beendet werden kann. Hierbei ist insbesondere zu beachten, wie die Informationen sicher von fremden Systemen (z.B. Cloud-Systemen) wieder entfernt werden können.

Anforderungen:

Hierzu muss gehören:
+ Eine Ausstiegsstrategie (Terminierungsprozess), welche das Löschen und Entfernen der Assets aus dem Cloud-Dienst umfasst, ist definiert.
+ Es ist sichergestellt, dass der Anbieter seinen Verantwortlichkeiten gerecht werden wird.

Hierzu sollte gehören:
+ Die Erfüllung der Verantwortlichkeiten des Anbieters ist vertraglich geregelt.
+ Eine Beschreibung des Terminierungsprozesses liegt vor und wird regelmäßig überprüft.
+ Die im Prozess vorgesehenen Verantwortlichkeiten ist dokumentiert und vom Anbieter anerkannt.

Hierzu kann gehören:
+ Die Verantwortlichkeiten werden anhand der vom Anbieter zugänglich gemachten Dienstdokumentation erhoben und dokumentiert.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

9 Access Control

☐ 9.1 **Inwieweit sind Regelungen und Verfahren bezüglich dem Zugang zu IT-Systemen vorhanden?**
(Referenz zu ISO 27001: Control A9.1.2)

Ziel: Die Identität des Benutzers eines Netzwerkdienstes, IT-Systems bzw. einer IT-Anwendung muss sicher festgestellt werden können, um Handlungen eindeutig zuordnen zu können. Um dies zu gewährleisten, müssen Authentifizierungsverfahren (Anmeldeverfahren) und -mechanismen von IT-Systemen bzw. IT-Anwendungen so gestaltet sein, dass Benutzer eindeutig identifiziert und authentifiziert werden.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Die eingesetzten Verfahren zur Benutzerauthentifizierung gelten als sicher und entsprechen dem aktuellen Stand der Technik.
+ Die Auswahl der Verfahren zur Benutzerauthentifizierung wurde auf Basis einer Risikobewertung getroffen. Mögliche Angriffsszenarien wurden berücksichtigt (z. B. direkte Zugriffsmöglichkeit aus dem Internet)
+ Weitere Interaktionen dürfen nur nach einer erfolgreichen Authentifizierung möglich sein.

Hierzu sollte gehören:
+ Eine Richtlinie auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen ist erstellt und dokumentiert.
+ Abhängig von der Kritikalität der verarbeiteten Informationen in den IT-Systemen bzw. IT-Anwendungen werden geeignete und sichere Authentifizierungsverfahren gefordert und eingesetzt.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
+ Daten mit hohem Schutzbedarf sind mindestens durch starke Passworte, nach Stand der Technik, abzusichern.
+ Abhängig von der Risikobewertung wurde das Authentifizierungsverfahren durch ergänzende Maßnahmen verstärkt
(z. B. dauerhaftes Monitoring der Zugriffe auf Unregelmäßigkeiten oder Einsatz einer starken Authentifizierung)

Zusätzlich bei sehr hohem Schutzbedarf:
+ Daten mit sehr hohem Schutzbedarf sind durch starke Authentifizierung (z. B. 2-Faktor-Authentifizierung) abzusichern.

☐ 9.2 **Inwieweit sind Verfahren zur Registrierung, Änderung und Löschung von Benutzern mit den zugehörigen Zugriffsrechten umgesetzt und erfolgt dabei insbesondere ein vertraulicher Umgang mit den Anmeldeinformationen?**
(Referenz zu ISO 27001: Control A9.2.1, A9.2.2, A9.2.4 und A9.2.5)

Ziel: Durch die Verwendung eindeutiger und personalisierter Benutzerkennungen (Benutzerkonten) wird gewährleistet, dass Handlungen eindeutig nachvollziehbar sind. Die Anmeldeinformationen (z. B. Passwörter) dürfen nur dem berechtigten Benutzer bekannt sein. Für den Lifecycle von Benutzerkonten sind definierte Prozesse vorhanden. Es erfolgt eine regelmäßige Überprüfung der vorhandenen Benutzerkonten auf ihre Notwendigkeit.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Der Management-Prozess für Benutzerkennungen ist dokumentiert und etabliert.
+ Die Verwendung von eindeutigen und personalisierten Benutzerkonten ist festgelegt.
+ Die Nutzung von "Sammel-Konten" ist geregelt (z. B. eingeschränkt, nur wenn auf den Nachweis der Handlungen verzichtet werden kann).
+ Benutzerkonten werden unmittelbar nach Verlassen des Unternehmens bzw. Ausscheiden aus dem Unternehmen (z. B. nach Ende des Arbeitsvertrags) gesperrt.
+ Es erfolgt eine sichere Zustellung der Anmeldeinformationen für Benutzer.

Hierzu sollte gehören:
+ Ein Basis-Benutzerkonto mit minimalen Zugriffsrechten und Funktionalitäten ist vorhanden und wird angewendet.
+ Die Vergabe der Basis-Zugriffsrechte und die Einrichtung von Benutzerkonten erfolgt durch die verantwortliche Stelle oder ist durch diese autorisiert.
+ Die Einrichtung von Benutzerkonten unterliegt einem Genehmigungsprozess (4-Augen-Grundsatz).
+ Sperrung der Benutzerkonten von Dienstleistern nach Beendigung der Aufgabe.
+ Sperr- und Löschfristen für Benutzerkonten sind definiert.
+ Abgestimmte Änderung der Benutzerkonten eines Anwenders nach dessen Wechsel in einen anderen Bereich.
+ Für die Übergabe von Anmeldeinformationen sind sichere Prozesse etabliert.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 9.3 **Inwieweit ist die Zuweisung sowie die Nutzung von privilegierten Benutzer- und technischen Konten geregelt und wird diese überprüft?**
(Referenz zu ISO 27001: Control A9.2.3)

Ziel: Durch die Verwendung eindeutiger und personalisierter administrativer Benutzerkonten wird gewährleistet, dass administrative Handlungen eindeutig nachvollziehbar sind. Administratoren dürfen für administrative Aufgaben nur das Benutzerkonto verwenden, welchem privilegierte Rechte zugewiesen sind und müssen für alle sonstigen Tätigkeiten (z. B. E-Mail, Internet) ihr Standard Benutzerkonto nutzen. So soll gewährleistet werden, dass nur Tätigkeiten, die privilegierte Rechte benötigen, auch in diesem Kontext ausgeführt werden.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Die Verwendung von eindeutigen und personalisierten administrativen Benutzerkonten ist geregelt und etabliert.
+ Eine Unterscheidung der Benutzerkonten (privilegiertes Benutzerkonto, "Office-Benutzerkonto") ist gewährleistet, z. B. durch den Besitz zweier oder mehrerer Benutzerkonten.
+ Der Management-Prozess(Vergabe/Änderung/Löschung) für privilegierte Benutzerkennungen ist dokumentiert und etabliert.
+ Die Vergabe von privilegierten Rechten erfolgt erst nach Genehmigung.
+ Es werden sichere Authentifizierungsverfahren für privilegierte Benutzerkonten verwendet.
+ Benutzerkonten mit privilegierten Rechten sind dokumentiert und werden regelmäßig überprüft.

Hierzu sollte gehören:
+ Eine Identifizierung der relevanten bzw. betroffenen IT-Systeme ist erfolgt und dokumentiert.
+ Die Vergabe von Rechten erfolgt bedarfsorientiert und entsprechend der Rolle und/oder Verantwortungsbereich (Beachtung der Funktionstrennung).
+ Folgende Punkte sind bei der Überprüfung der vergebenen privilegierten Rechte zu berücksichtigen:
  - Es erfolgt eine regelmäßige Überprüfungen von privilegierten Zugriffsrechten (angemessener Zeitraum z.B. vierteljährlich)
  - Die Überprüfungen werden dokumentiert
  - Veränderungen des Aufgabengebietes werden sofort berücksichtigt

Hier kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 9.4 **Inwieweit gibt es verbindliche Regeln für den Anwender zur Erstellung und im Umgang mit vertraulichen Anmeldeinformationen?**
(Referenz zu ISO 27001: Control A9.3.1 und A9.4.3)

Ziel: Werden in einem IT-System oder einer Anwendung Anmeldeinformationen verwendet, so ist die Informationssicherheit entscheidend von einem korrekten Gebrauch dieser Anmeldeinformationen (z. B. Passworte, PINs) abhängig. Daher ist es wichtig, dass Benutzer regelmäßig in Bezug auf den richtigen Umgang mit diesen Anmeldeinformationen sensibilisiert werden.

