Gegenüberstellung TISAX VDA ISA Katalog Version 4.1.1 und Version 5.0 bzw. 5.0.3

Was bleibt, was ist neu und was fällt weg?

Inhaltsverzeichnis

1 Einleitung

Bei der Durchführung von TISAX® Assessments wird der Fragenkatalog bzw. Prüfkatalog Information Security Assessment (ISA) des Verbands der Automobilindustrie (VDA) verwendet. Er enthält Anforderungen zu den Themen Informationssicherheit, Datenschutz und Prototypenschutz für Unternehmen der Automobilbranche.

Der VDA ISA Prüfkatalog wurde 2020 überarbeitet, insbesondere wurden der Aufbau des Katalogs umstrukturiert und Redundanzen entfernt. Des Weiteren wurden die Anforderungen auf Angemessenheit und Aktualität überprüft und entsprechend angepasst bzw. Ergänzungen vorgenommen.

In diesem Whitepaper werden die Versionen 4.1.1 und 5.0 bzw. 5.0.3 des VDA ISA Prüfkatalogs miteinander verglichen und Unterschiede gekennzeichnet. Dadurch lässt sich schnell erkennen, was bleibt, was neu ist und was zukunftig wegfällt.

Gerne möchten wir daraufhinweisen, dass das Whitepaper nicht durch den VDA überprüft wurde und es sich somit um keine durch den VDA freigegebene Gegenüberstellung handelt.

Hinweis: Leider darf der Text der Version 4.1.1 aus lizenzrechtlichen Gründen nicht in diesem Whitepaper dargestellt werden.

2 Zusammenfassung

2.1 Angaben gemäß Änderungshistorie in Version 5.0

Neustrukturierung des VDA ISA im Modul Informationssicherheit nach Themengebieten

- Neues Tabellenformat in allen Modulen zur besseren Übersicht und leichteren Exportmöglichkeiten
- Entfall des Moduls Anbindung Dritter und Übernahme der Anforderungen in das Modul Informationssicherheit
- Integration der Hinweise und Erläuterungen in das Modul Informationssicherheit, daher Entfall der Reiter Hinweise und Erläuterungen
- Überarbeitung aller Fragen, Ziele und Anforderungen
- Vereinheitlichung des Zielreifegrads über alle Controls auf Zielwert 3
- Integration des Controls 1.2 in das neue Control 1.2.1
- Integration des Controls 8.3 in das neue Control 3.1.4
- Integration des Controls 9.3 in das neue Control 4.2.1
- Integration des Controls 11.2 in das neue Control 3.1.2
- Integration des Controls 11.3 in das neue Control 3.1.1
- Integration des Controls 12.4 in das neue Control
- Integration des Controls 12.6 in das neue Control 5.2.4
- Integration des Controls 13.3 in das neue Control 5.2.7
- Integration der Controls 14.2 und 14.3 in das neue Control 5.3.1
- Integration des Controls 15.2 in das neue Control 6.1.1
- Integration des Controls 16.2 in das neue Control 1.6.1
- Entfall des Control 12.9
- Neues Control "mobiles Arbeiten" (2.1.4)
- Neues Control "Eignung von Mitarbeitern" (2.1.1)
- Neues Control "Umgang mit identifikationsmitteln" (4.1.1)

- Änderung der Lizenz auf Creative Commons BY ND 4.0 + spezielle Bedingungen zur Verbreitung von veränderten Versionen

2.2 Bemerkungen zur Änderungshistorie

- Teilweise sind die Anforderungen die in Version 4.1.1 unter „sollte“ waren, nun in Version 5.0.3 eine „muss“-Anforderung oder eine Zusatzanforderung bei hohem Schutzbedarf.
- An manchen Stellen sind „muss“-Anforderungen in Version 4.1.1, in Version 5.0.3 nun eine Zusatzanforderung bei hohem Schutzbedarf.
- Das „kann“ Kriterium ist entweder weggefallen oder in eine „sollte“-Anforderung aufgenommen worden.
- Modul „Informationssicherheit“
  - Integration des Controls 1.23 in das neue Control 1.2.1
  - Integration des Controls 8.3 in die neuen Controls 2.1.4, 3.1.3 und 3.1.4
  - Integration des Controls 9.3 in die neuen Controls 4.1.2, 4.1.3 und 4.2.1
  - Integration des Controls 9.4 in das Control 4.1.3
  - Integration des Controls 12.4 in das neue Control 3.1.2
- Modul „Anbindung Dritter“
  - Integration des Controls 23.7.2 in das neue Control 2.1.3
  - Control 23.9.2 ist entfallen
  - Integration des Controls 23.11.1 in das neue Control 3.1.1
  - Integration des Controls 23.13.3 in das neue Control 5.2.7
- Modul „Datenschutz“
  - Außer einer gramatikalischen Anpassung wurde das Modul vollständig in die neue Version aufgenommen.
  - Die Controls haben eine neue Anfangsnummer bekommen. Statt 24 wird nun mit 9 aufwärts gezählt.
- Modul „Prototypenschutz“
  - Die Controls haben eine neue Anfangsnummer bekommen. Statt 25 wird nun mit 8 aufwärts gezählt.
  - Kleine Änderungen wurden an den Controls 25.1.2 (NEU 8.1.2), 25.1.3 (NEU 8.1.3), 25.2.3 (NEU 8.2.3), 25.2.4 (NEU 8.2.4) vorgenommen.
- Änderung der Lizenz auf Creative Commons BY SA 4.0

2.3 Gültigkeiten

Folgende Gütligkeitsfristen gelten für den neuen bzw. den alten VDA ISA Katalog:

VDA ISA Katalog Version 4.1.1	VDA ISA Katalog Version 5.0
Bis zum 30.09.2020 für neu beginnende TISAX® Assessments gültig. Bis zum 31.03.2021 für laufende TISAX® Assessments gültig.	Ab dem 01.10.2020 für neu beginnende TISAX® Assessments gültig.

3 Lizenz

VDA ISA Katalog Version 4.1.1	VDA ISA Katalog Version 5.0.3
CC BY-ND 3.0 DE Namensnennung-Keine Bearbeitung	CC BY-SA 4.0 Namensnennung - Weitergabe unter gleichen Bedingungen

4 Legende

Was bleibt?	Text *Teilweise wurde der Text neu formuliert, der Sinn aber beibehalten. Zum besseren Verständnis wird der „alte“ Text zusätzlich angegeben und folgendermaßen gekennzeichnet:* *Text*
Was ist neu?	Text
Was fällt weg?	~~Text~~

5 Version 4.1.1 vs. Version 5.0.3

Nachfolgend werden die Inhalte der Versionen 4.1.1 und 5.0.3 des VDA ISA Katalogs miteinander verglichen. Änderungen wurden dementsprechend gekennzeichnet.

5.1 Modul Informationssicherheit

Control 1.1 -> Control 1.2.1

Version 5.0.3 Information Security Assessment
Control
1.2.1
Kontrollfrage:
Inwieweit wird in der Organisation Informationssicherheit gemanagt?
Anforderungen (muss)
+ Der Geltungsbereich (Scope) des ISMS (die vom ISMS gemanagte Organisation) ist festgelegt.
+ Die Anforderungen der Organisation an das ISMS sind ermittelt.
+ Die Organisationsleitung hat das ISMS beauftragt und freigegeben.
+ Das ISMS stellt der Organisationsleitung geeignete Kontroll- und Steuerungsmittel zur Verfügung (z. B. Management-Review).
+ Anwendbare Kontrollen wurden ermittelt (z. B. ISO 27001 Statement of Applicability, ausgefüllter ISA Katalog).
+ Die Wirksamkeit des ISMS wird regelmäßig durch das Management überprüft.
Anforderungen (sollte)
Keine.
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 1.2 -> Control 1.4.1

Version 5.0.3 Information Security Assessment
Control
1.4.1
Kontrollfrage:
Inwieweit werden Informationssicherheitsrisiken gemanagt?
Anforderungen (muss)

Version 5.0.3 Information Security Assessment
+ Risikobeurteilungen werden sowohl regelmäßig als auch anlassbezogen durchgeführt. + Informationssicherheitsrisiken werden in geeigneter Form (z. B. Eintrittswahrscheinlichkeit und potenzieller Schaden) bewertet. + Informationssicherheitsrisiken sind dokumentiert. + Jedem Informationssicherheitsrisiko ist ein Verantwortlicher (Risikoeigner) zugeordnet. Dieser ist für die Beurteilung und Behandlung der Informationssicherheitsrisiken verantwortlich.
Anforderungen (sollte)
+ Es existiert eine Vorgehensweise, wie Informationssicherheitsrisiken innerhalb der Organisation identifiziert, beurteilt und behandelt werden. + Kriterien für die Beurteilung und Behandlung von Informationssicherheitsrisiken sind vorhanden. + Maßnahmen zur Behandlung von Informationssicherheitsrisiken und deren Verantwortliche sind festgelegt und dokumentiert. - Es existiert ein Maßnahmenplan bzw. Statusübersicht der Maßnahmenumsetzung. + Bei Änderung des Umfelds (z. B. Organisationsstruktur, Standort, Änderung von Regelwerken) erfolgt eine zeitnahe Neubewertung.
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 1.3: Integration in Control 1.2.1

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
Siehe 1.2.1
Anforderungen (sollte)
-
Zusatzanforderungen bei hohem Schutzbedarf
-
Zusatzanforderungen bei sehr hohem Schutzbedarf

