Abdeckung NIS-2 durch TISAX

Bewertung des NIS-2-Erfüllungsgrades
einer TISAX-Prüfung gemäß Prüfkatalog ISA6

Published by

ENX Association
Bockenheimer Landstraße 97-99, 60325 Frankfurt am Main, Germany
20 rue Barthélémy Danjou, 92100 Boulogne-Billancourt, France

An Association according to the French Law of 1901, registered under No. W923004198 at the Sous-préfecture of Boulogne-Billancourt, France.

Editor

ENX WG ISA 2025

Contact

wg-isa@groups.enx.com

+49 69 9866927-79

Version

Date: 24.04.2025, Version: 1

Classification: public, ENX doc ID: 260

Legal Notices

Inhaltsverzeichnis

Executive Summary

Aus der NIS-2-Richtlinie ergeben sich Anforderungen an eine Vielzahl von Unternehmen der Automobilindustrie.

In der **Automobilindustrie** ist die Notwendigkeit branchenweiter Informations- und Cybersicherheit seit Jahren erkannt. Die Stärkung der **Cyber-Resilienz** wird strukturiert adressiert, u.a. durch die Etablierung des Prüfstandards TISAX im Jahr 2017 und den ihm zugrunde liegenden Anforderungskatalog ISA auf deren Basis derzeit bereits 17.500 Standorte geprüft sind.

Die strukturierte Analyse in diesem Dokument zeigt, dass Unternehmen, die ihre von der NIS-2 betroffenen Standorte TISAX-konform aufgestellt haben, damit die Anforderungen aus NIS-2 vollständig umsetzen. Der allen TISAX-Prüfungen zu Grunde liegende Anforderungskatalog (ISA) geht über die in der NIS-2 formulierten Anforderungen an die Informations- und Cybersicherheit von Unternehmen hinaus.

Der Anforderungskatalog wird durch ein Expertengremium kontinuierlich weiterentwickelt und von tausenden Unternehmen weltweit genutzt. Dabei werden neue Erkenntnisse aus dem Bereich der Informations- und Cybersicherheit berücksichtigt. Anforderungskatalog und Prüfstandard definieren damit den **Stand der Technik** in der Informations- und Cybersicherheit für die Industrie und halten diesen Anspruch permanent aufrecht.

Die jeweilige Umsetzung wird durch unabhängige Auditoren in einem Dreijahreszyklus bestätigt. Der Dreijahreszyklus der TISAX-Prüfung ist nach Einschätzung der Experten der Automobilindustrie für Informations- und Cybersicherheit als angemessen anzusehen.

Eine gemeinsamer Austauschmechanismus ermöglicht es den beteiligten Organisationen, den TISAX-Status eines Lieferanten oder Partners – und damit auch die Erfüllung der NIS-2-Anforderungen – jederzeit abzufragen.

Durch die intrinsisch motivierte Befassung der Automobilindustrie mit Informations- und Cybersicherheit über die vergangenen Jahre sind so bereits heute wesentliche Teile der Automobilzulieferindustrie und ihrer Partner auf die materiellen Anforderungen der Regulierung (NIS-2) vorbereitet.

Es verbleibt für alle betroffenen Organisationen die Notwendigkeit, die unterschiedlichen nationalstaatlichen Meldeanforderungen parallel zu pflegen und zu bedienen.

1 Einführung und Überblick

1.1 Zweck dieser Analyse

Die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, abgekürzt NIS-2-Richtlinie, ist eine EU-Richtlinie, die das Niveau der Cyber-Resilienz in der Europäischen Union stärken soll. Sie hat die EU-Richtlinie zur Netzwerk- und Informationssicherheit (Network and Information Security, NIS 1) aus dem Jahr 2016 ersetzt.

NIS-2 greift unter anderem die Vereinheitlichung der Spezifikation der betroffenen Unternehmen innerhalb der Mitgliedsstaaten auf und erweitert den Umfang der betroffenen Organisationen. Dies hat zur Folge, dass sich auch Unternehmen, die von der NIS 1-Richtlinie nicht betroffen waren, nun mit den Inhalten und Anforderungen auseinandersetzen müssen.

In der Automobilindustrie ist die Notwendigkeit branchenweiter Informations- und Cybersicherheit seit Jahren erkannt und wird strukturiert adressiert – u.a. durch den Aufbau des Prüfstandards TISAX und dem ihm zugrunde liegenden Anforderungskatalog ISA. Die im ISA formulierten Controls dienen dem gleichen Zweck, wie die in der NIS-2 definierten Maßnahmen: Es werden Cybersicherheitskapazitäten und -fähigkeiten in den Unternehmen aufgebaut und die Kontinuität von Diensten sichergestellt. Dies ist ein wesentlicher Beitrag zum reibungslosen Funktionieren von Wirtschaft und Gesellschaft in der Europäischen Union.

Um Unternehmen, die NIS-2 erfüllen müssen, bei der Bewertung umzusetzender Maßnahmen zu unterstützen, hat die Working Group (WG) ISA der ENX Association, eine Arbeitsgruppe führender Experten der Automobilindustrie für Informations- und Cybersicherheit, den aktuellen TISAX-Anforderungskatalog ISA6 mit den Anforderungen, die sich aus der NIS-2 ergeben, verglichen.

Es wurde betrachtet, ob und in welchem Umfang eine die Aufstellung und anschließende Prüfung einer Organisation nach ISA und TISAX die in der NIS-2 gestellten Anforderungen abdeckt.

1.2 Scope dieser Analyse

Diese Analyse befasst sich ausschließlich mit den Anforderungen, die in der NIS-2-Richtlinie definiert sind und die konkrete Umsetzungsvorgaben für Unternehmen enthalten.

Das Dokument gibt keine Hilfestellung bei der Implementierung oder Umsetzung eines Informationssicherheits-Managementsystems (ISMS) oder bei der Vorbereitung eines TISAX-Assessments und macht auch keine Aussage darüber, ob ein Unternehmen ausreichend für die Erfüllung der Anforderungen nach NIS-2 aufgestellt ist.

Bei der Bewertung des Erfüllungsgrades bezieht sich das Dokument auf eine nach den im ISA formulierten Anforderungen zur Informations- und Cybersicherheit durchgeführte TISAX-Prüfung.[1]

Die Analyse betrachtet die direkten Forderungen der NIS-2-Richtlinie. Länderspezifische Umsetzungen wie nationale Cybersicherheitsregularien, zuständige nationale Behörden, Behörden für das Cyberkrisenmanagement, zentrale Anlaufstellen für Cybersicherheit (zentrale Anlaufstellen) und Computer-Notfallteams (CSIRT) und mögliche materielle Zusatzanforderungen finden innerhalb dieses Dokuments keine Berücksichtigung.

Es bleibt hier im Verantwortungsbereich der geprüften Unternehmen, sich über mögliche länderspezifische Zusatzanforderungen zu informieren und diese gegen die umgesetzten Maßnahmen zu prüfen.

[1] Reine Prüfungen im Bereich des sog. Prototypenschutzes bieten im Hinblick auf die Informations- und Cybersicherheit keine hinreichende Aussagekraft.

TISAX-Prüfungen richten sich nach der Risikoexposition des geprüften Unternehmens. Dabei geht die Klassifizierung von Unternehmen nach dem Grad ihrer Kritikalität in Bezug auf ihren Sektor oder die Art der von ihnen erbrachten Leistungen konform zu den Forderungen der NIS-2.

Voraussetzung zur Anwendbarkeit der Schlussfolgerungen dieses Dokumentes ist, dass die Prüfziele das Gesamtrisiko, dem sich das Unternehmen ausgesetzt sieht, reflektieren und dass alle Unternehmensstandorte, die von Anforderungen der NIS-2-Richtlinie betroffen sind, über entsprechende TISAX-Label verfügen.

1.3 Zielgruppe des Dokumentes

Dieses Dokument richtet sich an Experten aller Unternehmen, die von der NIS-2-Richtlinie betroffen sind und TISAX für das Risikomanagement Ihrer Lieferketten und Wertschöpfungsnetzwerke in Bezug auf Informations- und Cybersicherheit einsetzen bzw. sich selbst einer TISAX-Prüfung unterziehen.

Weiter kann diese Analyse als Grundlage für eine Bewertung der Einhaltung der NIS-2-Anforderungen durch für die Cybersicherheit und die in Kapitel VII/ NIS-2 genannten Aufsichtsaufgaben zuständige Behörden (zuständige Behörden) oder Einrichtungen dienen.

1.4 Dokumentenstruktur und Methodik

Die Struktur des Dokumentes ist darauf ausgelegt, eine objektive Beurteilung, inwieweit eine TISAX-Prüfung als Nachweis der Erfüllung der Anforderungen aus der EU-Richtlinie 2022/2555 („NIS-2-Richtlinie“) gesehen werden kann, nachvollziehbar darzustellen. Die zugrunde liegende Beurteilung wurde durch führende Informations- und Cybersicherheitsexperten der Automobilindustrie sowie marktführender Prüfgesellschaften durchgeführt.

Das Dokument folgt der Methodik eines Gutachtens und ermöglicht dem Leser, in unterschiedlichen Detailebenen mit dem Dokument zu arbeiten.

Aufbau:

1. Jeder relevante Artikel der NIS-2-Richtlinie wird in einem Kapital dargestellt
2. Jeder relevante Absatz eines Artikels wird in einem Unterkapitel mit folgenden Abschnitten dargestellt:
    a) Nennung der Anforderung aus der NIS-2-Richtline
    b) Nennung der Kontrollfragen aus dem ISA6[2], die sich mit der Fragestellung beschäftigen
    c) Detaillierung der Kontrollfragen auf die einzelnen Controls, die die Fragestellung betreffen
    d) Abschließendes Resümee zum Erfüllungsgrad der Anforderungen des Absatzes

Eine übersichtshafte Aussage über die Erfüllung bietet damit jeweils der letzte Abschnitt (2d) in jedem Unterkapitel.

Für eine tiefere Betrachtung kann durch Einbeziehung des zweiten Abschnitts (2b) ein Rückschluss auf die zugehörigen Kontrollfragen aus dem ISA6 (Tabellenblatt Informationssicherheit, Spalte H) gezogen werden.

Der höchste Detaillierungsgrad wird durch die Erweiterung um die weiteren Abschnitte (2c) erreicht. Hier sind die einzelnen Controls genannt und detailliert aufgeführt, die die Anforderung der NIS-2 beinhalten. Zur besseren Kenntlichmachung wurde die Schriftfarbe der aus dem ISA6 eingefügten Kontrollfragen angepasst.

[2] https://portal.enx.com/de-DE/TISAX/downloads/

2 TISAX-Prüfung und zugrundeliegender Anforderungskatalog

2.1 Definition des TISAX-Prüfscopes

Das Dokument bezieht sich in der Bewertung auf nach dem ISA-Prüfkatalog in der Version 6 (ISA6) durchgeführte TISAX-Prüfungen. Die Prüfungen werden nach Beauftragung von einem unabhängigen Auditor in einem Dreijahreszyklus durchgeführt.

Es ist wichtig zu verstehen, dass die Definition des TISAX-Prüfscope sich von ISO-Management-System-Zertifizierungen unterscheidet, was die Vorgaben für die Festlegung des Prüfscopes betrifft.

Für die ISO/IEC 27001-Zertifizierung definiert die geprüfte Organisation den Scope seines ISMS (im „Scope-Statement“). Bei der Definition dieses Scopes ist sie völlig frei. Der Scope der Prüfung (auch „Audit-Scope“ genannt) muss jedoch mit dem Scope des ISMS identisch sein. Bei der ISO/IEC 27001-Zertifizierung kann durch die Art und Weise, wie der Scope des ISMS definiert wird, der Scope der Prüfung beeinflusst werden.

Im Gegensatz zur ISO/IEC 27001 wurde bei TISAX entschieden, dass folgender allgemein definierter Standardscope für TISAX-Prüfungen genutzt werden muss:

„Der TISAX-Scope definiert den Umfang der Prüfung. Die Prüfung umfasst alle Prozesse, Verfahren und beteiligte Ressourcen, die unter der Verantwortung der zu prüfenden Organisation stehen und die für die Sicherheit der in den genannten Prüfzielen definierten Schutzobjekte und deren Schutzziele an den aufgeführten Standorten relevant sind.

Die Prüfung wird mindestens im höchsten Assessment-Level durchgeführt, das in einem der aufgeführten Prüfziele gefordert ist. Alle in den aufgelisteten Prüfzielen geforderten Kriterien sind Gegenstand der Prüfung.“

Der Scope der Prüfung kann gleich oder kleiner sein als der Scope des ISMS. Er muss aber innerhalb des Scopes des ISMS liegen und umfasst stets alle Elemente, die ein ISMS ausmachen.

Dadurch sind TISAX-Bewertungen unternehmensübergreifend vergleichbar und stellen ein ähnliches Sicherheitsniveau her. Im Gegensatz zu anderen Prüfmechanismen (z. B. ISO Management System Zertifizierungen) besteht nicht die Gefahr einer verengten Sicht auf das zu prüfende Unternehmen durch individuell gestaltete Scopes.

Beiden Standards gemeinsam ist, dass die offizielle Konformitätsaussage jeweils nur für die Standorte gilt, die im Scope berücksichtigt wurden. Möchte ein Unternehmen seine Konformität mit NIS-2 auf der Basis von ISO/IEC 27001 oder TISAX beurteilen und verbessern, so müssen auch alle Standorte in den Scope genommen worden sein, um eine Aussage für das gesamte Unternehmen zu erzielen. Diese Annahme der Identität zwischen Unternehmen und beteiligten Standorten bildet eine wichtige Grundlage für die folgenden Aussagen dieses Gutachtens zu NIS-2 und TISAX.

2.2 TISAX-Prüfziele

In TISAX-Prüfungen dienen im Standard vorgegebene Prüfziele innerhalb des Prüfscopes als Maßstab für den Umfang, in dem das Informationssicherheits-Managementsystem geprüft wird. Damit hat das zu prüfende Unternehmen die Möglichkeit, die Prüfungsinhalte anhand der Risiken, also der Kritikalität und Art der verarbeiteten Informationen zu skalieren. Die in TISAX standardisierten Prüfziele sind in Tabelle 1 dargestellt.

Prüfziel	Beschreibung
Confidential	Umgang mit Informationen mit hohem Schutzbedarf im Rahmen der Vertraulichkeit (Zugriff auf vertrauliche Informationen)
Strictly Confidential	Umgang mit Informationen von sehr hohem Schutzbedarf im Rahmen der Vertraulichkeit (Zugriff auf streng vertrauliche Informationen)
High Availability	Umgang mit Informationen von hohem Schutzbedarf im Rahmen der Verfügbarkeit (hohe Verfügbarkeit der Informationen)
Very High Availability	Umgang mit Informationen von sehr hohem Schutzbedarf im Rahmen der Verfügbarkeit (sehr hohe Verfügbarkeit der Informationen)
Proto Parts	Schutz von Prototypenbauteilen und -Komponenten
Proto Vehicles	Schutz von Prototypenfahrzeugen
Test Vehicles	Umgang mit Erprobungsfahrzeugen
Proto Events	Schutz von Prototypen während Veranstaltungen und Film- und Fotoshootings
Data	Datenschutz gemäß Artikel 28 („Auftragsverarbeiter“) der Datenschutz Grundverordnung (DSGVO)
Special Data	Datenschutz gemäß Artikel 28 („Auftragsverarbeiter“) der Datenschutz Grundverordnung (DSGVO) mit besonderen Kategorien personenbezogener Daten wie in Artikel 9 der Datenschutz-Grundverordnung (DSGVO) angegeben

Tabelle 1 – TISAX-Prüfziele

Basierend auf der Auswahl der Prüfziele werden innerhalb des TISAX-Assessments verschiedene Kriterien in unterschiedlicher Ausprägung aus dem ISA6 Katalog herangezogen. Damit wird über die Prüfziele der Kontrollumfang und die zu verwendenden Assessment-Level (AL) spezifiziert.

2.3 TISAX-Kontrollumfang und zu verwendende Assessment-Level (AL)

Es findet eine Unterscheidung in die Assessment-Level 1, 2 und 3 statt. Die Assessment-Level sind den Prüfzielen explizit zugeordnet. Prüfungen im Assessment-Level 1 spielen meist eine Rolle für interne Zwecke im eigentlichen Sinne einer Selbsteinschätzung Self-Assessment). Bei einer Prüfung im Assessment-Level 1 prüft ein Prüfer, ob eine vollständige Selbsteinschätzung vorliegt. Er prüft nicht den Inhalt der Selbsteinschätzung. Er benötigt keine weiteren Nachweise. Die Ergebnisse von Prüfungen mit dem Assessment-Level 1 haben eine niedrige Vertrauensstufe und werden daher in TISAX nicht verwendet. Aber es ist natürlich möglich, dass Ihr Partner eine solche Selbsteinschätzung außerhalb von TISAX anfordert.

Bei der Verwendung von Prüfzielen mit unterschiedlichen Assessment-Leveln, wird das in der Wertigkeit am höchsten eingeordnete Prüfziel innerhalb des gesamten Assessments angewendet. Die Zuordnung von Prüfzielen zu Assessment-Leveln finden sich in Tabelle 2.

Bei einer Prüfung im Assessment-Level 2 führt der Prüfdienstleister eine Plausibilitätsprüfung der Selbsteinschätzung des zu prüfenden Unternehmens durch (für alle Standorte im Prüf-Scope). Er sichert dies ab, indem er Nachweise prüft und ein Interview mit dem Gesamtverantwortlichen für Informationssicherheit durchführt. Der Prüfdienstleister führt das Interview in der Regel als Webkonferenz durch.

TISAX-Prüfziel	Assessment-Level (AL)
Confidential	AL 2
Strictly Confidential	AL 3
High Availability	AL 2
Very High Availability	AL 3
Proto Parts	AL 3
Proto Vehicles	AL 3
Test Vehicles	AL 2
Proto Events	AL 2
Data	AL 2
Special Data	AL 3

Tabelle 2 – Abhängigkeit zwischen TISAX-Prüfziel und TISAX-Assessment-Level

Bei einer Prüfung im Assessment-Level 3 führt der Prüfdienstleister eine umfassende Überprüfung der Einhaltung der geltenden Anforderungen durch das geprüfte Unternehmen durch. Der Auditor verwendet die Selbsteinschätzung und die eingereichten Unterlagen, um die Prüfung vorzubereiten. Im Gegensatz zum Assessment-Level 2 wird der Prüfer jedoch alles überprüfen. Er wird:

- Dokumente und Umsetzungsnachweise prüfen
- geplante Interviews mit den Prozessverantwortlichen führen
- die örtlichen Gegebenheiten betrachten
- die Durchführung von Prozessen beobachten
- ungeplante Interviews mit Prozessbeteiligten führen

Methodisch unterscheiden sich die beiden Ansätze erheblich. Bei Prüfungen im Assessment-Level 2 wird der Prüfer nicht alles verifizieren. Er prüft lediglich die Plausibilität. Eine Prüfung im Assessment-Level 3 findet grundsätzlich bei allen im Scope befindlichen Standorten des zu prüfenden Unternehmens vor Ort statt. Eine Ausnahme bildet hier die Vereinfachte Gruppenprüfung (Simplified Group Assessment, SGA).

2.4 TISAX-Gruppenprüfungen

2.4.1 Vereinfachte Gruppenprüfung

Für Unternehmen mit vielen Standorten, bei denen ein Durchlaufen des regulären Prozesses bei Einzelprüfung jedes Standortes immens aufwendig wäre, bietet TISAX die vereinfachte Gruppenprüfung an. Dieses Verfahren steht nur Unternehmen offen, die über ein zentralisiertes und hoch entwickeltes ISMS verfügen.

In TISAX wird "zentralisiert und hoch entwickelt" wie folgt definiert:

- Der Hauptstandort muss in der Lage sein, die Einhaltung aller ISMS-bezogenen Regeln und Richtlinien an allen Standorten im Prüfscope zu gewährleisten
- Die abhängigen Standorte müssen über einen zuverlässigen Kanal zurück zum Hauptstandort verfügen.
- Ihre Rückmeldungen müssen mit den Erwartungen übereinstimmen, die durch die Regeln und Richtlinien des Hauptstandorts vorgegeben sind.

Es existieren zwei Varianten der vereinfachte Gruppenprüfung:

- Die vereinfachte Gruppenprüfung auf Stichprobenbasis (S-SGA) und
- die vereinfachte Gruppenprüfung auf Rotationsplanbasis (R-SGA).

Im Folgenden sind die beiden Bewertungsverfahren erklärt:

2.4.2 Vereinfachte Gruppenprüfung auf Stichprobenbasis (S-SGA)

Am Hauptstandort (in der Regel der Hauptsitz des Unternehmens) bewertet der TISAX-Auditor das ISMS umfangreicher als im regulären Prüfverfahren. Hierzu werden die im ISA6 formulierten Fragestellungen zusätzliche Anforderungen für die vereinfachte Gruppenprüfung genutzt. Ziel der zusätzlichen Prüfpunkte ist festzustellen, dass das Unternehmen über ein zentralisiertes und hoch entwickeltes ISMS verfügt. Weiter findet eine Prüfung von Stichprobenstandorten basierend auf der Anzahl der Gesamtstandorte des Scopes statt, die im gleichen Assessment-Level durchgeführt werden. Alle anderen Standorte werden um ein Assessment-Level geringer geprüft als im regulären Prüfverfahren.

2.4.3 Rotationsplanbasierte vereinfachte Gruppenprüfung (R-SGA)

Am Hauptstandort (in der Regel der Hauptsitz des Unternehmens) bewertet der TISAX-Auditor das ISMS umfangreicher als im regulären Begutachtungsverfahren. Hierzu werden die im ISA6 formulierten Fragestellungen zusätzliche Anforderungen für das vereinfachte Gruppenprüfung genutzt. Ziel der zusätzlichen Prüfpunkte ist festzustellen, dass das Unternehmen über ein zentralisiertes und hoch entwickeltes ISMS verfügt. Alle weiteren Standorte werden im gleichen Assessment-Level geprüft, aber gleichmäßig über die dreijährige Gültigkeit der TISAX-Label-Gültigkeitsdauer verteilt. Die Beurteilungsprozessoption R-SGA ist NICHT für die Prüfziele des Prototypenschutzes verfügbar (Prototypteile, Prototypfahrzeuge, Testfahrzeuge, Prototypveranstaltungen).

2.5 TISAX-Kontrollfragen und Anforderungen

Die dem Prüfziel zugeordneten Kontrollfragen wiederum sind in Anforderungen detailliert. Zu jeder Kontrollfrage kann es Anforderungen im Bereich muss, sollte, Zusatzanforderungen bei hohem Schutzbedarf, Zusatzanforderungen bei sehr hohem Schutzbedarf und Zusätzliche Anforderungen für das vereinfachte Gruppenprüfung geben. Die Bedeutung der einzelnen Anforderungsebenen finden sich in Tabelle 3.

Anforderung	**Beschreibung der Umsetzung**
Anforderungen (muss)	Die Anforderungen in dieser Spalte sind strenge Anforderungen, für die es keine Ausnahmen gibt.
Anforderungen (sollte)	Die Anforderungen in dieser Spalte müssen grundsätzlich von der Organisation umgesetzt werden. Es kann jedoch unter bestimmten Umständen eine valide Begründung geben, diese Anforderungen nicht zu erfüllen. Die Auswirkungen von Abweichungen müssen durch die Organisation verstanden werden, und die Abweichung muss nachvollziehbar begründet werden. Es liegt im Ermessensspielraum des Prüfers, ob eine Nichterfüllung akzeptabel ist.
Zusatzanforderungen bei hohem Schutzbedarf	Die Anforderungen in dieser Spalte müssen zusätzlich erfüllt werden, wenn das geprüfte Subjekt einen hohen Schutzbedarf hat.

Zusatzanforderungen bei sehr hohem Schutzbedarf	Die Anforderungen in dieser Spalte müssen zusätzlich erfüllt sein, wenn das geprüfte Subjekt einen sehr hohen Schutzbedarf hat.
Zusätzliche Anforderungen für das vereinfachte Gruppenprüfung (SGA, en: Simplified Group Assessments)	Die Anforderungen in dieser Spalte müssen bei vereinfachten Gruppenprüfungen zusätzlich erfüllt werden. Sie sind dann als „muss“ Anforderungen zu verstehen.

Tabelle 3 – Umsetzungsanforderungen

Die Anforderungen der Kategorie Zusatzanforderungen bei hohem – und sehr hohem Schutzbedarf sind zusätzlich untergliedert in die Schutzziele (Vertraulichkeit (C (Confidentiality)) Integrität (I (Integrity)) und Verfügbarkeit (A (Availability)). Die Klassifizierung in die Schutzziele dient der Unterscheidung der Zusatzanforderungen nach Prüfziel. So findet in Prüfungen mit dem Prüfziel Confidential und Strictly Confidential Kontrollfragen innerhalb der Zusatzanforderungen Anwendung, die durch das Schutzziel Vertraulichkeit „C“ gekennzeichnet sind.

In Prüfungen mit dem Prüfziel High Availability und Very High Availability werden die Kontrollfragen innerhalb der Zusatzanforderungen angewendet, die durch das Schutzziel Verfügbarkeit „A“ gekennzeichnet sind.

Das Schutzziel Integrität wird ebenfalls ausgewiesen. Die entsprechenden Anforderungen werden innerhalb der Prüfziele Availability oder Confidentiality stets mit abgeprüft.