Anforderungen:

Hierzu muss gehören:
+ Eine Regelung zum Umgang mit Anmeldeinformationen ist erstellt und berücksichtigt mindestens folgende Aspekte:
  - keine Weitergabe von Anmeldeinformationen an Dritte - auch nicht an Autoritätspersonen - unter Beachtung gesetzlicher Rahmenbedingungen
  - kein Notieren von Anmeldeinformationen oder unverschlüsselte Speicherung
  - sofortige Änderung der Anmeldeinformation bei Verdacht auf mögliche Kompromittierung
  - keine Verwendung von identischen Anmeldeinformationen für geschäftliche und nicht-geschäftliche Nutzung
  - Änderung von temporären oder Initial-Anmeldeinformationen nach dem 1. Login
  - Vorgaben für die Qualität von Anmeldeinformationen (z. B. Passwort-Länge, zu verwendende Zeichenarten).

Hierzu sollte gehören:
+ Anwender werden in Bezug auf die Regelungen (z. B. Passwortregeln) informiert und sensibilisiert.
+ Die Verwendung von Standard-Passworten wird technisch verhindert.
+ Beim Einsatz einer starker Authentifizierung wird das Medium (z. B. Faktor Besitz) sicher verwendet.

Hierzu kann gehören:
+ Hilfsmitteln zur sicheren Verwahren von Anmeldeinformationen (z. B. Passwort Safe) werden bereitgestellt.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

Information Security Assessment - Ziele und Anforderungen

9.5 **Inwieweit wird der Zugriff auf Informationen und Applikationen auf berechtigte Personen eingeschränkt?**

(Referenz zu ISO 27001: Control A9.4.1 und A9.4.2)

Ziel:	Durch die Autorisierung muss sichergestellt werden, dass nur berechtigte Benutzer auf Informationen und IT-Anwendungen (Applikationen) zugreifen können. Hierzu werden dem Benutzer Zugriffsberechtigungen zugewiesen und regelmäßig überprüft.
Anforderungen:	Hierzu muss gehören: + Die Anforderungen an den Zugriff auf Informationen und Applikationen sind ermittelt. + Eine Richtlinie zur Autorisierung ist erstellt und enthält mindestens folgende Aspekte: - Verfahren zur Beantragung, Prüfung und Genehmigung - Verwendung von Berechtigungs-Rollen - Funktionstrennung - Anwendung des Minimalitätsprinzips ("Need-to-know") + Die Richtlinie ist für alle Benutzer von Informationen und Applikationen bindend. + Es findet eine regelmäßige Überprüfung der gewährten Zugriffsrechte von Benutzern und technischen Konten statt. Hierzu sollte gehören: + Berechtigungskonzepte von Applikationen sind erstellt (z. B. ERP-Systeme). Hierzu kann gehören: Keine. Zusätzlich bei hohem Schutzbedarf: + Die Zugriffsberechtigungen sind durch den Informationsverantwortlichen (intern) freigegeben. + Bestehende Zugriffsberechtigungen werden regelmäßig überprüft. (angemessener Abstand z.B. vierteljährlich) Zusätzlich bei sehr hohem Schutzbedarf: + Funktionen in den Anwendungssystemen sind soweit möglich eingeschränkt. (z.B. Export und Druck) + Verschlüsselte Ablage von Daten zur Vermeidung von Zugriff und Kenntnisnahme durch nicht autorisierte Personen/Rollen (z. B. Administratoren) mindestens auf Dateiebene.

9.6 **Inwieweit ist eine Trennung der Daten innerhalb einer, mit fremden Organisationen gemeinsam genutzter Umgebungen gewährleistet?**
(Referenz zu ISO 27017: Control CLD.9.5.1 und CLD.9.5.2)

Ziel:	Insbesondere Cloud-Lösungen charakterisieren sich durch eine starke Standardisierung und einem hohen Grad an Virtualisierung auf von vielen Kunden gemeinsam genutzter Infrastruktur. In einer solchen kollaborativen Umgebung wird das Arbeiten von zahlreichen Cloud-Kunden ermöglicht. Damit die eigenen Informationen jederzeit geschützt werden, muss eine klare Trennung der Daten gewährleistet werden.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Es ist sichergestellt, dass durch eine wirksame Trennung unbefugte Nutzer anderer Organisationen nicht auf eigene Informationen zugreifen können.

Hierzu sollte gehören:
+ Das Trennungskonzept des Anbieters (z.B. Mandanten-Trennung) ist dokumentiert und wird regelmäßig geprüft. Dieses Konzept sollte mindestens beinhalten:
- Separierung von Daten, Applikationen, Betriebssystem, Storage und Netzwerk
- Separierung von Kunden- und internem Administrationsbereich
- Implementierung geeigneter Sicherheitsmaßnahmen für Mehrfachnutzer (in Mehrfachnutzer-Umgebungen)
- Risikobewertung für den Betrieb von Fremdsoftware innerhalb der geteilten Umgebung (insbesondere bei IaaS- / PaaS-Diensten)
+ Gemeinsam genutzte virtuelle Maschinen und/oder Applikationsinstanzen sind entsprechend gehärtet
- Einhaltung des Minimalprinzips (z. B. Einschränkung der Berechtigungen, Ports, Protokolle, Software)
- Nutzung technischer Schutzmaßnahmen (z. B. Anti-Virus, Logging)

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

10 Cryptography

10.1 **Inwieweit gibt es Regeln zur Verschlüsselung inkl. der Verwaltung des Schlüsselmaterials (kompletter Lifecycle) zum Schutz von Informationen bei Speicherung und Transport und sind diese umgesetzt worden?**
(Referenz zu ISO 27001: Control A10.1.1)

Ziel: Es muss sichergestellt werden, dass die Vertraulichkeit von Informationen sowohl bei Speicherung als auch bei der Übertragung
(z. B. bei Erlangen von physischem Zugriff auf Datenträger oder Datenübertragungsinfrastruktur) gesichert wird. In der Regel wird dieses durch Verschlüsselung erreicht. Beim Umgang mit Verschlüsselung ist es wesentlich, dass diese zu jedem Zeitpunkt die erwarteten Sicherheitseigenschaften bietet und nicht gleichzeitig unangemessen hohe Verfügbarkeitsrisiken erzeugt. Hierzu ist sicherzustellen, dass Verschlüsselungsbedarf zuverlässig erkannt wird. Wenn ein Bedarf erkannt wird, müssen stets Verfahren gewählt werden, die nach Stand der Wissenschaft und Technik als sicher gelten. Zusätzlich muss sichergestellt werden, dass die Geheimnisse (Schlüsselmaterial) über die Lebenszeit hinreichend vor technischen und organisatorischen Risiken für die Vertraulichkeit, aber auch für Integrität und die Verfügbarkeit, geschützt werden.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Alle produktiv eingesetzten Verschlüsselungstechnologien müssen dem Stand der Technik entsprechen.
+ Die rechtlichen Rahmenbedingungen für den Einsatz von Verschlüsselungstechnologien sind berücksichtigt.

Hierzu sollte gehören:
+ Erstellung eines Regelwerkes mit Anforderungen an die Verschlüsselung zum Schutz von Informationen gemäß ihrer Klassifizierung.
+ Ein Verschlüsselungskonzept zur Verschlüsselung mit mindestens folgenden Vorgaben ist definiert:
  - die Verschlüsselungsstärke
  - die Verwaltung der Schlüssel
  - den Verschlüsselungsalgorithmus
  - Verfahren für den kompletten Lebenszyklus, wie die Erzeugung, Speicherung, Archivierung, Abruf, Verteilung, Deaktivierung, Erneuerung und Löschung kryptographischer Schlüssel
+ Das Verschlüsselungskonzept ist etabliert.
+ Ein Notfallprozess zur Wiederherstellung von Schlüsselmaterial ist etabliert.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
+ Folgende Aspekte müssen dokumentiert sein:
  - Beschreibung der Schlüsselhoheit
  - Hoheit der Verwaltung des Schlüsselmaterials bei externer Verarbeitung (z.B. in der Cloud)
+ Informationen mit hohem Schutzbedarf sollten ausschließlich verschlüsselt transportiert oder übertragen werden.
+ Wenn eine Verschlüsselung nicht möglich ist, müssen Risiken durch vergleichbar wirksame Maßnahmen geschützt werden.