Version 5.0.3 Information Security Assessment
-

Control 5.1 -> Control 1.1.1

Version 5.0.3 Information Security Assessment
Control
1.1.1
Kontrollfrage:
Inwieweit sind Richtlinien zur Informationssicherheit vorhanden?
Anforderungen (muss)
+ Die Anforderungen an die Informationssicherheit sind ermittelt und dokumentiert. - Die Anforderungen sind an die Ziele der Organisation angepasst. - Eine Richtlinie ist erstellt und von der Organisationsleitung freigegeben. + Die Richtlinie enthält Ziele und den Stellenwert der Informationssicherheit in der Organisation.
Anforderungen (sollte)
+ 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 relevante Richtlinien zur Informationssicherheit sind erstellt. + Eine regelmäßige Prüfung und - falls notwendig - Überarbeitung der Richtlinien sind etabliert. + Die Richtlinien werden Mitarbeitern in geeigneter Form (z. B. Intranet) zur Verfügung gestellt. + Die Richtlinien werden fallbezogen (ggf. auch in Auszügen) an externe Geschäftspartner weitergegeben. + Mitarbeiter und externe Geschäftspartner werden über für sie relevante Änderungen informiert.
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 6.1 -> Control 1.2.2

Version 5.0.3 Information Security Assessment
Control
1.2.2
Kontrollfrage:

Version 5.0.3 Information Security Assessment
Inwieweit sind die Verantwortlichkeiten für Informationssicherheit organisiert?
Anforderungen (muss)
+ Verantwortlichkeiten für die Informationssicherheit in der Organisation sind definiert, dokumentiert und zugewiesen. + Die verantwortlichen Mitarbeiter sind definiert und für ihre Aufgabe qualifiziert. + Die notwendigen Ressourcen stehen zur Verfügung. + Die Ansprechpartner sind innerhalb der Organisation und relevanten Geschäftspartnern bekannt.
Anforderungen (sollte)
+ Es existiert eine Definition und Dokumentation einer geeigneten Informationssicherheitsstruktur in der Organisation.
Zusatzanforderungen bei hohem Schutzbedarf
+ Eine angemessene organisatorische Trennung von Verantwortlichkeiten sollte zur Vermeidung von Interessenskonflikten etabliert sein (Funktionstrennung, Separation of Duties).
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 6.2 -> Control 1.2.3

Version 5.0.3 Information Security Assessment
Control
1.2.3
Kontrollfrage:
Inwieweit werden Informationssicherheitsanforderungen in Projekten berücksichtigt?
Anforderungen (muss)
+ Projekte sind unter Berücksichtigung ihrer Anforderungen an die Informationssicherheit klassifiziert.
Anforderungen (sollte)
+ die Vorgehensweise und Kriterien zur Klassifizierung von Projekten sind dokumentiert. + in einer frühen Phase des Projektes wird eine Risikobewertung auf Basis der definierten Vorgehensweise durchgeführt und bei Änderungen des Projektes wiederholt. + Für identifizierte Informationssicherheitsrisiken werden Maßnahmen abgeleitet und im Projekt berücksichtigt.
Zusatzanforderungen bei hohem Schutzbedarf
+ Abgeleitete Maßnahmen werden im Verlauf des Projektes regelmäßig überprüft und bei Änderungen der Bewertungskriterien neu bewertet.

Version 5.0.3 Information Security Assessment
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 6.3 -> Control 3.1.4

Version 5.0.3 Information Security Assessment
Control
3.1.4
Kontrollfrage:
Inwieweit ist der Umgang mit mobilen IT-Geräten und mobilen Datenträgern gemanagt?
Anforderungen (muss)
+ Die Anforderungen an mobile IT-Geräte und mobilen Datenträgern sind ermittelt und erfüllt. Folgende Aspekte sind berücksichtigt: - Verschlüsselung - Zugriffsschutz (z. B. PIN, Passwort - Kennzeichnung (u. a. unter Berücksichtigung von Anforderungen zur Nutzung bei Kunden)
Anforderungen (sollte)
+ Registrierung der IT-Geräte. + Anwender sind über fehlende Datensicherung auf mobilen Geräten informiert.
Zusatzanforderungen bei hohem Schutzbedarf
+ Generelle Verschlüsselung der mobilen Datenträger oder der darauf gespeicherten Informationswerte. - Wenn dies technisch nicht möglich ist, werden Informationen durch vergleichbar wirksame Maßnahmen geschützt.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 6.4 -> Control 1.2.4

Version 5.0.3 Information Security Assessment
Control
1.2.4
Kontrollfrage:
Inwieweit sind die Verantwortlichkeiten zwischen Organisations-fremden IT-Service-Anbietern und der eigenen Organisation definiert?
Anforderungen (muss)
+ Eingesetzte betroffene IT-Dienste und IT-Dienstleistungen sind identifiziert.

Version 5.0.3 Information Security Assessment
+ Die für den IT-Dienst relevanten Sicherheitsanforderungen sind ermittelt.
+ Die verantwortliche Organisation für die Umsetzung der Anforderung ist definiert und sich ihrer Verantwortung bewusst.
+ Für gemeinsame Verantwortlichkeiten sind Mechanismen festgelegt und umgesetzt.
+ Die verantwortliche Organisation wird ihren jeweiligen Verantwortlichkeiten gerecht.
Anforderungen (sollte)
+ Bei IT-Diensten wurde die Konfiguration anhand der notwendigen Sicherheitsanforderungen konzipiert, umgesetzt und dokumentiert.
+ Das verantwortliche Personal ist entsprechend geschult.
Zusatzanforderungen bei hohem Schutzbedarf
+ Es existiert ein Verzeichnis betroffener IT-Dienstleistungen und IT-Dienste.
+ Die Anwendbarkeit der Controls des ISA wurde geprüft und dokumentiert.
+ Die Dienstkonfiguration ist in die regelmäßigen Sicherheitsprüfungen einbezogen.
+ Es liegen Nachweise vor, dass der IT-Dienstanbieter seiner Verantwortlichkeit gerecht wird.
+ Integration in lokale Schutzmaßnahmen (wie z. B. sichere Authentifikationsverfahren) ist etabliert und dokumentiert.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 7.1-> Control 2.1.2

Version 5.0.3 Information Security Assessment
Control
2.1.2
Kontrollfrage:
Inwieweit werden alle Mitarbeiter zur Einhaltung der Informationssicherheit verpflichtet?
Anforderungen (muss)
+ Es besteht eine Verpflichtung zur Geheimhaltung.
+ Es besteht eine Verpflichtung zur Einhaltung der Richtlinien zur Informationssicherheit.
Anforderungen (sollte)
+ Es besteht eine Verpflichtung zur Geheimhaltung über das Arbeitsverhältnis bzw. den Auftrag hinaus.
+ Informationssicherheit wird in den Arbeitsverträgen der Mitarbeiter berücksichtigt.
+ Eine Vorgehensweise bei Verstößen gegen oben genannte Verpflichtungen ist beschrieben.
Zusatzanforderungen bei hohem Schutzbedarf
Keine.

Version 5.0.3 Information Security Assessment
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 7.2 -> Control 2.1.3

Version 5.0.3 Information Security Assessment
Control
2.1.3
Kontrollfrage:
Inwieweit werden Mitarbeiter über die Risiken beim Umgang mit Informationen geschult und sensibilisiert?
Anforderungen (muss)
+ Mitarbeiter sind geschult und sensibilisiert.
Anforderungen (sollte)
+ Ein Konzept zur Sensibilisierung und Schulung der Mitarbeiter ist erstellt. Folgende Aspekte sind dabei mindestens berücksichtigt: - Richtlinie zur Informationssicherheit - Meldungen von Informationssicherheitsereignissen - Verhalten bei Auftreten von Schadsoftware - Richtlinien zu Benutzerkonten und Anmeldeinformationen (z. B. Passwortrichtlinie) - Compliance-Themen der Informationssicherheit - Anforderungen und Verfahren zum Einsatz von Geheimhaltungsvereinbarungen bei der Weitergabe von schutzbedürftigen Informationen - Einsatz organisationsfremder IT-Dienste + Zielgruppen für Schulungs- und Sensibilisierungsmaßnahmen (z. B. neue Mitarbeiter, Administratoren, Mitarbeiter mit Zugang zu Kundennetzwerken) sind ermittelt und in einem Schulungskonzept berücksichtigt. + Das Konzept wurde vom verantwortlichen Management 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.
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 8.1 -> Control 1.3.1

Version 5.0.3 Information Security Assessment
Control
1.3.1
Kontrollfrage:
Inwieweit werden Informationswerte (Assets) identifiziert und erfasst?
Anforderungen (muss)
+ Die für die Organisation kritischen Informationswerte sind identifiziert und erfasst. - Diesen Informationswerten ist ein Verantwortlicher zugeordnet. + Informationsträger, welche die Informationswerte verarbeiten, sind identifiziert und erfasst. - Diesen Informationsträgern ist ein Verantwortlicher zugeordnet.
Anforderungen (sollte)
'+ Es existiert ein Verzeichnis der kritischen Informationswerte. - Jedem kritischen Informationswert sind die Informationsträger zugeordnet. - Eine regelmäßige Überprüfung des Verzeichnisses findet statt.
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 8.2 -> Control 1.3.2

Version 5.0.3 Information Security Assessment
Control
1.3.2
Kontrollfrage:
Inwieweit werden Informationswerte hinsichtlich ihres Schutzbedarfs klassifiziert und gemanagt?
Anforderungen (muss)
'+ Ein einheitliches Schema zur Klassifizierung von Informationswerten hinsichtlich des Schutzziels Vertraulichkeit ist vorhanden. + Es wird eine Bewertung der identifizierten Informationswerte nach den definierten Kriterien durchgeführt und dem vorhandenen Schema zur Klassifizierung zugeordnet. + Vorgaben für den Umgang mit Informationsträgern (z. B. Kennzeichnung, korrekte Handhabung, Transport, Speicherung, Rückgabe, Löschung/Entsorgung) in Abhängigkeit von der Klassifizierung der Informationswerte sind vorhanden und werden angewendet.
Anforderungen (sollte)
+ Die Schutzziele Integrität und Verfügbarkeit werden berücksichtigt.