Bei einer regulären TISAX-Prüfung besteht ausdrücklich nicht die Möglichkeit, einzelne Kontrollfragen des Prüfkataloges als nicht anwendbar oder not applicable (n/a) zu bewerten und damit auszuschließen. Die Kontrollfragen und deren Anforderungen sind vom Unternehmen ganzheitlich umzusetzen. Lediglich in der Bewertung, was als angemessene Umsetzung gesehen wird, gibt TISAX den Prüfern den notwendigen Ermessensspielraum.

2.6 Umgang mit Abweichungen im TISAX-Modell

Die TISAX-Prüfung beinhaltet neben der Kontrolle von Dokumenten und Prozessen auf Vorhandensein auch die Prüfung der Umsetzung und deren Dokumentation. Hierzu ist neben den Kontrollfragen (Controls) ein Reifegradmodell etabliert, dass unabhängig von der formellen Betrachtung die praktische Reife der Umsetzung bewertet. Das Reifegradmodell lässt sechs Bewertungsebenen pro Kontrollfrage zu.[3] Der Zielreifegrad für eine erfolgreiche TISAX-Prüfung ist Ebene drei „etabliert“. Eine detaillierte Auflistung der Reifegrade und der zugehörigen Spezifikation der Beurteilungsvoraussetzungen ist im Anhang I aufgeführt.

Sollten während der Prüfung Abweichungen von den geforderten Inhalten festgestellt werden, so sind diese innerhalb eines angemessenen Zeitraumes, beginnend mit dem Abschluss der Prüfung, umzusetzen. Die umzusetzenden Maßnahmen zum Abarbeiten der Abweichungen und die dazugehörigen Zeiträume zur Umsetzung werden in einem Maßnahmenplan (Corrective Action Plan) definiert, und vom Prüfer, bei Erfüllung der Anforderung durch Umsetzung der Maßnahme, freigegeben. Die Angemessenheit des Abarbeitungszeitraumes wird hier durch den Auditor festgelegt, ein Zeitraum von bis zu drei Monaten wird in der Regel ohne hinterfragen akzeptiert. In begründeten Fällen durch besonders aufwändige oder langfristige Maßnahmen kann diese Frist auf sechs Monate oder, mit entsprechender Begründung, auf bis zu neun Monate verlängert werden.

Der Auditor prüft die fristgerechte Einhaltung der definierten Maßnahmen in einem sogenannten Corrective Action Plan Assessment nach Ablauf des vereinbarten Zeitraumes. Wenn einzelne oder alle Abweichungen nicht innerhalb der neunmonatigen Frist abgestellt sind, wird die Prüfung als nicht bestanden angesehen und muss in vollem Umfang wiederholt werden. Die Vorlage eines Maßnahmenplans ist die Grundlage zur Vergabe von temporären Labels, die nach dem Abstellen aller Abweichungen in permanente Labels umgewandelt werden.

[3] Die Bewertungsebenen sind: unvollständig; durchgeführt; gesteuert; etabliert; vorhersagbar und optimierend.

2.7 Gültigkeitszeitraum von TISAX-Prüfungen

Der Gültigkeitszeitraum einer TISAX-Prüfung ist drei Jahre. Nach Ablauf dieser drei Jahre wird zur Aufrechterhaltung der Gültigkeit eine erneute Vollprüfung der im ISA definierten Controls nach definiertem Scope notwendig. Im Verlauf dieser drei Jahre ist das Unternehmen dazu verpflichtet, die in der Prüfung angegebenen Maßnahmen weiter zu verfolgen und die Umsetzung zu dokumentieren.

Darüber hinaus muss das Unternehmen regelmäßig interne Prüfungen von Richtlinien und Verfahren der Informationssicherheit durchführen und die Ergebnisse der durchgeführten Überprüfungen aufzeichnen und aufbewahren. Diese Dokumente werden als Nachweis der aktiven Umsetzung in der nächsten Prüfung oder bei Zwischenprüfungen herangezogen.

Zwischenprüfungen kommen zum Tragen, wenn es innerhalb des Unternehmens Veränderungen gab, die sich direkt auf das ISMS oder die physischen Gegebenheiten des Unternehmens beziehen. In diesen Fällen ist das Unternehmen dazu verpflichtet, diese zu melden und eine Zwischenprüfung zur Aufrechterhaltung des Prüfstatus bei dem Prüfdienstleister zu beauftragen, der auch die Hauptprüfung durchgeführt hat.

Zur Quantifizierung der Aufrechterhaltung der Prozesse über den gesamten Label-Gültigkeitszeitraum ist im TISAX-Prüfprozess das weiter oben bereits beschriebene Reifegradmodell etabliert.

3 NIS-2 Artikel 20

3.1 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 20 (1)

3.1.1 Anforderung aus der NIS-2

NIS-2 Artikel 20 (1) fordert, dass das Leitungsorgan einer Organisation geeignete Strukturen geschaffen hat, um die zur Einhaltung von Artikel 21 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit umzusetzen und ihre Umsetzung zu überwachen.

3.1.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls die Erfüllung der Forderung nach NIS-2 Artikel 20 (1) geprüft:

- 1.2.1: „Inwieweit wird in der Organisation Informationssicherheit gemanagt?“
- 1.2.2: „Inwieweit sind die Verantwortlichkeiten für Informationssicherheit organisiert?“
- 1.4.1: „Inwieweit werden Informationssicherheitsrisiken gemanagt?“
- 1.5.1: „Inwieweit wird die Einhaltung der Informationssicherheit in Verfahren und Prozessen sichergestellt?“
- 1.5.2: „Inwieweit wird das ISMS von einer unabhängigen Stelle überprüft?“
- 7.1.1: „Inwieweit wird die Einhaltung regulatorischer und vertraglicher Bestimmungen sichergestellt?“

3.1.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.2.1 „Inwieweit wird in der Organisation Informationssicherheit gemanagt?“

Der Auditor prüft, ob der durch das Informationssicherheits-Managementsystem (ISMS) zu managende Bereich definiert ist *(Control 1.2.1; Anforderungen (muss); Erster Unterpunkt: „+ Der Geltungsbereich (Scope) des ISMS (die vom ISMS gemanagte Organisation) ist festgelegt“)* und die Anforderungen zur Umsetzung spezifiziert sind *(Control 1.2.1; Anforderungen (muss); Zweiter Unterpunkt: „+ Die Anforderungen der Organisation an das ISMS sind ermittelt“)*. Weiter prüft er, dass die Organisationsleitung das ISMS beauftragt und freigegeben hat *(Control 1.2.1; Anforderungen (muss); dritter Unterpunkt: Die Organisationsleitung hat das ISMS beauftragt und freigegeben)*, um sicherzustellen, dass Informationssicherheit nicht nur ein Ergebnis von Zufällen und individuellem Engagement, sondern von nachhaltigem Management ist.

Ebenfalls geprüft werden die implementierten Kommunikationskanäle zwischen der Unternehmensleitung und den Ausführenden des ISMS *(Control 1.2.1; Anforderungen (muss); vierter Unterpunkt: + Das ISMS stellt der Organisationsleitung geeignete Kontroll- und Steuerungsmittel zur Verfügung (z. B. Management-Review))*, um sicherzustellen, dass die Kontroll- und Steuerungsmittel auch regelmäßig genutzt werden, um die Funktionalität des ISMS aufrecht zu erhalten *(Control 1.2.1; Anforderungen (muss); sechster Unterpunkt: Die Wirksamkeit des ISMS wird regelmäßig durch das Management überprüft)*.

1.2.2 „Inwieweit sind die Verantwortlichkeiten für Informationssicherheit organisiert?“

Weiter wird geprüft, dass die Verantwortlichkeiten für das ISMS definiert *(Control 1.2.2; Anforderungen (muss); Erster Unterpunkt: „+ Verantwortlichkeiten für die Informationssicherheit in der Organisation sind definiert, dokumentiert und zugewiesen“)* und kommuniziert *(Control 1.2.2; Anforderungen (muss); Vierter Unterpunkt: „+*

Die Ansprechpartner sind innerhalb der Organisation und relevanten Geschäftspartnern bekannt“) und die notwendigen Mittel freigegeben wurden *(Control 1.2.2; Anforderungen (muss); dritter Unterpunkt: Die notwendigen Ressourcen stehen zur Verfügung)*. Der Auditor prüft weiter, ob eine geeignete Informationssicherheitsstruktur vorhanden ist *(Control 1.2.2; Anforderungen (sollte); Erster Unterpunkt: „+ Es ist eine Definition und Dokumentation einer geeigneten Informationssicherheitsstruktur in der Organisation vorhanden“)* und das weitere Sicherheitsaufgaben berücksichtigt wurden *(Control 1.2.2; Anforderungen (sollte); Zweiter Unterpunkt: „+ Weitere relevante Sicherheitsaufgaben werden berücksichtigt“)*. Außerdem, dass die im Bereich des ISMS eingesetzten Mitarbeiter für ihre Aufgabe qualifiziert sind oder werden *(Control 1.2.2; Anforderungen (muss); zweiter Unterpunkt: + Die verantwortlichen Mitarbeiter sind definiert und für ihre Aufgabe qualifiziert)* und das diese keinen Interessenskonflikten unterliegen *(Control 1.2.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Eine angemessene organisatorische Trennung von Verantwortlichkeiten sollte zur Vermeidung von Interessenskonflikten etabliert sein (Funktionstrennung). (C, I, A)“)*.

1.4.1 „Inwieweit werden Informationssicherheitsrisiken gemanagt?“

Um die Funktionalität und kontinuierliche Sicherstellung und Weiterentwicklung des risikobasierten Ansatzes des Informationssicherheits-Managementsystems sicherzustellen, prüft der Auditor die regelmäßige und anlassbezogene Risikobewertung *(Control 1.4.1; Anforderungen (muss); Erster Unterpunkt: + Risikobewertungen werden sowohl in regelmäßigen Abständen als auch als Reaktion auf Ereignisse durchgeführt)*, sowie die Klassifizierung und Zuordnung der erkannten Risiken *(Control 1.4.1; Anforderungen (muss); Zweiter Unterpunkt: + Informationssicherheitsrisiken werden angemessen (z. B. hinsichtlich Eintrittswahrscheinlichkeit und potenziellem Schaden) bewertet)* und den Umgang mit Sicherheitsrisiken *(Control 1.4.1; Anforderungen (sollte); Erste Drei Unterpunkte: + Es ist ein Verfahren vorhanden, das festlegt, wie Sicherheitsrisiken innerhalb der Organisation zu identifizieren, bewerten und behandeln sind; + Kriterien für die Bewertung und Behandlung von Sicherheitsrisiken sind vorhanden; + Maßnahmen für den Umgang mit Sicherheitsrisiken und die dafür Verantwortlichen sind festgelegt und dokumentiert: Es wird nach einem Maßnahmenplan oder einer Übersicht über den Umsetzungsstatus der Maßnahmen vorgegangen)*. Weiter prüft er, ob den identifizierten Risiken ein Verantwortlicher zugeordnet ist, der die Bewertung des identifizierten Riskos und dessen Behandlung durch definierte Folgemaßnahmen verantwortet *(Control 1.4.1; Anforderungen (muss); Vierter Unterpunkt: + Jedem Informationssicherheitsrisiko ist ein Verantwortlicher (Risikoeigner) zugeordnet. Dieser ist für die Bewertung und Behandlung der Informationssicherheitsrisiken verantwortlich)* und dass bei Änderungen des Umfelds eine Neubewertung stattfindet *(Control 1.4.1; Anforderungen (sollte); Vierter Unterpunkt: + Bei Änderungen des Umfelds (z. B. Organisationsstruktur, Standort, Änderungen von Regelwerken) erfolgt eine rechtzeitige Neubewertung)*.

1.5.1 „Inwieweit wird die Einhaltung der Informationssicherheit in Verfahren und Prozessen sichergestellt?“

In einem weiteren Teil der Prüfung beschäftigt sich der Auditor mit der Einhaltung der Informationssicherheit in Verfahren und Prozessen *(Control 1.5.1; Anforderungen (muss); Erster Unterpunkt: + Die Einhaltung von Richtlinien wird organisationsweit überprüft)*. Er prüft weiterhin, dass die Prüfungen der Einhaltung der Informationssicherheit in Verfahren und Prozessen in regelmäßigen Abständen *(Control 1.5.1; Anforderungen (muss); Zweiter Unterpunkt: + Prüfungen von Richtlinien und Verfahren der Informationssicherheit werden regelmäßig durchgeführt)* nach einem definierten Plan *(Control 1.5.1; Anforderungen (sollte); Erster Unterpunkt: + Ein Plan über Inhalt und Rahmenbedingungen (Zeitplan, Umfang, Kontrollen) der durchzuführenden Überprüfungen liegt vor)* erfolgen und nachvollziehbar dokumentiert werden *(Control 1.5.1; Anforderungen (muss); Fünfter Unterpunkt: + Die Ergebnisse der durchgeführten Überprüfungen werden aufgezeichnet und aufbewahrt)*.

1.5.2 „Inwieweit wird das ISMS von einer unabhängigen Stelle überprüft?“

Der Auditor prüft ebenfalls, dass eine Prüfung durch eine unabhängige Stelle durchgeführt wird, die in regelmäßigen Abständen und bei wesentlichen Änderungen stattfindet *(Control 1.5.2; Anforderungen (muss); Erster Unterpunkt: + Prüfungen der Informationssicherheit werden von einer unabhängigen und sachkundigen Stelle in regelmäßigen Abständen und bei wesentlichen Änderungen durchgeführt)* und dass deren Ergebnisse dokumentiert und an die Organisationsleitung berichtet werden*(Control 1.5.2; Anforderungen (sollte); Erster Unterpunkt:*

+ Die Ergebnisse der durchgeführten Prüfungen werden dokumentiert und an die Organisationsleitung berichtet). Teil seiner Prüfung ist auch, sicherzustellen, dass für mögliche Abweichungen Korrekturmaßnahmen eingeleitet und verfolgt werden (*Control 1.5.2; Anforderungen (muss); Zweiter Unterpunkt: + Korrekturmaßnahmen für mögliche Abweichungen werden eingeleitet und verfolgt).*

7.1.1 „Inwieweit wird die Einhaltung regulatorischer und vertraglicher Bestimmungen sichergestellt?“

Parallel zur Spezifikation und Umsetzung von Zielen und Inhalten des ISMS wird auch die Kenntnis das Unternehmen betreffender regulatorischer und vertraglicher Bestimmungen , und deren Berücksichtigung bei der Implementierung von ISMS Maßnahmen geprüft *(Control 7.1.1; Anforderungen (muss); Erster Unterpunkt: + Gesetzliche, regulatorische und vertragliche Bestimmungen mit Relevanz für die Informationssicherheit werden in regelmäßigen Abständen ermittelt),* um zu verhindern, dass bei Nichteinhaltung dieser Vorgabe durch externe Einflüsse von Gesetzen und regulatorischen Vorgaben Risiken bezüglich der Durchsetzungsfähigkeit der eigenen Informationssicherheit entstehen.

3.1.4 Resümee

Die Anforderung, dass das Leitungsorgan einer Organisation geeignete Strukturen geschaffen hat, um die zur Einhaltung von Artikel 21 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit umzusetzen und ihre Umsetzung zu überwachen (NIS-2 Artikel 20 (1)), ist durch die im ISA6-Prüfstandard definierten Controls beschrieben und wird vollumfänglich innerhalb eines TISAX-Assessments durch den Auditor auf Vorhandensein und Umsetzung geprüft. Der Auditor stellt hierbei, durch die Kontrolle von entsprechenden Nachweisen, sicher, dass die definierten Inhalte dauerhaft und regelmäßig Umsetzung finden.

Unter Berücksichtigung der Verpflichtung für die Betreiber Kritischer Infrastrukturen im Sinne des IT-Sicherheitsgesetzes gemäß BSI-Gesetz (BSIG) und BSI-Kritisverordnung, alle zwei Jahre einen Nachweis zur Erfüllung der Anforderungen vorzulegen und dem Risikobasierten Ansatz der NIS-2-Richtlinie, wird der Dreijahreszyklus der TISAX-Prüfung als angemessen angesehen.

3.2 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 20 (2)

3.2.1 Anforderung aus der NIS-2

NIS-2 Artikel 20 (2) fordert, dass Mitglieder des Leitungsorgans sowie weitere relevante Mitglieder an regelmäßigen Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

3.2.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls die Erfüllung der Forderung nach NIS-2 Artikel 20 (2) geprüft:

- 2.1.3: „Inwieweit werden Mitarbeiter hinsichtlich der Risiken beim Umgang mit Informationen geschult und sensibilisiert?“

3.2.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

2.1.3: „Inwieweit werden Mitarbeiter hinsichtlich der Risiken beim Umgang mit Informationen geschult und sensibilisiert?“

Der Auditor prüft, ob alle Mitarbeiter (einschließlich der Leitungsebene) des Unternehmens ganzheitlich hinsichtlich der Risiken beim Umgang mit Informationen geschult und sensibilisiert werden *(Control 2.1.3; Anforderungen (muss); erster Unterpunkt: + Mitarbeiter sind geschult und sensibilisiert).* Weiter wird geprüft, dass ein Schulungskonzept vorliegt, das für die Informationssicherheit relevante Bereiche abdeckt *(Control 2.1.3; Anforderungen (sollte); erster Unterpunkt: + Ein Konzept zur Sensibilisierung und Schulung der Mitarbeiter ist erstellt. Dabei werden mindestens die folgenden Aspekte berücksichtigt: Richtlinie zur Informationssicherheit, Meldungen von Informationssicherheitsereignissen, Verhalten bei Auftreten von Schadsoftware, Richtlinien zu Benutzerkonten und Anmeldeinformationen (z. B. Passwort-Richtlinie), Compliance-Themen der Informationssicherheit, Anforderungen und Verfahren zum Einsatz von Geheimhaltungsvereinbarungen bei der gemeinsamen Nutzung schutzbedürftiger Informationen, Nutzung organisationsfremder IT-Dienste)* und in dem die Zielgruppen für Schulungskonzepte Berücksichtigung finden *(Control 2.1.3; Anforderungen (sollte); zweiter Unterpunkt: Zielgruppen für Schulungs- und Sensibilisierungsmaßnahmen (d. h. Personen, die in bestimmten risikobehafteten Umgebungen arbeiten, wie Administratoren, Mitarbeiter mit Zugang zu Kundennetzwerken, Personal in Fertigungsbereichen) sind ermittelt und in einem Schulungskonzept berücksichtigt)* und die Schulungsmaßnahmen entsprechend der Kritikalität der verarbeiteten Information angemessen sind. Der Auditor wird ebenfalls prüfen, ob die Schulungs- und Sensibilisierungsmaßnahmen in regelmäßigen Abständen und anlassbezogen durchgeführt werden *(Control 2.1.3; Anforderungen (sollte); vierter Unterpunkt: + Schulungs- und Sensibilisierungsmaßnahmen werden sowohl in regelmäßigen Abständen als auch als Reaktion auf Ereignisse durchgeführt)* und eine entsprechende Dokumentation vorliegt *(Control 2.1.3; Anforderungen (sollte); fünfter Unterpunkt: + Die Teilnahme an Schulungs- und Sensibilisierungsmaßnahmen wird dokumentiert)*.

3.2.4 Resümee

Die Anforderungen, dass Mitglieder des Leitungsorgans sowie weitere relevante Mitglieder an regelmäßigen Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben, der NIS-2 Artikel 20 (2) sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments durch den Auditor auf Vorhandensein und Umsetzung geprüft. Der Auditor stellt hierbei durch die Kontrolle von entsprechenden Nachweisen sicher, dass die definierten Inhalte dauerhaft und regelmäßig Umsetzung finden. Auch wenn der direkte Bezug zur Schulung der Mitglieder des Leitungsorgans sowie weiterer relevanter Mitglieder im ISA nicht explizit aufgeführt ist, wird die Schulung aller Mitarbeiter und eine Differenzierung nach Zielgruppen gefordert. Diese Anforderung erfüllt ebenfalls den Anspruch, da den Mitgliedern des Leitungsorgans sowie weiteren relevanten Mitgliedern bei der Kritikalitätseinstufung entsprechend der von diesen Personen verarbeiteten Informationen, hohe Relevanz zugewiesen werden muss.

4 NIS-2 Artikel 21

4.1 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 21 (1)

4.1.1 Anforderung aus der NIS-2

NIS-2 Artikel 21 (1) fordert, dass Unternehmen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergriffen haben, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

Die in Unterabsatz 1 genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, dass dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

4.1.2 Anwendbare Kontrollfragen des ISA6

Das Ziel der TISAX-Prüfung ist zu verifizieren, ob ein Management-System etabliert ist, das dafür sorgt, dass stets geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergriffen werden, um die Risiken für die Informations- und Cybersicherheit zu beherrschen und Kunden und die eigene Organisation vor Auswirkungen von Sicherheitsvorfällen zu schützen. Ein wesentlicher Aspekt ist hierbei der Schutz von Netz- und Informationssystemen.

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls *die Erfüllung der Forderung nach NIS-2 Artikel 21 (1) geprüft:*

- 1.2.1: „Inwieweit wird in der Organisation Informationssicherheit gemanagt?“ und
- 1.4.1: „Inwieweit werden Informationssicherheitsrisiken gemanagt?“

4.1.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.2.1 „Inwieweit wird in der Organisation Informationssicherheit gemanagt?“

Der Auditor prüft, ob sowohl der Geltungsbereich des ISMS festgelegt ist *(Control 1.2.1; Anforderungen (muss); Erster Unterpunkt: + Der Geltungsbereich (Scope) des ISMS (die vom ISMS gemanagte Organisation) ist festgelegt)* als auch dass das ISMS sich an den durch das Unternehmen definierten Anforderungen orientiert *(Control 1.2.1; Anforderungen (muss); Zweiter Unterpunkt: + Die Anforderungen der Organisation an das ISMS sind ermittelt).*

1.4.1 „Inwieweit werden Informationssicherheitsrisiken gemanagt?“

Weiter prüft der Auditor das Vorhandensein einer Risikobewertung *(Control 1.4.1; Anforderungen (muss); Dritter Unterpunkt: + Informationssicherheitsrisiken sind dokumentiert)*, die einen aktuellen Stand aufweist und regelmäßig oder als Reaktion auf Vorfälle zu aktualisieren ist *(Control 1.4.1; Anforderungen (muss); Erster*

Unterpunkt: + Risikobewertungen werden sowohl in regelmäßigen Abständen als auch als Reaktion auf Ereignisse durchgeführt). Bei der Prüfung kontrolliert der Auditor, dass den identifizierten Risiken ein Risikoeigner zugeordnet ist *(Control 1.4.1; Anforderungen (muss); Vierter Unterpunkt: Jedem Informationssicherheitsrisiko ist ein Verantwortlicher (Risikoeigner) zugeordnet. Dieser ist für die Bewertung und Behandlung der Informationssicherheitsrisiken verantwortlich)* und ein Maßnahmenplan zur Behandlung der Risiken besteht *(Control 1.4.1; Anforderungen (sollte); Dritter Unterpunkt: + Maßnahmen für den Umgang mit Sicherheitsrisiken und die dafür Verantwortlichen sind festgelegt und dokumentiert – Es wird nach einem Maßnahmenplan oder einer Übersicht über den Umsetzungsstatus der Maßnahmen vorgegangen)*, der vom entsprechenden Risikoeigner umgesetzt wird.

4.1.4 Resümee

Die Anforderungen der NIS-2 Artikel 21 (1) sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments durch den Auditor auf Vorhandensein und Umsetzung geprüft. Weiter trägt die Prüfung des ISA-Anforderungskataloges durch den Auditor in seiner Gänze dazu bei, festzustellen, dass das ISMS auf einem risikobasierten Ansatz die Gegebenheiten des Unternehmens berücksichtigt und sich daran orientiert.

Das implementierte und geprüfte ISMS sorgt dafür, dass Unternehmen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergriffen haben, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

4.2 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 21 (2)

4.2.1 Anforderung aus der NIS-2

NIS-2 Artikel 21 (2) fordert, dass die Maßnahmen auf einem gefahrenübergreifenden Ansatz beruhen müssen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen.

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
b) Bewältigung von Sicherheitsvorfällen
c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

4.2.2 Umsetzung

Die in NIS-2 Artikel 21 (2) geforderten Einzelmaßnahmen a bis j werden der Übersichtlichkeit halber in den folgenden Kapiteln einzeln aufgearbeitet. Der Artikel 21 (2) beinhaltet keine weiteren umzusetzenden Maßnahmen außer den eben genannten.

4.3 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 21 (2) a)

4.3.1 Anforderung aus der NIS-2

NIS-2 Artikel 21 (2) a) fordert vorhandene Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme

4.3.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls die Erfüllung der Forderung nach NIS-2 Artikel 21 (2) a) geprüft:

- 1.4.1: „Inwieweit werden Informationssicherheitsrisiken gemanagt?“,
- 5.2.7: „Inwieweit wird das Netzwerk der Organisation verwaltet?“ und
- 5.3.1: „Inwieweit wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt?“

4.3.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.4.1 „Inwieweit werden Informationssicherheitsrisiken gemanagt?“

Der Auditor prüft, ob im Unternehmen Verfahren vorhanden sind, um Sicherheitsrisiken zu identifizieren, zu bewerten und zu behandeln *(Control 1.4.1; Anforderungen (sollte); Erster Unterpunkt: „+ Es ist ein Verfahren vorhanden, das festlegt, wie Sicherheitsrisiken innerhalb der Organisation zu identifizieren, bewerten und behandeln sind“)* und ob diese im Zuge des Verfahrens bewertet und behandelt werden *(Control 1.4.1; Anforderungen (muss); Vierter Unterpunkt: „+ Jedem Informationssicherheitsrisiko ist ein Verantwortlicher (Risikoeigner) zugeordnet. Dieser ist für die Bewertung und Behandlung der Informationssicherheitsrisiken verantwortlich“*.