Zusätzlich bei sehr hohem Schutzbedarf:
+ Informationen mit sehr hohem Schutzbedarf werden verschlüsselt gespeichert.
+ Bei der externen Bearbeitung bzw. Übertragung ist sicherzustellen:
  - Verpflichtende Ende-zu-Ende-Verschlüsselung (vorzugsweise mit Schlüsselmaterial aus unternehmenseigener Umgebung)

Anforderungen:

11 Physical and Environmental Security

11.1 **Inwieweit sind Sicherheitszonen für den Schutz von schutzbedürftigen oder kritischen Informationen sowie informationsverarbeitenden Einrichtungen definiert, abgesichert und überwacht (Zutrittssicherungen)?**
(Referenz zu ISO 27001: Control A11.1.1 und A11.1.2)

Ziel: Es muss sichergestellt sein, dass Information-Assets nicht außerhalb des Wirkungsbereichs der Maßnahmen verarbeitet werden, die für das zu erreichende Informationssicherheitsniveau vorgesehenen vorgesehen sind. Da es in der Regel nicht möglich ist, entsprechende Maßnahmen für alle Bereiche des Standortes umzusetzen, wird ein Zonenkonzept genutzt, welches definiert, in welchen Bereichen welche Art von Informationen verarbeitet werden dürfen.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Anforderungen zum Schutz von betroffenen Assets sind ermittelt (siehe Control 8.1).
+ Sicherheitszonen unter Berücksichtigung von Geländen/Gebäuden/ Räumen sind festgelegt und dokumentiert.
+ Das Sicherheitszonenkonzept ist etabliert und allen Personen, die mit schützenswerten Informationen umgehen bekannt.
+ Die Sicherheitszonen sind gemäß der getroffenen Risikoeinstufung durch angemessene Schutzmaßnahmen abgesichert. (Beispiele siehe Hinweise).

Hierzu sollte gehören:
+ Verfahren zur Vergabe und zum Entzug von Zutrittsberechtigungen sind etabliert.
+ Regelungen für das Besuchermanagement inkl. Registrierung und Begleitung von Besuchern sind definiert.
+ Die Sicherheitszonen werden angemessen überwacht. (Beispiele s. Hinweise)
+ Externe Liegenschaften zur Lagerung und Verarbeitung von Informations-Assets sind im Rahmen des Sicherheitszonenkonzeptes berücksichtigt. (z. B. Lagerräume, Garagen, Werkstätten, Teststrecken, Rechenzentren)

Hierzu kann gehören:
+ Die Sicherheitszonen sind gekennzeichnet.

Zusätzlich bei hohem Schutzbedarf:
+ Bei extern stationierten IT-Systeme, z. B. externes Housing im Rahmen eines Notfallrechenzentrums, sollte sichergestellt werden, dass Administratoren des externen Dienstleisters keinen direkten Zugriff zu den Systemen haben. (z. B. durch verschlossene Racks).

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 11.2 **Inwieweit hat das Unternehmen Maßnahmen gegen die Auswirkungen von Naturkatastrophen, vorsätzlichen Angriffen oder Unfällen getroffen?**
(Referenz zu ISO 27001: Control A11.1.4)

Ziel: Naturkatastrophen, vorsätzliche Angriffe oder Unfälle können die Verfügbarkeit von IT-Systemen kritisch beeinträchtigen. Es muss sichergestellt werden, dass die Auswirkungen auf kritische IT-Systeme bekannt, entsprechend ihrer Kritikalität bewertet und angemessene Schutzmaßnahmen definiert und umgesetzt wurden.

Anforderungen:

Hierzu muss gehören:
+ Natürliche Bedrohungen, wie z. B. Überflutung, sind erfasst.
+ Gesellschaftliche Bedrohungen, wie z. B. politische Instabilität oder Unfälle von Industrieanlagen, sind erfasst.
+ Potentiell betroffene Infrastruktur, Assets und IT-Systeme sind erfasst.

Hierzu sollte gehören:
+ Angemessene Schutzmaßnahmen, wie z.B. Brandmeldeanlage, Brandschutz, Wassermelder, sind umgesetzt und werden regelmäßig geprüft.
+ Eine redundante Medienversorgung (Strom, Kommunikationsverbindungen, usw.) ist vorhanden.
+ Notfallpläne sind definiert und werden regelmäßig geprüft.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

Information Security Assessment - Ziele und Anforderungen

☐ 11.3 **Inwieweit werden Schutzmaßnahmen in Anlieferungs- und Versandbereichen bzgl. des Zutritts unbefugter Personen getroffen?**
(Referenz zu ISO 27001: Control A11.1.6)

Ziel:	Es muss sichergestellt werden, dass alle Zugänge zu geschützten Zonen mit angemessenen Maßnahmen vor unbefugten Zutritt geschützt werden. Besondere Anforderungen treten hierbei oftmals in Anlieferungs- und Versandbereichen auf, insbesondere wenn diese für die Anlieferung und den Versand von großen Objekten (z. B. Fahrzeugen oder großen Werkzeugen) ausgelegt sein müssen.
Anforderungen:	Hierzu muss gehören: + Die Anforderungen zum Schutz der Anlieferungs- und Versandbereiche sind erfasst. + Die Versandbereiche sind im Sicherheitszonenkonzept integriert. + Notwendige Schutzmaßnahmen sind definiert und umgesetzt. + Der Zutritt ist nur für identifiziertes und berechtigtes Personal gestattet. Hierzu sollte gehören: + Sensible IT-Systeme werden von Anlieferungs- und Versandbereichen getrennt. Hierzu kann gehören: + Es besteht eine separate Sicherheitszone für die Anlieferung durch Zulieferer ohne Zutritt zu weiteren Bereichen der Organisation + Eine Schleusenfunktion im Bereich der Anlieferungs- und Ladezone ist vorhanden. + Das gelieferte Material wird auf potentielle Bedrohungen untersucht. Zusätzlich bei hohem Schutzbedarf: Keine. Zusätzlich bei sehr hohem Schutzbedarf: Keine.

☐ 11.4 **Inwieweit sind Richtlinien und Verfahren für den Gebrauch von Assets, einschließlich ihrer Mitnahme, Entsorgung und Wiederverwendung vorhanden und umgesetzt?**
(Referenz zu ISO 27001: Control A11.2.5, A11.2.6 und A11.2.7)

Ziel:	Verlassen Assets (z. B. IT-Geräte, Informationen) das Gelände einer Organisation, sind diese höheren Risiken ausgesetzt. So besteht z. B. das Risiko für Diebstahl oder unberechtigter Einsichtnahme. Um den Risiken geeignet zu begegnen, müssen die Sicherheitsanforderungen, die sich aus der Mitnahme ergeben, ermittelt werden. Dies gilt auch für die Entsorgung oder Wiederverwendung von Assets (z. B. Notebooks).
Anforderungen:	Hierzu muss gehören: + Sicherheitsanforderungen für den Gebrauch und der Mitnahme von Assets sind identifiziert. + Richtlinien und Verfahren für den Gebrauch und der Mitnahme von Assets sind definiert und werden umgesetzt. + IT-Geräte, die sensible Daten enthalten, werden so gelöscht, dass die Daten nicht wiederhergestellt werden können. Hierzu sollte gehören: + Informationen müssen in Abhängigkeit ihres Schutzbedarfs durch geeignete Maßnahmen geschützt werden. Hierzu kann gehören: Keine. Zusätzlich bei hohem Schutzbedarf: + Die Entsorgung von Datenträgern erfolgt gemäß eines der gängigen Standards (z.B. DIN 66399 Sicherheitsstufe 4). Zusätzlich bei sehr hohem Schutzbedarf: + Die Entsorgung von Datenträgern erfolgt gemäß eines der gängigen Standards (z.B. DIN 66399 Sicherheitsstufe 5).

Information Security Assessment - Ziele und Anforderungen

12 Operations Security

12.1 **Inwieweit werden Änderungen von Organisation, Geschäftsprozessen, informationsverarbeitenden Einrichtungen und Systemen bzgl. ihrer Sicherheitsrelevanz gesteuert und umgesetzt?**

(Referenz zu ISO 27001: Control A12.1.2)

Ziel:	Bei Änderungen in der Organisation, den Geschäftsprozessen, informationsverarbeitenden Einrichtungen und Systemen sind Informationssicherheitsaspekte zu berücksichtigen. Ziel ist es, sicherzustellen, dass alle Änderungen unter Berücksichtigung und Einhaltung der Anforderungen an die Informationssicherheit durchgeführt werden.
Anforderungen:	Hierzu muss gehören: + Sicherheitsrelevante Anforderungen bei der Änderung von Organisation, Geschäftsprozessen, informationsverarbeitenden Einrichtungen und Systemen werden ermittelt und umgesetzt. Hierzu sollte gehören: + Ein formales Genehmigungsverfahren ist definiert. + Rückfall Lösungen für den Fehlerfall sind eingerichtet. + Änderungen mit Auswirkung auf die Informationssicherheit werden geplant und getestet. Hierzu kann gehören: Keine. Zusätzlich bei hohem Schutzbedarf: + Die Einhaltung der Informationssicherheitsanforderungen wird bei Änderungen überprüft. Zusätzlich bei sehr hohem Schutzbedarf: Keine.