Version 5.0.3 Information Security Assessment
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 8.3: Integration in Control 2.1.4, 3.1.3 und 3.1.4

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
-
Anforderungen (sollte)
Siehe 3.1.3
Zusatzanforderungen bei hohem Schutzbedarf
Siehe 2.1.4, 3.1.3 und 3.1.4
Zusatzanforderungen bei sehr hohem Schutzbedarf
-

Control 8.4 -> Control 5.3.3

Version 5.0.3 Information Security Assessment
Control
5.3.3
Kontrollfrage:
Inwieweit ist die Rückgabe und das sichere Entfernen von Informationswerten aus Organisationsfremden IT-Diensten geregelt?
Anforderungen (muss)
'+ Ein Verfahren zur Rückgabe und sicheren Entfernung der Informationswerte aus jedem organisationsfremden IT-Dienst ist definiert und umgesetzt.
Anforderungen (sollte)
+ Die Erfüllung der Verantwortlichkeiten des Anbieters ist vertraglich geregelt.
+ Eine Beschreibung des Terminierungsprozesses liegt vor und wird bei Änderungen angepasst.
+ Die im Verfahren vorgesehenen Verantwortlichkeiten sind dokumentiert und vom Anbieter anerkannt.

Version 5.0.3 Information Security Assessment

Zusatzanforderungen bei hohem Schutzbedarf

Keine.

Zusatzanforderungen bei sehr hohem Schutzbedarf

Keine.

Control 9.1 -> Control 4.1.2

Version 5.0.3 Information Security Assessment

Control

4.1.2

Kontrollfrage:

Inwieweit wird der Zugang von Benutzern zu Netzwerkdiensten, IT-Systemen und IT-Anwendungen gesichert?

Anforderungen (muss)

+ Die Auswahl der Verfahren zur Benutzerauthentifizierung wurde auf Basis einer Risikobewertung getroffen. Mögliche Angriffsszenarien wurden berücksichtigt (z. B. direkte Zugriffsmöglichkeit aus dem Internet).

+ Die eingesetzten Verfahren zur Benutzerauthentifizierung entsprechen dem aktuellen Stand der Technik.

Anforderungen (sollte)

+ Die Verfahren zur Benutzerauthentifizierung werden auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen definiert und umgesetzt.

+ Es werden höherwertige Verfahren zur Authentifizierung von privilegierten Benutzerkonten verwendet (z. B. Privileged Access Management, 2-Faktor-Authentifizierung).

Zusatzanforderungen bei hohem Schutzbedarf

+ Benutzer werden vor dem Zugriff auf Daten mit hohem Schutzbedarf mindestens durch starke Passworte nach Stand der Technik authentifiziert.

+ Abhängig von der Risikobewertung wurde das Authentifizierungsverfahren und der Zugriffsschutz durch ergänzende Maßnahmen verstärkt (z. B. dauerhaftes Monitoring der Zugriffe auf Unregelmäßigkeiten oder Einsatz einer starken Authentifizierung, automatische Abmeldung oder Sperrung bei Inaktivität).

Zusatzanforderungen bei sehr hohem Schutzbedarf

+ Benutzer werden vor dem Zugriff auf Daten mit sehr hohem Schutzbedarf durch starke Authentifizierung nach Stand der Technik (z. B. 2-Faktor-Authentifizierung) authentifiziert.

Version 5.0.3 Information Security Assessment

Control 9.2 -> Control 4.1.3

Version 5.0.3 Information Security Assessment

Control

4.1.3

Kontrollfrage:

Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewandt?

Anforderungen (muss)

+ Die Anlage, Änderung und Löschung (Life-Cycle) von Benutzerkonten wird durchgeführt.

+ Es werden eindeutige und personalisierte Benutzerkonten verwendet.

+ 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 der Organisation bzw. Ausscheiden aus der Organisation (z. B. nach Ende des Arbeitsvertrags) gesperrt.

+ Benutzerkonten werden in regelmäßigen Abständen überprüft.

+ Es erfolgt eine sichere Zustellung der Anmeldeinformationen für Benutzer.

+ Eine Richtlinie zum Umgang mit Anmeldeinformationen ist definiert und umgesetzt. Folgende Aspekte sind berücksichtigt:

- Keine Weitergabe von Anmeldeinformationen an Dritte - auch nicht an Autoritätspersonen - unter Beachtung gesetzlicher Rahmenbedingungen

- Kein Notieren von Anmeldeinformationen oder deren 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).

+ Die Anmeldeinformationen (z. B. Passwörter) eines personalisierten Benutzerkontos dürfen nur dem zugeordneten Benutzer bekannt sein.

Anforderungen (sollte)

+ Ein Basis-Benutzerprofil mit minimalen Zugriffsrechten und Funktionalitäten ist vorhanden und wird angewendet.

+ Herstellerseitig vorgegebene Standardkonten und -Passwörter werden deaktiviert (z. B. durch Sperrung oder Änderung des Passworts).

+ Die Einrichtung von Benutzerkonten erfolgt durch die verantwortliche Stelle oder ist durch diese autorisiert.

+ Die Einrichtung von Benutzerkonten unterliegt einem Genehmigungsprozess (4-Augen-Grundsatz).

+ Benutzerkonten von Dienstleistern werden nach Beendigung der Aufgabe gesperrt.

+ Sperr- und Löschfristen für Benutzerkonten sind definiert.

+ Die Verwendung von Standard-Passworten wird technisch verhindert.

+ Beim Einsatz einer starken Authentifizierung wird das Medium (z. B. Faktor Besitz) sicher verwendet.

Version 5.0.3 Information Security Assessment
+ Es findet eine regelmäßige Überprüfung der Benutzerkonten statt. Dazu gehören auch Benutzerkonten in IT-Systemen von Kunden.
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 9.3: Integration in Control 4.1.2, 4.1.3 und 4.2.1

Version 5.0.3 Information Security Assessment
Control
-
-
Siehe Control 4.1.2, 4.1.3 und 4.2.1
Siehe Control 4.2.1
-
-

Control 9.4: Integration in Control 4.1.3

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
Siehe Control 4.1.3
Anforderungen (sollte)
Siehe Control 4.1.3

Version 5.0.3 Information Security Assessment
Zusatzanforderungen bei hohem Schutzbedarf
-
Zusatzanforderungen bei sehr hohem Schutzbedarf
-

Control 9.5 -> Control 4.2.1

Version 5.0.3 Information Security Assessment
Control
4.2.1
Kontrollfrage:
Inwieweit werden Zugriffsberechtigungen vergeben und gemanagt?
Anforderungen (muss)
+ Die Anforderungen an das Management von Zugriffsberechtigungen (Autorisierung) sind ermittelt und erfüllt. Folgende Aspekte sind berücksichtigt: - Verfahren zur Beantragung, Prüfung und Genehmigung - Anwendung des Minimalitätsprinzips ("Need-to-know") + Es findet eine regelmäßige Überprüfung der gewährten Zugriffsberechtigungen von normalen und privilegierten Benutzerkonten sowie technischen Konten statt, auch in IT-Systemen von Kunden.
Anforderungen (sollte)
+ Berechtigungskonzepte für den Zugriff auf Informationen sind erstellt. + Berechtigungs-Rollen werden verwendet. + Die Vergabe von Rechten erfolgt bedarfsorientiert und entsprechend der Rolle bzw. Verantwortungsbereich. + Normalen Benutzerkonten werden keine privilegierten Zugriffsberechtigungen erteilt + Die Zugriffsrechte des Benutzerkontos eines Anwenders wird nach dessen Wechsel (z. B. in einen anderen Verantwortungsbereich) angepasst.
Zusatzanforderungen bei hohem Schutzbedarf
+ Die Zugriffsberechtigungen sind durch den Informationsverantwortlichen (intern) freigegeben. + Bestehende Zugriffsberechtigungen werden in kürzeren Abständen regelmäßig überprüft. (z. B. vierteljährlich) + Bei externem Betrieb der IT-Infrastruktur (z. B. Server) und/oder Cloud-Lösungen ist sichergestellt, dass die Anforderungen zur Verschlüsselung gemäß Kontrollfrage 5.1.1 eingehalten werden.
Zusatzanforderungen bei sehr hohem Schutzbedarf
+ Verhinderung von Zugriff und Kenntnisnahme durch nicht autorisierte Personen (privilegierte Nutzer): - Informationen werden auf inhaltlicher Ebene (z. B. Dateiebene) verschlüsselt gespeichert. - Wenn eine Verschlüsselung nicht möglich ist, müssen Informationen durch vergleichbar wirksame Maßnahmen geschützt werden.

Version 5.0.3 Information Security Assessment

Control 9.6 -> Control 5.3.4

Version 5.0.3 Information Security Assessment

Control

5.3.4

Kontrollfrage:

Inwieweit sind Informationen in gemeinsam genutzten organisationsfremden IT-Diensten geschützt?

Anforderungen (muss)

+ Es ist sichergestellt, dass durch eine wirksame Trennung (z. B. Mandantentrennung) unbefugte Nutzer anderer Organisationen nicht auf eigene Informationen zugreifen können.