5.2.7: „Inwieweit wird das Netzwerk der Organisation verwaltet?“

Außerdem wird vom Auditor geprüft, ob die Anforderungen an die Steuerung und Segmentierung von Netzwerken umgesetzt sind *(Control 5.2.7; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen zur Verwaltung und Steuerung von Netzwerken sind ermittelt und erfüllt“* und ob die notwendigen Sicherheitsaspekte nach Stand der Technik umgesetzt sind *(Control 5.2.7; Anforderungen (sollte); Zweiter Unterpunkt: „+ Für eine risikobasierte Segmentierung des Netzwerks werden die folgenden Aspekte berücksichtigt: – Beschränkungen bei der Anbindung von IT-Systemen an das Netzwerk, – Anwendung von Sicherheitstechnologien, – Betrachtungen hinsichtlich Leistung, Vertrauen, Verfügbarkeit, Informationssicherheit und Funktionssicherheit – Begrenzung der Auswirkungen im Falle kompromittierter IT-Systeme – Erkennung möglicher Angriffe und der lateralen Bewegung von Angreifern – Trennung von Netzwerken mit unterschiedlichem Betriebszweck (z. B. Test- und Entwicklungsnetzwerke, Büronetzwerk, Produktionsnetzwerke) – Das erhöhte Risiko aufgrund von Netzwerkdiensten, die über das Internet zugänglich sind, – Technologiespezifische Trennungsmöglichkeit bei Nutzung externer IT-Dienste, –*

Angemessene Trennung zwischen den eigenen Netzwerken und Kundennetzwerken unter Berücksichtigung der Kundenanforderungen – Erkennung und Verhinderung von Datenverlust/Datenlecks“.

5.3.1: „Inwieweit wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt?“

Weiter prüft der Auditor, dass bei der Neu- oder Weiterentwicklung von IT Systemen die Informationssicherheit Berücksichtigung findet *(Control 5.3.1; Anforderungen (muss); Erster Unterpunkt: „+ Die Anforderungen an die Informationssicherheit bei der Planung und Entwicklung von IT-Systemen sind ermittelt und werden berücksichtigt“* und die Ansprüche des ISMS an die Systeme vor deren Anwendung geprüft und sichergestellt werden *(Control 5.3.1; Anforderungen (sollte); Dritter Unterpunkt: „+ Eine Prüfung des IT-Systems auf Einhaltung der Vorgaben vor dem produktiven Einsatz wird durchgeführt“*.

4.3.4 Resümee

Die Anforderungen, dass Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme vorhanden sind, NIS-2 Artikel 21 (1) a), sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments durch den Auditor auf Vorhandensein und Umsetzung geprüft. Der TISAX-Prüfstandard geht über die geforderten vorhandenen Konzepte hinaus und prüft, dass diese implementiert und aktiv sind.

4.4 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 21 (2) b)

4.4.1 Anforderung aus der NIS-2

NIS-2 Artikel 21 (2) b) fordert die Bewältigung von Sicherheitsvorfällen;

4.4.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls die Erfüllung der Forderung nach NIS-2 Artikel 21 (2) b) geprüft:

- 1.6.1: „Inwieweit werden für die Informationssicherheit relevante Ereignisse oder Beobachtungen gemeldet?“ und
- 1.6.2: „Inwieweit werden gemeldete Sicherheitsereignisse verwaltet?“

4.4.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.6.1: „Inwieweit werden für die Informationssicherheit relevante Ereignisse oder Beobachtungen gemeldet?“

Der Auditor prüft, ob definiert ist, an welchen Parametern sich ein berichtspflichtiges Ereignis messen lässt *(Control 1.6.1; Anforderungen (muss); Erster Unterpunkt: „+ Es ist eine Definition für ein berichtspflichtiges Sicherheitsereignis oder eine berichtspflichtige sicherheitsrelevante Beobachtung vorhanden, die den Mitarbeitern und maßgeblichen Beteiligten bekannt ist. Die folgenden Aspekte werden berücksichtigt: –Ereignisse und Beobachtungen in Bezug auf Personal (z. B. Verfehlung/Fehlverhalten) – Ereignisse und Beobachtungen in Bezug auf die physische Sicherheit (z. B. Einbruch, Diebstahl, unbefugter Zugang zu Sicherheitszonen, Schwachstellen in den Sicherheitszonen) – Ereignisse und Beobachtungen in Bezug auf die IT und Cybersicherheit (z. B. anfällige IT-Systeme, erkannte erfolgreiche oder nicht erfolgreiche Angriffe) – Ereignisse und Beobachtungen in Bezug auf*

Lieferanten und andere Geschäftspartner (z. B. alle Vorfälle, die sich negativ auf die Sicherheit der eigenen Organisation auswirken können“) und dass eine Verpflichtung zur Meldung solcher Ereignisse besteht *(Control 1.6.1; Anforderungen (sollte); Dritter Unterpunkt: „+ Mitarbeiter sind verpflichtet, relevante Ereignisse zu melden und sind entsprechend geschult“)*. Weiter wird geprüft, dass die dafür notwendigen Meldekanäle zur Verfügung stehen *(Control 1.6.1; Anforderungen (muss); Dritter Unterpunkt: „+ Es sind geeignete Kommunikationskanäle für die Ereignisse meldenden Personen vorhanden“* und *(Control 1.6.1; Anforderungen (sollte); Zweiter Unterpunkt: „+ Je nach dem wahrgenommenen Schweregrad stehen unterschiedliche Meldewege zur Verfügung (d. h. Echtzeitkommunikation für signifikante Ereignisse/Notfälle zusätzlich zu asynchronen Mechanismen wie Tickets oder E-Mail“)* und die Adressaten der Meldung bekannt sind *(Control 1.6.1; Anforderungen (sollte); Erster Unterpunkt: „+ Es ist ein einheitlicher Ansprechpartner (SPOC, en: single point of contact) für die Meldung von Ereignissen vorhanden“)*. Ein weiterer Teil der Prüfung ist die Sicherstellung, dass ebenfalls Meldungen durch organisationsfremde Parteien ermöglicht sind und die notwendigen Kanäle für den externen Meldenden zur Verfügung stehen *(Control 1.6.1; Anforderungen (sollte); Vierter Unterpunkt: + Meldungen von Sicherheitsereignissen durch organisationsfremde Parteien werden berücksichtigt. – Es ist eine von außen zugängliche Möglichkeit, um Sicherheitsereignisse zu melden, vorhanden und wird kommuniziert, – Die Reaktion auf Sicherheitsereignis-Meldungen von organisationsfremden Parteien ist definiert“)*

1.6.2: „Inwieweit werden gemeldete Sicherheitsereignisse verwaltet?“

Die Prüfung des Umgangs mit Meldungen beinhaltet die Kategorisierung nach Klasse, Kategorie und Schweregrad *(Control 1.6.2; Anforderungen (sollte); Erster Unterpunkt: „+ Während der Bearbeitung werden gemeldete Ereignisse kategorisiert (z. B. nach der Verantwortung in das Personal, die physische Sicherheit und die Cybersicherheit betreffende Ereignisse), qualifiziert (z. B. nicht sicherheitsrelevant, Beobachtung, vorgeschlagene Verbesserung der Sicherheit, Sicherheitsschwachstelle, Sicherheitsvorfall) und priorisiert (z. B. niedriger, mittlerer, hoher, kritischer Schweregrad)“)* und die der Klasse zugewiesene Reaktion in einem definierten Zeitrahmen *(Control 1.6.2; Anforderungen (muss); Erste zwei Unterpunkte: „+ Gemeldete Ereignisse werden ohne unnötige Verzögerung bearbeitet. + Eine angemessene Reaktion auf gemeldete Sicherheitsereignisse ist sichergestellt“)* und unter Einbeziehung der notwendigen Verantwortlichen *(Control 1.6.2; Anforderungen (sollte); Zweiter Unterpunkt: „+Verantwortlichkeiten für den Umgang mit Ereignissen sind auf der Grundlage der Ereigniskategorie definiert und zugewiesen. Die folgenden Aspekte werden berücksichtigt: – Koordinierung von Vorfällen und Schwachstellen über mehrere Kategorien – Qualifikation und Ressourcen – Kontaktverfahren auf der Grundlage der Art und Priorität (z. B. nicht-zeitkritische Kommunikation, zeitkritische Kommunikation, Notfallkommunikation) – Abwesenheits-management“)*. Außerdem wird geprüft, dass die Meldepflichten und die zugehörigen Kontaktinformationen bekannt sind *(Control 1.6.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Dritter Unterpunkt: „+ Gesetzliche, regulatorische und vertragliche Meldepflichten und entsprechende Kontaktinformationen sind bekannt. (C, I, A)“)* und eine Kommunikationsstrategie vorhanden ist, die die Adressaten, Meldezeiträume und Meldeform berücksichtigt *(Control 1.6.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Vierter Unterpunkt: „+ Eine Kommunikationsstrategie für sicherheitsbezogene Ereignisse ist vorhanden. Die folgenden Aspekte werden berücksichtigt: (C, I, A) – Mit wem zu kommunizieren ist (z. B. Gesellschafter, betroffene Geschäftspartner und Kunden, weitere Gesellschafter, allgemeine Öffentlichkeit) – Wann zu kommunizieren ist – Verantwortlichkeiten für die Kommunikation – Ermächtigung und Freigabe der Kommunikation – Gesetzliche und regulatorische Einschränkungen der Kommunikation – Was zu kommunizieren ist (z. B. vorbereitete Vorlagen und Bausteine für bestimmte Szenarien) – Wie zu kommunizieren ist (z. B. Kommunikationskanäle)“)*.

4.4.4 Resümee

Die Anforderungen der NIS-2 Artikel 21 (2) Unterpunkt b), die Bewältigung von Sicherheitsvorfällen, sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments

durch den Auditor auf Vorhandensein und Umsetzung geprüft. Die Verfahren zu Feststellung, Meldewegen und -verfahren, Klassifizierung, Abarbeitung und Eskalation im Bedarfsfall gehen über die in der NIS-2 geforderte Anforderung hinaus.

4.5 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 21 (2) c)

4.5.1 Anforderung aus der NIS-2

NIS-2 Artikel 21 (2) Unterpunkt c) fordert die Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement.

4.5.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls *die Erfüllung der Forderung nach NIS-2 Artikel 21 (2) c) geprüft:*

- 1.6.3: „In welchem Maße ist die Organisation vorbereitet, mit Krisensituationen umzugehen?“,
- 5.2.8: „Inwieweit ist eine Kontinuitätsplanung für IT-Dienste vorhanden?“ und
- 5.2.9: „Inwieweit wird die Sicherung und Wiederherstellung von Daten und IT-Diensten sichergestellt?“.

4.5.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.6.3: „In welchem Maße ist die Organisation vorbereitet, mit Krisensituationen umzugehen?“

In Bezug auf das Krisenmanagement wird vom Auditor geprüft, ob in der Organisation die Verantwortlichkeiten und Befugnisse im Umgang mit Krisen definiert sind *(Control 1.6.3; Anforderungen (muss); Dritter Unterpunkt: „+ Verantwortlichkeiten und Befugnisse für das Krisenmanagement in der Organisation sind definiert, dokumentiert und zugewiesen“)* und ob die Verantwortlichen die entsprechende Qualifikation aufweisen *(Control 1.6.3; Anforderungen (muss); Vierter Unterpunkt: „+ Die verantwortlichen Mitarbeiter sind definiert und für ihre Aufgabe qualifiziert“)*, diese Aufgabe wahrnehmen zu können. Die Rahmenbedingungen einer Krise *(Control 1.6.3; Anforderungen (sollte); Erster Unterpunkt: „+ Verfahren zum Erkennen von Krisensituationen sind etabliert – Allgemeine Hinweise auf eine vorliegende oder bevorstehende Krisensituation und eine bestimmte vorhersehbare Krise sind identifiziert)* und den Prozess zum Ausruf einer solchen *(Control 1.6.3; Anforderungen (sollte); Zweiter Unterpunkt: „+ Ein Verfahren zum Abrufen und/oder Eskalieren des Krisenmanagements ist vorhanden“)* sind ebenfalls Teil der Prüfung.

5.2.8: „Inwieweit ist eine Kontinuitätsplanung für IT-Dienste vorhanden?“

Der Auditor prüft, ob eine Kontinuitätsplanung für IT-Dienste *(Control 5.2.8; Anforderungen (muss); Erster Unterpunkt: „+ Kritische IT-Dienste werden identifiziert, und die geschäftlichen Auswirkungen werden betrachtet“)* und IT Systeme *(Control 5.2.8; Anforderungen (sollte); Erster Unterpunkt: „Kritische IT-Systeme werden identifiziert – die maßgeblichen Systeme sind nach dem entsprechenden Schutzbedarf klassifiziert – angemessene und geeignete Sicherheitsmaßnahmen werden umgesetzt)* besteht, die auf einer Bewertung der Kritikalität der vorhandenen Dienste bzw. Systeme beruht und die den maßgeblichen verantwortlichen bekannt ist *(Control 5.2.8; Anforderungen (muss); Zweiter Unterpunkt: „+ Anforderungen und Verantwortlichkeiten für die Kontinuität und Wiederherstellung dieser IT-Dienste sind den maßgeblichen Beteiligten bekannt und werden erfüllt“)*.

Außerdem prüft der Auditor das Vorhandensein von Spezifikationen zu unterschiedlichen Szenarien *(Control 5.2.8; Anforderungen (sollte); Zweiter Unterpunkt: „+ Die Kontinuitätsplanung schließt mindestens die folgenden Szenarien ein, welche kritische IT-Systeme betreffen: – (Distributed) Denial-of-Service-Angriffe – Erfolgreiche Ransomware-Angriffe und andere Sabotageaktivitäten – Systemausfall – Naturkatastrophe* und Backupstrategien *(Control 5.2.8; Anforderungen (sollte); Dritter Unterpunkt: „+ Bei der Kontinuitätsplanung werden die folgenden Fälle berücksichtigt: – Alternative Kommunikationsstrategien, falls primäre Kommunikationsmittel nicht verfügbar sind – Alternative Speicherungsstrategien, falls primäre Mittel zur Speicherung nicht verfügbar sind – Alternative Energieversorgung und alternatives Netzwerk“),* deren Aktualität anhand von Überprüfungsprotokollen geprüft wird *(Control 5.2.8; Anforderungen (sollte); Vierter Unterpunkt: „+ Die Kontinuitätsplanung wird regelmäßig überprüft und aktualisiert“).*

Ein weiterer Teil der Prüfung dient der Sicherstellung, dass sich Backups in einem Wiederherstellungsfähigen Zustand befinden *(Control 5.2.8; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Fünfter Unterpunkt: „+ Eine Sicherungs- und Wiederherstellungsstrategie für kritische IT-Dienste und Informationen ist definiert und umgesetzt. Die folgenden Aspekte werden berücksichtigt: – Backups sind vor unbefugter Änderung oder Löschung durch Schadsoftware geschützt. (I, A) -Backups sind vor unbefugtem Zugriff durch Schadsoftware oder deren Betreiber geschützt (C, I)“)* und die im Backup befindlichen Daten nicht korrupt sind und über den gesamten Zeitraum der Vorhaltung vor Manipulation geschützt werden.

5.2.9: „Inwieweit wird die Sicherung und Wiederherstellung von Daten und IT-Diensten sichergestellt?“

Zur Sicherstellung von Sicherungen und Wiederherstellungsfähigkeit von Daten und IT-Diensten prüft der Auditor das Vorhandensein von Backupkonzepten für maßgebliche Systeme *(Control 5.2.9; Anforderungen (muss); Erster Unterpunkt: „+ Für die maßgeblichen IT-Systeme sind Backup-Konzepte vorhanden. Die folgenden Aspekte werden berücksichtigt: – Entsprechende Schutzmaßnahmen, um die Vertraulichkeit, Integrität und Verfügbarkeit für Daten-Backups sicherzustellen. Integrität und Verfügbarkeit für Daten-Backups sicherzustellen“)* und Wiederherstellungskonzepten für maßgebliche IT-Dienste, *(Control 5.2.9; Anforderungen (muss); Zweiter Unterpunkt: „+ Für die maßgeblichen IT-Dienste sind Wiederherstellungs-Konzepte vorhanden“)* die die Abhängigkeiten bei der Wiederherstellung berücksichtigen. *(Control 5.2.9; Anforderungen (sollte); Erster Unterpunkt: „+ Für jeden maßgeblichen IT-Dienst ist ein Sicherungs- und Wiederherstellungs-Konzept vorhanden. – Abhängigkeiten zwischen IT-Diensten und die Reihenfolge für die Wiederherstellung werden berücksichtigt“).* Weiter prüft der Auditor bei Organisationen, bei denen die Verfügbarkeit wesentlich ist, Nachweise, dass methodische Überprüfungen der Konzepte sattfinden, *(Control 5.2.9; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Sicherungs- und Wiederherstellungskonzepte werden in regelmäßigen Abständen methodisch überprüft.“)* die allgemeine Wiederherstellungskapazität berücksichtigt und geprüft wird *(Control 5.2.9; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Zweiter Unterpunkt: „+ Die allgemeine Wiederherstellungskapazität wird berücksichtigt und geprüft (z. B. Stichprobenprüfung, Prüfsysteme)“)* und dass relevante Aspekte Berücksichtigung finden *(Control 5.2.9; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Dritter Unterpunkt: „+ Sicherungs- und Wiederherstellungskonzepte berücksichtigen die folgenden Aspekte: - Zielsetzung für den Wiederherstellungspunkt (RPO, en Recovery Point Objective). – Zeitvorgabe für die Wiederherstellung (RTO, en: Recovery Time Objective). – Erforderliche Ressourcen für die Wiederherstellung (unter Berücksichtigung der Kapazität und Leistung einschließlich Personal und Hardware). – Vermeidung von Überlastungsszenarien während der Wiederherstellung. – Angemessene räumliche Redundanz (z. B. separater Raum, separater Brandabschnitt, separates Rechenzentrum, separater Standort)“).*

4.5.4 Resümee

Die Anforderungen der NIS-2 Artikel 21 (2) Unterpunkt c), die Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement, sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments durch den Auditor auf

Vorhandensein und Umsetzung geprüft. Der Auditor stellt fest, inwieweit die Organisation vorbereitet ist, mit Krisensituationen umzugehen, ob eine Kontinuitätsplanung für IT-Dienste vorhanden ist und ob die Sicherung und Wiederherstellung von Daten und IT-Diensten sichergestellt ist.

4.6 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 21 (2) d)

4.6.1 Anforderung aus der NIS-2

NIS-2 Artikel 21 (2) Unterpunkt d) fordert die Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Dienstanbietern.

4.6.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls *die Erfüllung der Forderung nach NIS-2 Artikel 21 (2) d) geprüft:*

- 1.2.4: „Inwieweit sind die Verantwortlichkeiten zwischen organisationsfremden IT-Dienstleistern und der eigenen Organisation definiert?“,
- 1.3.3: „Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene organisationsfremde IT-Dienste zum Verarbeiten von Informationswerten der Organisation eingesetzt werden?“,
- 1.6.1: „Inwieweit werden für die Informationssicherheit relevante Ereignisse oder Beobachtungen gemeldet?“,
- 1.6.2: „Inwieweit werden gemeldete Sicherheitsereignisse verwaltet?“,
- 5.3.3: „Inwieweit ist die Rückgabe und das sichere Entfernen von Informationswerten aus organisationsfremden IT-Diensten geregelt?“,
- 6.1.1: „Inwieweit wird die Informationssicherheit bei Auftragnehmern und Kooperationspartnern sichergestellt?“ und
- 6.1.2: „Inwieweit ist Geheimhaltung beim Austausch von Informationen vertraglich vereinbart?“

4.6.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.2.4 „Inwieweit sind die Verantwortlichkeiten zwischen organisationsfremden IT-Dienstleistern und der eigenen Organisation definiert?“

Der Auditor prüft, dass IT-Dienste und Dienstleistungen, die Maßnahmen zur Informationssicherheit unterliegen, identifiziert *(Control 1.2.4; Anforderungen (muss); Erster Unterpunkt: „+ Die betreffenden eingesetzten Dienste und IT-Dienstleistungen sind identifiziert*“), in einem Verzeichnis protokolliert *(Control 1.2.4; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Es existiert ein Verzeichnis der betreffenden IT-Dienste und der jeweils verantwortlichen IT-Dienstleister. (C, I, A)“)* und dass die für die Umsetzung der Maßnahmen verantwortliche Organisation definiert und sich ihrer Verantwortung bewusst ist *(Control 1.2.4; Anforderungen (muss); Dritter Unterpunkt:* „*+ Die für die Umsetzung der Anforderung verantwortliche Organisation ist definiert und sich ihrer Verantwortung bewusst“)*. Weiter wird geprüft, dass die Aufteilung gemeinsamer Verantwortlichkeiten geregelt und umgesetzt ist *(Control 1.2.4; Anforderungen (muss); Vierter Unterpunkt:* „*+ Für gemeinsame Verantwortlichkeiten sind Mechanismen festgelegt und umgesetzt“)* und dass die jeweils

verantwortliche Organisation diesen gerecht wird (*(Control 1.2.4; Anforderungen (muss); Fünfter Unterpunkt: „+ Die verantwortliche Organisation wird ihren jeweiligen Verantwortlichkeiten gerecht“*). Zur Kontrolle der Funktionalität der geforderten Maßnahmen wird vom Auditor außerdem geprüft, dass entsprechende Nachweise vorliegen (*Control 1.2.4; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Vierter Unterpunkt: „+ Es liegen Nachweise vor, dass die IT-Dienstleister ihrer Verantwortung gerecht werden. (C, I, A)“).*

1.3.3 „Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene organisationsfremde IT-Dienste zum Verarbeiten von Informationswerten der Organisation eingesetzt werden?“

Im Hinblick auf die Nutzung organisationfremder IT-Dienste prüft der Auditor, dass diese nicht ohne Bewertung und Umsetzung der aus der Bewertung resultierenden Maßnahmen (*(Control 1.3.3; Anforderungen (muss); Erster Unterpunkt: „+ 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“*) eingesetzt werden und dass die Anforderungen an die Dienste dem Schutzbedarf der zu verarbeitenden Information angemessen sind (*(Control 1.3.3; Anforderungen (muss); Zweiter Unterpunkt: „+ Die organisationsfremden IT-Dienste wurden auf den Schutzbedarf der verarbeiteten Informationswerte abgestimmt“).* Um die Umsetzung und Einhaltung der Maßnahmen sicherzustellen, kontrolliert der Prüfer, dass ein Freigabeverfahren etabliert (*(Control 1.3.3; Anforderungen (sollte); Zweiter Unterpunkt: „+ Ein Verfahren zur Freigabe unter Berücksichtigung des Schutzbedarfs ist etabliert“*) und dokumentiert *(Control 1.3.3; Anforderungen (sollte); Dritter Unterpunkt: „+ Organisationsfremde IT-Dienste und deren Freigabe sind dokumentiert.“*) ist und dass eine Regelmäßige Prüfung der Einhaltung durchgeführt *(Control 1.3.3; Anforderungen (sollte); Vierter Unterpunkt: „+ Es wird regelmäßig überprüft, dass nur freigegebene organisationsfremde IT-Dienste eingesetzt werden)* wird.

1.6.1: „Inwieweit werden für die Informationssicherheit relevante Ereignisse oder Beobachtungen gemeldet?“

Der Auditor prüft, dass bei eintretenden Sicherheitsereignissen innerhalb der Lieferkette ein Kommunikationskanal besteht, über den Meldungen eingehen können und diese dann auch entsprechend bewertet und bearbeitet werden *(Control 1.6.1; Anforderungen (sollte); Vierter Unterpunkt: „+ Meldungen von Sicherheitsereignissen durch organisationsfremde Parteien werden berücksichtigt. – Es ist eine von außen zugängliche Möglichkeit um Sicherheitsereignisse zu melden vorhanden und wird kommuniziert, – Die Reaktion auf Sicherheitsereignis-Meldungen von organisationsfremden Parteien ist definiert“).*

1.6.2: „Inwieweit werden gemeldete Sicherheitsereignisse verwaltet?“

Weiter prüft er das Vorhandensein von definierten Reaktionen auf solche Meldungen (Control 1.6.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Fünfter Unterpunkt: „+ Verfahren für die Reaktion auf Sicherheitsvorfälle bei Lieferanten sind etabliert. Die folgenden Aspekte werden berücksichtigt: (C, I, A) – Analyse der Auswirkungen auf die eigene Organisation und Abrufen entsprechender interner Mechanismen – Die Notwendigkeit zur Meldung entsprechend den eigenen Meldeverfahren“).