12.2 **Inwieweit sind die Entwicklungs- und Testumgebungen von den Produktivumgebungen getrennt?**

(Referenz zu ISO 27001: Control A12.1.4)

Ziel:	Eine Trennung von Entwicklungs-, Test- und Produktivumgebungen hat zum Ziel, dass Fehler im Rahmen der Entwicklung sich nicht auf die Produktivumgebung auswirken. Eine Testumgebung dient z.B. als Zwischenschritt um Software-Entwicklungen mit den Umgebungsvariablen einer Produktivumgebung zu testen und deren Funktionen auf Verfügbarkeit, Zuverlässigkeit und Integrität zu überprüfen.
Anforderungen:	Hierzu muss gehören: + Eine Risikobewertung der IT-Systeme wurde durchgeführt, um zu ermitteln, inwiefern eine Trennung der IT-Systeme in Entwicklungs- und Produktivsysteme notwendig ist. Hierzu sollte gehören: + Die Anforderungen an Entwicklungs- und Testumgebungen sind ermittelt, z. B.: - Trennung von Entwicklungs-, Test- und Produktivsystemen - Keine Entwicklungs- und Systemwerkzeuge auf Produktivsystemen (außer solchen, die für den Betrieb relevant sind) - Verwendung von unterschiedlichen Benutzerprofilen auf Test- und Produktivsystemen - Soweit möglich verwendung von nicht sensitiven bzw. anonymisierten Test-Daten + Vorgaben zur Überführung von Software aus dem Entwicklungs- und Teststatus in den Produktivstatus sind festgelegt. + Die ermittelten Anforderungen sind umgesetzt. Hierzu kann gehören: Keine. Zusätzlich bei hohem Schutzbedarf: Keine. Zusätzlich bei sehr hohem Schutzbedarf: Keine.

Information Security Assessment - Ziele und Anforderungen

☐ 12.3 **Inwieweit ist der Schutz (z.B. "end-point security") vor Schadsoftware (Viren, Würmer, Trojaner, Spyware, …) in Verbindung mit der Sensibilisierung von Benutzern ausgeprägt?**
(Referenz zu ISO 27001: Control A12.2.1)

Ziel:	Zum Schutz gegen Schadsoftware sind zwei Aspekte von besonderer Bedeutung - zum einen die Software zum Schutz gegen Schadsoftware und zum anderen sensibilisierte Benutzer. Die Schulung der Benutzer ist besonders wichtig, da trotz aller Schutzmaßnahmen an Hard- und Software der Anwender durch seine Aktionen Schadsoftware unabsichtlich aktivieren kann.
Anforderungen:	Hierzu muss gehören: + Anforderungen an den Schutz vor Schadsoftware sind ermittelt. + Technische und organisatorische Maßnahmen zum Schutz vor Schadsoftware sind definiert und umgesetzt. Hierzu sollte gehören: + Benutzerkonten haben keine administrativen Berechtigungen (siehe Control 9.3). + Software zum Schutz vor Schadsoftware ist installiert und wird regelmäßig automatisch aktualisiert. (z. B. Virenscanner) + Eine automatische Überprüfung von empfangenen Dateien und Programmen vor deren Ausführung auf Schadsoftware (On-Access-Scan). + Eine regelmäßige Untersuchung des gesamten Datenbestandes aller Systeme auf Schadsoftware wird durchgeführt. + Eine automatische Überprüfung der von zentralen Gateways transportierten Daten (z.B. E-Mail, Internet, Netze von Dritten) mittels einer Schutzsoftware (incl. verschlüsselter Verbindungen) erfolgt. + Maßnahmen zur Sicherstellung, dass Schutzsoftware nicht durch Benutzer deaktiviert oder verändert werden kann, sind definiert und umgesetzt. + Mitarbeiter werden anlassbezogen sensibilisiert. Hierzu kann gehören: + Systeme mit hohem Selbstschutz (z.B. spezielle Härtung, wenig Dienste, keine aktiven User) können ohne Virenscanner betrieben werden. Zusätzlich bei hohem Schutzbedarf: Keine. Zusätzlich bei sehr hohem Schutzbedarf: Keine.

☐ 12.4 **Inwieweit werden Datensicherungen unter Berücksichtigung einer entsprechenden Regelung erstellt und regelmäßig getestet?**
(Referenz zu ISO 27001: Control A12.3.1)

Ziel:	Ziel einer funktionierenden Datensicherungsstrategie ist es, im Falle eines Systemausfalls oder Datenverlustes anderer Art (z.B. Ransomware), die Funktionsfähigkeit bzw. Verfügbarkeit der Informationen in der geforderten Zeit wiederherstellen zu können. Datensicherungen (Backups) müssen dabei unter Beachtung einer entsprechenden Richtlinie erstellt und regelmäßig getestet werden.
Anforderungen:	Hierzu muss gehören: + Anforderungen an die Datensicherung sind ermittelt und umfassen: die zu sichernden Systeme, deren Sicherungsintervalle sowie die Aufbewahrung und den Transport von Datensicherungs-Medien. + Angemessene Schutzmaßnahmen, z.B. durch Verschlüsselung, erfolgt bei Lagerung. + Die Lagerung der Sicherungsmedien erfolgt örtlich getrennt (unterschiedliche Brandschutzzonen). + Ein Datensicherungskonzept ist erstellt und wird umgesetzt. + Eine angemessene Überprüfung der Datensicherung findet statt. Hierzu sollte gehören: Keine. Hierzu kann gehören: Keine. Zusätzlich bei hohem Schutzbedarf: Keine. Zusätzlich bei sehr hohem Schutzbedarf: + Es ist bei Informationen mit sehr hohem Schutzbedarf mit geeigneten Maßnahmen (z.B. Verschlüsselung) sicherzustellen, dass Zugriff nur durch den berechtigten Kreis möglich ist.

Information Security Assessment - Ziele und Anforderungen

12.5 **Inwieweit werden Ereignis-Logs, die z.B. Benutzeraktivitäten, Ausnahmen, Fehler und Sicherheitsereignisse beinhalten können, erzeugt, aufbewahrt, überprüft und gegen Veränderungen abgesichert?**
(Referenz zu ISO 27001: Control A12.4.1 und A12.4.2)

Ziel:	Ereignis-Logs helfen bei einem Sicherheitsvorfall nachzuvollziehen, was passiert ist. Dazu ist es notwendig, für die Ermittlung der Ursachen notwendige Ereignisse aufzuzeichnen und gegen Veränderung gesichert aufzubewahren.
Anforderungen:	Hierzu muss gehören: + Anforderungen an die Informationssicherheit bezüglich Umgang mit Ereignis-Logs sind ermittelt. + Soweit extern betriebene Dienste (insbes. Cloud-Dienste) genutzt werden, sind Informationen über Monitoring-Möglichkeiten eingeholt - z.B. Angriffserkennung und Meldungsmöglichkeiten (Incident-Responce) + Gesetzliche Anforderungen wie z.B. Aufbewahrungsfristen und Schutz des Persönlichkeitsrechts werden eingehalten. + Regeln und Verfahren zur Erfüllung der ermittelten Anforderungen sind definiert und umgesetzt. Hierzu sollte gehören: + Ereignis-Logs werden gegen Veränderungen geschützt aufbewahrt. Hierzu kann gehören: Keine. Zusätzlich bei hohem Schutzbedarf: + Sicherheitsrelevante Anforderungen an die Informationssicherheit bezüglich Umgang mit Ereignis-Logs, wie z. B. Anforderungen aus Verträgen sind ermittelt und umgesetzt. Zusätzlich bei sehr hohem Schutzbedarf: Keine.

12.6 **Inwieweit werden die Aktivitäten von Systemadministratoren und -operatoren protokolliert, die Ablage der Protokolle gegen Veränderungen abgesichert und regelmäßig überprüft?**
(Referenz zu ISO 27001: Control A12.4.3)

Ziel:	Mit den umfangreichen Berechtigungen von Systemadministratoren und -operatoren können diese weitreichende Änderungen an IT-Systemen durchführen. Um im Anschluss an Informationssicherheitsereignisse ermitteln zu können, von wem Änderungen an IT-Systemen durchgeführt wurden, ist eine Protokollierung und Auswertung der Aktivitäten unter Berücksichtigung der gültigen Gesetzgebung (u.a. Datenschutz und Betriebsverfassungsgesetz) notwendig.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Sicherheitsrelevante Anforderungen bei der Protokollierung von Aktivitäten der Systemadministratoren und -operatoren sind ermittelt und umgesetzt.
+ Die verwendeten IT-Systeme sind bezüglich der Notwendigkeit der Protokollierung bewertet.
+ Soweit extern betriebene Dienste (insbes. Cloud-Dienste) genutzt werden, sind Informationen über Monitoring-Möglichkeiten eingeholt und in die Bewertung mit einbezogen.
 - z.B. Audit-Logs für Konfigurationsänderungen und Nutzung von / Zugriff auf eDiscovery-Funktionen oder Backup.
+ Verfahren zum Umgang mit Regelverstößen sind definiert.
+ Eine regelmäßige Überprüfung der Protokolle auf Regelverstöße, im Rahmen der zulässigen gesetzlichen und betrieblichen Bestimmungen, wird durchgeführt.
+ Die Art der Protokollierung bezüglich Zeitpunkt, Aktivitätslevel und Aufbewahrungsfristen ist definiert und umgesetzt.