Anforderungen (sollte)

+ Das Trennungskonzept des Anbieters ist dokumentiert und wird bei Änderungen angepasst. Folgende Aspekte sind berücksichtigt:
  - Separierung von Daten, Funktionen, Applikationen, Betriebssystem, Speicher und Netzwerk.
  - Risikobewertung für den Betrieb von Fremdsoftware innerhalb der geteilten Umgebung.

+ Gemeinsam genutzte IT-Systeme sind entsprechend gehärtet.

Zusatzanforderungen bei hohem Schutzbedarf

Keine.

Zusatzanforderungen bei sehr hohem Schutzbedarf

Keine.

Control 10.1 -> Control 5.1.1

Version 5.0.3 Information Security Assessment

Control

5.1.1

Kontrollfrage:

Inwieweit wird die Nutzung kryptografischer Verfahren gemanagt?

Anforderungen (muss)

+ Alle eingesetzten kryptographischen Verfahren (z. B. Verschlüsselungs-, Signatur, und Hash-Algorithmen, Protokolle, Applikationen) bieten nach dem Stand der Technik die notwendige Sicherheit für das Einsatzgebiet.

Version 5.0.3 Information Security Assessment
+ Rechtliche Rahmenbedingungen für den Einsatz von Kryptographie sind berücksichtigt.
Anforderungen (sollte)
'+ Erstellung eines technischen Regelwerkes mit Anforderungen an die Verschlüsselung zum Schutz von Informationen gemäß ihrer Klassifizierung. + Ein Nutzungskonzept für Kryptographie ist definiert und umgesetzt. Folgende Aspekte sind berücksichtigt: - Kryptographische Verfahren - Schlüsselstärken - Verfahren für den kompletten Lebenszyklus von kryptographischen Schlüsseln inkl. Erzeugung, Speicherung, Archivierung, Abruf, Verteilung, Deaktivierung, Erneuerung und Löschung. + Ein Notfallprozess zur Wiederherstellung von Schlüsselmaterial ist etabliert.
Zusatzanforderungen bei hohem Schutzbedarf
+ Anforderungen an Schlüsselhoheit sind ermittelt und erfüllt. - Risiken bei organisationsfremder Verarbeitung (z. B. in der Cloud) sind berücksichtigt.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 11.1 -> Control 3.1.1

Version 5.0.3 Information Security Assessment
Control
3.1.1
Kontrollfrage:
Inwieweit werden Sicherheitszonen für den Schutz von Informationswerten gemanagt?
Anforderungen (muss)
+ Ein Sicherheitszonenkonzept inkl. der zugehörigen Schutzmaßnahmen basierend auf den Anforderungen zum Umgang mit Informationswerten ist definiert und dokumentiert. + Sicherheitszonen sind unter Berücksichtigung von Geländen/Gebäuden/Räumen definiert und dokumentiert. Dies schließt Anlieferungs- und Versandbereiche mit ein. + Die definierten Schutzmaßnahmen sind umgesetzt. + Die Verhaltensregeln für Sicherheitszonen sind allen betroffenen Personen bekannt.
Anforderungen (sollte)
+ Verfahren zur Vergabe und zum Entzug von Zutrittsberechtigungen sind etabliert. + Richtlinien für das Besuchermanagement (inkl. Registrierung und Begleitung von Besuchern) sind definiert. + Richtlinien für Einbringen und Nutzung von mobilen IT-Geräten und mobilen Datenträgern (z. B. Registrierung vor Mitnahme auch bei Gästen, Kennzeichnungspflichten) sind definiert und umgesetzt.

Version 5.0.3 Information Security Assessment
+ Netzwerk-/Infrastrukturkomponenten (eigene oder Kundennetzwerke) sind vor unautorisiertem Zugang geschützt. + Externe Liegenschaften zur Lagerung und Verarbeitung von Informationswerten sind im Rahmen des Sicherheitszonenkonzeptes berücksichtigt (z. B. Lagerräume, Garagen, Werkstätten, Teststrecken, Rechenzentren).
Zusatzanforderungen bei hohem Schutzbedarf
+ Maßnahmen zum Schutz gegen einfaches Mithören und Einsichtnahme sind umgesetzt.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 11.2: Integration in Control 3.1.2

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
Siehe Control 3.1.2.
Anforderungen (sollte)
Siehe Control 3.1.2.
Zusatzanforderungen bei hohem Schutzbedarf
-
Zusatzanforderungen bei sehr hohem Schutzbedarf
-

Control 11.3: Integration in Control 3.1.1

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
Siehe Control 3.1.1.
Anforderungen (sollte)
-
Zusatzanforderungen bei hohem Schutzbedarf

Version 5.0.3 Information Security Assessment
-
Zusatzanforderungen bei sehr hohem Schutzbedarf
-

Control 11.4 -> Control 3.1.3

Version 5.0.3 Information Security Assessment
Control
3.1.3
Kontrollfrage:
Inwieweit ist der Umgang mit Informationsträgern gemanagt?
Anforderungen (muss)
+ Die Anforderungen an den Umgang mit Informationsträgern (z. B. Transport, Aufbewahrung, Reparatur, Verlust, Rückgabe, Entsorgung) sind ermittelt und erfüllt.
Anforderungen (sollte)
Keine.
Zusatzanforderungen bei hohem Schutzbedarf
'+ Informationsträger werden geschützt. Die Entsorgung von Informationsträgern erfolgt gemäß eines der gängigen Standards (z. B. ISO21964, mind. Sicherheitsstufe 4).
Zusatzanforderungen bei sehr hohem Schutzbedarf
+ Die Entsorgung von Informationsträgern erfolgt gemäß eines der gängigen Standards (z. B. ISO21964, mind. Sicherheitsstufe 5).

Control 12.1 -> Control 5.2.1

Version 5.0.3 Information Security Assessment
Control
5.2.1
Kontrollfrage:
Inwieweit werden Änderungen gesteuert?
Anforderungen (muss)
+ Anforderungen der Informationssicherheit bei Änderungen von Organisation, Geschäftsprozessen, IT-Systemen werden ermittelt und umgesetzt.

Version 5.0.3 Information Security Assessment
Anforderungen (sollte)
+ Ein formales Genehmigungsverfahren ist etabliert. + Änderungen werden bezüglich möglicher Auswirkungen auf die Informationssicherheit geprüft und bewertet. + Änderungen mit Auswirkung auf die Informationssicherheit werden geplant und getestet. + Verfahren für den Rückfall im Fehlerfall sind berücksichtigt.
Zusatzanforderungen bei hohem Schutzbedarf
+ Die Einhaltung der Anforderungen der Informationssicherheit wird während und nach der Umsetzung der Änderungen überprüft.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 12.2 -> Control 5.2.2

Version 5.0.3 Information Security Assessment
Control
5.2.2
Kontrollfrage:
Inwieweit sind die Entwicklungs- und Testumgebungen von den Produktivumgebungen getrennt?
Anforderungen (muss)
+ Eine Risikobewertung der IT-Systeme wurde durchgeführt, um zu ermitteln, inwiefern eine Trennung der IT-Systeme in Entwicklungs- und Produktivsysteme notwendig ist. + Eine Segmentierung ist auf Basis der Ergebnisse der Risikoanalyse umgesetzt.
Anforderungen (sollte)
'+ Die Anforderungen an Entwicklungs- und Testumgebungen sind ermittelt und umgesetzt. Folgende Aspekte sind berücksichtigt: - Trennung von Entwicklungs-, Test- und Produktivsystemen - Keine Entwicklungs- und Systemwerkzeuge auf Produktivsystemen (außer solchen, die für den Betrieb notwendig sind) - Verwendung von unterschiedlichen Benutzerprofilen auf Test- und Produktivsystemen
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf

Version 5.0.3 Information Security Assessment
Keine.

Control 12.3 -> Control 5.2.3

Version 5.0.3 Information Security Assessment
Control
5.2.3
Kontrollfrage:
Inwieweit werden IT-Systeme vor Schadsoftware geschützt?
Anforderungen (muss)
+ Anforderungen an den Schutz vor Schadsoftware sind ermittelt. + Technische und organisatorische Maßnahmen zum Schutz vor Schadsoftware sind definiert und umgesetzt.
Anforderungen (sollte)
+ Nicht benötigte Netzwerkdienste sind deaktiviert. + Zugriff auf Netzwerkdienste ist mit geeigneten Schutzmaßnahmen (siehe Beispiele) auf die benötigten Zugriffe eingeschränkt. + Eine 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 erfolgt. - Verschlüsselte Verbindungen werden berücksichtigt. + Maßnahmen zur Sicherstellung, dass Schutzsoftware nicht durch Benutzer deaktiviert oder verändert werden kann, sind definiert und umgesetzt. + Die fallbezogene Sensibilisierung von Mitarbeiter. + Für IT-Systeme, die ohne Software zum Schutz von Schadsoftware betrieben werden, sind alternative Maßnahmen (z. B. spezielle Härtung, wenig Dienste, keine aktiven User, Netzisolierung) umgesetzt.
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 12.4: Integration in Control 3.1.2

Version 5.0.3 Information Security Assessment

Control

-

Kontrollfrage:

-

Anforderungen (muss)

Siehe Control 3.1.2.

Anforderungen (sollte)

-

Zusatzanforderungen bei hohem Schutzbedarf

-

Zusatzanforderungen bei sehr hohem Schutzbedarf

-

Control 12.5 -> Control 5.2.4

Version 5.0.3 Information Security Assessment

Control

5.2.4

Kontrollfrage:

Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert?

Anforderungen (muss)

+ Anforderungen an die Informationssicherheit bezüglich der Handhabung von Ereignisprotokollen sind ermittelt und erfüllt.