5.3.3 „Inwieweit ist die Rückgabe und das sichere Entfernen von Informationswerten aus organisationsfremden IT-Diensten geregelt?“

Weiter wird vom Auditor innerhalb des Assessments geprüft, dass Informationswerte, die in organisationsfremden Diensten liegen, sicher rückgeführt und entfernt werden *(Control 5.3.3; Anforderungen (muss); Erster Unterpunkt: „+ Ein Verfahren zur Rückgabe und sicheren Entfernung von Informationswerten aus jedem organisationsfremden IT-Dienst ist definiert und umgesetzt“)* und der Auditor kontrolliert die vertragliche Grundlage und den Terminierungsprozess hierzu *(Control 5.3.3; Anforderungen (sollte); Erster Unterpunkt: „+ Eine Beschreibung des Terminierungsprozesses liegt vor, wird bei Änderungen angepasst und ist vertraglich geregelt“).*

6.1.1 „Inwieweit wird die Informationssicherheit bei Auftragnehmern und Kooperationspartnern sichergestellt?“

Im Hinblick auf Auftragsnehmer und Kooperationspartner und deren Informationssicherheitsstandard prüft der Auditor, dass eine Risikobewertung bezüglich dieser durchgeführt wird, *(Control 6.1.1; Anforderungen (muss); Erster Unterpunkt: „+ Auftragnehmer und Kooperationspartner werden einer Risikobewertung bezüglich der Informationssicherheit unterzogen“)* und dabei entsprechende Nachweise zum Niveau der Informationssicherheit

eingeholt werden *(Control 6.1.1; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Es liegt ein Nachweis vor, dass das Informationssicherheitsniveau des Lieferanten für den Schutzbedarf der Informationen angemessen ist (z. B. Zertifikat, Bescheinigung, interne Revision). (C, I, A)“).* Weiter wird geprüft, dass die Anforderungen an die Informationssicherheit vertraglich vereinbart *(Control 6.1.1; Anforderungen (muss); Zweiter Unterpunkt: + Mit Auftragnehmern und Kooperationspartnern wird durch vertragliche Vereinbarungen ein angemessenes Informationssicherheitsniveau sichergestellt.“)* und sowohl an Auftragnehmer und Kooperationspartner *(Control 6.1.1; Anforderungen (muss); Dritter Unterpunkt: „+ Vertragliche Vereinbarungen mit Auftraggebern werden, soweit zutreffend, an Auftragnehmer und Kooperationspartner weitergegeben“)* als auch an deren Unterauftragnehmer weiteregegeben *(Control 6.1.1; Anforderungen (sollte); Erster Unterpunkt: „+ Auftragnehmer und Kooperationspartner werden vertraglich verpflichtet, alle Anforderungen an ein angemessenes Informationssicherheitsniveau an ihre Unterauftragnehmer weiterzugeben“)* werden und entsprechende Nachweise zur Einhaltung der vertraglichen Vereinbarungen vorliegen *(Control 6.1.1; Anforderungen (muss); Vierter Unterpunkt: „+ Die Einhaltung vertraglicher Vereinbarungen wird verifiziert“)* und die von den Auftragnehmern und Kooperationspartner gelieferten Serviceberichte und Dokumente nach Erhalt auf Einhaltung geprüft werden *(Control 6.1.1; Anforderungen (sollte); Zweiter Unterpunkt: „+ Serviceberichte und Dokumente von Auftragnehmern und Kooperationspartnern werden überprüft“).*

6.1.2 „Inwieweit ist Geheimhaltung beim Austausch von Informationen vertraglich vereinbart?“

Der Auditor prüft, dass Anforderungen an die Geheimhaltung ermittelt sind, *(Control 6.1.2; Anforderungen (muss); Erster Unterpunkt: „+ Die Anforderungen an die Geheimhaltung sind ermittelt und erfüllt“),* dass es Verfahren zum Einsatz von Geheimhaltungsvereinbarungen gibt *(Control 6.1.2; Anforderungen (muss); Dritter Unterpunkt: „+ Vor der Weitergabe von sensiblen Informationen werden gültige Geheimhaltungsvereinbarungen abgeschlossen“)* und diese auch allen Personen, die schutzbedürftige Informationen weitergeben, bekannt sind *(Control 6.1.2; Anforderungen (muss); Zweiter Unterpunkt: „+ Anforderungen und Verfahren zum Einsatz von Geheimhaltungsvereinbarungen sind allen Personen bekannt, die schutzbedürftige Informationen weitergeben“).* Weiter prüft der Auditor, dass eine regelmäßige Überprüfung der Einhaltung stattfindet *(Control 6.1.2; Anforderungen (muss); Vierter Unterpunkt: „+ Die Anforderungen und Verfahren für die Anwendung von Geheimhaltungsvereinbarungen und den Umgang mit schutzbedürftigen Informationen werden in regelmäßigen Abständen überprüft“).*

4.6.4 Resümee

Die Anforderungen der NIS-2 Artikel 21 (2) Unterpunkt d), die Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern, sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments durch den Auditor auf Vorhandensein und Umsetzung geprüft. Die Anforderungen im ISA6-Prüfstandard gehen über die Anforderungen der NIS-2 hinaus und beinhalten z.B. auch die Einhaltung von Informationssicherheitsstandards über die unmittelbaren Anbieter oder Diensteanbieter hinaus.

4.7 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 21 (2) e)

4.7.1 Anforderung aus der NIS-2

NIS-2 Artikel 21 (2) Unterpunkt e) fordert Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

4.7.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls *die Erfüllung der Forderung nach NIS-2 Artikel 21 (2) e) geprüft:*

- 1.2.3: „Inwieweit werden Informationssicherheitsanforderungen in Projekten berücksichtigt?“,
- 1.2.4: „Inwieweit sind die Verantwortlichkeiten zwischen organisationsfremden IT-Dienstleistern und der eigenen Organisation definiert?“,
- 1.3.4: „Inwieweit wird sichergestellt, dass nur evaluierte und zugelassene Software zum Verarbeiten von Informationswerten der Organisation eingesetzt wird?“,
- 5.2.1: „Inwieweit werden Änderungen verwaltet?“,
- 5.2.4: „Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert?“,
- 5.2.5: „Inwieweit werden Schwachstellen erkannt und behandelt?“,
- 5.2.6: „Inwieweit werden IT-Systeme und -Dienste technisch überprüft (System- und Dienst-Audit)?“,
- 5.3.1: „Inwieweit wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt?“,
- 5.3.2: „Inwieweit sind Anforderungen an Netzwerkdienste definiert?“,
- 5.3.3: „Inwieweit ist die Rückgabe und das sichere Entfernen von Informationswerten aus organisationsfremden IT-Diensten geregelt?“ und
- 5.3.4: „Inwieweit sind Informationen in gemeinsam genutzten organisationsfremden IT-Diensten geschützt?“

4.7.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.2.3: „Inwieweit werden Informationssicherheitsanforderungen in Projekten berücksichtigt?“

Der Auditor prüft, ob bei der Durchführung von jeglicher Art von Projekten eine Klassifizierung bezüglich der Informationssicherheit durchgeführt wird *(Control 1.2.3 ; Anforderungen (muss); Erster Unterpunkt: „+ Projekte sind unter Berücksichtigung der Anforderungen an die Informationssicherheit klassifiziert“)* und als Resultat entsprechende Maßnahmen zur Risikobehandlung abgeleitet werden *(Control ; Anforderungen (sollte); Dritter Unterpunkt: „+ Für identifizierte Informationssicherheitsrisiken werden Maßnahmen abgeleitet und im Projekt berücksichtigt“).*

1.2.4 „Inwieweit sind die Verantwortlichkeiten zwischen organisationsfremden IT-Dienstleistern und der eigenen Organisation definiert?“

Der Auditor prüft, dass IT-Dienste und -Dienstleistungen, die Maßnahmen zur Informationssicherheit unterliegen, identifiziert *(Control 1.2.4; Anforderungen (muss); Erster Unterpunkt: „+ Die betreffenden eingesetzten Dienste und IT-Dienstleistungen sind identifiziert*“), in einem Verzeichnis protokolliert *(Control 1.2.4; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Es existiert ein Verzeichnis der betreffenden IT-Dienste und der jeweils verantwortlichen IT-Dienstleister. (C, I, A)“)* und dass die für die Umsetzung der Maßnahmen verantwortliche Organisation definiert und sich ihrer Verantwortung bewusst ist *(Control 1.2.4; Anforderungen (muss); Dritter Unterpunkt: „+ Die für die Umsetzung der Anforderung verantwortliche Organisation ist definiert und sich ihrer Verantwortung bewusst“)*. Weiter wird geprüft, dass die Aufteilung gemeinsamer Verantwortlichkeiten geregelt und umgesetzt ist *(Control 1.2.4; Anforderungen (muss); Vierter Unterpunkt: „+ Für gemeinsame Verantwortlichkeiten sind Mechanismen festgelegt und umgesetzt“)* und dass die jeweils verantwortliche Organisation diesen gerecht wird (*(Control 1.2.4; Anforderungen (muss); Fünfter Unterpunkt: „+ Die verantwortliche Organisation wird ihren jeweiligen Verantwortlichkeiten gerecht“*). Zur Kontrolle

der Funktionalität der geforderten Maßnahmen wird vom Auditor außerdem geprüft, dass entsprechende Nachweise vorliegen (*Control 1.2.4; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Vierter Unterpunkt: „+ Es liegen Nachweise vor, dass die IT-Dienstleister ihrer Verantwortung gerecht werden. (C, I, A)“).*

1.3.4: „Inwieweit wird sichergestellt, dass nur evaluierte und zugelassene Software zum Verarbeiten von Informationswerten der Organisation eingesetzt wird?“

Um sicherzustellen, dass nur zugelassene Software Anwendung findet, prüft der Auditor, ob eine solche Zulassung stattgefunden hat (Control 1.3.4; Anforderungen (muss); Erster Unterpunkt: „+ Vor der Installation oder Nutzung wird die Software zugelassen. Die folgenden Aspekte werden berücksichtigt: – Begrenzte Freigabe für bestimmte Anwendungsfälle oder Aufgaben – Übereinstimmung mit den Anforderungen an die Informationssicherheit – Nutzungsrechte und Lizensierung der Software – Quelle/Ansehen der Software“), ob die zu verwaltenden Software-Typen ermittelt sind *(Control 1.3.4 ; Anforderungen (sollte); Erster Unterpunkt: „+ Die zu verwaltenden Software-Typen wie z. B. Firmware, Betriebssysteme, Anwendungen, Bibliotheken, Gerätetreiber sind ermittelt“)*; ob eine regelmäßige Überprüfung der Aktualität der freigegebenen Software durchgeführt wird *(Control 1.3.4; Anforderungen (sollte); Vierter Unterpunkt: „+ Die Freigabe der Software wird regelmäßig überprüft“)* und die aktuellen Software-Versionen und Patch-Levels bekannt sind *(Control 1.3.4; Anforderungen (sollte); Fünfter Unterpunkt: „+Software-Versionen und Patch-Levels sind bekannt“)*. Der Auditor prüft außerdem das Vorhandensein von Software-Repositorys *(Control 1.3.4; Anforderungen (sollte); Zweiter Unterpunkt: „+ Repositorys der verwalteten Software sind vorhanden“)* und den Schutz dieser vor unbefugter Manipulation *(Control 1.3.4; Anforderungen (sollte); Dritter Unterpunkt: „+ Die Software-Repositorys sind vor unbefugter Manipulation geschützt“)*.

5.2.1: „Inwieweit werden Änderungen verwaltet?“

In Bezug auf Änderungen prüft der Auditor, dass die Anforderungen an die Informationssicherheit ermittelt und umgesetzt werden *(Control 5.2.1; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen an die Informationssicherheit bei Änderungen von Organisation, Geschäftsprozessen, IT-Systemen werden ermittelt und umgesetzt“ und* eine Bewertung in Bezug auf die Auswirkung in Richtung der Informationssicherheit stattfindet *(Control 5.2.1; Anforderungen (sollte); Zweiter Unterpunkt: „+ Änderungen werden bezüglich möglicher Auswirkungen auf die Informationssicherheit verifiziert und bewertet“)*. Weiter wird vom Auditor geprüft, dass bei Änderungen mit Auswirkung auf die Informationssicherheit, ein formales Genehmigungsverfahren etabliert ist *(Control 5.2.1; Anforderungen (sollte); Erster Unterpunkt: „+ Ein formales Genehmigungsverfahren ist etabliert“),* und diese geplant und geprüft werden *(Control 5.2.1; Anforderungen (sollte); Dritter Unterpunkt: „+ Änderungen mit Auswirkung auf die Informationssicherheit werden geplant und geprüft“),* dass die Änderungen während und nach der Umsetzung verifiziert werden *(Control 5.2.1; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Die Einhaltung der Anforderungen an die Informationssicherheit wird während und nach der Umsetzung der Änderungen verifiziert. (C, I, A)“)* und das Notfallverfahren im Falle von Fehlern berücksichtigt werden *(Control 5.2.1; Anforderungen (sollte); Vierter Unterpunkt: „+ Notfallverfahren im Falle von Fehlern sind berücksichtigt“).*

5.2.4: „Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert?“

Um die Rückverfolgbarkeit von Ereignissen im Falle eines Sicherheitsvorfalls sicherzustellen, prüft der Auditor, dass eine Ereignisprotokollierung stattfindet und das diese in ihrer Handhabung die Anforderungen der Informationssicherheit berücksichtigt *(Control 5.2.4; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen an die Informationssicherheit bezüglich der Handhabung von Ereignisprotokollen sind ermittelt und erfüllt*“) und dabei eine angemessene Überwachung und Aufzeichnung aller informationssicherheitsrelevanten Aktionen im Netzwerk sicherstellt *(Control 5.2.4; Anforderungen (sollte); Dritter Unterpunkt: „+ Eine angemessene Überwachung und Aufzeichnung aller informationssicherheitsrelevanten Aktionen im Netzwerk sind etabliert“)*. Außerdem stellt der Auditor fest, ob Sicherheitsrelevante Anforderungen an die Protokollierung der Aktivitäten von Systemadministratoren und Nutzern ermittelt sind und erfüllt werden *(Control 5.2.4; Anforderungen (muss); Zweiter Unterpunkt: „+ Sicherheitsrelevante Anforderungen an die Protokollierung der Aktivitäten von Systemadministratoren und Nutzern sind ermittelt und erfüllt“).* Er prüft weiterhin, dass eingesetzte IT-Systeme hinsichtlich der Protokollierung bewertet werden *(Control 5.2.4; Anforderungen (muss); Dritter Unterpunkt: „+ Die eingesetzten*

IT-Systeme werden hinsichtlich der Notwendigkeit der Protokollierung bewertet“) und das speziell bei organisationsfremden IT-Systemen die Überwachungsmöglichkeiten bekannt sind und Berücksichtigung finden *(Control 5.2.4; Anforderungen (muss); Vierter Unterpunkt: „+ Bei der Nutzung organisationsfremder IT-Dienste werden Informationen zu den Überwachungsmöglichkeiten eingeholt und im Assessment berücksichtigt“).* Außerdem prüft er, dass die eingerichteten Zugriffe beim Auf- und Abbau von organisationsfremden Netzwerkverbindungen protokolliert werden *(Control 5.2.4; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Zweiter Unterpunkt: „+ Zugriffe beim Auf- und Abbau von organisationsfremden Netzwerkverbindungen (z. B. Fernwartung) werden protokolliert. (C, I, A)“).* Der Auditor prüft ebenfalls das Vorhandensein von Nachweisen über die regelmäßige Kontrolle von Ereignisprotokollen *(Control 5.2.4; Anforderungen (muss); Fünfter Unterpunkt: „+ Ereignisprotokolle werden regelmäßig auf Regelverstöße und Auffälligkeiten im Einklang mit den zulässigen gesetzlichen und betrieblichen Bestimmungen überprüft“)* und dass ein Eskalationsverfahren bei relevanten Ereignissen Anwendung findet *(Control 5.2.4; Anforderungen (sollte); Erster Unterpunkt: „+ Ein Verfahren zur Eskalation von relevanten Ereignissen an die zuständige Stelle (z. B. Sicherheitsvorfall-Meldung, Datenschutz, Unternehmenssicherheit, IT-Sicherheit) ist definiert und etabliert“).* Er kontrolliert weiter, dass die für die Sicherheit während der Handhabung relevanten Informationssicherheitsanforderungen definiert sind und eingehalten werden *(Control 5.2.4; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Informationssicherheitsanforderungen, die für die Sicherheit während der Handhabung von Ereignisprotokollen relevant sind, z. B. vertragliche Anforderungen, sind ermittelt und umgesetzt. (C, I, A)“)* und dass die Protokolle gegen Änderungen geschützt werden *(Control 5.2.4; Anforderungen (sollte); Zweiter Unterpunkt: „+ Ereignisprotokolle (Inhalte und Metadaten) sind gegen Änderungen geschützt. (z. B. durch eine dedizierte Umgebung)“).*

5.2.5: „Inwieweit werden Schwachstellen erkannt und behandelt?“

In Bezug auf die Schwachstellenanalyse prüft der Auditor, dass Informationen über technische Schwachstellen gesammelt werden *(Control 5.2.5; Anforderungen (muss); Erster Unterpunkt: „+ Informationen über technische Schwachstellen zu den genutzten IT-Systemen werden gesammelt (z. B. Information vom Hersteller, System-Audits, CVS-Datenbank) und beurteilt (z. B. Allgemeines Bewertungssystem für Schwachstellen, en: Common Vulnerability Scoring System, CVSS)“)* und die erlangten Erkenntnisse zur Behandlung solcher eingesetzt werden *(Control 5.2.5; Anforderungen (muss); Zweiter Unterpunkt: „+ Potenziell betroffene IT-Systeme und Software werden identifiziert, bewertet und Schwachstellen behandelt“)* und dass Risiken auf ein Mindestmaß reduziert werden *(Control 5.2.4; Anforderungen (sollte); Zweiter Unterpunkt: „+ Maßnahmen zur Verringerung von Risiken auf ein Mindestmaß sind, soweit notwendig, umgesetzt “).* Der Auditor prüft außerdem, dass ein Patch-Management etabliert ist *(Control 5.2.5; Anforderungen (sollte); Erster Unterpunkt: „+ Ein angemessenes Patch-Management ist definiert und umgesetzt (z. B. Prüfung und Installation von Patches)“)* und dass die erfolgreiche Installation verifiziert wird *(Control 5.2.5; Anforderungen (sollte); Dritter Unterpunkt: „+ Die erfolgreiche Installation von Patches ist in geeigneter Weise verifiziert“).*

5.2.6: „Inwieweit werden IT-Systeme und -Dienste technisch überprüft (System- und Dienst-Audit)?“

Zur Verifizierung der technischen Überprüfung von IT-Systemen und -Diensten prüft der Auditor, dass die Anforderungen an die Auditierung dieser Systeme und Dienste definiert sind *(Control 5.2.6; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen an die Auditierung von IT-Systemen oder -Diensten sind ermittelt“),* die Audits regelmäßig durchgeführt werden *(Control 5.2.6; Anforderungen (sollte); Zweiter Unterpunkt: „+ Regelmäßige System- oder Dienst-Audits werden durchgeführt – von Fachpersonal durchgeführt – geeignete Werkzeuge (z. B. Schwachstellen-Scanner) werden für System- und Dienst-Audits verwendet (sofern anwendbar) – vom Internet und dem internen Netzwerk durchgeführt“),* dass die Audits im Umfang festgelegt *(Control 5.2.6; Anforderungen (muss); Zweiter Unterpunkt: „+ Der Umfang des Systemaudits ist rechtzeitig festgelegt“* und im Hinblick auf die entstehenden Sicherheitsrisiken bewertet werden. *(Control 5.2.6; Anforderungen (sollte); Erster Unterpunkt: „+ System- und Dienst-Audits werden unter Berücksichtigung aller Sicherheitsrisiken geplant, die dadurch hervorrufen werden, könnten (z. B. Störungen)“).* Weiter prüft der Auditor, dass sie mit den Betreibern und Nutzer abgestimmt sind *(Control 5.2.6; Anforderungen (muss); Dritter Unterpunkt: „+ System- oder Dienst-Audits sind mit dem Betreiber und den Nutzern der IT-Systeme oder -Dienste abgestimmt“).* Für kritische IT-Systeme oder -

Dienste und Unternehmen, deren Verfügbarkeit in der Lieferkette wesentlich ist, prüft der Auditor außerdem, dass zusätzliche Anforderungen an das Audit identifiziert und berücksichtigt wurden *(Für kritische IT-Systeme oder -Dienste wurden zusätzliche Anforderungen an das System- oder Dienst-Audit identifiziert, die erfüllt werden (z. B. dienstspezifische Tests und Werkzeuge und/oder Penetrationstests, risikobasierte Zeitintervalle) (A))*.

Die Prüfung beinhaltet auch die Kontrolle eines Nachweises zur Durchführung *(Control 5.2.6; Anforderungen (sollte); Dritter Unterpunkt: „+ Innerhalb eines angemessenen Zeitraums nach Abschluss des Audits wird ein Bericht erstellt)* sowie zur Speicherung und zur Weitermeldung der Ergebnisse an das Management *(Control 5.2.6; Anforderungen (muss); Vierter Unterpunkt: „+ Die Ergebnisse von System- oder Dienst-Audits werden rückverfolgbar gespeichert und an das zuständige Management berichtet“)* und das auf dem Bericht basierende Ableiten entsprechender Maßnahmen *(Control 5.2.6; Anforderungen (muss); Fünfter Unterpunkt: „+ Von den Ergebnissen werden Maßnahmen abgeleitet“)*.

5.3.1: „Inwieweit wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt?“

Der Auditor prüft die Berücksichtigung der Informationssicherheit bei der Planung und Entwicklung *(Control 5.3.1; Anforderungen (muss); Erster Unterpunkt: „+ Die Anforderungen an die Informationssicherheit bei der Planung und Entwicklung von IT-Systemen sind ermittelt und werden berücksichtigt“)* sowie bei Beschaffung oder Erweiterung *(Control 5.3.1; Anforderungen (muss); Zweiter Unterpunkt: „+ Die Anforderungen an die Informationssicherheit bei der Beschaffung oder Erweiterung von IT-Systemen und IT-Komponenten sind ermittelt und werden berücksichtigt“)* und der Weiterentwicklung von IT-Systemen *(Control 5.3.1; Anforderungen (muss); Dritter Unterpunkt: „+ Anforderungen an die Informationssicherheit bei Änderungen in entwickelten IT-Systemen sind berücksichtigt“)*. Der Auditor prüft weiter, ob Lastenhefte angelegt wurden *(Control 5.3.1; Anforderungen (sollte); Erster Unterpunkt: „+ Lastenhefte sind erstellt. Die folgenden Aspekte werden berücksichtigt: – Die Anforderungen an die Informationssicherheit – Empfehlungen des Verkäufers und bewährte Verfahren für eine sichere Konfiguration und Implementierung – Bewährte Verfahren und Sicherheitsleitlinien – Ausfallsicher (so konzipiert, dass im Falle eines Ausfalls oder einer Fehlfunktion eine Rückkehr in einen sicheren Zustand erfolgt)“)* und diese gegen die Informationssicherheit geprüft wurden *(Control 5.3.1; Anforderungen (sollte); Zweiter Unterpunkt: „+ Lastenhefte werden gegen die Anforderungen an die Informationssicherheit geprüft“)*. Er prüft auch, ob und welche Daten für Testzwecke verwendet wurden und ob im Falle der Verwendung von Produktivdaten ausreichend Sicherheitsmechanismen implementiert wurden *(Control 5.3.1; Anforderungen (sollte); Vierter Unterpunkt: „+ Es wird so weit wie möglich vermieden, produktive Daten für Testzwecke zu verwenden (falls anwendbar, Anonymisierung oder Pseudonymisierung): – Wenn produktive Daten für Testzwecke genutzt werden, muss sichergestellt werden, dass im Testsystem vergleichbare Schutzmaßnahmen wie im Produktivsystem vorhanden sind – Anforderungen an den Lebenszyklus von Testdaten (z. B. Löschung, höchste Lebensdauer im IT-System) – Es werden fallbezogene Vorgaben für die Erstellung von Testdaten definiert“)*. Außerdem beinhaltet die Prüfung die Kontrolle von Nachweisen, dass Prüfungen der IT-Systeme vor deren produktivem Einsatz durchgeführt wurden *(Control 5.3.1; Anforderungen (sollte); Dritter Unterpunkt: „+ Eine Prüfung des IT-Systems auf Einhaltung der Vorgaben vor dem produktiven Einsatz wird durchgeführt“)* und dass Systemabnahmetests unter Berücksichtigung der Anforderungen an die Informationssicherheit durchgeführt werden *(Control 5.3.1; Anforderungen (muss); Vierter Unterpunkt: „+ Systemabnahmetests werden unter Berücksichtigung der Anforderungen an die Informationssicherheit durchgeführt“)*.

5.3.2: „Inwieweit sind Anforderungen an Netzwerkdienste definiert?“

In Bezug auf Netzwerkdienste prüft der Auditor, dass die Anforderungen an die Informationssicherheit ermittelt und erfüllt sind *(Control 5.3.2; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen an die Informationssicherheit von Netzwerkdiensten sind ermittelt und erfüllt“)* und dass diese in Form von SLAs vereinbart sind *(Control 5.3.2; Anforderungen (sollte); Zweiter Unterpunkt: „+ Die Anforderungen werden in Form von SLAs vereinbart“)*. Der Prüfer stellt auch fest, ob ein Verfahren zur Absicherung und Nutzung *(Control 5.3.2; Anforderungen (sollte);Erster Unterpunkt: „+ Ein Verfahren für die Absicherung und Nutzung von Netzwerkdiensten ist definiert und umgesetzt“)* und, für den Fall dass die Verfügbarkeit wesentlich ist, zur Überwachung der Qualität definiert und umgesetzt ist *(Control 5.3.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster*

Unterpunkt: „+ Verfahren zur Überwachung der Qualität des Netzwerkverkehrs (z. B. Verkehrsflussanalysen, Verfügbarkeitsmessungen) sind definiert und werden durchgeführt.(A)).