Hierzu sollte gehören:
+ Ein Prozess zur Meldung von Verstößen an die zuständige Stelle (z. B. CERT) ist etabliert.
+ Die Protokolldateien sind vor Veränderungen geschützt. (z. B. Einsatz einer dedizierten Umgebung)

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
+ Zugriffe beim Auf- und Abbau von externen Verbindungen (z. B. Fernwartung) werden protokolliert.

Zusätzlich bei sehr hohem Schutzbedarf:
+ Protokollierung von allen Zugriffen
  - soweit technisch möglich
  - auf Daten mit sehr hohem Schutzbedarf.

☐ 12.7 **Inwieweit werden Informationen über technische Schwachstellen der IT-Systeme zeitnah beschafft, beurteilt und geeignete Maßnahmen ergriffen (z.B. Patch-Management)?**
(Referenz zu ISO 27001: Control A12.6.1 und A12.6.2)

Ziel: Bekannte Schwachstellen erhöhen das Risiko für die IT-Systeme, die Anforderungen an Vertraulichkeit, Verfügbarkeit und Integrität nicht mehr erfüllen zu können, in dem sie z. B. Angreifern Zugriff zum IT-System ermöglichen oder die Systemstabilität gefährden.

Anforderungen:

Hierzu muss gehören:
+ Informationen über technische Schwachstellen zu den genutzten Assets werden gesammelt und bewertet.
+ Potenziell betroffene Systemen und Software (Assets) werden identifiziert. (z. B. Hersteller, Version, Installationsort)

Hierzu sollte gehören:
+ Ein angemessenes Patch-Management ist definiert und umgesetzt. (z. B. Test- und Installation von Patches)
+ Soweit notwendig sollten risikominimierende Maßnahmen umgesetzt werden. Hierzu zählen z. B.:
  - Abtrennung der betroffenen Systeme
  - Abschalten des betroffenen Service
  - Anpassung von Zugriffsmöglichkeiten wie z. B. Firewalls
  - Anpassen des Monitorings
  - Erhöhung der Awareness der Anwender

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

Information Security Assessment - Ziele und Anforderungen

12.8 **Inwieweit werden Auditanforderungen und -aktivitäten, die zur Überprüfung von IT-Systemen dienen, geplant, abgestimmt, und die IT-Systeme in der Folge technisch überprüft (Systemaudit)?**

(Referenz zu ISO 27001: Control A12.7.1, A18.2.3)

Ziel:	Im Rahmen von Audits (speziell technische Audits) kann es zu Problemen mit der Stabilität der geprüften IT-Systeme kommen. Audittätigkeiten, welche eine Überprüfung von IT-Systemen beinhalten, sollten geplant und vereinbart werden, um Störungen der betroffenen Prozesse zu vermeiden.
Anforderungen:	Hierzu muss gehören: + Anforderungen an die Auditierung von IT-Systemen sind ermittelt. + Der Umfang des Audits ist rechtzeitig festgelegt. + Systemaudits sind mit dem Betreiber und den Nutzern der IT-Systeme abgestimmt. + Die Ergebnisse von Systemaudits werden nachvollziehbar gespeichert und an das relevante Management berichtet. + Maßnahmen aus den Ergebnissen werden abgeleitet. + Eine Nachverfolgung der abgeleiteten Maßnahmen im Rahmen des ISMS erfolgt. Hierzu sollte gehören: + Systemaudits werden von ausgebildeten Spezialisten durchgeführt. + Für Abweichungen müssen in angemessenen Zeiträumen Maßnahmen definiert und abgestimmt sein. + Die Erstellung und Abstimmung des Audit-Reports muss in einem angemessenem Zeitraum erfolgt sein. Hierzu kann gehören: Keine. Zusätzlich bei hohem Schutzbedarf: Keine. Zusätzlich bei sehr hohem Schutzbedarf: Keine.

12.9 **Inwieweit wurden Auswirkungen kritischer administrativer Funktionen von externen IT-Diensten (insbes. Cloud-Dienste) berücksichtigt?**
(Referenz zu ISO 27017: Control CLD.12.1.5)

Ziel:	Viele Cloud-Dienste bieten Funktionen, die zu weitreichenden Änderungen in operativ genutzten Diensten führen können. Diese Funktionen können die Vertraulichkeit der Informationen gefährden oder nicht oder nur mit erheblichen Aufwand reversibel sein und damit Verfügbarkeit oder Integrität beeinträchtigen. Diese Funktionen werden administrativen Nutzern oft über eine einfach zu nutzende, automatisierte Konfigurationsschnittstelle zur Verfügung gestellt. Bei Ausführung eines administrativen Users werden solche Aktionen ohne weitere menschliche Prüfung durchgeführt. Es muss sichergestellt sein, dass solche Funktionen weder versehentlich noch durch einen bösartigen Administrator ohne besonderen Aufwand dazu genutzt werden können, Schaden in Bezug auf Vertraulichkeit, Verfügbarkeit oder Integrität erzeugen.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Kritische Funtkionen aller betroffenen Dienste sind ermittelt und bewertet.

Hierzu sollte gehören:
+ Kritische Funktionen aller betroffenen Dienste sind gemeinsam mit ihrem Risiko dokumentiert. Hierbei wurden (soweit zutreffend) unter anderem folgende Aspekte berücksichtigt:
 - Installation, Änderung oder Löschung von virtuellen Ressourcen (z. B. virtuelle Server, virtuelle Netzwerke und virtuellen Speicher)
 - Terminierung von Diensten (Kündigung)
 - Autorisierung von weiteren Nutzern
 - Freigabe und Veröffentlichungsfunktionen
 - Backup und Recoveryfunktionen
+ Die Möglichkeiten, durch Konfiguration und Rechtevergabe entgegenzuwirken, sind bekannt und dokumentiert.
+ Durch Konfiguration und Rechtevergabe sind die daraus entstehenden Risiken minimiert.
 - Kritische nicht-administrative Funktionen wurden in der Funktion soweit sinnvoll eingeschränkt.
 - der Zugriff auf kritische nicht-administrative und administrative Funktion ist - soweit möglich - auf einen möglichst kleinen Personenkreis eingeschränkt.
 - soweit technisch und ohne dem adressierten Risiko unangemessene Einschränkung der gewünschten Funktionalität möglich wurden kritische administrative und nicht-administrative Funktionen deaktiviert.
+ Ein Notfallkonzept, welches den Umgang mit Schadensszenarien beschreibt, existiert und ist getestet.

Hierzu kann gehören:
+ Nutzung des Mehr-Augen Prinzips für kritische Funktionen.
+ Vertraglich vereinbarte Einschränkung der Funktionalität durch den Anbieter (z.B. durch den Einsatz von geeigneten Rahmenverträgen)

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

13 Communications Security

☐ 13.1 **Inwieweit werden Netzwerke verwaltet und gesteuert, um Informationen in IT-Systemen und Anwendungen zu schützen?**
(Referenz zu ISO 27001: Control A13.1.1)

Ziel: Der Schutz von Informationen in Netzwerken, IT-Systemen und IT-Anwendungen muss sichergestellt werden. Hierzu müssen Maßnahmen umgesetzt werden, die den Schutz vor unbefugtem Zugriff gewährleisten. Darunter zählt der Einsatz geeigneter Steuerungsmaßnahmen, unterstützt durch Hilfsmittel zur Überwachung der Netzwerke, IT-Systeme und IT-Anwendungen.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Verfahren zur Verwaltung und Steuerung der Netzwerke sind definiert.

Hierzu sollte gehören:
+ Anforderungen an die Steuerung und Verwaltung von Netzwerken sind ermittelt und umgesetzt. Hierzu zählen z. B.:
- Beschränkungen bei der Anbindung von IT-Systemen an das Netzwerk
- Besondere Schutzmaßnahmen bei Netzwerkverbindungen über potentiell unsichere Netze (z.B. Verschlüsselung)
- Angemessenes Überwachen und Aufzeichnen von informationssicherheitsrelevanten Aktionen im Netzwerk
- Einsatz von Hilfsmitteln wie z.B. Firewall-Systemen, Intrusion Detection und Prevention Systemen (IDS/IPS), Netzwerkverwaltungswerkzeugen, Sicherheitssoftware für Netzwerke
- Bei Einsatz von aus dem Internet erreichbaren extern betriebenen Netzwerkdiensten (Cloud-Diensten) ist das hierdurch entstehende erhöhte Risiko bewertet und in den Applikationen adressiert.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
+ Erweiterte Anforderungen an die Steuerung und Verwaltung von Netzwerken sind ermittelt und umgesetzt. Hierzu zählen z. B.:
- Authentifizierung von IT-Systemen im Netzwerk

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 13.2 **Inwieweit werden Anforderungen an Sicherheitsmechanismen sowie Service Levels und Managementanforderungen an Netzwerkdienste identifiziert und in Service-Level-Agreements dokumentiert?**
(Referenz zu ISO 27001: Control A13.1.2)

Ziel: Sicherheitsmechanismen, Qualität der Leistungserbringung und Anforderungen an die Verwaltung aller Netzwerkdienste müssen ermittelt und sowohl für interne als auch für externe Netzwerke in Vereinbarungen (Service Level Agreements, SLAs) aufgenommen werden.