+ Sicherheitsrelevante Anforderungen an die Protokollierung der Aktivitäten von Systemadministratoren und Nutzern sind ermittelt und erfüllt.

+ Die eingesetzten IT-Systeme werden hinsichtlich der Notwendigkeit der Protokollierung bewertet.

+ Bei der Nutzung extern betriebener Dienste (insbesondere Cloud Services) werden Informationen zu den Überwachungsmöglichkeiten eingeholt und in der Bewertung berücksichtigt.

+ Die Ereignisprotokolle werden regelmäßig auf Regelverstöße und Auffälligkeiten im Einklang mit den zulässigen gesetzlichen und betrieblichen Bestimmungen überprüft.

+ Es werden Verfahren für den Umgang mit Regelverstößen festgelegt (z. B. Weiterleitung autorisierte Stellen).

Anforderungen (sollte)

+ Ein Verfahren zur Meldung von Verstößen an die autorisierte Stelle (z. B. Security Incident Meldung, Datenschutz, Unternehmenssicherheit, IT-Sicherheit) ist definiert und etabliert.

+ Die Ereignisprotokolle (Inhalte und Metadaten) sind gegen Änderungen geschützt. (z. B. durch eine dedizierte Umgebung).

Version 5.0.3 Information Security Assessment
+ Angemessenes Überwachen und Aufzeichnen von informationssicherheitsrelevanten Aktionen im Netzwerk sind etabliert.
Zusatzanforderungen bei hohem Schutzbedarf
+ Sicherheitsrelevante Anforderungen an die Informationssicherheit bezüglich des Umgangs mit Ereignisprotokollen, wie z. B. Anforderungen aus Verträgen sind ermittelt und umgesetzt. + Zugriffe beim Auf- und Abbau von organisationsfremden Netzwerkverbindungen (z. B. Fernwartung) werden protokolliert.
Zusatzanforderungen bei sehr hohem Schutzbedarf
+ Protokollierung von allen Zugriffen auf Daten mit sehr hohem Schutzbedarf, soweit technisch möglich und im Rahmen der gesetzlichen und betrieblichen Bestimmungen zulässig.

Control 12.6: Integration in Control 5.2.4

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
Siehe Control 5.2.4.
Anforderungen (sollte)
Siehe Control 5.2.4.
Zusatzanforderungen bei hohem Schutzbedarf
Siehe Control 5.2.4.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Siehe Control 5.2.4.

Control 12.7 -> Control 5.2.5

Version 5.0.3 Information Security Assessment
Control
5.2.5
Kontrollfrage:
Inwieweit werden Schwachstellen erkannt und behandelt?
Anforderungen (muss)

Version 5.0.3 Information Security Assessment
'+ Informationen über technische Schwachstellen zu den genutzten IT-Systemen werden gesammelt (z. B. Information vom Hersteller, System-Audits, CVS-Datenbank) und bewertet (z. B. Common Vulnerability Scoring System CVSS). + Potenziell betroffene IT-Systeme und Software werden identifiziert, beurteilt und Schwachstellen behandelt.
Anforderungen (sollte)
+ Ein angemessenes Patch-Management ist definiert und umgesetzt (z. B. Test und Installation von Patches). + Risikominimierende Maßnahmen sind, soweit notwendig, umgesetzt. + Die erfolgreiche Installation von Patches ist in geeigneter Weise überprüft.
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 12.8 -> Control 5.2.6

Version 5.0.3 Information Security Assessment
Control
5.2.6
Kontrollfrage:
Inwieweit werden IT-Systeme technisch überprüft (Systemaudit)?
Anforderungen (muss)
+ Anforderungen an die Auditierung von IT-Systemen sind ermittelt. + Der Umfang des Systemaudits 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 Management berichtet. + Maßnahmen aus den Ergebnissen werden abgeleitet.
Anforderungen (sollte)
+ Systemaudits werden unter Berücksichtigung von ggf. dadurch erzeugten Sicherheitsrisiken (z. B. Störungen) geplant. + Systemaudits werden von ausgebildeten Spezialisten durchgeführt. + Für Systemaudits stehen geeignete Werkzeuge (z. B. Schwachstellen-Scanner) zur Verfügung. + Nach dem Audit wird in einem angemessenen Zeitraum ein Report erstellt.

Version 5.0.3 Information Security Assessment
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 12.9: Entfallen

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
-
Anforderungen (sollte)
-
Zusatzanforderungen bei hohem Schutzbedarf
-
Zusatzanforderungen bei sehr hohem Schutzbedarf
-

Control 13.1 -> Control 5.2.7

Version 5.0.3 Information Security Assessment
Control
5.2.7
Kontrollfrage:
Inwieweit wird das Netzwerk der Organisation gemanagt?
Anforderungen (muss)
+ Anforderungen zur Verwaltung und Steuerung von Netzwerken sind ermittelt und erfüllt. + Anforderungen an eine Segmentierung des Netzwerkes sind ermittelt und erfüllt.
Anforderungen (sollte)
+ Verfahren zur Verwaltung und Steuerung der Netzwerke sind definiert. + Bei der Segmentierung des Netzwerkes sind folgende Aspekte berücksichtigt: - Beschränkungen bei der Anbindung von IT-Systemen an das Netzwerk.

Version 5.0.3 Information Security Assessment
- Einsatz von Sicherheitstechnologien (siehe Beispiele) - Das erhöhte Risiko durch aus dem Internet erreichbare Netzwerkdienste (z.B. Nutzung von DMZ-Netzwerken) - Technologie-spezifische Trennungsmöglichkeiten (z. B. durch eine Firewall) bei Nutzung von organisationsfremden IT-Diensten - Geeignete Trennung von eigenen Netzwerken und Kundennetzwerken unter Berücksichtigung von Kundenanforderungen
Zusatzanforderungen bei hohem Schutzbedarf
+ Erweiterte Anforderungen an die Steuerung und Verwaltung von Netzwerken sind ermittelt und umgesetzt. Folgende Aspekte sind berücksichtigt: - Authentifizierung von IT-Systemen im Netzwerk - Der Zugriff auf die Managementschnittstellen von IT-Systemen ist eingeschränkt
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 13.2 -> Control 5.3.2

Version 5.0.3 Information Security Assessment
Control
5.3.2
Kontrollfrage:
Inwieweit sind Anforderungen an Netzwerkdienste definiert?
Anforderungen (muss)
+ Anforderungen an die Informationssicherheit von Netzwerkdiensten sind ermittelt und erfüllt.
Anforderungen (sollte)
+ Eine Verfahren für die Absicherung und Nutzung von Netzwerkdiensten sind definiert und umgesetzt. + Die Anforderungen werden in Form von SLAs vereinbart. + Angemessene Redundanzlösungen sind umgesetzt.
Zusatzanforderungen bei hohem Schutzbedarf
+ Verfahren zur Überwachung der Qualität des Netzwerkverkehrs (z. B. Verkehrsflussanalysen, Verfügbarkeitsmessungen) sind definiert und werden durchgeführt.
Zusatzanforderungen bei sehr hohem Schutzbedarf

Version 5.0.3 Information Security Assessment
Keine.

Control 13.3: Integration in Control 5.2.7

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
Siehe Control 5.2.7.
Anforderungen (sollte)
Siehe Control 5.2.7.
Zusatzanforderungen bei hohem Schutzbedarf
Zusatzanforderungen bei sehr hohem Schutzbedarf

Control 13.4 -> Control 5.1.2

Version 5.0.3 Information Security Assessment
Control
5.1.2
Kontrollfrage:
Inwieweit werden Informationen während der Übertragung geschützt?
Anforderungen (muss)
'+ Die verwendeten Netzwerkdienste zur Übertragung von Informationen sind identifiziert und dokumentiert. + Richtlinien und Verfahren gemäß den Vorgaben der Klassifizierung zur Nutzung der Netzwerkdienste sind definiert und umgesetzt. + Maßnahmen zum Schutz der übertragenen Inhalte vor unberechtigtem Zugriff sind umgesetzt.
Anforderungen (sollte)
+ Maßnahmen zur Sicherstellung der korrekten Adressen und des korrekten Transports von Informationen sind umgesetzt. + Der elektronische Datenaustausch erfolgt abhängig von der Klassifizierung durch Inhalts- und/oder Transportverschlüsselung.

Version 5.0.3 Information Security Assessment
Zusatzanforderungen bei hohem Schutzbedarf
+ Informationen sollten verschlüsselt transportiert oder übertragen werden. - Wenn eine Verschlüsselung nicht möglich ist, müssen Informationen durch vergleichbar wirksame Maßnahmen geschützt werden.
Zusatzanforderungen bei sehr hohem Schutzbedarf
+ E-Mails werden mittels Ende-zu-Ende-Verschlüsselung übertragen. + Verpflichtende Ende-zu-Ende-Verschlüsselung zu extern gehosteten IT-Systemen (vorzugsweise mit Schlüsselmaterial aus Organisations-eigenen IT-Systemen).