5.3.3 „Inwieweit ist die Rückgabe und das sichere Entfernen von Informationswerten aus organisationsfremden IT-Diensten geregelt?“

Weiter wird vom Auditor innerhalb des Assessments geprüft, dass Informationswerte, die in organisationsfremden Diensten liegen, sicher rückgeführt und entfernt werden *(Control 5.3.3; Anforderungen (muss); Erster Unterpunkt: „+ Ein Verfahren zur Rückgabe und sicheren Entfernung von Informationswerten aus jedem organisationsfremden IT-Dienst ist definiert und umgesetzt“)* und kontrolliert die vertragliche Grundlage und den Terminierungsprozess hierzu *(Control 5.3.3; Anforderungen (sollte); Erster Unterpunkt: „+ Eine Beschreibung des Terminierungsprozesses liegt vor, wird bei Änderungen angepasst und ist vertraglich geregelt“).*

5.3.4: „Inwieweit sind Informationen in gemeinsam genutzten organisationsfremden IT-Diensten geschützt?“

Der Auditor prüft außerdem, das bei gemeinsam genutzten IT-Diensten eine wirksame Trennung der Informationen ein unbefugter Zugriff verhindert wird *(Control 5.3.4; Anforderungen (muss); Erster Unterpunkt: „+ Eine wirksame Trennung (z. B. Mandantentrennung) verhindert, dass von unbefugten Nutzern anderer Organisationen auf die eigenen Informationen zugegriffen wird“)* und dass das Abgrenzungskonzept des Anbieters dokumentiert ist und einer Anpassung im Bedarfsfall unterliegt *(Control 5.3.4; Anforderungen (sollte); Erster Unterpunkt: „+ Das Abgrenzungskonzept des Anbieters ist dokumentiert und wird bei Änderungen angepasst. Die folgenden Aspekte werden berücksichtigt: – Separierung von Daten, Funktionen, kundenspezifischer Software, Betriebssystem, Speichersystem und Netzwerk, – Risikobewertung für den Betrieb von Fremdsoftware innerhalb der gemeinsam genutzten Umgebung“)*.

4.7.4 Resümee

Die Anforderungen der NIS-2 Artikel 21 (2) Unterpunkt e), Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen, sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments durch den Auditor auf Vorhandensein und Umsetzung geprüft. Innerhalb der Prüfung wird der Komplette Nutzungszyklus von Netz- und Informationssystemen abgebildet und auf Vorhandensein von Prozessen und Kontrollmechanismen zur Sicherstellung der Informationssicherheit in jedem Stadium der Nutzung kontrolliert. Die Prüfung geht mit der Betrachtung der Rückgabe und dem sicheren Entfernen von Informationswerten aus organisationsfremden IT-Diensten über die Anforderungen der NIS-2 hinaus.

4.8 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 21 (2) f)

4.8.1 Anforderung aus der NIS-2

NIS-2 Artikel 21 (2) Unterpunkt f) fordert Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit

4.8.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls die Erfüllung der Forderung nach NIS-2 Artikel 21 (2) f) geprüft:

- 1.2.1: „Inwieweit wird in der Organisation Informationssicherheit gemanagt?“,

- 1.4.1: „Inwieweit werden Informationssicherheitsrisiken gemanagt?“,
- 1.5.1: „Inwieweit wird die Einhaltung der Informationssicherheit in Verfahren und Prozessen sichergestellt?“,
- 1.5.2: „Inwieweit wird das ISMS von einer unabhängigen Stelle überprüft?“,
- 1.6.2: „Inwieweit werden gemeldete Sicherheitsereignisse verwaltet?“ und
- 5.2.6: „Inwieweit werden IT-Systeme und -Dienste technisch überprüft (System- und Dienst-Audit)?“

4.8.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.2.1 „Inwieweit wird in der Organisation Informationssicherheit gemanagt?“

Im TISAX-Assessment nach dem aktuellen Standard ISA6 prüft der Auditor, dass Kommunikationskanäle zwischen der Unternehmensleitung und den Ausführenden des ISMS implementiert wurden *(Control 1.2.1; Anforderungen (muss); vierter Unterpunkt: + Das ISMS stellt der Organisationsleitung geeignete Kontroll- und Steuerungsmittel zur Verfügung (z. B. Management-Review))*, um sicherzustellen, dass die Kontroll- und Steuerungsmittel auch regelmäßig genutzt werden, um die Funktionalität des ISMS aufrecht zu erhalten *(Control 1.2.1; Anforderungen (muss); sechster Unterpunkt: Die Wirksamkeit des ISMS wird regelmäßig durch das Management überprüft)*.

1.4.1 „Inwieweit werden Informationssicherheitsrisiken gemanagt?“

Der Auditor prüft das Vorhandensein einer Risikobewertung *(Control 1.4.1; Anforderungen (muss); Dritter Unterpunkt: + Informationssicherheitsrisiken sind dokumentiert)*, die einen aktuellen Stand aufweist und regelmäßig oder als Reaktion auf Vorfälle zu aktualisieren ist *(Control 1.4.1; Anforderungen (muss); Erster Unterpunkt: + Risikobewertungen werden sowohl in regelmäßigen Abständen als auch als Reaktion auf Ereignisse durchgeführt)*.

1.5.1 „Inwieweit wird die Einhaltung der Informationssicherheit in Verfahren und Prozessen sichergestellt?“

Im Weiteren prüft der Auditor, dass die Prüfungen der Einhaltung der Informationssicherheit in Verfahren und Prozessen in regelmäßigen Abständen erfolgen *(Control 1.5.1; Anforderungen (muss); Zweiter Unterpunkt: + Prüfungen von Richtlinien und Verfahren der Informationssicherheit werden regelmäßig durchgeführt)*

1.5.2 „Inwieweit wird das ISMS von einer unabhängigen Stelle überprüft?“

Der Auditor prüft ebenfalls, dass eine Prüfung durch eine unabhängige Stelle durchgeführt wird, die in regelmäßigen Abständen und bei wesentlichen Änderungen stattfindet *(Control 1.5.2; Anforderungen (muss); Erster Unterpunkt: + Prüfungen der Informationssicherheit werden von einer unabhängigen und sachkundigen Stelle in regelmäßigen Abständen und bei wesentlichen Änderungen durchgeführt).*

1.6.2: „Inwieweit werden gemeldete Sicherheitsereignisse verwaltet?“

Die Prüfung des Umgangs mit Meldungen beinhaltet die Abarbeitung gemeldeter Ereignisse unter Ausschluss unnötiger Verzögerungen *(Control 1.6.2; Anforderungen (muss); Erster Unterpunkt: „+ Gemeldete Ereignisse werden ohne unnötige Verzögerung bearbeitet“)*, unter Verwendung einer angemessenen Reaktion *(Control 1.6.2; Anforderungen (muss); Zweiter Unterpunkt: „+ Eine angemessene Reaktion auf gemeldete Sicherheitsereignisse ist sichergestellt“)* und unter Verwendung der Erkenntnisse zur ständigen Verbesserung *(Control 1.6.2; Anforderungen (muss); Dritter Unterpunkt: + Diesbezüglich gewonnene Erfahrungen werden in die ständige Verbesserung einbezogen“)*.

5.2.6: „Inwieweit werden IT-Systeme und -Dienste technisch überprüft (System- und Dienst-Audit)?“

Zur Verifizierung der technischen Überprüfung von IT-Systemen und -Diensten prüft der Auditor, dass die Anforderungen an die Auditierung dieser Systeme und Dienste definiert sind *(Control 5.2.6; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen an die Auditierung von IT-Systemen oder -Diensten sind ermittelt“)* und dass die Audits regelmäßig durchgeführt werden *(Control 5.2.6; Anforderungen (sollte); Zweiter Unterpunkt: „+*

Regelmäßige System- oder Dienst-Audits werden durchgeführt – von Fachpersonal durchgeführt – geeignete Werkzeuge (z. B. Schwachstellen-Scanner) werden für System- und Dienst-Audits verwendet (sofern anwendbar) – vom Internet und dem internen Netzwerk durchgeführt“). Bei Unternehmen, bei denen die Verfügbarkeit wesentlich ist, prüft der Auditor außerdem bei kritischen IT-Systeme oder -Diensten, dass zusätzliche Anforderungen an das Audit identifiziert und berücksichtigt wurden *(Control 5.2.6; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Für kritische IT-Systeme oder -Dienste wurden zusätzliche Anforderungen an das System- oder Dienst-Audit identifiziert, die erfüllt werden (z. B. dienstspezifische Tests und Werkzeuge und/oder Penetrationstests, risikobasierte Zeitintervalle) (A)“.*

Die Prüfung beinhaltet auch die Kontrolle eines Nachweises zur Durchführung von Audits *(Control 5.2.6; Anforderungen (sollte); Dritter Unterpunkt: „+ Innerhalb eines angemessenen Zeitraums nach Abschluss des Audits wird ein Bericht erstellt)* sowie die Speicherung und die Weitermeldung der Ergebnisse an das Management *(Control 5.2.6; Anforderungen (muss); Vierter Unterpunkt: „+ Die Ergebnisse von System- oder Dienst-Audits werden rückverfolgbar gespeichert und an das zuständige Management berichtet“)* und das auf dem Bericht basierende Ableiten entsprechender Maßnahmen *(Control 5.2.6; Anforderungen (muss); Fünfter Unterpunkt: „+ Von den Ergebnissen werden Maßnahmen abgeleitet“)*.

4.8.4 Resümee

Die Anforderungen der NIS-2 Artikel 21 (1) f), Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit, sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments durch den Auditor auf Vorhandensein und Umsetzung geprüft.

Unter Berücksichtigung der Verpflichtung für die Betreiber kritischer Infrastrukturen im Sinne des IT-Sicherheitsgesetzes gemäß BSI-Gesetz (BSIG) und BSI-Kritisverordnung, alle zwei Jahre einen Nachweis zur Erfüllung der Anforderungen vorzulegen und des risikobasierten Ansatzes der NIS-2-Richtlinie, wird ein Dreijahreszyklus als angemessen angesehen.

4.9 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 21 (2) g)

4.9.1 Anforderung aus der NIS-2

NIS-2 Artikel 21 (2) Unterpunkt g) fordert grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit

4.9.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls die Erfüllung Forderung nach NIS-2 Artikel 21 (2) g) geprüft:

- 1.1.1: „Inwieweit sind Richtlinien zur Informationssicherheit vorhanden?“,
- 2.1.2: „Inwieweit werden alle Mitarbeiter vertraglich zur Einhaltung der Informationssicherheitsrichtlinien verpflichtet?“,
- 2.1.3: „Inwieweit werden Mitarbeiter hinsichtlich der Risiken beim Umgang mit Informationen geschult und sensibilisiert?“,

- 4.1.3: „Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewendet?“,
- 4.2.1: „Inwieweit werden Zugriffsrechte vergeben und verwaltet?“,
- 5.1.1: „Inwieweit wird die Nutzung kryptografischer Verfahren verwaltet?“,
- 5.1.2: „Inwieweit werden Informationen während der Übertragung geschützt?“,
- 5.2.1: „Inwieweit werden Änderungen verwaltet?“,
- 5.2.2: „Inwieweit sind Entwicklungs- und Testumgebungen von Produktivumgebungen getrennt?“,
- 5.2.3: „Inwieweit werden IT-Systeme vor Schadsoftware geschützt?“,
- 5.2.4: „Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert?“,
- 5.2.5: „Inwieweit werden Schwachstellen erkannt und behandelt?“,
- 5.2.6: „Inwieweit werden IT-Systeme und -Dienste technisch überprüft (System- und Dienst-Audit)?“,
- 5.2.7: „Inwieweit wird das Netzwerk der Organisation verwaltet?“,
- 5.2.8: „Inwieweit ist eine Kontinuitätsplanung für IT-Dienste vorhanden?“,
- 5.2.9: „Inwieweit wird die Sicherung und Wiederherstellung von Daten und IT-Diensten sichergestellt?“,
- 5.3.1: „Inwieweit wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt?“,
- 5.3.2: „Inwieweit sind Anforderungen an Netzwerkdienste definiert?“,
- 5.3.3: „Inwieweit ist die Rückgabe und das sichere Entfernen von Informationswerten aus organisationsfremden IT-Diensten geregelt?“ und
- 5.3.4: „Inwieweit sind Informationen in gemeinsam genutzten organisationsfremden IT-Diensten geschützt?“

4.9.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.1.1 „Inwieweit sind Richtlinien zur Informationssicherheit vorhanden??“

Im TISAX-Assessment nach dem aktuellen Standard ISA6 prüft der Auditor, dass die Anforderungen an die Informationssicherheit festgelegt und in einer Richtlinie dokumentiert ist *(Control 1.1.1; Anforderungen (muss); Erster Unterpunkt: „+ Die Anforderungen an die Informationssicherheit wurden festgelegt und dokumentiert: – Die Anforderungen sind an die Ziele der Organisation angepasst, – Eine Richtlinie ist erstellt und von der Organisation freigegeben“)* und dass diese Informationssicherheitsrichtlinie den Mitarbeitern zugänglich gemacht wird *(Control 1.1.1; Anforderungen (sollte); Fünfter Unterpunkt: „+ Die Richtlinien werden Mitarbeitern in geeigneter Form (z. B. Intranet) zur Verfügung gestellt (in angemessenem Umfang)“)* und über relevante Änderungen informiert wird. *(Control 1.1.1; Anforderungen (sollte); Sechster Unterpunkt: „+ Mitarbeiter und externe Geschäftspartner werden über alle für sie relevanten Änderungen informiert“).*

2.1.2: „Inwieweit werden alle Mitarbeiter vertraglich zur Einhaltung der Informationssicherheitsrichtlinien verpflichtet?“

Der Auditor prüft auch, ob die Mitarbeiter zur Einhaltung der Richtlinien zur Informationssicherheit *(Control 2.1.2; Anforderungen (muss); Zweiter Unterpunkt: „+ Es besteht eine Verpflichtung zur Einhaltung der Richtlinien zur Informationssicherheit“)* und zur Geheimhaltung *(Control 2.1.2; Anforderungen (muss); Erster Unterpunkt: „+ Es besteht eine Verpflichtung zur Geheimhaltung“)* über die Dauer des Arbeitsverhältnisses bzw. des Auftrags und darüber hinaus *(Control 2.1.2; Anforderungen (sollte); Erster Unterpunkt: „+ Es besteht eine Verpflichtung zur Geheimhaltung über das Arbeitsverhältnis bzw. den Auftrag hinaus“)* verpflichtet ist. Weiter prüft der Auditor, dass Informationssicherheit in Arbeitsverträgen Berücksichtigung findet *(Control 2.1.2; Anforderungen (sollte);*

Zweiter Unterpunkt: „+ Informationssicherheit wird in den Arbeitsverträgen der Mitarbeiter berücksichtigt“) und eine Vorgehensweise bei Verstößen beschrieben ist *(Control 2.1.2; Anforderungen (sollte); Dritter Unterpunkt: „+ Eine Vorgehensweise bei Verstößen gegen die vorstehenden Verpflichtungen ist beschrieben“).*

2.1.3: „Inwieweit werden Mitarbeiter hinsichtlich der Risiken beim Umgang mit Informationen geschult und sensibilisiert?“

Der Auditor prüft, ob die Mitarbeiter des Unternehmens ganzheitlich hinsichtlich der Risiken beim Umgang mit Informationen geschult und sensibilisiert werden *(Control 2.1.3; Anforderungen (muss); erster Unterpunkt: + Mitarbeiter sind geschult und sensibilisiert).* Weiter wird geprüft, dass ein Schulungskonzept vorliegt, das für die Informationssicherheit relevante Bereiche abdeckt *(Control 2.1.3; Anforderungen (sollte); erster Unterpunkt: + Ein Konzept zur Sensibilisierung und Schulung der Mitarbeiter ist erstellt. Dabei werden mindestens die folgenden Aspekte berücksichtigt: Richtlinie zur Informationssicherheit, Meldungen von Informationssicherheitsereignissen, Verhalten bei Auftreten von Schadsoftware, Richtlinien zu Benutzerkonten und Anmeldeinformationen (z. B. Passwort-Richtlinie), Compliance-Themen der Informationssicherheit, Anforderungen und Verfahren zum Einsatz von Geheimhaltungsvereinbarungen bei der gemeinsamen Nutzung schutzbedürftiger Informationen, Nutzung organisationsfremder IT-Dienste)*, in dem die Zielgruppen für Schulungskonzepte Berücksichtigung finden und *dass* die Schulungsmaßnahmen entsprechend der Kritikalität der verarbeiteten Information angemessen sind *(Control 2.1.3; Anforderungen (sollte); zweiter Unterpunkt: Zielgruppen für Schulungs- und Sensibilisierungsmaßnahmen (d. h. Personen, die in bestimmten risikobehafteten Umgebungen arbeiten, wie Administratoren, Mitarbeiter mit Zugang zu Kundennetzwerken, Personal in Fertigungsbereichen) sind ermittelt und in einem Schulungskonzept berücksichtigt) und dass das Schulungskonzept durch das Management freigegeben ist (Control 2.1.3; Anforderungen (sollte); Dritter Unterpunkt: + Das Konzept wurde vom verantwortlichen Management freigegeben)*. Der Auditor wird ebenfalls prüfen, ob die Schulungs- und Sensibilisierungsmaßnahmen in regelmäßigen Abständen und anlassbezogen durchgeführt werden *(Control 2.1.3; Anforderungen (sollte); vierter Unterpunkt: + Schulungs- und Sensibilisierungsmaßnahmen werden sowohl in regelmäßigen Abständen als auch als Reaktion auf Ereignisse durchgeführt)* und eine entsprechende Dokumentation vorliegt *(Control 2.1.3; Anforderungen (sollte); fünfter Unterpunkt: + Die Teilnahme an Schulungs- und Sensibilisierungsmaßnahmen wird dokumentiert)*. Zur Kontrolle der wirksamen Überprüfung prüft der Auditor, dass die Ansprechpartner für Informationssicherheit den Mitarbeitern bekannt sind *(Control 2.1.3; Anforderungen (sollte); sechster Unterpunkt: + Mitarbeitern sind die Ansprechpartner für Informationssicherheit bekannt)*.

4.1.3. „Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewendet?“

Weiterer Teil des Assessments ist die Prüfung, dass der Zugang zu Informationen und IT-Systemen über validierte Benutzerkonten erfolgt und dass Anmeldeinformationen geschützt werden und die Rückverfolgbarkeit von Transaktionen und Zugriffen sichergestellt wird. Hierzu prüft der Auditor, dass Benutzerkonten über ihren Lebenszyklus verwaltet werden *(Control 4.1.3; Anforderungen (muss); Erster Unterpunkt: „+ Die Erstellung, Änderung und Löschung von Benutzerkonten wird durchgeführt“), (Control 4.1.3; Anforderungen (muss); Vierter Unterpunkt: „+ Benutzerkonten werden unmittelbar nachdem der Benutzer aus der Organisation ausgeschieden ist oder diese verlassen hat (z. B. bei Beendigung des Arbeitsverhältnisses) gesperrt“)* und dass eine regelmäßige Überprüfung auf Aktualität der Zuteilung stattfindet *(Control 4.1.3; Anforderungen (muss); Fünfter Unterpunkt: „+ Benutzerkonten werden in regelmäßigen Abständen überprüft“)*. Weiter prüft der Auditor, dass die Konten personalisiert werden *(Control 4.1.3; Anforderungen (muss); Zweiter Unterpunkt: „+ Es werden eindeutige und personalisierte Benutzerkonten verwendet“)* oder im Bedarfsfall die Vergabe von Sammelkonten einer Regelung unterliegt *(Control 4.1.3; Anforderungen (muss); Dritter Unterpunkt: „+ Die Nutzung von „Sammel-Konten“ ist geregelt (z. B. auf Fälle beschränkt, bei denen die Rückverfolgbarkeit von Aktionen verzichtbar ist)“)*. Die sichere Übermittlung der Konteninformationen *(Control 4.1.3; Anforderungen (muss); Sechster Unterpunkt: „+ Es erfolgt eine sichere Zustellung der Anmeldeinformationen an den Benutzer“),* die Sicherstellung der Geheimhaltung der Anmeldeinformation *(Control 4.1.3; Anforderungen (muss); Achter Unterpunkt: „+ Die Anmeldeinformationen (z. B. Passwörter) eines personalisierten Benutzerkontos dürfen nur dem zugeordneten Benutzer bekannt sein“)* und die zugehörigen Verhaltensweisen *(Control 4.1.3; Anforderungen (muss); Siebter Unterpunkt: „+ Eine*

Richtlinie zum Umgang mit Anmeldeinformationen ist definiert und umgesetzt. Die folgenden Aspekte werden berücksichtigt: – 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)“) werden vom Auditor ebenfalls geprüft.

In Bezug auf Benutzerprofile prüft der Auditor, dass ein Standardprofil besteht *(Control 4.1.3; Anforderungen (sollte); Erster Unterpunkt: „+ Ein Basis-Benutzerprofil mit minimalen Zugriffsrechten und Funktionalitäten ist vorhanden und wird angewendet“)*. Außerdem prüft er, dass Herstellerseitige Standardkonten deaktiviert werden *(Control 4.1.3; Anforderungen (sollte); Zweiter Unterpunkt: „+ Herstellerseitig vorgegebene Standardkonten und -Passwörter werden deaktiviert (z. B. durch Sperrung oder Änderung des Passworts)“)*, dass es einen definierten Prozess zur Erstellung von Konten gibt *(Control 4.1.3; Anforderungen (sollte); Vierter Unterpunkt: „+ Die Einrichtung von Benutzerkonten unterliegt einem Genehmigungsprozess (4-Augen-Grundsatz)“)* und dass die Einrichtung von Konten durch eine autorisierte Stelle erfolgt *(Control 4.1.3; Anforderungen (sollte); Dritter Unterpunkt: „+ Die Einrichtung von Benutzerkonten erfolgt durch die verantwortliche Stelle oder wird durch diese autorisiert“)*. Er prüft weiterhin, dass Sperr- und Löschfristen definiert *(Control 4.1.3; Anforderungen (sollte); Sechster Unterpunkt: „+ Sperr- und Löschfristen für Benutzerkonten sind definiert“)* und auch bei Dienstleisterkonten umgesetzt werden *(Control 4.1.3; Anforderungen (sollte); Fünfter Unterpunkt: „+ Benutzerkonten von Dienstleistern werden nach Abschluss von deren Aufgabe gesperrt“)*. Der Auditor prüft auch, dass die Verwendung von Standard-Passwörtern verhindert wird *(Control 4.1.3; Anforderungen (sollte); Siebter Unterpunkt: „+ Die Verwendung von Standard-Passworten wird technisch verhindert“)*, dass die interaktive Anmeldung bei Dienste-Konten technisch verhindert wird, *(Control 4.1.3; Anforderungen (sollte); Zehnter Unterpunkt: „+ Die interaktive Anmeldung bei Dienstkonten (technischen Konten) wird technisch verhindert“),* dass beim Einsatz starker Authentifizierung das Medium sicher verwendet wird *(Control 4.1.3; Anforderungen (sollte); Achter Unterpunkt: „+ Beim Einsatz einer starken Authentifizierung wird das Medium (z. B. Faktor Besitz) sicher verwendet“)* und schließlich, dass eine regelmäßige Überprüfung der Konten stattfindet *(Control 4.1.3; Anforderungen (sollte); Neunter Unterpunkt: „+ Es findet eine Überprüfung der Benutzerkonten in regelmäßigen Abständen statt. Dazu gehören auch Benutzerkonten in IT-Systemen von Kunden“)*.