Anforderungen:

Hierzu muss gehören:
+ Anforderungen an die Informationssicherheit von Netzwerkdiensten sind ermittelt und umgesetzt.

Hierzu sollte gehören:
+ Verfahren für die Absicherung und Nutzung von Netzwerkdiensten sind definiert und implementiert.
+ SLAs sind definiert und für intern und extern betriebene Netzwerkdienste implementiert.
+ Angemessene Redundanzlösungen sind implementiert.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
+ Verfahren zur Überwachung des Netzwerkes (z. B. Verkehrsflussanalysen, Verfügbarkeitsmessungen) sind definiert und werden durchgeführt.

Zusätzlich bei sehr hohem Schutzbedarf:
+ Out-of-Band-Management wird eingesetzt.

☐ 13.3 **Inwieweit werden Gruppen von Informationsdiensten, Benutzer und Informationssysteme innerhalb des Netzwerks segmentiert?**
(Referenz zu ISO 27001: Control A13.1.3)

Ziel: IT-Systeme innerhalb des Netzwerkes haben gewöhnlich unterschiedliche Schutzbedarfe. So sind i.d.R. IT-Systeme, die direkt mit dem Internet verbunden sind, anderen Gefahren ausgesetzt als IT-Systeme im Büronet+E269z. Um ungewollten Datenaustausch zwischen IT-Systemen mit unterschiedlichen Schutzbedarf zu erkennen und zu unterbinden, müssen entsprechende Gruppen innerhalb des Netzwerkes gebildet und diese von anderen Gruppen getrennt werden.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Anforderungen an eine Segmentierung des Netzwerkes sind ermittelt.
  - Bei Nutzung von Cloud-Diensten sind hierbei Möglichkeiten (virtueller) Netzwerke einbezogen

Hierzu sollte gehören:
+ Regeln und Verfahren zur Segmentierung des Netzwerkes sind definiert und umgesetzt.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 13.4 **Inwieweit werden Informationen während des Austauschs oder der Übermittlung geschützt?**
(Referenz zu ISO 27001: Control A13.2.1 und A13.2.3)

Ziel: Bei der Übermittlung und dem Austausch von Informationen müssen Anforderungen an die Informationssicherheit beachtet werden. Hierzu muss definiert sein, welche Dienste in der Organisation für welche Art von Daten verwendet werden dürfen und welche Schutzmaßnahmen bei der Verwendung der Dienste beachtet werden müssen.

Anforderungen:

Hierzu muss gehören:
+ Die verwendeten Dienste (z. B. E-Mail, EDI, Voice over IP) zur Übertragung sind ermittelt.
+ Regeln und Verfahren gemäß den Vorgaben der Klassifizierung zur Nutzung der Dienste sind definiert und umgesetzt.
+ Maßnahmen zum Schutz der übertragenen Inhalte vor unberechtigtem Zugriff sind umgesetzt.

Hierzu sollte gehören:
+ Maßnahmen zur Sicherstellung der korrekten Adressen und des korrekten Transports der Nachricht sind umgesetzt.
+ Ein Genehmigungsprozess für die Verwendung von externen Diensten (z.B. Instant Messaging, Web Meeting, Web-Mail) ist etabliert.
+ Der elektronische Datenaustausch erfolgt abhängig von der Klassifizierung durch Content-Verschlüsselung und/oder mit verschlüsselten Transportwegen (z.B. VPN, verschlüsselte Verbindungen (HTTPS, SFTP, TLS)).

Hierzu kann gehören:
+ Digitaler Signaturen werden unter Beachtung rechtlicher Vorgaben verwendet.

Zusätzlich bei hohem Schutzbedarf:
+ E-Mails werden mittels Transport-Verschlüsselung übertragen (z. B. TLS).
+ Eine geeignete Verschlüsselung bei Datenübertragungen zu extern gehosteten IT-Systemen wird eingesetzt (siehe Controls 10.1, 15.1).

Zusätzlich bei sehr hohem Schutzbedarf:
+ E-Mails werden mittels Ende-zu-Ende-Verschlüsselung übertragen (z. B. PGP, S/MIME, ZIP-Verschlüsselung).

☐ 13.5 **Inwieweit werden vor dem Austausch von Informationen Geheimhaltungsvereinbarungen abgeschlossen und werden die Anforderungen bzw. Erfordernisse zum Schutz der Informationen dokumentiert und regelmäßig überprüft?**
(Referenz zu ISO 27001: Control A13.2.4)

Ziel: Auch wenn sensible Informationen außerhalb der Organisation weitergegeben werden, muss sichergestellt werden, dass externe Organisationen verpflichtet sind, die Anforderungen an die Informationssicherheit zu erfüllen und dafür notwendige Maßnahmen umzusetzen. Die notwendige rechtliche Grundlage für die Verpflichtung wird durch Geheimhaltungsvereinbarungen geschaffen. Daher muss sichergestellt werden, dass sensible Informationen nur dann weitergegeben werden, wenn eine entsprechende Geheimhaltungsvereinbarung rechtswirksam abgeschlossen wurde.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Mit allen Dienstleistern und Mitarbeitern, die mit sensiblen Informationen arbeiten, sind gültige Geheimhaltungsvereinbarungen abgeschlossen.
+ Es sind Regeln und Verfahren zum Einsatz von Geheimhaltungsvereinbarungen definiert und allen Personen bekannt gegeben, die sensible Informationen weitergeben.
+ Die Anforderungen, Regeln und Verfahren zur Verwendung von Geheimhaltungsvereinbarungen werden regelmäßig geprüft.

Hierzu sollte gehören:
+ Vorlagen für Geheimhaltungsvereinbarungen sind vorhanden und auf rechtliche Anwendbarkeit geprüft.
+ Die Vorlagen sehen klare Angaben zu:
  - den beteiligte Personen/Firmen
  - der Art der von der Vereinbarung umfassten Informationen,
  - den Gegenstand der Vereinbarung
  - die Gültigkeitsdauer der Vereinbarung (befristet oder dauerhaft)
  - den Verantwortlichkeiten des Verpflichteten
+ Die Vorlagen enthalten Bestimmungen zu den Nutzungsrechten an Informationen über das Vertragsverhältnis hinaus.
+ Mögliche Nachweise zur Einhaltung von Vorgaben (z. B. Prüfung eines unabhängigen Dritten oder Auditrechte) sind definiert.
+ Ein Prozess, mit dem die Gültigkeitsdauer von befristeten Vereinbarungen überwacht und rechtzeitig eine Verlängerung der Vereinbarung angestoßen wird, ist definiert und umgesetzt.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

14 System acquisition, development and maintenance

☐ 14.1 **Inwieweit werden sicherheitsspezifische Anforderungen bei neuen IT-Systemen (einschließlich öffentlich zugänglicher IT-Systeme) und bei Erweiterungen für bestehende IT-Systeme berücksichtigt?**

(Referenz zu ISO 27001: Control A14.1.1, A14.1.2 und A14.1.3))

Ziel: Informationssicherheit muss ein fester Bestandteil über den gesamten Lebenszyklus von IT-Systemen sein. Dies umfasst insbesondere die Berücksichtigung von Anforderungen an die Informationssicherheit bei der Entwicklung, Beschaffung und Wartung von IT-Systemen.

Anforderungen:

Hierzu muss gehören:
+ Die Anforderungen an die Informationssicherheit bei der Beschaffung oder Erweiterung von IT-Systemen sind ermittelt.

Hierzu sollte gehören:
+ Eine Prüfung von Lastenheften gegen die Richtlinien zur Informationssicherheit erfolgt.
+ Eine Prüfung des IT-Systems auf Einhaltung der Vorgaben vor dem produktiven Einsatz wird durchgeführt.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

Information Security Assessment - Ziele und Anforderungen

☐ 14.2 **Inwieweit werden sicherheitsrelevante Aspekte im Software-Entwicklungsprozess (inkl. Change Management) berücksichtigt?**
(Referenz zu ISO 27001: Control A14.2.1 - A14.2.9)

Ziel: Der Entwicklungsprozess für Software und IT-Systeme innerhalb einer Organisation muss die Anforderungen an die Informationssicherheit berücksichtigen. Diese müssen im jeweiligen Vorgehensmodell als Anforderungen und Meilensteine mit aufgenommen werden.