Control 13.5 -> Control 6.1.2

Version 5.0.3 Information Security Assessment
Control
6.1.2
Kontrollfrage:
Inwieweit ist Geheimhaltung beim Austausch von Informationen vertraglich vereinbart?
Anforderungen (muss)
+ Die Anforderungen an die Geheimhaltung sind ermittelt und erfüllt. + Anforderungen und Verfahren zum Einsatz von Geheimhaltungsvereinbarungen sind allen Personen bekannt, die schutzbedürftigen Informationen weitergeben. + Vor der Weitergabe von schutzbedürftigen Informationen werden gültige Geheimhaltungsvereinbarungen abgeschlossen. + Die Anforderungen und Verfahren zur Verwendung von Geheimhaltungsvereinbarungen und zum Umgang mit schutzbedürftigen Informationen werden regelmäßig überprüft.
Anforderungen (sollte)
+ Vorlagen für Geheimhaltungsvereinbarungen sind vorhanden und auf rechtliche Anwendbarkeit geprüft. + Geheimhaltungsvereinbarungen enthalten folgende Angaben: - beteiligte Personen/beteiligte Organisationen, - der Art der von der Vereinbarung umfassten Informationen, - den Gegenstand der Vereinbarung, - die Gültigkeitsdauer der Vereinbarung (befristet oder dauerhaft), - den Verantwortlichkeiten des/der Verpflichteten. + Geheimhaltungsvereinbarungen enthalten Bestimmungen zum Umgang mit den schutzbedürftigen 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 Geheimhaltungsvereinbarungen überwacht und rechtzeitig eine Verlängerung der Geheimhaltungsvereinbarungen angestoßen wird, ist definiert und umgesetzt.

Version 5.0.3 Information Security Assessment

Zusatzanforderungen bei hohem Schutzbedarf

Keine.

Zusatzanforderungen bei sehr hohem Schutzbedarf

Keine.

Control 14.1 -> Control 5.3.1

Version 5.0.3 Information Security Assessment

Control

5.3.1

Kontrollfrage:

Inwieweit wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt?

Anforderungen (muss)

+ Die Anforderungen an die Informationssicherheit bei der Planung und Entwicklung von IT-Systemen sind ermittelt und werden berücksichtigt.

+ Die Anforderungen an die Informationssicherheit bei der Beschaffung oder Erweiterung von IT-Systemen und IT-Komponenten sind ermittelt und werden berücksichtigt.

+ Anforderungen an die Informationssicherheit bei Änderungen in entwickelten IT-Systemen sind berücksichtigt.

+ Systemabnahmetests unter Berücksichtigung der Anforderungen an die Informationssicherheit werden durchgeführt.

Anforderungen (sollte)

+ Lastenhefte werden unter Berücksichtigung der Anforderungen zur Informationssicherheit erstellt.

+ Eine Prüfung von Lastenheften gegen die Anforderungen zur Informationssicherheit erfolgt.

+ Eine Prüfung des IT-Systems auf Einhaltung der Vorgaben vor dem produktiven Einsatz wird durchgeführt.

+ Es wird weitgehend vermieden, Produktivdaten zu Testzwecken zu nutzen (ggf. Anonymisierung oder Pseudonymisierung).

- Wenn Produktivdaten zu Testzwecken genutzt werden, muss sichergestellt werden, dass im Testsystem vergleichbare Schutzmaßnahmen wie im Produktivsystem vorhanden sind.

- Für den Lebenszyklus von Testdaten werden Anforderungen definiert (z. B. Löschung, max. Lebensdauer im IT-System).

- Es werden fallbezogene Vorgaben für die Erstellung von Testdaten definiert.

Zusatzanforderungen bei hohem Schutzbedarf

Keine.

Version 5.0.3 Information Security Assessment
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 14.2: Integration in Control 5.3.1

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
-
Anforderungen (sollte)
Siehe Control 5.3.1.
Zusatzanforderungen bei hohem Schutzbedarf
-
Zusatzanforderungen bei sehr hohem Schutzbedarf
-

Control 14.3: Integration in Control 5.3.1

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
-
Anforderungen (sollte)
Siehe Control 5.3.1.
Zusatzanforderungen bei hohem Schutzbedarf
-
Zusatzanforderungen bei sehr hohem Schutzbedarf
-

Control 14.4 -> Control 1.3.3

Version 5.0.3 Information Security Assessment
Control
1.3.3
Kontrollfrage:
Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene organisationsfremde IT-Dienste zum Verarbeiten von Informationswerten der Organisation eingesetzt werden?
Anforderungen (muss)
+ Es werden keine organisationsfremden IT-Dienste ohne explizite Bewertung und Umsetzung der Informationssicherheitsanforderungen eingesetzt - Eine Risikobewertung der organisationsfremden IT-Dienste liegt vor - Gesetzliche, regulatorische und vertragliche Anforderungen sind berücksichtigt + Die organisationsfremden IT-Dienste sind mit dem Schutzbedarf der verarbeiteten Informationswerte abgeglichen
Anforderungen (sollte)
+ Anforderungen an die Beschaffung, Inbetriebnahme und Freigabe zur Nutzung von organisationsfremden IT-Diensten sind ermittelt und erfüllt. + Ein Freigabeverfahren ist etabliert. + Die Einhaltung wird regelmäßig überprüft. + Organisationsfremde IT-Dienste und deren Freigabe je nach Schutzbedarf sind dokumentiert.
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 15.1 -> Control 6.1.1

Version 5.0.3 Information Security Assessment
Control
6.1.1
Kontrollfrage:
Inwieweit wird die Informationssicherheit bei Auftragnehmern und Kooperationspartnern sichergestellt?
Anforderungen (muss)
'+ Auftragnehmer und Kooperationspartner werden einer Risikobewertung bzgl. der Informationssicherheit unterzogen. + Mit Auftragnehmern und Kooperationspartnern wird durch vertragliche Vereinbarungen ein angemessenes Informationssicherheitsniveau sichergestellt. + Mit Auftraggebern vereinbarte vertragliche Vereinbarungen werden, soweit zutreffend, an Auftragnehmer und Kooperationspartner weitergegeben. + Eine Überprüfung der Einhaltung vertraglicher Vereinbarungen findet statt.

Version 5.0.3 Information Security Assessment
Anforderungen (sollte)
+ Auftragnehmer und Kooperationspartner werden vertraglich verpflichtet, Anforderungen an ein angemessenes Informationssicherheitsniveau zusätzlich an Unterauftragnehmer weiterzugeben. + Serviceberichte und Dokumente von Auftragnehmer und Kooperationspartner werden kontrolliert.
Zusatzanforderungen bei hohem Schutzbedarf
+ Ein Nachweis für ein dem Schutzbedarf der Informationen angemessenes Level der Informationssicherheit des Lieferanten (z. B. Zertifikat, Testat, eigene Auditierung) liegt vor.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 15.2: Integration in Control 6.1.1

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
Siehe Control 6.1.1.
Anforderungen (sollte)
Siehe Control 6.1.1.
Zusatzanforderungen bei hohem Schutzbedarf
-
Zusatzanforderungen bei sehr hohem Schutzbedarf
-

Control 16.1 -> Control 1.6.1

Version 5.0.3 Information Security Assessment
Control
1.6.1
Kontrollfrage:
Inwieweit werden Informationssicherheitsereignisse verarbeitet?

Version 5.0.3 Information Security Assessment
Anforderungen (muss)
+ Es existiert eine Definition von Informationssicherheitsereignissen/-schwachstellen. + Eine Vorgehensweise zur Meldung und Erfassung von Informationssicherheitsereignissen/-schwachstellen ist definiert und umgesetzt. + Folgende Aspekte sind berücksichtigt: - Verhalten bei Informationssicherheitsereignissen/-schwachstellen - Meldeformular und Meldeweg - Bearbeitende Stelle - Feedbackverfahren - Hinweise auf technische und organisatorische Maßnahmen (z. B. Disziplinarmaßnahmen). + 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. + Es existiert eine Strategie, um angemessen auf Vorfälle der Verletzung der Informationssicherheit zu reagieren. - Das beinhaltet u. a. Vorgehensweisen zur Eskalation, Wiederherstellung und Kommunikation an relevante interne und externe Stellen sowie eine Vorgehensweise zur Entscheidung, ob ein Cybercrime-Angriff strafrechtlich verfolgt wird.
Anforderungen (sollte)
+ Informationssicherheitsereignisse/-schwachstellen (Problem-Management) werden ausgewertet. + Maßnahmen zur Verhinderung des erneuten Auftretens ähnlicher Informationssicherheitsereignisse sind definiert und umgesetzt.
Zusatzanforderungen bei hohem Schutzbedarf
+ Anforderungen aus Geschäftsbeziehungen (z. B. Meldepflichten an die Auftraggeber) sind ermittelt und umgesetzt.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 16.2: Integration in Control 1.6.1

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-

Version 5.0.3 Information Security Assessment
Anforderungen (muss)
Siehe Control 1.6.1.
Anforderungen (sollte)
Siehe Control 1.6.1.
Zusatzanforderungen bei hohem Schutzbedarf
-
Zusatzanforderungen bei sehr hohem Schutzbedarf
-

Control 17.1 -> Control 3.1.2

Version 5.0.3 Information Security Assessment
Control
3.1.2
Kontrollfrage:
Inwieweit ist in Ausnahmesituationen die Informationssicherheit sichergestellt?
Anforderungen (muss)
+ Mögliche Ausnahmesituationen sind ermittelt und erfasst.
+ Potenziell bedrohte Infrastrukturkomponenten (z. B. Zugänge, IT-Systeme) sind ermittelt und erfasst.
+ Maßnahmen zur Begrenzung von Auswirkungen der Bedrohungen sind ermittelt und umgesetzt.
+ Für Ausnahmesituationen sind informationssicherheitsrelevante Aspekte in Verfahren, Prozessen und Abläufe berücksichtigt.
Anforderungen (sollte)
+ Notfallpläne sind definiert und werden regelmäßig geprüft.
+ Die physische Sicherheit wird auch in Ausnahmesituationen grundsätzlich aufrechterhalten.
+ IT Services werden auch in Ausnahmesituationen aufrechterhalten.
- Wiederherstellung von Daten und Applikationen mittels Backup- und Redundanzkonzepten
+ Strategien zur Vermeidung von dauerhaftem Informationsverlust sind definiert.
+ Angemessene Schutzmaßnahmen (z. B. Brandmeldeanlage, Brandschutz, Wassermelder) sind umgesetzt und werden regelmäßig geprüft.
+ Eine redundante Medienversorgung (z. B. Strom, Kommunikationsverbindungen) ist vorhanden.
+ Berücksichtigung der Informationssicherheit im Business Continuity Management.
+ Informationssicherheitsmaßnahmen für den Krisenfall werden regelmäßig getestet.
Zusatzanforderungen bei hohem Schutzbedarf
Keine.