4.2.1. „Inwieweit werden Zugriffsrechte vergeben und verwaltet?“

Zur Sicherstellung, dass nur berechtigte (autorisierte) Benutzer Zugriff auf Informationen und IT-Dienstleistungen haben, prüft der Auditor, dass die Anforderungen an das Management von Zugriffsrechten ermittelt und erfüllt wurden *(Control 4.2.1; Anforderungen (muss); Erster Unterpunkt: „+ Die Anforderungen an das Management von Zugriffsrechten (Autorisierung) sind ermittelt und erfüllt. Die folgenden Aspekte werden berücksichtigt: – Verfahren zur Beantragung, Verifizierung und Genehmigung, – Anwendung des Minimal- („Need-to-know"-/“Least-Privilege“) -Prinzips. – Zugriffsrechte werden widerrufen, wenn sie nicht mehr benötigt werden“)*, dass Berechtigungskonzepte erstellt wurden *(Control 4.2.1; Anforderungen (sollte); Erster Unterpunkt: „+ Berechtigungskonzepte für den Zugriff auf Informationen sind erstellt“)*, Berechtigungs-Rollen Verwendung finden *(Control 4.2.1; Anforderungen (sollte); Zweiter Unterpunkt: „+ Berechtigungs-Rollen werden verwendet“)*, dass normalen Nutzern keine privilegierten Zugriffsrechte zugeteilt werden *(Control 4.2.1; Anforderungen (sollte); Vierter Unterpunkt: „+ Normalen Benutzerkonten werden keine privilegierten Zugriffsrechte erteilt“)* und die Zugriffsrechte durch den Informationsverantwortlichen freigegeben wurden *(Control 4.2.1; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Die Zugriffsrechte sind durch den internen Informationsverantwortlichen freigegeben. (C, I, A)“)*. Er prüft weiter, dass die Vergabe von Berechtigungen bedarfsorientiert vorgenommen wird, *(Control 4.2.1; Anforderungen (sollte); Dritter Unterpunkt: „+ Die Vergabe von Rechten erfolgt bedarfsorientiert und entsprechend der Rolle und/oder dem Verantwortungsbereich“)*, die Rechte regelmäßig kontrolliert werden *(Control 4.2.1; Anforderungen (muss); Zweiter Unterpunkt: „+ Die erteilten Zugriffsrechte für*

normale und privilegierte Benutzerkonten sowie technische Konten werden in regelmäßigen Abständen auch in IT-Systemen von Kunden überprüft“) und dass auch bei Wechseln in z.B. andere Verantwortungsbereiche eine Aktualisierung vorgenommen wird *(Control 4.2.1; Anforderungen (sollte); Fünfter Unterpunkt: „+ Die Zugriffsrechte eines Benutzerkontos eines Anwenders werden nach dessen Wechsel (z. B. in einen anderen Verantwortungsbereich) angepasst“).*

5.1.1. „Inwieweit wird die Nutzung kryptografischer Verfahren verwaltet?“

Zum Einsatz von kryptografischen Verfahren prüft der Auditor, dass diese der anerkannten Industrienorm entsprechen und die das Unternehmen betreffenden Gesetze und Regelungen berücksichtigen *(Control 5.1.1; Anforderungen (muss); Erster Unterpunkt: „+ Alle angewendeten kryptografischen Verfahren (z. B. Verschlüsselung, Signatur und Hash-Algorithmen, Protokolle) bieten die für das jeweilige Anwendungsgebiet notwendige Sicherheit entsprechend der anerkannten Industrienorm – soweit wie rechtlich möglich“)*. Er prüft, dass ein technisches Regelwerk erstellt *(Control 5.1.1; Anforderungen (sollte); Erster Unterpunkt: „+ Erstellung eines technischen Regelwerkes mit Anforderungen an die Verschlüsselung zum Schutz von Informationen entsprechend ihrer Klassifizierung“)* und ein Nutzungskonzept definiert ist *(Control 5.1.1; Anforderungen (sollte); Zweiter Unterpunkt: „„+ Ein Nutzungskonzept für Kryptografie ist definiert und umgesetzt. Die folgenden Aspekte werden berücksichtigt: - Kryptografische Verfahren - Schlüsselstärken - Verfahren für den vollständigen Lebenszyklus von kryptografischen Schlüsseln einschließlich Erzeugung, Speicherung, Archivierung, Abruf, Verteilung, Deaktivierung, Erneuerung und Löschung)*. Außerdem ist Teil des Assessments zu prüfen, dass die Anforderungen an die Schlüsselhoheit ermittelt und erfüllt sind *(Control 5.1.1; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Ein Nutzungskonzept für Kryptografie ist definiert und umgesetzt. Die folgenden Aspekte werden berücksichtigt: - Kryptografische Verfahren - Schlüsselstärken - Verfahren für den vollständigen Lebenszyklus von kryptografischen Schlüsseln einschließlich Erzeugung, Speicherung, Archivierung, Abruf, Verteilung, Deaktivierung, Erneuerung und Löschung“)* und ein Notfallprozess zur Wiederherstellung von Schlüsseln etabliert ist *(Control 5.1.1; Anforderungen (sollte); Dritter Unterpunkt: + Ein Notfallprozess zur Wiederherstellung von Schlüsselmaterial ist etabliert“)*.

5.1.2 „Inwieweit werden Informationen während der Übertragung geschützt?“

Zur Sicherstellung des Schutzes von Informationen bei deren Übertragung prüft der Auditor, dass zur Übertragung genutzte Netzwerkdienste identifiziert und dokumentiert sind *(Control 5.1.2; Anforderungen (muss); Erster Unterpunkt: + Die zur Übertragung von Informationen genutzten Netzwerkdienste sind identifiziert und dokumentiert“)*, dass Richtlinien und Verfahren zur Nutzung von Netzwerkdiensten definiert und umgesetzt sind *(Control 5.1.2; Anforderungen (muss); Zweiter Unterpunkt: „+ Richtlinien und Verfahren entsprechend den Klassifizierungsvorgaben zur Nutzung von Netzwerkdiensten sind definiert und umgesetzt“)* und dass Maßnahmen zum Schutz übertragener Inhalte umgesetzt sind *(Control 5.1.2; Anforderungen (muss); Dritter Unterpunkt: + Maßnahmen zum Schutz von übertragenen Inhalten vor unberechtigtem Zugriff sind umgesetzt“)*. Außerdem ist bei Organisationen, für die die Vertraulichkeit wesentlich ist, teil der Prüfung, dass Informationen in verschlüsselter Form transportiert oder übertragen werden *(Control 5.1.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: + Informationen werden in verschlüsselter Form transportiert oder übertragen: - Wenn eine Verschlüsselung nicht möglich ist, müssen Informationen durch ähnlich wirksame Maßnahmen geschützt werden“(C) (Control 5.1.2; Anforderungen (sollte); Zweiter Unterpunkt: „+ Der elektronische Datenaustausch erfolgt entsprechend der jeweiligen Klassifizierung durch Inhalts- oder Transportverschlüsselung“)* und dass sichergestellt ist, dass die verwendeten Adressen korrekt sind *(Control 5.1.2; Anforderungen (sollte); Erster Unterpunkt: „+ Maßnahmen zur Sicherstellung der korrekten Adressen und des korrekten Transports von Informationen sind umgesetzt“)*. Weiter wird vom Auditor geprüft, dass Fernzugriffsverbindungen über angemessene Sicherheitsmerkmale und -fähigkeiten verfügen *(Control 5.1.2; Anforderungen (sollte); Dritter Unterpunkt: „+ Fernzugriffsverbindungen werden dahingehend verifiziert, dass sie über angemessene Sicherheitsmerkmale (z. B. Verschlüsselung, Gewähren und Beenden des Zugriffs) und -fähigkeiten verfügen“).*

5.2.1: „Inwieweit werden Änderungen verwaltet?“

In Bezug auf Änderungen prüft der Auditor, dass die Anforderungen an die Informationssicherheit ermittelt und umgesetzt werden *(Control 5.2.1; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen an die Informationssicherheit bei Änderungen von Organisation, Geschäftsprozessen, IT-Systemen werden ermittelt und umgesetzt“ und* eine Bewertung in Bezug auf die Auswirkung in Richtung der Informationssicherheit stattfindet *(Control 5.2.1; Anforderungen (sollte); Zweiter Unterpunkt: „+ Änderungen werden bezüglich möglicher Auswirkungen auf die Informationssicherheit verifiziert und bewertet“)*. Weiter wird vom Auditor geprüft, dass bei Änderungen mit Auswirkung auf die Informationssicherheit, ein formales Genehmigungsverfahren etabliert ist *(Control 5.2.1; Anforderungen (sollte); Erster Unterpunkt: „+ Ein formales Genehmigungsverfahren ist etabliert“),* und diese geplant und geprüft werden *(Control 5.2.1; Anforderungen (sollte); Dritter Unterpunkt: „+ Änderungen mit Auswirkung auf die Informationssicherheit werden geplant und geprüft“),* dass die Änderungen während und nach der Umsetzung verifiziert werden *(Control 5.2.1; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Die Einhaltung der Anforderungen an die Informationssicherheit wird während und nach der Umsetzung der Änderungen verifiziert. (C, I, A)“)* und das Notfallverfahren im Falle von Fehlern berücksichtigt werden *(Control 5.2.1; Anforderungen (sollte); Vierter Unterpunkt: „+ Notfallverfahren im Falle von Fehlern sind berücksichtigt“).*

5.2.2: „Inwieweit sind Entwicklungs- und Testumgebungen von Produktivumgebungen getrennt?“

Der Auditor prüft auf Vorhandensein einer Risikobewertung bezüglich der Notwendigkeit einer Trennung von Produktiv- und Testsystemen (muss1) *(Control 5.2.2; Anforderungen (muss); Erster Unterpunkt: + Die IT-Systeme wurden einer Risikobewertung unterzogen, um zu ermitteln, inwiefern deren Trennung in Entwicklungs-, Test- und Produktivsysteme notwendig ist“)*, die Umsetzung der Ergebnisse *(Control 5.2.2; Anforderungen (muss); Zweiter Unterpunkt: + Eine Segmentierung ist auf Basis der Ergebnisse der Risikoanalyse umgesetzt“)* und dass Anforderungen an Entwicklungs- und Testumgebungen ermittelt und umgesetzt sind *(Control 5.2.2; Anforderungen (sollte); Erster Unterpunkt: „+ Die Anforderungen an Entwicklungs- und Testumgebungen sind ermittelt und umgesetzt. Die folgenden Aspekte werden 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 für Entwicklungs-, Test- und Produktivsysteme“)*.

5.2.3: „Inwieweit werden IT-Systeme vor Schadsoftware geschützt?“

Um den Schutz von IT-Systemen vor Schadsoftware sowohl technisch als auch organisatorisch sicherzustellen prüft der Auditor, dass Technische und organisatorische Maßnahmen zum Schutz vor Schadsoftware definiert und umgesetzt sind *(Control 5.2.3; Anforderungen (muss); Zweiter Unterpunkt: „+ Technische und organisatorische Maßnahmen zum Schutz vor Schadsoftware sind definiert und umgesetzt“)* und dass die Anforderungen an den Schutz vor Schadsoftware ermittelt sind *(Control 5.2.3; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen an den Schutz vor Schadsoftware sind ermittelt“)*. Außerdem gehört zur Prüfung, dass nicht benötigte Netzwerkdienste deaktiviert sind *(Control 5.2.3; Anforderungen (sollte); Erster Unterpunkt: „+ Nicht benötigte Netzwerkdienste sind deaktiviert“)*, der Zugriff auf die benötigten Zugriffe eingeschränkt ist *(Control 5.2.3; Anforderungen (sollte); Zweiter Unterpunkt: „+ Zugriff auf Netzwerkdienste ist mit geeigneten Schutzmaßnahmen (siehe Beispiele) auf die benötigten Zugriffe eingeschränkt“)*, eine Software zum Schutz vor Schadsoftware installiert ist und regelmäßig aktualisiert wird *(Control 5.2.3; Anforderungen (sollte); Dritter Unterpunkt: „+ Eine Software zum Schutz vor Schadsoftware ist installiert und wird in regelmäßigen Abständen automatisch aktualisiert (z. B. Virenscanner)“)* und dass Empfangene Dateien und empfangene Software automatisch auf Schadsoftware überprüft werden *(Control 5.2.3; Anforderungen (sollte); Vierter Unterpunkt: „+ Empfangene Dateien und empfangene Software werden vor ihrer Ausführung automatisch auf Schadsoftware überprüft (On-Access-Scan)“)*. Weiter prüft der Auditor, dass regelmäßig auf Schadsoftware überprüft wird *(Control 5.2.3; Anforderungen (sollte); Fünfter Unterpunkt: „+ Der gesamte Datenbestand aller Systeme wird regelmäßig auf Schadsoftware überprüft“)*, dass von zentralen Gateways übertragene Daten automatisch überprüft werden *(Control 5.2.3; Anforderungen (sollte); Sechster Unterpunkt: „+ Von zentralen Gateways übertragene Daten (z. B. E-Mail,*

Internet, Netze von Dritten) werden automatisch mittels einer Schutzsoftware überprüft: – Verschlüsselte Verbindungen werden berücksichtigt“) und dass Verschlüsselte Verbindungen Berücksichtigung finden.

Im Hinblick auf den User prüft der Auditor, dass verhindert ist, dass Schutzsoftware durch Benutzer deaktiviert oder verändert wird *(Control 5.2.3; Anforderungen (sollte); Siebter Unterpunkt: „+ Maßnahmen zur Verhinderung, dass Schutzsoftware durch Benutzer deaktiviert oder verändert wird, sind definiert und umgesetzt“)* und das fallbezogene Sensibilisierungsmaßnahmen stattfinden *(Control 5.2.3; Anforderungen (sollte); Achter Unterpunkt: „+ Fallbezogene Sensibilisierungsmaßnahmen der Mitarbeiter“)*. Für IT-Systeme, die ohne Software zum Schutz vor Schadsoftware betrieben werden, prüft der Auditor, dass alternative Maßnahmen umgesetzt sind (*Control 5.2.3; Anforderungen (sollte); Neunter Unterpunkt: „+ Für IT-Systeme, die ohne Software zum Schutz vor Schadsoftware betrieben werden, sind alternative Maßnahmen (z. B. spezielle Resilienz-Maßnahmen, wenig Dienste, keine aktiven User, Netzisolierung) umgesetzt“).*

5.2.4: „Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert?“

Um die Rückverfolgbarkeit von Ereignissen im Falle eines Sicherheitsvorfalls sicherzustellen, prüft der Auditor, dass eine Ereignisprotokollierung stattfindet und das diese in ihrer Handhabung die Anforderungen der Informationssicherheit berücksichtigt *(Control 5.2.4; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen an die Informationssicherheit bezüglich der Handhabung von Ereignisprotokollen sind ermittelt und erfüllt“)* und dabei eine angemessene Überwachung und Aufzeichnung aller informationssicherheitsrelevanten Aktionen im Netzwerk sicherstellt *(Control 5.2.4; Anforderungen (sollte); Dritter Unterpunkt: „+ Eine angemessene Überwachung und Aufzeichnung aller informationssicherheitsrelevanten Aktionen im Netzwerk sind etabliert“)*. Außerdem stellt der Auditor fest, ob Sicherheitsrelevante Anforderungen an die Protokollierung der Aktivitäten von Systemadministratoren und Nutzern ermittelt sind und erfüllt werden *(Control 5.2.4; Anforderungen (muss); Zweiter Unterpunkt: „+ Sicherheitsrelevante Anforderungen an die Protokollierung der Aktivitäten von Systemadministratoren und Nutzern sind ermittelt und erfüllt“).* Er prüft weiterhin, dass eingesetzte IT Systeme hinsichtlich der Protokollierung bewertet werden *(Control 5.2.4; Anforderungen (muss); Dritter Unterpunkt: „+ Die eingesetzten IT-Systeme werden hinsichtlich der Notwendigkeit der Protokollierung bewertet“)* und das speziell bei organisationsfremden IT Systemen die Überwachungsmöglichkeiten bekannt sind und Berücksichtigung finden *(Control 5.2.4; Anforderungen (muss); Vierter Unterpunkt: „+ Bei der Nutzung organisationsfremder IT-Dienste werden Informationen zu den Überwachungsmöglichkeiten eingeholt und im Assessment berücksichtigt“).* Außerdem prüft er, dass die eingerichteten Zugriffe beim Auf- und Abbau von organisationsfremden Netzwerkverbindungen protokolliert werden *(Control 5.2.4; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Zweiter Unterpunkt: „+ Zugriffe beim Auf- und Abbau von organisationsfremden Netzwerkverbindungen (z. B. Fernwartung) werden protokolliert. (C, I, A)“).*Der Auditor prüft ebenfalls das Vorhandensein von Nachweisen zur regelmäßigen Kontrolle von Ereignisprotokollen *(Control 5.2.4; Anforderungen (muss); Fünfter Unterpunkt: „+ Ereignisprotokolle werden regelmäßig auf Regelverstöße und Auffälligkeiten im Einklang mit den zulässigen gesetzlichen und betrieblichen Bestimmungen überprüft“)* und dass ein Eskalationsverfahren bei relevanten Ereignissen Anwendung findet *(Control 5.2.4; Anforderungen (sollte); Erster Unterpunkt: „+ Ein Verfahren zur Eskalation von relevanten Ereignissen an die zuständige Stelle (z. B. Sicherheitsvorfall-Meldung, Datenschutz, Unternehmenssicherheit, IT-Sicherheit) ist definiert und etabliert“).* Er kontrolliert weiter, dass die für die Sicherheit während der Handhabung relevanten Informationssicherheitsanforderungen definiert sind und eingehalten werden *(Control 5.2.4; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Informationssicherheitsanforderungen, die für die Sicherheit während der Handhabung von Ereignisprotokollen relevant sind, z. B. vertragliche Anforderungen, sind ermittelt und umgesetzt. (C, I, A)“)* und dass die Protokolle gegen Änderungen geschützt werden *(Control 5.2.4; Anforderungen (sollte); Zweiter Unterpunkt: „+ Ereignisprotokolle (Inhalte und Metadaten) sind gegen Änderungen geschützt. (z. B. durch eine dedizierte Umgebung)“)*.

5.2.5: „Inwieweit werden Schwachstellen erkannt und behandelt?“

In Bezug auf die Schwachstellenanalyse prüft der Auditor, dass Informationen über technische Schwachstellen gesammelt werden *(Control 5.2.5; Anforderungen (muss); Erster Unterpunkt: „+ Informationen über technische Schwachstellen zu den genutzten IT-Systemen werden gesammelt (z. B. Information vom Hersteller, System-*

Audits, CVS-Datenbank) und beurteilt (z. B. Allgemeines Bewertungssystem für Schwachstellen, en: Common Vulnerability Scoring System, CVSS)“) und die erlangten Erkenntnisse zur Behandlung solcher eingesetzt werden *(Control 5.2.5; Anforderungen (muss); Zweiter Unterpunkt: „+ Potenziell betroffene IT-Systeme und Software werden identifiziert, bewertet und Schwachstellen behandelt“)* und dass Risiken auf ein Mindestmaß reduziert werden *(Control 5.2.4; Anforderungen (sollte); Zweiter Unterpunkt: „+ Maßnahmen zur Verringerung von Risiken auf ein Mindestmaß sind, soweit notwendig, umgesetzt “)*. Der Auditor prüft außerdem, dass ein Patch-Management etabliert ist *(Control 5.2.5; Anforderungen (sollte); Erster Unterpunkt: „+ Ein angemessenes Patch-Management ist definiert und umgesetzt (z. B. Prüfung und Installation von Patches)“)* und das die erfolgreiche Installation verifiziert wird *(Control 5.2.5; Anforderungen (sollte); Dritter Unterpunkt: „+ Die erfolgreiche Installation von Patches ist in geeigneter Weise verifiziert“).*

5.2.6: „Inwieweit werden IT-Systeme und -Dienste technisch überprüft (System- und Dienst-Audit)?“

Zur Verifizierung der technischen Überprüfung von IT-Systemen und -Diensten prüft der Auditor, dass die Anforderungen an die Auditierung dieser Systeme und Dienste definiert sind *(Control 5.2.6; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen an die Auditierung von IT-Systemen oder -Diensten sind ermittelt“),* diese regelmäßig durchgeführt werden *(Control 5.2.6; Anforderungen (sollte); Zweiter Unterpunkt: „+ Regelmäßige System- oder Dienst-Audits werden durchgeführt – von Fachpersonal durchgeführt – geeignete Werkzeuge (z. B. Schwachstellen-Scanner) werden für System- und Dienst-Audits verwendet (sofern anwendbar) – vom Internet und dem internen Netzwerk durchgeführt“),* dass die Audits im Umfang festgelegt *(Control 5.2.6; Anforderungen (muss); Zweiter Unterpunkt: „+ Der Umfang des Systemaudits ist rechtzeitig festgelegt“* und im Hinblick auf die entstehenden Sicherheitsrisiken bewertet werden. *(Control 5.2.6; Anforderungen (sollte); Erster Unterpunkt: „+ System- und Dienst-Audits werden unter Berücksichtigung aller Sicherheitsrisiken geplant, die dadurch hervorrufen werden, könnten (z. B. Störungen)“).* Weiter prüft der Auditor, dass sie den Betreibern und Nutzer bekannt gemacht werden *(Control 5.2.6; Anforderungen (muss); Dritter Unterpunkt: „+ System- oder Dienst-Audits sind mit dem Betreiber und den Nutzern der IT-Systeme oder -Dienste abgestimmt“).* Für kritische IT-Systeme oder -Dienste prüft der Auditor außerdem bei Organisationen, bei denen Verfügbarkeit wesentlich ist, dass zusätzliche Anforderungen an das Audit identifiziert und berücksichtigt wurden *(Control 5.2.6; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Für kritische IT-Systeme oder -Dienste wurden zusätzliche Anforderungen an das System- oder Dienst-Audit identifiziert, die erfüllt werden (z. B. dienstspezifische Tests und Werkzeuge und/oder Penetrationstests, risikobasierte Zeitintervalle(A)).*

Die Prüfung beinhaltet auch die Kontrolle eines Nachweises zur Durchführung *(Control 5.2.6; Anforderungen (sollte); Dritter Unterpunkt: „+ Innerhalb eines angemessenen Zeitraums nach Abschluss des Audits wird ein Bericht erstellt)* sowie die Speicherung und die Weitermeldung der Ergebnisse an das Management *(Control 5.2.6; Anforderungen (muss); Vierter Unterpunkt: „+ Die Ergebnisse von System- oder Dienst-Audits werden rückverfolgbar gespeichert und an das zuständige Management berichtet“)* und das auf dem Bericht basierende Ableiten entsprechender Maßnahmen *(Control 5.2.6; Anforderungen (muss); Fünfter Unterpunkt: „+ Von den Ergebnissen werden Maßnahmen abgeleitet“).*

5.2.7: „Inwieweit wird das Netzwerk der Organisation verwaltet?“

Außerdem wird vom Auditor geprüft, ob die Anforderungen an die Steuerung und Segmentierung von Netzwerken umgesetzt ist *(Control 5.2.7; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen zur Verwaltung und Steuerung von Netzwerken sind ermittelt und erfüllt“* und ob die notwendigen Sicherheitsaspekte nach Stand der Technik umgesetzt sind *(Control 5.2.7; Anforderungen (sollte); Zweiter Unterpunkt: „+ Für eine risikobasierte Segmentierung des Netzwerks werden die folgenden Aspekte berücksichtigt: – Beschränkungen bei der Anbindung von IT-Systemen an das Netzwerk, – Anwendung von Sicherheitstechnologien, – Betrachtungen hinsichtlich Leistung, Vertrauen, Verfügbarkeit, Informationssicherheit und Funktionssicherheit – Begrenzung der Auswirkungen im Falle kompromittierter IT-Systeme – Erkennung möglicher Angriffe und der lateralen Bewegung von Angreifern – Trennung von Netzwerken mit unterschiedlichem Betriebszweck (z. B. Test- und Entwicklungsnetzwerke, Büronetzwerk, Produktionsnetzwerke) – Das erhöhte Risiko aufgrund von Netzwerkdiensten, die über das Internet zugänglich sind, – Technologiespezifische Trennungsmöglichkeit bei Nutzung externer IT-Dienste, –*

Angemessene Trennung zwischen den eigenen Netzwerken und Kundennetzwerken unter Berücksichtigung der Kundenanforderungen – Erkennung und Verhinderung von Datenverlust/Datenlecks“.

5.2.8: „Inwieweit ist eine Kontinuitätsplanung für IT-Dienste vorhanden?“

Der Auditor prüft, ob eine Kontinuitätsplanung für IT-Dienste *(Control 5.2.8; Anforderungen (muss); Erster Unterpunkt: „+ Kritische IT-Dienste werden identifiziert, und die geschäftlichen Auswirkungen werden betrachtet“)* und IT-Systeme *(Control 5.2.8; Anforderungen (sollte); Erster Unterpunkt: „Kritische IT-Systeme werden identifiziert – die maßgeblichen Systeme sind nach dem entsprechenden Schutzbedarf klassifiziert – angemessene und geeignete Sicherheitsmaßnahmen werden umgesetzt)* besteht, die auf einer Bewertung der Kritikalität der vorhandenen Dienste bzw. Systeme beruht und die den maßgeblichen Verantwortlichen bekannt ist *(Control 5.2.8; Anforderungen (muss); Zweiter Unterpunkt: „+ Anforderungen und Verantwortlichkeiten für die Kontinuität und Wiederherstellung dieser IT-Dienste sind den maßgeblichen Beteiligten bekannt und werden erfüllt“)*.

Außerdem prüft der Auditor das Vorhandensein von Spezifikationen zu unterschiedlichen Szenarien *(Control 5.2.8; Anforderungen (sollte); Zweiter Unterpunkt: „+ Die Kontinuitätsplanung schließt mindestens die folgenden Szenarien ein, welche kritische IT-Systeme betreffen: – (Distributed) Denial-of-Service-Angriffe – Erfolgreiche Ransomware-Angriffe und andere Sabotageaktivitäten – Systemausfall – Naturkatastrophe* und Backupstrategien *(Control 5.2.8; Anforderungen (sollte); Dritter Unterpunkt: „+ Bei der Kontinuitätsplanung werden die folgenden Fälle berücksichtigt: – Alternative Kommunikationsstrategien, falls primäre Kommunikationsmittel nicht verfügbar sind – Alternative Speicherungsstrategien, falls primäre Mittel zur Speicherung nicht verfügbar sind – Alternative Energieversorgung und alternatives Netzwerk*“) deren Aktualität anhand von Überprüfungsprotokollen geprüft wird *(Control 5.2.8; Anforderungen (sollte); Vierter Unterpunkt: „+ Die Kontinuitätsplanung wird regelmäßig überprüft und aktualisiert“).*

Ein weiterer Teil der Prüfung dient der Sicherstellung, dass sich Backups in einem Wiederherstellungsfähigen Zustand befinden *(Control 5.2.8; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Fünfter Unterpunkt: „+ Eine Sicherungs- und Wiederherstellungsstrategie für kritische IT-Dienste und Informationen ist definiert und umgesetzt. Die folgenden Aspekte werden berücksichtigt: – Backups sind vor unbefugter Änderung oder Löschung durch Schadsoftware geschützt. (I, A) -Backups sind vor unbefugtem Zugriff durch Schadsoftware oder deren Betreiber geschützt (C, I)“)* und die im Backup befindlichen Daten nicht korrupt sind und über den gesamten Zeitraum der Vorhaltung vor Manipulation geschützt werden.