Anforderungen:

Hierzu muss gehören:
Keine.

Hierzu sollte gehören:
+ Eine Richtlinie für die Entwicklung von Software und IT-Systemen ist erstellt und enthält mindestens folgender Aspekte:
- Anforderungen an die Informationssicherheit der Entwicklungsumgebung
- Anforderungen an die Informationssicherheit im Software-Entwicklungs-Lebenszyklus
- Anforderungen an die Informationssicherheit in der Designphase
- Prüfpunkte zur Informationssicherheit im Rahmen von Projekt-Meilensteinen
- Informationssicherheit bei der Versionskontrolle und Repositories
- Kenntnisse zur Informationssicherheit von Anwendungssystemen
- Anforderungen an die Entwickler zur Erstellung von Systemen/Anwendungen unter Berücksichtigung von Aspekten zur Informationssicherheit (Vermeidung, Entdeckung und Behebung von Schwachstellen)

+ Anforderungen an die Informationssicherheit beim Change Management sind berücksichtigt.
+ Definierte Engineering-Prinzipien zur sicheren Systementwicklung sind definiert und werden umgesetzt.
+ Sichere Entwicklungsprozesse sind auch bei Erstellung von Systemen durch Dritte definiert.
+ Systemabnahmetests unter Berücksichtigung der Anforderungen an die Informationssicherheit werden durchgeführt.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 14.3 **Inwieweit wird sichergestellt, dass Testdaten sorgfältig erstellt, geschützt und kontrolliert eingesetzt werden?**
(Referenz zu ISO 27001: Control A14.3.1)

Ziel: Oftmals sind Testdaten notwendig, um im Rahmen von Software-Entwicklung oder des Change-Managements Tests durchzuführen. Tests werden in Testumgebungen durchgeführt, zu denen der Zugang oftmals weniger stark kontrolliert wird und oftmals Personen (z.B. Dienstleister oder Entwickler) Zugang haben, die keinen Zugang zu den Produktivdaten benötigen. Es muss sichergestellt werden, dass durch die Testumgebung kein erhöhtes Risiko durch Verlust oder Offenlegung von Produktivdaten entsteht.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
Keine.

Hierzu sollte gehören:
+ Es wird weitgehend vermieden, Produktivdaten zu Testzwecken zu nutzen.
+ Wenn Produktivdaten zu Testzwecken genutzt werden, muss sichergestellt werden:
  - Entsprechend der rechtlichen Vorgaben erfolgen Anonymisierung oder Pseudonymisierung der Produktivdaten
  - Im Testsystem sind die identischen Zugriffskontrollen wie im Produktivsystem vorhanden
+ Es werden fallbezogene Vorgaben für die Erstellung von Testdaten definiert.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
+ Das Kopieren von Informationen aus der Produktivumgebung muss im Vorfeld über einen definierten Genehmigungsprozess freigegeben werden.
+ Betriebsrelevante Informationen werden mit Abschluss des Tests aus dem Testsystem umgehend entfernt.
+ Der Kopiervorgang und die Nutzung von organisationsrelevanten Informationen als Testdaten werden zur späteren Prüfung aufgezeichnet (Audit Trail).

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 14.4 **Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene externe IT-Dienste (insbes. Cloud-Dienste) zum Verarbeiten von Unternehmensdaten eingesetzt werden?**
-

Ziel:

Insbesondere bei Cloud-Diensten, die oft mit verhältnismäßig geringen Kosten oder kostenfrei genutzt werden können, besteht ein erhöhtes Risiko, dass etablierte Beschaffungsprozesse umgangen werden und die Beschaffung und Inbetriebnahme damit auch ohne geeignete Berücksichtigung der technischen und vertraglichen Anforderungen an die Informationssicherheit erfolgt. Wenn externe IT-Dienste ohne die Berücksichtigung der Sicherheitsvorgaben genutzt werden, kann die Sicherheit an dieser Stelle nicht gewährleistet werden.

Es muss daher sichergestellt sein, dass eine Inbetriebnahme von externen IT-Diensten nicht erfolgt, ohne dass die dafür vorgesehenen Prozesse durchlaufen werden und so die Informationssicherheitsprozesse und Vorgaben vor Inbetriebnahme berücksichtigt wurden.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Alle Personen mit Zugriff auf sensible Informationen sind sich bewusst, dass der Einsatz von externen IT-Diensten ohne explizite Bewertung und Umsetzung der Informationssicherheitsanforderungen nicht zulässig ist.
- Dies beinhaltet auch externe IT-Dienste, die kostenfrei genutzt werden können.

Hierzu sollte gehören:
+ Vorgaben zur Beschaffung, Inbetriebnahme und Freigabe zur Nutzung von externen IT-Dienstleistungen sind etabliert.
+ Die Inbetriebnahme und Nutzung von externen IT-Diensten ist durch eine für alle Mitarbeiter verbindliche Anweisungen geregelt.
+ Alle Mitarbeiter werden in regelmäßigen Schulungen entsprechend sensibilisiert.
- z.B. im Rahmen der regelmäßigen Informationssicherheitsschulungen.
+ Die Einhaltung der Anweisung wird regelmäßig überprüft.
+ Die freigegebenen IT-Dienste und deren zulässige Nutzung sind katalogisiert.

Hierzu kann gehören:
+ Es wurden Rahmenverträge mit wesentlichen Cloud-Dienstleistern abgeschlossen, die den Einsatz nur in geeigneten und bewerteten Konfigurationen zulassen und die in der Organisation Verantwortlichen informiert.
+ Kataloge zulässiger IT-Dienste werden entsprechenden Fachabteilungen zur Verfügung gestellt.

Zusätzlich bei hohem Schutzbedarf:
+ Es wird in internen Audits regelmäßig geprüft, dass keine unzulässigen externe IT-Dienste genutzt werden.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

15 Supplier Relationships

☐ 15.1 **Inwieweit werden Anforderungen an die Informationssicherheit bei einem Lieferanten zur Risikoreduzierung vertraglich vereinbart, wenn dieser Zugriff auf Unternehmenswerte erhält (insbesondere Informations- und Kommunikationsdienste sowie beim Einsatz von Unterauftragnehmern)?**

(Referenz zu ISO 27001: Control A15.1.1 - A15.1.3)

☐ 15.2 **Inwieweit werden die erbrachten Leistungen eines Lieferanten bzw. beim Unterauftragnehmer regelmäßig überwacht, überprüft und auditiert?**
(Referenz zu ISO 27001: Control A15.2.1)

16 Information Security Incident Management

☐ 16.1 **Inwieweit sind Verantwortlichkeiten, Verfahren, Meldewege und Kritikalitäts-Stufen im Umgang mit Informationssicherheitsereignissen oder -schwachstellen festgelegt?**
(Referenz zu ISO 27001: Control A16.1.1 - A16.1.3)

Ziel: Die Erkennung und Abwehr von Sicherheitsereignissen benötigt in der Regel eine wirksame und konsistente Herangehensweise. Hierzu müssen die Verantwortlichkeiten und Verfahren zum Umgang mit Informationssicherheitsereignissen festgelegt werden damit eine schnelle Reaktion auf Informationssicherheitsereignisse sichergestellt ist. Wesentliches Element der Verfahren sind hierbei geeignete Meldewege und eine Sensibilisierung aller Mitarbeiter.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Eine Richtlinie zur Meldung von Informationssicherheitsereignissen oder -schwachstellen, welche mindestens die folgenden Vorgaben enthält, ist erstellt:
- Verhalten bei Informationssicherheitsereignissen gemäß definierter Kritikalitätsstufen
- Meldeformular
- Meldeweg
- bearbeitende Organisation
- Vorgaben für ein Feedbackverfahren
- Hinweise auf technische und organisatorische Maßnahmen (u. a. Disziplinarmaßnahmen)

Hierzu sollte gehören:
Keine.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
+ Anforderungen aus Geschäftsbeziehungen (z. B. Meldepflichten an die Auftraggeber) sind ermittelt und umgesetzt.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

☐ 16.2 **Inwieweit erfolgt eine Bearbeitung von Informationssicherheitsereignissen?**
(Referenz zu ISO 27001: Control A16.1.4 - A16.1.7)

Ziel: Informationssicherheitsereignisse müssen bewertet werden. Auf Basis von definierten Verfahren muss eine angemessene Reaktion auf Informationssicherheitsereignisse erfolgen. Im Nachgang zu Informationssicherheitsereignissen müssen die Erkenntnisse dazu genutzt werden die Eintrittswahrscheinlichkeit zukünftiger Ereignisse zu verringern.