Version 5.0.3 Information Security Assessment

Zusatzanforderungen bei sehr hohem Schutzbedarf

Keine.

Control 18.1 -> Control 7.1.1

Version 5.0.3 Information Security Assessment

Control

7.1.1

Kontrollfrage:

Inwieweit wird die Einhaltung regulatorischer und vertraglicher Bestimmungen sichergestellt?

Anforderungen (muss)

'+ Gesetzliche, regulatorische und vertragliche Anforderungen und Vorgaben mit Relevanz zur Informationssicherheit (siehe Beispiele) werden regelmäßig ermittelt.

+ Richtlinien zur Erfüllung der Anforderungen sind definiert, umgesetzt und an die verantwortlichen Personen kommuniziert.

Anforderungen (sollte)

+ 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 vertraglichen, regulatorischen oder gesetzlichen Verpflichtungen und Geschäftsanforderungen ist berücksichtigt.

Zusatzanforderungen bei hohem Schutzbedarf

Keine.

Zusatzanforderungen bei sehr hohem Schutzbedarf

Keine.

Control 18.2 -> Control 7.1.2

Version 5.0.3 Information Security Assessment

Control

7.1.2

Kontrollfrage:

Version 5.0.3 Information Security Assessment
Inwieweit wird der Schutz von personenbezogenen Daten bei der Umsetzung der Informationssicherheit berücksichtigt?
Anforderungen (muss)
'+ Gesetzliche und vertragliche Anforderungen an die Informationssicherheit bezüglich der Verfahren und der Prozesse bei der Verarbeitung von personenbezogenen Daten sind ermittelt. + Richtlinien bzgl. der Erfüllung von gesetzlichen und vertraglichen Anforderungen zum Schutz personenbezogener Daten sind definiert und den beauftragten Personen bekannt. + Prozesse und Verfahren zum Schutz personenbezogener Daten sind im Informationssicherheitsmanagementsystem berücksichtigt.
Anforderungen (sollte)
Keine.
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Control 18.3 -> Control 1.5.2

Version 5.0.3 Information Security Assessment
Control
1.5.2
Kontrollfrage:
Inwieweit wird das ISMS von einer unabhängigen Instanz überprüft?
Anforderungen (muss)
+ 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.
Anforderungen (sollte)
+ Die Ergebnisse der durchgeführten Prüfungen werden dokumentiert und an die Organisationsleitung berichtet.
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

Version 5.0.3 Information Security Assessment

Control 18.4 -> Control 1.5.1

Version 5.0.3 Information Security Assessment
Control
1.5.1
Kontrollfrage:
Inwieweit wird die Einhaltung der Informationssicherheit in Verfahren und Prozessen sichergestellt?
Anforderungen (muss)
+ Die Einhaltung von Richtlinien wird organisationsweit überprüft. + Prüfungen von Richtlinien und Verfahren der Informationssicherheit werden regelmäßig durchgeführt. + Korrekturmaßnahmen für mögliche Nicht-Konformitäten (Abweichungen) werden eingeleitet und verfolgt. + Die Einhaltung von Anforderungen der Informationssicherheit (z. B. technische Vorgaben) werden regelmäßig überprüft. + Die Ergebnisse der durchgeführten Prüfungen werden aufgezeichnet und aufbewahrt.
Anforderungen (sollte)
+ Eine Planung über Inhalt und Rahmenbedingungen (Zeitplanung, Umfang, Kontrollen) der durchzuführenden Prüfungen liegt vor.
Zusatzanforderungen bei hohem Schutzbedarf
Keine.
Zusatzanforderungen bei sehr hohem Schutzbedarf
Keine.

NEU Control 2.1.1

Version 5.0.3 Information Security Assessment
Control
2.1.1
Kontrollfrage:
Inwieweit wird die Eignung von Mitarbeitern für sensible Tätigkeitsbereiche sichergestellt?
Anforderungen (muss)
+ Sensible Tätigkeitsbereiche und Stellen sind ermittelt. + Die Anforderungen an Mitarbeiter bezüglich ihres Stellenprofils sind ermittelt und erfüllt. + Die Identität von potenziellen Mitarbeitern wird überprüft (z. B. Prüfung von Ausweisdokumenten).

Version 5.0.3 Information Security Assessment

Anforderungen (sollte)

+ Die persönliche Eignung von potenziellen Mitarbeitern wird mit einfachen Methoden überprüft (z. B. Einstellungsgespräch).

+ Es findet eine erweiterte Prüfung der Eignung abhängig vom Tätigkeitsbereich und Stelle statt. (z. B. Assessment-Center, psychologische Analyse, Prüfung von Referenzen, Zeugnissen und Diplomen, Einsichtnahme in Führungszeugnisse, Prüfung des beruflichen und privaten Hintergrunds).

Zusatzanforderungen bei hohem Schutzbedarf

Keine.

Zusatzanforderungen bei sehr hohem Schutzbedarf

Keine.

NEU Control 2.1.4

Version 5.0.3 Information Security Assessment

Control

2.1.4

Kontrollfrage:

Inwieweit ist mobiles Arbeiten geregelt?

Anforderungen (muss)

+ Die Anforderungen an mobiles Arbeiten sind ermittelt und erfüllt. Folgende Aspekte sind berücksichtigt:

- Sicherer Umgang mit und Zugriff auf Informationen (sowohl elektronisch als auch auf Papier) unter Berücksichtigung des Schutzbedarfs und der vertraglichen Anforderungen in privaten (z. B. im Home-Office) und öffentlichen Bereichen (z. B. auf Reisen)
- Verhalten in privaten Bereichen
- Verhalten in öffentlichen Bereichen
- Maßnahmen zum Schutz vor Diebstahl (z. B. in öffentlichen Bereichen)

+ Der Zugang zum Netzwerk der Organisation erfolgt über eine gesicherte Verbindung (z. B. VPN) und über eine starke Authentifizierung.

Anforderungen (sollte)

+ Folgende Aspekte sind berücksichtigt:

- Maßnahmen bei Reisen (z. B. bei Einsichtnahme durch Behörden)
- Maßnahmen bei Reisen in sicherheitskritische Länder

+ Mitarbeitersensibilisierung.

Zusatzanforderungen bei hohem Schutzbedarf

+ Maßnahmen zum Schutz gegen Mithören und Einsichtnahme sind umgesetzt.

Zusatzanforderungen bei sehr hohem Schutzbedarf

Keine.

NEU Control 4.1.1

Version 5.0.3 Information Security Assessment

Control

4.1.1

Kontrollfrage:

Inwieweit ist der Umgang mit Identifikationsmitteln gemanagt?

Anforderungen (muss)

+ Die Anforderungen an den Umgang mit Identifikationsmitteln über den gesamten Lebenszyklus sind ermittelt und erfüllt. Folgende Aspekte sind berücksichtigt:
  - Erstellung, Übergabe, Rückgabe und Vernichtung
  - Gültigkeitszeiträume
  - Umgang mit Verlust

Anforderungen (sollte)

+ Die Produktion von Identifikationsmitteln ist nur unter kontrollierten Bedingungen möglich.
+ Die Ausgabe von Identifikationsmitteln wird protokolliert.
+ Die Rückgabe von Identifikationsmitteln ist geregelt.

Zusatzanforderungen bei hohem Schutzbedarf

+ Die Gültigkeit von Identifikationsmitteln ist auf einen angemessenen Zeitraum beschränkt.
+ Ein Konzept zur Sperrung bzw. Invalidierung von Identifikationsmitteln bei Verlust ist - soweit möglich - erstellt und umgesetzt.

Zusatzanforderungen bei sehr hohem Schutzbedarf

Keine.

5.2 Modul Anbindung Dritter

Das Modul „Anbindung Dritter“ wurde in das Modul „Informationssicherheit“ integriert.

Control 23.7.2: Integration in Control 2.1.3

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
Siehe Control 2.1.3.
Anforderungen (sollte)
-
Zusatzanforderungen bei hohem Schutzbedarf
-
Zusatzanforderungen bei sehr hohem Schutzbedarf
-

Control 23.9.2: Entfallen

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
-
Anforderungen (sollte)
-
Zusatzanforderungen bei hohem Schutzbedarf
-
Zusatzanforderungen bei sehr hohem Schutzbedarf
-

Control 23.11.1: Integration in Control 3.1.1

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
-
Anforderungen (sollte)
-
Zusatzanforderungen bei hohem Schutzbedarf
Siehe Control 3.1.1.
Zusatzanforderungen bei sehr hohem Schutzbedarf
-

Control 23.13.3: Integration in Control 5.2.7

Version 5.0.3 Information Security Assessment
Control
-
Kontrollfrage:
-
Anforderungen (muss)
Siehe Control 5.2.7.
Anforderungen (sollte)
-
Zusatzanforderungen bei hohem Schutzbedarf
Siehe Control 5.2.7.
Zusatzanforderungen bei sehr hohem Schutzbedarf
-

5.3 Modul Datenschutz

Control 24.1 -> Control 9.1

Das Control 24.1 wurde unverändert in Control 9.1 der Version 5.0.3 übernommen.