5.2.9: „Inwieweit wird die Sicherung und Wiederherstellung von Daten und IT-Diensten sichergestellt?“

Zur Sicherstellung von Sicherungen und Wiederherstellungsfähigkeit von Daten und IT-Diensten prüft der Auditor das Vorhandensein von Backupkonzepten für maßgebliche Systeme *(Control 5.2.9; Anforderungen (muss); Erster Unterpunkt: „+ Für die maßgeblichen IT-Systeme sind Backup-Konzepte vorhanden. Die folgenden Aspekte werden berücksichtigt: – Entsprechende Schutzmaßnahmen, um die Vertraulichkeit, Integrität und Verfügbarkeit für Daten-Backups sicherzustellen. Integrität und Verfügbarkeit für Daten-Backups sicherzustellen“)* und Wiederherstellungskonzepten für maßgebliche IT-Dienste, *(Control 5.2.9; Anforderungen (muss); Zweiter Unterpunkt: „+ Für die maßgeblichen IT-Dienste sind Wiederherstellungs-Konzepte vorhanden“)* die die Abhängigkeiten bei der Wiederherstellung berücksichtigen. *(Control 5.2.9; Anforderungen (sollte); Erster Unterpunkt: „+ Für jeden maßgeblichen IT-Dienst ist ein Sicherungs- und Wiederherstellungs-Konzept vorhanden. – Abhängigkeiten zwischen IT-Diensten und die Reihenfolge für die Wiederherstellung werden berücksichtigt“).* Weiter prüft der Auditor Nachweise, dass methodische Überprüfungen der Konzepte Stattfinden, *(Control 5.2.9; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Sicherungs- und Wiederherstellungskonzepte werden in regelmäßigen Abständen methodisch überprüft. (A)“)* die allgemeine Wiederherstellungskapazität berücksichtigt und geprüft wird *(Control 5.2.9; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Zweiter Unterpunkt: „+ Die allgemeine Wiederherstellungskapazität wird berücksichtigt und geprüft (z. B. Stichprobenprüfung, Prüfsysteme) (I, A)“)* und dass folgende Aspekte Berücksichtigung finden *(Control 5.2.9; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Dritter Unterpunkt: „+ Sicherungs- und Wiederherstellungskonzepte berücksichtigen die folgenden Aspekte: (A) - Zielsetzung für den Wiederherstellungspunkt*

(RPO, en Recovery Point Objective). – Zeitvorgabe für die Wiederherstellung (RTO, en: Recovery Time Objective). – Erforderliche Ressourcen für die Wiederherstellung (unter Berücksichtigung der Kapazität und Leistung einschließlich Personal und Hardware). – Vermeidung von Überlastungsszenarien während der Wiederherstellung. – Angemessene räumliche Redundanz (z. B. separater Raum, separater Brandabschnitt, separates Rechenzentrum, separater Standort)").

5.3.1: „Inwieweit wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt?"

Der Auditor prüft die Berücksichtigung der Informationssicherheit bei der Planung und Entwicklung *(Control 5.3.1; Anforderungen (muss); Erster Unterpunkt: „+ Die Anforderungen an die Informationssicherheit bei der Planung und Entwicklung von IT-Systemen sind ermittelt und werden berücksichtigt")* sowie bei Beschaffung oder Erweiterung *(Control 5.3.1; Anforderungen (muss); Zweiter Unterpunkt: „+ Die Anforderungen an die Informationssicherheit bei der Beschaffung oder Erweiterung von IT-Systemen und IT-Komponenten sind ermittelt und werden berücksichtigt")* und der Weiterentwicklung von IT-Systemen *(Control 5.3.1; Anforderungen (muss); Dritter Unterpunkt: „+ Anforderungen an die Informationssicherheit bei Änderungen in entwickelten IT-Systemen sind berücksichtigt")*. Der Auditor prüft weiter, ob Lastenhefte angelegt wurden *(Control 5.3.1; Anforderungen (sollte); Erster Unterpunkt: „+ Lastenhefte sind erstellt. Die folgenden Aspekte werden berücksichtigt: – Die Anforderungen an die Informationssicherheit – Empfehlungen des Verkäufers und bewährte Verfahren für eine sichere Konfiguration und Implementierung – Bewährte Verfahren und Sicherheitsleitlinien – Ausfallsicher (so konzipiert, dass im Falle eines Ausfalls oder einer Fehlfunktion eine Rückkehr in einen sicheren Zustand erfolgt)")* und diese gegen die Informationssicherheit geprüft wurden *(Control 5.3.1; Anforderungen (sollte); Zweiter Unterpunkt: „+ Lastenhefte werden gegen die Anforderungen an die Informationssicherheit geprüft").* Er prüft auch, welche Daten für Testzwecke verwendet wurden und ob im Falle der Verwendung von Produktivdaten ausreichend Sicherheitsmechanismen implementiert wurden *(Control 5.3.1; Anforderungen (sollte); Vierter Unterpunkt: „+ Es wird so weit wie möglich vermieden, produktive Daten für Testzwecke zu verwenden (falls anwendbar, Anonymisierung oder Pseudonymisierung): – Wenn produktive Daten für Testzwecke genutzt werden, muss sichergestellt werden, dass im Testsystem vergleichbare Schutzmaßnahmen wie im Produktivsystem vorhanden sind – Anforderungen an den Lebenszyklus von Testdaten (z. B. Löschung, höchste Lebensdauer im IT-System) – Es werden fallbezogene Vorgaben für die Erstellung von Testdaten definiert")*. Außerdem beinhaltet die Prüfung die Kontrolle von Nachweisen, dass Prüfungen der IT-Systeme vor deren produktiven Einsatz durchgeführt wurden *(Control 5.3.1; Anforderungen (sollte); Dritter Unterpunkt: „+ Eine Prüfung des IT-Systems auf Einhaltung der Vorgaben vor dem produktiven Einsatz wird durchgeführt")* und dass Systemabnahmetests unter Berücksichtigung der Anforderungen an die Informationssicherheit durchgeführt werden *(Control 5.3.1; Anforderungen (muss); Vierter Unterpunkt: „+ Systemabnahmetests werden unter Berücksichtigung der Anforderungen an die Informationssicherheit durchgeführt").*

5.3.2: „Inwieweit sind Anforderungen an Netzwerkdienste definiert?"

In Bezug auf Netzwerkdienste prüft der Auditor, dass die Anforderungen an die Informationssicherheit ermittelt und erfüllt sind *(Control 5.3.2; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen an die Informationssicherheit von Netzwerkdiensten sind ermittelt und erfüllt")* und dass diese in Form von SLAs vereinbart sind *(Control 5.3.2; Anforderungen (sollte); Zweiter Unterpunkt: „+ Die Anforderungen werden in Form von SLAs vereinbart")*. Der Prüfer stellt auch fest, ob ein Verfahren zur Absicherung und Nutzung *(Control 5.3.2; Anforderungen (sollte);Erster Unterpunkt: „+ Ein Verfahren für die Absicherung und Nutzung von Netzwerkdiensten ist definiert und umgesetzt")* und zur Überwachung der Qualität definiert und umgesetzt sind *(Control 5.3.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Verfahren zur Überwachung der Qualität des Netzwerkverkehrs (z. B. Verkehrsflussanalysen, Verfügbarkeitsmessungen) sind definiert und werden durchgeführt. (A)").*

5.3.3 „Inwieweit ist die Rückgabe und das sichere Entfernen von Informationswerten aus organisationsfremden IT-Diensten geregelt?"

Weiter wird vom Auditor innerhalb des Assessments geprüft, dass Informationswerte, die in organisationsfremden Diensten liegen, sicher rückgeführt und entfernt werden *(Control 5.3.3; Anforderungen (muss); Erster Unterpunkt: „+ Ein Verfahren zur Rückgabe und sicheren Entfernung von Informationswerten aus jedem organisationsfremden IT-Dienst ist definiert und umgesetzt“)* und kontrolliert die vertragliche Grundlage und den Terminierungsprozess hierzu *(Control 5.3.3; Anforderungen (sollte); Erster Unterpunkt: „+ Eine Beschreibung des Terminierungsprozesses liegt vor, wird bei Änderungen angepasst und ist vertraglich geregelt“).*

5.3.4: „Inwieweit sind Informationen in gemeinsam genutzten organisationsfremden IT-Diensten geschützt?“

Der Auditor prüft außerdem, das bei gemeinsam genutzten IT-Diensten eine wirksame Trennung der Informationen ein unbefugter Zugriff verhindert wird *(Control 5.3.4; Anforderungen (muss); Erster Unterpunkt: „+ Eine wirksame Trennung (z. B. Mandantentrennung) verhindert, dass von unbefugten Nutzern anderer Organisationen auf die eigenen Informationen zugegriffen wird“)* und dass das Abgrenzungskonzept des Anbieters dokumentiert ist und aktuell gehalten wird *(Control 5.3.4; Anforderungen (sollte); Erster Unterpunkt: „+ Das Abgrenzungskonzept des Anbieters ist dokumentiert und wird bei Änderungen angepasst. Die folgenden Aspekte werden berücksichtigt: – Separierung von Daten, Funktionen, kundenspezifischer Software, Betriebssystem, Speichersystem und Netzwerk, – Risikobewertung für den Betrieb von Fremdsoftware innerhalb der gemeinsam genutzten Umgebung“).*

4.9.4 Resümee

Die Anforderungen der NIS-2 Artikel 21 (1) g), grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit, in Bezug auf Cyberhygiene sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments durch den Auditor auf Vorhandensein und Umsetzung geprüft.

4.10 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 21 (2) h)

4.10.1 Anforderung aus der NIS-2

NIS-2 Artikel 21 (2) Unterpunkt h) fordert Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung

4.10.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls die Erfüllung der Forderung nach NIS-2 Artikel 21 (2) h) geprüft:

- 5.1.1: „Inwieweit wird die Nutzung kryptografischer Verfahren verwaltet?“
- 5.1.2: „Inwieweit werden Informationen während der Übertragung geschützt?“

4.10.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

5.1.1. „Inwieweit wird die Nutzung kryptografischer Verfahren verwaltet?“

Zum Einsatz von kryptografischen Verfahren prüft der Auditor, dass diese der anerkannten Industrienorm entsprechen und die das Unternehmen betreffenden Gesetze und Regelungen berücksichtigen *(Control 5.1.1;*

Anforderungen (muss); Erster Unterpunkt: „+ Alle angewendeten kryptografischen Verfahren (z. B. Verschlüsselung, Signatur und Hash-Algorithmen, Protokolle) bieten die für das jeweilige Anwendungsgebiet notwendige Sicherheit entsprechend der anerkannten Industrienorm – soweit wie rechtlich möglich“). Er prüft, dass ein technisches Regelwerk erstellt *(Control 5.1.1; Anforderungen (sollte); Erster Unterpunkt: „+ Erstellung eines technischen Regelwerkes mit Anforderungen an die Verschlüsselung zum Schutz von Informationen entsprechend ihrer Klassifizierung“)* und ein Nutzungskonzept definiert ist *(Control 5.1.1; Anforderungen (sollte); Zweiter Unterpunkt: „+ Ein Nutzungskonzept für Kryptografie ist definiert und umgesetzt. Die folgenden Aspekte werden berücksichtigt: - Kryptografische Verfahren - Schlüsselstärken - Verfahren für den vollständigen Lebenszyklus von kryptografischen Schlüsseln einschließlich Erzeugung, Speicherung, Archivierung, Abruf, Verteilung, Deaktivierung, Erneuerung und Löschung)*. Außerdem ist Teil des Assessments zu prüfen, dass die Anforderungen an die Schlüsselhoheit ermittelt und erfüllt sind *(Control 5.1.1; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Ein Nutzungskonzept für Kryptografie ist definiert und umgesetzt. Die folgenden Aspekte werden berücksichtigt: - Kryptografische Verfahren - Schlüsselstärken - Verfahren für den vollständigen Lebenszyklus von kryptografischen Schlüsseln einschließlich Erzeugung, Speicherung, Archivierung, Abruf, Verteilung, Deaktivierung, Erneuerung und Löschung“)* und ein Notfallprozess zur Wiederherstellung von Schlüsseln etabliert ist *(Control 5.1.1; Anforderungen (sollte); Dritter Unterpunkt: + Ein Notfallprozess zur Wiederherstellung von Schlüsselmaterial ist etabliert“)*.

5.1.2 „Inwieweit werden Informationen während der Übertragung geschützt?“

Zur Sicherstellung des Schutzes von Informationen bei deren Übertragung prüft der Auditor, dass zur Übertragung genutzten Netzwerkdienste identifiziert und dokumentiert sind *(Control 5.1.2; Anforderungen (muss); Erster Unterpunkt: + Die zur Übertragung von Informationen genutzten Netzwerkdienste sind identifiziert und dokumentiert“)*, dass Richtlinien und Verfahren zur Nutzung von Netzwerkdiensten definiert und umgesetzt sind *(Control 5.1.2; Anforderungen (muss); Zweiter Unterpunkt: „+ Richtlinien und Verfahren entsprechend den Klassifizierungsvorgaben zur Nutzung von Netzwerkdiensten sind definiert und umgesetzt“)* und dass Maßnahmen zum Schutz übertragener Inhalte umgesetzt sind *(Control 5.1.2; Anforderungen (muss); Dritter Unterpunkt: + Maßnahmen zum Schutz von übertragenen Inhalten vor unberechtigtem Zugriff sind umgesetzt“)*. Außerdem ist Teil der Prüfung, dass Informationen in verschlüsselter Form transportiert oder übertragen werden *(Control 5.1.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: + Informationen werden in verschlüsselter Form transportiert oder übertragen: (C) - Wenn eine Verschlüsselung nicht möglich ist, müssen Informationen durch ähnlich wirksame Maßnahmen geschützt werden“) (Control 5.1.2; Anforderungen (sollte); Zweiter Unterpunkt: „+ Der elektronische Datenaustausch erfolgt entsprechend der jeweiligen Klassifizierung durch Inhalts- oder Transportverschlüsselung“)* und dass sichergestellt ist, dass die verwendeten Adressen korrekt sind *(Control 5.1.2; Anforderungen (sollte); Erster Unterpunkt: „+ Maßnahmen zur Sicherstellung der korrekten Adressen und des korrekten Transports von Informationen sind umgesetzt“).* Weiter wird vom Auditor geprüft, dass Fernzugriffsverbindungen über angemessene Sicherheitsmerkmale und -fähigkeiten verfügen *(Control 5.1.2; Anforderungen (sollte); Dritter Unterpunkt: „+ Fernzugriffsverbindungen werden dahingehend verifiziert, dass sie über angemessene Sicherheitsmerkmale (z. B. Verschlüsselung, Gewähren und Beenden des Zugriffs) und -fähigkeiten verfügen“).*

4.10.4 Resümee

Die Anforderungen der NIS-2 Artikel 21 (1) h), Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung, sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments durch den Auditor auf Vorhandensein und Umsetzung geprüft.

4.11 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 21 (2) i)

4.11.1 Anforderung aus der NIS-2

NIS-2 Artikel 21 (2) Unterpunkt i) fordert Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen.

4.11.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls die Erfüllung der Forderung nach NIS-2 Artikel 21 (2) i) geprüft:

- 1.3.1: „Inwieweit werden Informationswerte (Assets) identifiziert und erfasst?“
- 1.3.2: „Inwieweit werden Informationswerte hinsichtlich ihres Schutzbedarfs klassifiziert und gemanagt?“
- 1.3.3: „Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene organisationsfremde IT-Dienste zum Verarbeiten von Informationswerten der Organisation eingesetzt werden?“
- 2.1.1: „Inwieweit wird die Eignung von Mitarbeitern für sensible Tätigkeitsbereiche sichergestellt?“
- 2.1.2: „Inwieweit werden alle Mitarbeiter vertraglich zur Einhaltung der Informationssicherheitsrichtlinien verpflichtet?“
- 2.1.3: „Inwieweit werden Mitarbeiter hinsichtlich der Risiken beim Umgang mit Informationen geschult und sensibilisiert?“
- 2.1.4: „Inwieweit ist mobiles Arbeiten geregelt?“
- 3.1.3 „Inwieweit ist der Umgang mit Informationsträgern gemanagt?“
- 3.1.4 „Inwieweit ist der Umgang mit mobilen IT-Geräten und mobilen Datenträgern gemanagt?“
- 4.1.1: „Inwieweit ist der Umgang mit Identifikationsmitteln verwaltet?“
- 4.1.2: „Inwieweit wird der Zugang von Benutzern zu IT-Diensten und IT-Systemen gesichert?“
- 4.1.3: „Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewendet?“
- 4.2.1: „Inwieweit werden Zugriffsrechte vergeben und verwaltet?“
- 5.2.1: „Inwieweit werden Änderungen verwaltet? „
- 5.2.2: „Inwieweit sind Entwicklungs- und Testumgebungen von Produktivumgebungen getrennt?“
- 5.2.3: „Inwieweit werden IT-Systeme vor Schadsoftware geschützt?“
- 5.2.4: „Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert?“
- 5.2.5: „Inwieweit werden Schwachstellen erkannt und behandelt?“
- 5.2.6: „Inwieweit werden IT-Systeme und -Dienste technisch überprüft (System- und Dienst-Audit)?“
- 5.2.7: „Inwieweit wird das Netzwerk der Organisation verwaltet?“
- 5.2.8: „Inwieweit ist eine Kontinuitätsplanung für IT-Dienste vorhanden?“
- 5.2.9: „Inwieweit wird die Sicherung und Wiederherstellung von Daten und IT-Diensten sichergestellt?“

4.11.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.3.1 „Inwieweit werden Informationswerte (Assets) identifiziert und erfasst?“

Im TISAX-Assessment prüft der Auditor, dass die Informationswerte und Assets, die einen Wert für das Unternehmen darstellen, bekannt sind *(Control 1.3.1 Anforderung (muss); Erster Unterpunkt: „+ Informationswerte und andere Assets, deren Sicherheit für die Organisation relevant ist, sind identifiziert und erfasst. - Diesen Informationswerten ist ein Verantwortlicher zugeordnet*“ und einem Verantwortlichem zugeordnet sind. Außerdem, dass die zugehörigen Informationsträger identifiziert sind (muss 2) *(Control 1.3.1; Anforderungen (muss); Zweiter Unterpunkt: „ + Die Informationsträger, die die Informationswerte verarbeiten, sind identifiziert und erfasst: – Diesen Informationsträgern ist ein Verantwortlicher zugeordnet)* und die gesammelten Informationen in einem aktuellen Verzeichnis gesammelt wurden *(Control 1.3.1; Anforderungen (sollte); Erster Unterpunkt: „ + Es ist ein Verzeichnis der relevanten Informationswerte vorhanden: – Jedem relevanten Informationswert sind die entsprechenden Informationsträger zugeordnet. – Eine regelmäßige Überprüfung des Verzeichnisses findet statt“*.

1.3.2 „Inwieweit werden Informationswerte hinsichtlich ihres Schutzbedarfs klassifiziert und gemanagt?“

Der Auditor prüft weiterhin, dass ein einheitliches Schema zur Klassifizierung vorliegt *(Control 1.3.2; Anforderungen (muss); Erster Unterpunkt: „ + Ein einheitliches Schema zur Klassifizierung von Informationswerten hinsichtlich des Schutzziels Vertraulichkeit ist verfügbar“*, dass die Informationswerte entsprechend dem Schema bewertet wurden *(Control 1.3.2; Anforderungen (muss); Zweiter Unterpunkt: „ + Es wird eine Beurteilung der identifizierten Informationswerte entsprechend den definierten Kriterien vorgenommen und dem vorhandenen Klassifizierungsschema zugeordnet“* und dass aus der Klassifizierung entsprechende Maßnahmen abgeleitet und eingehalten werden *(Control 1.3.2; Anforderungen (muss); Dritter Unterpunkt: „ + 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 umgesetzt“*. Zur vollumfänglichen Bewertung über die Vertraulichkeit hinaus prüft der Auditor die Ausweitung der Bewertung auf die Integrität und Verfügbarkeit *(Control 1.3.2; Anforderungen (sollte); Erster Unterpunkt: „+ Die Schutzziele Integrität und Verfügbarkeit werden berücksichtigt“*.

1.3.3 „Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene organisationsfremde IT-Dienste zum Verarbeiten von Informationswerten der Organisation eingesetzt werden?“

Im Hinblick auf die Nutzung organisationfremder IT-Dienste prüft der Auditor, dass diese nicht ohne Bewertung und Umsetzung der aus der Bewertung resultierenden Maßnahmen (*(Control 1.3.3; Anforderungen (muss); Erster Unterpunkt: „+ 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“*) eingesetzt werden, und dass die Anforderungen an die Dienste dem Schutzbedarf der zu verarbeitenden Information angemessen sind (*(Control 1.3.3; Anforderungen (muss); Zweiter Unterpunkt: „+ Die organisationsfremden IT-Dienste wurden auf den Schutzbedarf der verarbeiteten Informationswerte abgestimmt“).*

2.1.1: „Inwieweit wird die Eignung von Mitarbeitern für sensible Tätigkeitsbereiche sichergestellt?“

Zur Sicherstellung der Eignung von Mitarbeitern, die auf sensible Informationen zugreifen, prüft der Auditor, dass die sensiblen Stellen bekannt sind *(Control 2.1.1; Anforderungen (muss); Erster Unterpunkt: „ + Sensible Tätigkeitsbereiche und Stellen sind ermittelt“* und die Anforderungen an die Mitarbeiter auf diesen Stellen bekannt sind *(Control 2.1.1; Anforderungen (muss); Zweiter Unterpunkt: „ + Die Anforderungen an Mitarbeiter bezüglich ihres Stellenprofils sind ermittelt und erfüllt“* und dass eine Prüfung der Mitarbeiter auf deren Identität *(Control 2.1.1; Anforderungen (muss); Dritter Unterpunkt: „ + Die Identität von potenziellen Mitarbeitern wird überprüft (z. B. Prüfung von Ausweisdokumenten)* und Eignung stattfindet *(Control 2.1.1; Anforderungen (sollte); Erster Unterpunkt: „ + Die persönliche Eignung von potenziellen Mitarbeitern wird mit einfachen Verfahren überprüft (z. B. Einstellungsgespräch)“* die nach Bedarf erweitert wird *(Control 2.1.1; Anforderungen (sollte); Zweiter Unterpunkt: „ + Es findet eine erweiterte Prüfung der Eignung abhängig vom jeweiligen Tätigkeitsbereich und der jeweiligen Stelle statt. (Z. B. Assessment-Center, psychologische Analyse, Prüfung von Referenzen, Zeugnissen und Diplomen, Einsichtnahme in Führungszeugnisse, Prüfung des beruflichen und privaten Hintergrunds)“*.