Anforderungen:

Hierzu muss gehören:
+ Verfahren zur Sicherstellung der Nachweisbarkeit bei Informationssicherheitsereignissen/-schwachstellen sind etabliert und dokumentiert.
+ Informationssicherheitsereignisse/-schwachstellen werden bewertet und zur Sicherstellung der Nachweisbarkeit dokumentiert.
+ Eine angemessene Reaktion auf Informationssicherheitsereignisse/-schwachstellen erfolgt.

Hierzu sollte gehören:
+ Informationssicherheitsereignisse/-schwachstellen (Problem-Management) werden ausgewertet.
+ Maßnahmen zur Verhinderung des erneuten Auftretens ähnlicher Informationssicherheitsereignisse sind definiert und umgesetzt.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

17 Information Security Aspects of Business Continuity Management

☐ 17.1 **Inwieweit werden die Anforderungen an Informationssicherheit (inkl. Redundanz entsprechender Einrichtungen) und die Weiterführung eines ISMS in Krisensituationen definiert, umgesetzt, überprüft und beurteilt?**
(Referenz zu ISO 27001: Control A17.1.1 - A17.1.3 und A17.2.1)

Ziel: In Krisensituationen ist die Informationssicherheit besonders gefährdet. Daher muss sichergestellt werden, dass auch in diesen Fällen die definierten Maßnahmen des ISMS weiterhin wirksamen Schutz bieten bzw. vorab definierte Ersatzmaßnahmen greifen.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Potenziell betroffene IT-Systeme und Software sind identifiziert.
+ Für den Krisenfall sind informationssicherheitsrelevante Verfahren, Prozesse und Abläufe berücksichtigt.

Hierzu sollte gehören:
+ Berücksichtigung der Informationssicherheit im BCM (Business Continuity Management) bzw. im Disaster Recovery Prozess, soweit vorhanden.
+ Informationssicherheitsmaßnahmen für den Krisenfall werden regelmäßig getestet.

Hierzu kann gehören:
+ Die Verantwortlichen für Informationssicherheit (siehe Control 6.1) sind in den Krisenstab integriert.
+ Die Redundanz im Bereich der IT-Einrichtungen und IT-Systemen (Verfügbarkeitsaspekte) wird sichergestellt.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

18 Compliance

18.1 **Inwieweit wird die Einhaltung gesetzlicher (länderspezifisch) und vertraglicher Bestimmungen sichergestellt (z.B. Schutz des geistiges Eigentums, Einsatz von Verschlüsselungstechniken und Schutz von Aufzeichnungen)?**
(Referenz zu ISO 27001: Control A18.1.1, A18.1.2, A18.1.3, A18.1.5)

Ziel: Ein wesentlicher Aspekt der Compliance ist die Einhaltung gesetzlicher, regulatorischer, vertraglicher und geschäftlicher Anforderungen und Vorgaben. Eine Organisation muss die für sie relevanten Anforderungen und Vorgaben kennen und einhalten. Dies umfasst unter anderem die Betrachtung der geistigen Eigentumsrechte. Weiterhin müssen für Aufzeichnungen Anforderungen zum Schutz vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung eingehalten werden. Auch die Verwendung kryptographischer Maßnahmen muss unter Einhaltung der relevanten Vereinbarungen, Gesetze und Vorschriften umgesetzt werden.

Anforderungen:

Hierzu muss gehören:
+ Gesetzliche, regulatorische und vertragliche Anforderungen und Vorgaben mit Relevanz zur Informationssicherheit, wie z. B. im Bereich Urheberrecht, werden regelmäßig ermittelt.
+ Regelungen bzgl. der Erfüllung von gesetzlichen, regulatorischen und vertraglichen Anforderungen sind definiert, umgesetzt und an die beauftragten Personen kommuniziert.

Hierzu sollte gehören:
+ Maßnahmen zur Erfüllung der Anforderungen mit Bezug auf geistige Eigentumsrechte und der Verwendung von urheberrechtlich geschützten Softwareprodukten (Beschaffung und Lizenzmanagement) sind definiert und umgesetzt.
+ Sensibilisierungsmaßnahmen zu Compliance-Themen der Informationssicherheit für Mitarbeiter werden regelmäßig durchgeführt.
+ Die Integrität von Aufzeichnungen gemäß vertraglicher, regulatorischer oder gesetzlicher Verpflichtungen und Geschäftsanforderungen sowie der Klassifizierung (Zugriffsschutz, Aufbewahrung) ist berücksichtigt.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.

Information Security Assessment - Ziele und Anforderungen

☐ 18.2 **Inwieweit werden Vertraulichkeit und Schutz von personenbezogenen Informationen gewährleistet (abhängig von nationalen Gesetzgebungen)?**
(Referenz zu ISO 27001: Control A18.1.4)

Ziel:	Die Privatsphäre und der Schutz von personenbezogener Information müssen entsprechend den Anforderungen der relevanten Gesetze und Vorschriften sichergestellt werden. Hierzu müssen Prozesse und Verfahren umgesetzt werden die einen geeigneten Schutz der personenbezogenen Informationen sicherstellen.
Anforderungen:	Hierzu muss gehören: + Gesetzliche und vertragliche Anforderungen bezüglich der Verfahren und der Prozesse bei der Verarbeitung von personenbezogenen Informationen sind ermittelt. + Information-Assets werden bzgl. personenbezogener Informationen klassifiziert. + Regelungen bzgl. der Erfüllung von gesetzlichen und vertraglichen Anforderungen zum Schutz personenbezogener Informationen sind definiert und an die beauftragten Personen kommuniziert. + Prozesse und Verfahren zum Schutz personenbezogener Informationen sind umgesetzt. Hierzu sollte gehören: Keine. Hierzu kann gehören: Keine. Zusätzlich bei hohem Schutzbedarf: Keine. Zusätzlich bei sehr hohem Schutzbedarf: Keine.

☐ 18.3 **Inwieweit wird das ISMS von einer unabhängigen Instanz in regelmäßigen Abständen oder bei signifikanten Änderungen geprüft?**
(Referenz zu ISO 27001: Control A18.2.1)

Ziel:	Als wesentliches Kontrollwerkzeug reicht es nicht aus, die Wirksamkeit des ISMS ausschließlich aus einer Innensicht zu bewerten. Es muss stattdessen zusätzlich in regelmäßigen Abständen und bei signifikanten Änderungen eine unabhängige und damit unbefangene Bewertung eingeholt werden.
Anforderungen:	Hierzu muss gehören: + Eine unabhängige und kompetente Instanz führt regelmäßig und nach signifikanten Änderungen der Organisation Prüfungen der Informationssicherheit durch. + Korrekturmaßnahmen für mögliche Abweichungen werden eingeleitet und verfolgt. Hierzu sollte gehören: + Die Ergebnisse der durchgeführten Prüfungen werden aufgezeichnet und aufbewahrt. + Die Ergebnisse der durchgeführten Prüfungen werden an die Organisationsleitung berichtet. Hierzu kann gehören: Keine. Zusätzlich bei hohem Schutzbedarf: Keine. Zusätzlich bei sehr hohem Schutzbedarf: Keine.

☐ 18.4 **Inwieweit wird sichergestellt, dass Richtlinien, Regelungen und andere relevante Informationssicherheitsstandards in Verfahren und Prozessen eingehalten werden?**
(Referenz zu ISO 27001: Control A18.2.2, A18.2.3)

Ziel:	Die Wirksamkeit von Richtlinien, Regelungen und relevanten Informationssicherheitsstandards muss kontinuierlich sichergestellt werden. Hierzu müssen regelmäßige Prüfungen bezüglich der Einhaltung der jeweils anzuwendenden Sicherheitsrichtlinien und -standards erfolgen. Dies schließt auch die Prüfung der Einhaltung von technischen Vorgaben der Informationssicherheitsrichtlinien mit ein. Die Ergebnisse der durchgeführten Prüfungen müssen aufgezeichnet werden und die Aufzeichnungen müssen aufbewahrt werden.

Information Security Assessment - Ziele und Anforderungen

Anforderungen:

Hierzu muss gehören:
+ Die Einhaltung von Richtlinien, Regelungen und Informationssicherheitsstandards wird überwacht.
+ Prüfungen zu Regelungen und Verfahren der Informationssicherheit werden regelmäßig organisationsweit durchgeführt.
+ Korrekturmaßnahmen für mögliche Nicht-Konformitäten (Abweichungen) werden eingeleitet und verfolgt.

Hierzu sollte gehören:
+ Die Ergebnisse der durchgeführten Prüfungen werden aufgezeichnet und aufbewahrt.
+ Eine Planung über Inhalt und Rahmenbedingungen (Zeitplanung, Umfang, Kontrollen) der durchzuführenden Prüfungen liegt vor.

Hierzu kann gehören:
Keine.

Zusätzlich bei hohem Schutzbedarf:
Keine.

Zusätzlich bei sehr hohem Schutzbedarf:
Keine.