Control 24.2 -> Control 9.2

Das Control 24.2 wurde mit gramatikalischen Änderungen in Control 9.2 der Version 5.0.3 übernommen.

Control 24.3 -> Control 9.3

Das Control 24.3 wurde unverändert in Control 9.3 der Version 5.0.3 übernommen.

Control 24.4 -> Control 9.4

Das Control 24.4 wurde unverändert in Control 9.4 der Version 5.0.3 übernommen.

5.4 Modul Prototypenschutz

Control 25.1.1-> Control 8.1.1

Das Control 25.1.1 wurde unverändert in Control 8.1.1 der Version 5.0.3 übernommen.

Control 25.1.2-> Control 8.1.2

Version 5.0.3 Zusatzanforderungen Prototypenschutz
Control
8.1.2
Kontrollfrage:
Inwieweit ist eine Perimetersicherung vorhanden, die einen unberechtigten Zutritt zu den zu schützenden Objekten der Liegenschaften verhindert?
Anforderungen (muss)
+ Ein unberechtigter Zutritt zu Liegenschaften ist nicht möglich.
Anforderungen (sollte)
+ Geeignete Barrieren sind vorhanden wie: - künstliche Barrieren (Zaunsysteme, Mauern) - technische Barrieren (Detektion) - natürliche Barrieren (Bewuchs, Vegetation).
Zusatzanforderungen bei als schutzbedürftig klassifizierten Fahrzeugen
Keine.

Control 25.1.3-> Control 8.1.3

Version 5.0.3 Zusatzanforderungen Prototypenschutz
Control
8.1.3
Kontrollfrage:
Inwieweit ist die Außenhaut der zu schützenden Gebäude in einer Form ausgeführt, die ein Entfernen oder Öffnen von Außenhautkomponenten mit handelsüblichen Werkzeugen nicht ermöglichen?
Anforderungen (muss)
+ Ein unberechtigter Zutritt in Gebäude / Sicherheitsbereiche ist nicht möglich.
Anforderungen (sollte)
+ Eine massive Bauweise (Mauerwerk, Beton, Stahlbeton oder Spannbeton). + Fenster und Türen in der Außenhaut sind in Anlehnung an RC2 oder höher auszuführen.
Zusatzanforderungen bei als schutzbedürftig klassifizierten Fahrzeugen

Version 5.0.3 Zusatzanforderungen Prototypenschutz
Keine.

Control 25.1.4-> Control 8.1.4

Das Control 25.1.4 wurde unverändert in Control 8.1.4 der Version 5.0.3 übernommen.

Control 25.1.5-> Control 8.1.5

Das Control 25.1.5 wurde unverändert in Control 8.1.5 der Version 5.0.3 übernommen.

Control 25.1.6-> Control 8.1.6

Das Control 25.1.6 wurde unverändert in Control 8.1.6 der Version 5.0.3 übernommen.

Control 25.1.7-> Control 8.1.7

Das Control 25.1.7 wurde unverändert in Control 8.1.7 der Version 5.0.3 übernommen.

Control 25.1.8-> Control 8.1.8

Das Control 25.1.8 wurde unverändert in Control 8.1.8 der Version 5.0.3 übernommen.

Control 25.2.1-> Control 8.2.1

Das Control 25.2.1 wurde unverändert in Control 8.2.1 der Version 5.0.3 übernommen.

Control 25.2.2-> Control 8.2.2

Das Control 25.2.2 wurde unverändert in Control 8.2.2 der Version 5.0.3 übernommen.

Control 25.2.3-> Control 8.2.3

Version 5.0.3 Zusatzanforderungen Prototypenschutz
Control
8.2.3
Kontrollfrage:
Inwieweit werden Mitarbeiter und Projektbeteiligte über den Umgang mit Prototypen nachweislich geschult und sensibilisiert?
Anforderungen (muss)
+ Sicherstellung der Durchführung von Schulungen/Sensibilisierungsprogrammen durch das Management + Schulung von Mitarbeitern und Projektbeteiligten im Umgang mit Prototypen bei Projekteinstieg + regelmäßige (min. jährliche) Schulung von Mitarbeitern im Umgang mit Prototypen + Sicherstellung der Kenntnis über die jeweiligen Schutzbedarfe und die daraus resultierenden Maßnahmen im Unternehmen bei den Mitarbeitern und Projektbeteiligten + verpflichtende Teilnahme an den Schulungen und Sensibilisierungsmaßnahmen für jeden Mitarbeiter und Projektbeteiligten + Die erfolgten Durchführungen sind zu dokumentieren.

Version 5.0.3 Zusatzanforderungen Prototypenschutz
+ das Schulungskonzept für den Prototypenschutz ist in dem allgemeinen Schulungskonzept verankert (siehe auch Control 2.1.3 Informationssicherheit)
Anforderungen (sollte)
Keine.
Zusatzanforderungen bei als schutzbedürftig klassifizierten Fahrzeugen
Keine.

Control 25.2.4-> Control 8.2.4

Version 5.0.3 Zusatzanforderungen Prototypenschutz
Control
8.2.4
Kontrollfrage:
Inwieweit sind die Sicherheitseinstufungen des Projekts und die daraus resultierenden Maßnahmen zur Absicherung bekannt?
Anforderungen (muss)
'+ Sicherstellung, dass jedem Projektbeteiligtem die Sicherheitseinstufung und die Sicherheitsvorgaben je nach Projektfortschritt bekannt gemacht sind. + Berücksichtigung von Stufenplänen, Maßnahmen zur Geheimhaltung und Tarnung, Entwicklungsrichtlinien. + Die Anforderungen werden als Anforderung für die Informationssicherheit des Projektes berücksichtigt (siehe Controls 1.2.3 und 7.1.1 Informationssicherheit).
Anforderungen (sollte)
Keine.
Zusatzanforderungen bei als schutzbedürftig klassifizierten Fahrzeugen
Keine.

Control 25.2.5-> Control 8.2.5

Das Control 25.2.5 wurde unverändert in Control 8.2.5 der Version 5.0.3 übernommen.

Control 25.2.6-> Control 8.2.6

Das Control 25.2.6 wurde unverändert in Control 8.2.6 der Version 5.0.3 übernommen.

Control 25.2.7-> Control 8.2.7

Das Control 25.2.7 wurde unverändert in Control 8.2.7 der Version 5.0.3 übernommen.

Control 25.3.1-> Control 8.3.1

Das Control 25.3.1 wurde unverändert in Control 8.3.1 der Version 5.0.3 übernommen.

Control 25.3.2 -> Control 8.3.2

Das Control 25.3.2 wurde unverändert in Control 8.3.2 der Version 5.0.3 übernommen.

Control 25.4.1 -> Control 8.4.1

Das Control 25.4.1 wurde unverändert in Control 8.4.1 der Version 5.0.3 übernommen.

Control 25.4.2 -> Control 8.4.2

Das Control 25.4.2 wurde unverändert in Control 8.4.2 der Version 5.0.3 übernommen.

Control 25.4.3 -> Control 8.4.3

Das Control 25.4.3 wurde unverändert in Control 8.4.3 der Version 5.0.3 übernommen.

Control 25.5.1 -> Control 8.5.1

Das Control 25.5.1 wurde unverändert in Control 8.5.1 der Version 5.0.3 übernommen.

Control 25.5.2 -> Control 8.5.2

Das Control 25.5.2 wurde unverändert in Control 8.5.2 der Version 5.0.3 übernommen.

Über uns

abat ist ein internationaler SAP-Dienstleister und Produktanbieter, der Unternehmensprozesse optimiert und mit eigenen Lösungen weiterentwickelt. Unsere Leistungen erbringen wir vorwiegend in den Branchen Automotive, Diskrete Fertigung und Logistik. Auch in den Bereichen Nachhaltigkeitsmanagement sowie Informationssicherheit können wir Sie unterstützen.

Wir sind deutschlandweit mit Standorten in Bremen, München, Oldenburg, St. Ingbert, Walldorf und Wolfsburg vertreten und besitzen Niederlassungen in den USA, Mexiko und Belarus. abat ist SAP Gold Partner sowie Entwicklungspartner im SAP Partner Edge Program for Application Development und besitzt darüber hinaus Recognized Expertise für Automotive, Travel and Transportation, Supply Chain Management sowie Consumer Products.

Im Bereich Automotive arbeiten wir für viele Hersteller, wie etwa Audi, BMW, Daimler, MAN, Porsche, Volkswagen und Qoros. Mit unserer eigenentwickelten Software PLUS auf Basis von SAP, werden die Produktionsprozesse bei Daimler gesteuert. Für Logistiker und Logistikdienstleister bietet abat Lösungen zur Optimierung der Supply Chain, z.B. in der Intralogistik und im Transportmanagement. Hier arbeiten wir unter anderem für Brose, Bosch, Daimler, DHL, thyssenkrupp und VS HEIBO Logistics. Bei der Sportsoftware SAP Sports One sind wir im Moment der einzige Einführungspartner der SAP. Im Nachhaltigkeitsmanagement bietet abat eine ganzheitliche Beratung an und zusätzlich die Unterstützung bei der Nachhaltigkeitsberichterstattung durch unsere Software ID-Report. Last but not least bieten wir im Bereich Informationssicherheit Beratungsleistungen zu den Themen ISO 27001 sowie TISAX® und helfen so, die Werte unserer Kunden und wiederum deren Kundschaft zu schützen.

Melissa Thesing
Senoir Consultant

isms-consulting@abat.de