2.1.2: „Inwieweit werden alle Mitarbeiter vertraglich zur Einhaltung der Informationssicherheitsrichtlinien verpflichtet?“

Der Auditor prüft auch, ob die Mitarbeiter zur Einhaltung der Richtlinien zur Informationssicherheit *(Control 2.1.2; Anforderungen (muss); Zweiter Unterpunkt: „+ Es besteht eine Verpflichtung zur Einhaltung der Richtlinien zur Informationssicherheit“)* und zur Geheimhaltung *(Control 2.1.2; Anforderungen (muss); Erster Unterpunkt: „+ Es besteht eine Verpflichtung zur Geheimhaltung“)* über die Dauer des Arbeitsverhältnisses bzw. des Auftrags und darüber hinaus *(Control 2.1.2; Anforderungen (sollte); Erster Unterpunkt: „+ Es besteht eine Verpflichtung zur Geheimhaltung über das Arbeitsverhältnis bzw. den Auftrag hinaus“)* verpflichtet sind. Weiter prüft der Auditor, dass Informationssicherheit in Arbeitsverträgen Berücksichtigung findet *(Control 2.1.2; Anforderungen (sollte); Zweiter Unterpunkt: „+ Informationssicherheit wird in den Arbeitsverträgen der Mitarbeiter berücksichtigt“)* und eine Vorgehensweise bei Verstößen beschrieben ist *(Control 2.1.2; Anforderungen (sollte); Dritter Unterpunkt: „+ Eine Vorgehensweise bei Verstößen gegen die vorstehenden Verpflichtungen ist beschrieben“).*

2.1.3: „Inwieweit werden Mitarbeiter hinsichtlich der Risiken beim Umgang mit Informationen geschult und sensibilisiert?“

Der Auditor prüft, ob die Mitarbeiter des Unternehmens ganzheitlich hinsichtlich der Risiken beim Umgang mit Informationen geschult und sensibilisiert werden *(Control 2.1.3; Anforderungen (muss); erster Unterpunkt: + Mitarbeiter sind geschult und sensibilisiert).* Weiter wird geprüft, dass ein Schulungskonzept vorliegt, das für die Informationssicherheit relevante Bereiche abdeckt *(Control 2.1.3; Anforderungen (sollte); erster Unterpunkt: + Ein Konzept zur Sensibilisierung und Schulung der Mitarbeiter ist erstellt. Dabei werden mindestens die folgenden Aspekte berücksichtigt: Richtlinie zur Informationssicherheit, Meldungen von Informationssicherheitsereignissen, Verhalten bei Auftreten von Schadsoftware, Richtlinien zu Benutzerkonten und Anmeldeinformationen (z. B. Passwort-Richtlinie), Compliance-Themen der Informationssicherheit, Anforderungen und Verfahren zum Einsatz von Geheimhaltungsvereinbarungen bei der gemeinsamen Nutzung schutzbedürftiger Informationen, Nutzung organisationsfremder IT-Dienste)*, in dem die Zielgruppen für Schulungskonzepte Berücksichtigung finden und *dass* die Schulungsmaßnahmen entsprechend der Kritikalität der verarbeiteten Information angemessen sind *(Control 2.1.3; Anforderungen (sollte); zweiter Unterpunkt: Zielgruppen für Schulungs- und Sensibilisierungsmaßnahmen (d. h. Personen, die in bestimmten risikobehafteten Umgebungen arbeiten, wie Administratoren, Mitarbeiter mit Zugang zu Kundennetzwerken, Personal in Fertigungsbereichen) sind ermittelt und in einem Schulungskonzept berücksichtigt) und dass das Schulungskonzept durch das Management freigegeben ist (Control 2.1.3; Anforderungen (sollte); Dritter Unterpunkt: + Das Konzept wurde vom verantwortlichen Management freigegeben).* Der Auditor wird ebenfalls prüfen, ob die Schulungs- und Sensibilisierungsmaßnahmen in regelmäßigen Abständen und anlassbezogen durchgeführt werden *(Control 2.1.3; Anforderungen (sollte); vierter Unterpunkt: + Schulungs- und Sensibilisierungsmaßnahmen werden sowohl in regelmäßigen Abständen als auch als Reaktion auf Ereignisse durchgeführt)* und eine entsprechende Dokumentation vorliegt *(Control 2.1.3; Anforderungen (sollte); fünfter Unterpunkt: + Die Teilnahme an Schulungs- und Sensibilisierungsmaßnahmen wird dokumentiert)*. Zur Kontrolle der wirksamen Überprüfung prüft der Auditor, dass die Ansprechpartner für Informationssicherheit den Mitarbeitern bekannt sind *(Control 2.1.3; Anforderungen (sollte); sechster Unterpunkt: + Mitarbeitern sind die Ansprechpartner für Informationssicherheit bekannt)*.

2.1.4: „Inwieweit ist mobiles Arbeiten geregelt?“

Der Auditor prüft auch, dass beim Arbeiten außerhalb der speziell dafür festgelegten Sicherheitszonen die hieraus resultierenden Maßnahmen *(Control 2.1.4; Anforderungen (muss); Erster Unterpunkt: „+ Die Anforderungen an mobiles Arbeiten sind ermittelt und erfüllt. Die folgenden Aspekte werden berücksichtigt:*

- Sicherer Umgang mit und Zugriff auf Informationen (sowohl elektronisch als auch in Papierform) 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)“) sowie gesonderte Maßnahmen für Reiseaktivitäten *(Control 2.1.4; Anforderungen (sollte); Erster Unterpunkt: „ + Die folgenden Aspekte werden*

berücksichtigt: – Maßnahmen bei Reisen (z. B. Einsichtnahme durch Behörden), – Maßnahmen bei Reisen in sicherheitskritische Länder“) ermittelt und erfüllt sind. Außerdem prüft er, dass ein Zugriff auf das Netzwerk der Organisation über eine gesicherte Verbindung möglich ist *(Control 2.1.4; Anforderungen (muss); Zweiter Unterpunkt: „+ Der Zugang zum Netzwerk der Organisation erfolgt über eine gesicherte Verbindung (z. B. VPN) und über eine starke Authentifizierung“)* und dass betroffene Mitarbeiter über alle genannten Maßnahmen in Kenntnis gesetzt wurden *(Control 2.1.4; Anforderungen (sollte); Zweiter Unterpunkt: „+ Mitarbeitersensibilisierung“)*.

3.1.3: „Inwieweit ist der Umgang mit Informationsträgern gemanagt?“

Zur Sicherstellung des Sicherheitsbewussten Umgangs mit Datenträgern prüft der Auditor, dass Anforderungen definiert und umgesetzt sind, die deren gesamten Lebenszyklus abbilden *(Control 3.1.3; Anforderungen (muss); Erster Unterpunkt: „+ Die Anforderungen an den Umgang mit Informationsträgern (z. B. Transport, Aufbewahrung, Reparatur, Verlust, Rückgabe, Entsorgung) sind ermittelt und erfüllt“).*

3.1.4: „Inwieweit ist der Umgang mit mobilen IT-Geräten und mobilen Datenträgern gemanagt?“

In Bezug auf den Umgang mit mobilen IT-Geräten prüft der Auditor, dass Anforderungen an mobile IT-Geräte und mobile Datenträger ermittelt und erfüllt *(Control 3.1.4; Anforderungen (muss); Erster Unterpunkt: „+ Die Anforderungen an mobile IT-Geräte und mobile Datenträger sind ermittelt und erfüllt. Die folgenden Aspekte werden berücksichtigt: - Verschlüsselung - Zugangsschutz (z. B. PIN, Passwort) - Kennzeichnung (auch unter Berücksichtigung von Anforderungen zur Nutzung in Gegenwart von Kunden)“)* und dass die Anwender über fehlenden Datenschutz auf mobilen Geräten informiert sind *(Control 3.1.4; Anforderungen (sollte); Zweiter Unterpunkt: „+ Anwender sind über fehlenden Datenschutz auf mobilen Geräten informiert“).*

4.1.1: „Inwieweit ist der Umgang mit Identifikationsmitteln verwaltet?“

Der Auditor prüft außerdem, dass Anforderungen an den Umgang mit Identifikationsmitteln über den gesamten Lebenszyklus ermittelt und erfüllt sind *(Control 4.1.1; Anforderungen (muss); Erster Unterpunkt: „+ Die Anforderungen an den Umgang mit Identifikationsmitteln über den gesamten Lebenszyklus sind ermittelt und erfüllt. Die folgenden Aspekte werden berücksichtigt: - Erstellung, Übergabe, Rückgabe und Vernichtung - Gültigkeitszeiträume - Rückverfolgbarkeit - Umgang mit Verlust“)*, dass die Herstellung kontrolliert stattfindet *(Control 4.1.1; Anforderungen (sollte); Erster Unterpunkt: „+ Identifikationsmittel können nur unter kontrollierten Bedingungen hergestellt werden“)*, dass Gültigkeitszeiträume definiert sind *(Control 4.1.1; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf);Erster Unterpunkt: „ + Die Gültigkeit von Identifikationsmitteln ist auf einen angemessenen Zeitraum begrenzt. (C, I, A)“)* und dass ein Konzept zur Sperrung oder Ungültigmachung bei Verlust definiert ist *(Control 4.1.1; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Zweiter Unterpunkt: „+ Ein Konzept zur Sperrung oder Ungültigmachung von Identifikationsmitteln bei Verlust ist, soweit möglich, erstellt und umgesetzt. (C, I, A)“)*.

4.1.2: „Inwieweit wird der Zugang von Benutzern zu IT-Diensten und IT-Systemen gesichert?“

Teil des Audits ist auch, dass der Auditor prüft, dass das Verfahren zur Benutzerauthentifizierung auf Basis einer Risikobewertung getroffen wurde, die unterschiedliche Angriffsszenarien berücksichtigt *(Control 4.1.2; Anforderungen (muss); Erster Unterpunkt: „+ Die Auswahl der Verfahren zur Benutzerauthentifizierung wurde auf Basis einer Risikobewertung getroffen. Mögliche Angriffsszenarien wurden berücksichtigt (z. B. direkte Zugänglichkeit über das Internet)“)* und das auf dem aktuellen Stand der Technik basiert *(Control 4.1.2; Anforderungen (muss); Zweiter Unterpunkt: „+ Für die Benutzerauthentifizierung werden Verfahren auf dem aktuellen Stand der Technik angewendet“)*. Außerdem wird geprüft, dass die Verfahren auf Grundlage der geschäftsbezogenen und sicherheitsrelevanten Anforderungen festgelegt und umgesetzt *(Control 4.1.2; Anforderungen (sollte); Erster Unterpunkt: „ + Die Verfahren zur Benutzerauthentifizierung werden auf der Grundlage der geschäftsbezogenen und sicherheitsrelevanten Anforderungen festgelegt und umgesetzt: – Benutzer werden mindestens mittels starker Passwörter entsprechend dem aktuellen Stand der Technik authentifiziert“),* der Kritikalität der Konten angepasst *(Control 4.1.2; Anforderungen (sollte); Zweiter Unterpunkt: „+ Es werden höherwertige Verfahren zur Authentifizierung von privilegierten Benutzerkonten angewendet (z. B. Privilegiertes Zugangsmanagement, 2-Faktor-Authentifizierung)“)* und nach Bedarf durch weitere Maßnahmen ergänzt wurden *(Control 4.1.2;*

Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Abhängig von der Risikobewertung wurden das Authentifizierungsverfahren und die Zugriffskontrolle durch ergänzende Maßnahmen verstärkt (z. B. dauerhafte Zugriffsüberwachung hinsichtlich Unregelmäßigkeiten oder Einsatz einer starken Authentifizierung, automatische Abmeldung, Sperrung bei Inaktivität oder Schutz vor Brute-Force-Angriffen). (C, I, A)“).

4.1.3. „Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewendet?“

Weiterer Teil des Assessments ist die Prüfung, dass der Zugang zu Informationen und IT-Systemen über validierte Benutzerkonten erfolgt und dass Anmeldeinformationen geschützt werden und die Rückverfolgbarkeit von Transaktionen und Zugriffen sichergestellt wird. Hierzu prüft der Auditor, dass Benutzerkonten über ihren Lebenszyklus verwaltet werden *(Control 4.1.3; Anforderungen (muss); Erster Unterpunkt: „+ Die Erstellung, Änderung und Löschung von Benutzerkonten wird durchgeführt“), (Control 4.1.3; Anforderungen (muss); Vierter Unterpunkt: „+ Benutzerkonten werden unmittelbar nachdem der Benutzer aus der Organisation ausgeschieden ist oder diese verlassen hat (z. B. bei Beendigung des Arbeitsverhältnisses) gesperrt“)* und dass eine regelmäßige Überprüfung auf Aktualität der Zuteilung stattfindet *(Control 4.1.3; Anforderungen (muss); Fünfter Unterpunkt: „+ Benutzerkonten werden in regelmäßigen Abständen überprüft“)*. Weiter prüft der Auditor, dass die Konten personalisiert werden *(Control 4.1.3; Anforderungen (muss); Zweiter Unterpunkt: „+ Es werden eindeutige und personalisierte Benutzerkonten verwendet“)* oder im Bedarfsfall die Vergabe von Sammelkonten einer Regelung unterliegt *(Control 4.1.3; Anforderungen (muss); Dritter Unterpunkt: „+ Die Nutzung von „Sammel-Konten“ ist geregelt (z. B. auf Fälle beschränkt, bei denen die Rückverfolgbarkeit von Aktionen verzichtbar ist)“)*. Die sichere Übermittlung der Konteninformationen *(Control 4.1.3; Anforderungen (muss); Sechster Unterpunkt: „+ Es erfolgt eine sichere Zustellung der Anmeldeinformationen an den Benutzer“),* die Sicherstellung der Geheimhaltung der Anmeldeinformation *(Control 4.1.3; Anforderungen (muss); Achter Unterpunkt: „+ Die Anmeldeinformationen (z. B. Passwörter) eines personalisierten Benutzerkontos dürfen nur dem zugeordneten Benutzer bekannt sein“)* und die zugehörigen Verhaltensweisen *(Control 4.1.3; Anforderungen (muss); Siebter Unterpunkt: „+ Eine Richtlinie zum Umgang mit Anmeldeinformationen ist definiert und umgesetzt. Die folgenden Aspekte werden berücksichtigt: – 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)“)* werden vom Auditor ebenfalls geprüft.

In Bezug auf Benutzerprofile prüft der Auditor, dass ein Standardprofil besteht *(Control 4.1.3; Anforderungen (sollte); Erster Unterpunkt: „+ Ein Basis-Benutzerprofil mit minimalen Zugriffsrechten und Funktionalitäten ist vorhanden und wird angewendet“)*. Außerdem prüft er, dass Herstellerseitige Standardkonten deaktiviert werden *(Control 4.1.3; Anforderungen (sollte); Zweiter Unterpunkt: „+ Herstellerseitig vorgegebene Standardkonten und -Passwörter werden deaktiviert (z. B. durch Sperrung oder Änderung des Passworts)“)*, dass es einen definierten Prozess zur Erstellung von Konten gibt *(Control 4.1.3; Anforderungen (sollte); Vierter Unterpunkt: „+ Die Einrichtung von Benutzerkonten unterliegt einem Genehmigungsprozess (4-Augen-Grundsatz)“)* und dass die Einrichtung von Konten durch eine autorisierte Stelle erfolgt *(Control 4.1.3; Anforderungen (sollte); Dritter Unterpunkt: „+ Die Einrichtung von Benutzerkonten erfolgt durch die verantwortliche Stelle oder wird durch diese autorisiert“)*. Er prüft weiterhin, dass Sperr- und Löschfristen definiert *(Control 4.1.3; Anforderungen (sollte); Sechster Unterpunkt: „+ Sperr- und Löschfristen für Benutzerkonten sind definiert“)* und auch bei Dienstleisterkonten umgesetzt werden *(Control 4.1.3; Anforderungen (sollte); Fünfter Unterpunkt: „+ Benutzerkonten von Dienstleistern werden nach Abschluss von deren Aufgabe gesperrt“)*. Der Auditor prüft auch, dass die Verwendung von Standard-Passwörtern verhindert wird *(Control 4.1.3; Anforderungen (sollte); Siebter Unterpunkt: „+ Die Verwendung von Standard-Passworten wird technisch verhindert“)*, dass die interaktive Anmeldung bei Dienste-Konten technisch verhindert wird, *(Control 4.1.3; Anforderungen (sollte); Zehnter Unterpunkt: „+ Die interaktive Anmeldung bei Dienstkonten (technischen Konten) wird technisch verhindert“),* dass beim Einsatz

starker Authentifizierung das Medium sicher verwendet wird *(Control 4.1.3; Anforderungen (sollte); Achter Unterpunkt: „+ Beim Einsatz einer starken Authentifizierung wird das Medium (z. B. Faktor Besitz) sicher verwendet“)* und schließlich, dass eine regelmäßige Überprüfung der Konten stattfindet *(Control 4.1.3; Anforderungen (sollte); Neunter Unterpunkt: „+ Es findet eine Überprüfung der Benutzerkonten in regelmäßigen Abständen statt. Dazu gehören auch Benutzerkonten in IT-Systemen von Kunden“)*.

4.2.1. „Inwieweit werden Zugriffsrechte vergeben und verwaltet?“

Zur Sicherstellung, dass nur berechtigte (autorisierte) Benutzer Zugriff auf Informationen und IT-Dienstleistungen haben, prüft der Auditor, dass die Anforderungen an das Management von Zugriffsrechten ermittelt und erfüllt wurden *(Control 4.2.1; Anforderungen (muss); Erster Unterpunkt: „+ Die Anforderungen an das Management von Zugriffsrechten (Autorisierung) sind ermittelt und erfüllt. Die folgenden Aspekte werden berücksichtigt: – Verfahren zur Beantragung, Verifizierung und Genehmigung, – Anwendung des Minimal- („Need-to-know"-/“Least-Privilege“) -Prinzips. – Zugriffsrechte werden widerrufen, wenn sie nicht mehr benötigt werden“)*, dass Berechtigungskonzepte erstellt wurden *(Control 4.2.1; Anforderungen (sollte); Erster Unterpunkt: „+ Berechtigungskonzepte für den Zugriff auf Informationen sind erstellt“)*, Berechtigungs-Rollen Verwendung finden *(Control 4.2.1; Anforderungen (sollte); Zweiter Unterpunkt: „+ Berechtigungs-Rollen werden verwendet“)*, dass normalen Nutzern keine privilegierten Zugriffsrechte zugeteilt werden *(Control 4.2.1; Anforderungen (sollte); Vierter Unterpunkt: „+ Normalen Benutzerkonten werden keine privilegierten Zugriffsrechte erteilt“)* und die Zugriffsrechte durch den Informationsverantwortlichen freigegeben wurden *(Control 4.2.1; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Die Zugriffsrechte sind durch den internen Informationsverantwortlichen freigegeben. (C, I, A)“)*. Er prüft weiter, dass die Vergabe von Berechtigungen bedarfsorientiert vorgenommen wird, *(Control 4.2.1; Anforderungen (sollte); Dritter Unterpunkt: „+ Die Vergabe von Rechten erfolgt bedarfsorientiert und entsprechend der Rolle und/oder dem Verantwortungsbereich“)*, die Rechte regelmäßig kontrolliert werden *(Control 4.2.1; Anforderungen (muss); Zweiter Unterpunkt: „+ Die erteilten Zugriffsrechte für normale und privilegierte Benutzerkonten sowie technische Konten werden in regelmäßigen Abständen auch in IT-Systemen von Kunden überprüft“)* und dass auch bei Wechseln in z.B. andere Verantwortungsbereiche eine Aktualisierung vorgenommen wird *(Control 4.2.1; Anforderungen (sollte); Fünfter Unterpunkt: „+ Die Zugriffsrechte eines Benutzerkontos eines Anwenders werden nach dessen Wechsel (z. B. in einen anderen Verantwortungsbereich) angepasst“)*.

5.2.1: „Inwieweit werden Änderungen verwaltet?“

In Bezug auf Änderungen prüft der Auditor, dass die Anforderungen an die Informationssicherheit ermittelt und umgesetzt werden *(Control 5.2.1; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen an die Informationssicherheit bei Änderungen von Organisation, Geschäftsprozessen, IT-Systemen werden ermittelt und umgesetzt“ und)* eine Bewertung in Bezug auf die Auswirkung in Richtung der Informationssicherheit stattfindet *(Control 5.2.1; Anforderungen (sollte); Zweiter Unterpunkt: „+ Änderungen werden bezüglich möglicher Auswirkungen auf die Informationssicherheit verifiziert und bewertet“)*. Weiter wird vom Auditor geprüft, dass bei Änderungen mit Auswirkung auf die Informationssicherheit, ein formales Genehmigungsverfahren etabliert ist *(Control 5.2.1; Anforderungen (sollte); Erster Unterpunkt: „+ Ein formales Genehmigungsverfahren ist etabliert“),* und diese geplant und geprüft werden *(Control 5.2.1; Anforderungen (sollte); Dritter Unterpunkt: „+ Änderungen mit Auswirkung auf die Informationssicherheit werden geplant und geprüft“),* dass die Änderungen während und nach der Umsetzung verifiziert werden *(Control 5.2.1; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Die Einhaltung der Anforderungen an die Informationssicherheit wird während und nach der Umsetzung der Änderungen verifiziert. (C, I, A)“)* und das Notfallverfahren im Falle von Fehlern berücksichtigt werden *(Control 5.2.1; Anforderungen (sollte); Vierter Unterpunkt: „+ Notfallverfahren im Falle von Fehlern sind berücksichtigt“)*.

5.2.2: „Inwieweit sind Entwicklungs- und Testumgebungen von Produktivumgebungen getrennt?“

Der Auditor prüft auf Vorhandensein einer Risikobewertung bezüglich der Notwendigkeit einer Trennung von Produktiv- und Testsystemen *(Control 5.2.2; Anforderungen (muss); Erster Unterpunkt: + Die IT-Systeme wurden*

einer Risikobewertung unterzogen, um zu ermitteln, inwiefern deren Trennung in Entwicklungs-, Test- und Produktivsysteme notwendig ist“), die Umsetzung der Ergebnisse *(Control 5.2.2; Anforderungen (muss); Zweiter Unterpunkt: + Eine Segmentierung ist auf Basis der Ergebnisse der Risikoanalyse umgesetzt“)* und dass Anforderungen an Entwicklungs- und Testumgebungen ermittelt und umgesetzt sind *(Control 5.2.2; Anforderungen (sollte); Erster Unterpunkt: „+ Die Anforderungen an Entwicklungs- und Testumgebungen sind ermittelt und umgesetzt. Die folgenden Aspekte werden berücksichtigt: - Trennung von Entwicklungs-, Test- und Produktivsystemen - Keine Entwicklungs- und Systemwerkzeuge auf Produktivsystemen (außer solchen, die für den Betrieb notwendig sind) - 1Verwendung von unterschiedlichen Benutzerprofilen für Entwicklungs-, Test- und Produktivsysteme“).*

5.2.3: „Inwieweit werden IT-Systeme vor Schadsoftware geschützt?“

Um den Schutz von IT-Systemen vor Schadsoftware sowohl technisch als auch organisatorisch sicherzustellen prüft der Auditor, dass Technische und organisatorische Maßnahmen zum Schutz vor Schadsoftware definiert und umgesetzt sind *(Control 5.2.3; Anforderungen (muss); Zweiter Unterpunkt: „+ Technische und organisatorische Maßnahmen zum Schutz vor Schadsoftware sind definiert und umgesetzt“)* und dass die Anforderungen an den Schutz vor Schadsoftware ermittelt sind *(Control 5.2.3; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen an den Schutz vor Schadsoftware sind ermittelt“)*. Außerdem gehört zur Prüfung, dass nicht benötigte Netzwerkdienste deaktiviert sind *(Control 5.2.3; Anforderungen (sollte); Erster Unterpunkt: „+ Nicht benötigte Netzwerkdienste sind deaktiviert“)*, der Zugriff auf die benötigten Zugriffe eingeschränkt ist *(Control 5.2.3; Anforderungen (sollte); Zweiter Unterpunkt: „+ Zugriff auf Netzwerkdienste ist mit geeigneten Schutzmaßnahmen (siehe Beispiele) auf die benötigten Zugriffe eingeschränkt“),* eine Software zum Schutz vor Schadsoftware installiert ist und regelmäßig aktualisiert wird *(Control 5.2.3; Anforderungen (sollte); Dritter Unterpunkt: „+ Eine Software zum Schutz vor Schadsoftware ist installiert und wird in regelmäßigen Abständen automatisch aktualisiert (z. B. Virenscanner)“)* und dass Empfangene Dateien und empfangene Software automatisch auf Schadsoftware überprüft werden *(Control 5.2.3; Anforderungen (sollte); Vierter Unterpunkt: „+ Empfangene Dateien und empfangene Software werden vor ihrer Ausführung automatisch auf Schadsoftware überprüft (On-Access-Scan)“)*. Weiter prüft der Auditor, dass regelmäßig auf Schadsoftware überprüft wird *(Control 5.2.3; Anforderungen (sollte); Fünfter Unterpunkt: „+ Der gesamte Datenbestand aller Systeme wird regelmäßig auf Schadsoftware überprüft“)*, dass von zentralen Gateways übertragene Daten automatisch überprüft werden *(Control 5.2.3; Anforderungen (sollte); Sechster Unterpunkt: „+ Von zentralen Gateways übertragene Daten (z. B. E-Mail, Internet, Netze von Dritten) werden automatisch mittels einer Schutzsoftware überprüft: – Verschlüsselte Verbindungen werden berücksichtigt“)* und dass Verschlüsselte Verbindungen Berücksichtigung finden.

Im Hinblick auf den User prüft der Auditor, dass verhindert ist, dass Schutzsoftware durch Benutzer deaktiviert oder verändert wird *(Control 5.2.3; Anforderungen (sollte); Siebter Unterpunkt: „+ Maßnahmen zur Verhinderung, dass Schutzsoftware durch Benutzer deaktiviert oder verändert wird, sind definiert und umgesetzt“)* und das fallbezogene Sensibilisierungsmaßnahmen stattfinden *(Control 5.2.3; Anforderungen (sollte); Achter Unterpunkt: „+ Fallbezogene Sensibilisierungsmaßnahmen der Mitarbeiter“)*. Für IT-Systeme, die ohne Software zum Schutz vor Schadsoftware betrieben werden, prüft der Auditor, dass alternative Maßnahmen umgesetzt sind (*Control 5.2.3; Anforderungen (sollte); Neunter Unterpunkt: „+ Für IT-Systeme, die ohne Software zum Schutz vor Schadsoftware betrieben werden, sind alternative Maßnahmen (z. B. spezielle Resilienz-Maßnahmen, wenig Dienste, keine aktiven User, Netzisolierung) umgesetzt“).*

5.2.4: „Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert?“

Um die Rückverfolgbarkeit von Ereignissen im Falle eines Sicherheitsvorfalls sicherzustellen, prüft der Auditor, dass eine Ereignisprotokollierung stattfindet und das diese in ihrer Handhabung die Anforderungen der Informationssicherheit berücksichtigt *(Control 5.2.4; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen an die Informationssicherheit bezüglich der Handhabung von Ereignisprotokollen sind ermittelt und erfüllt“)* und dabei eine angemessene Überwachung und Aufzeichnung aller informationssicherheitsrelevanten Aktionen im Netzwerk sicherstellt *(Control 5.2.4; Anforderungen (sollte); Dritter Unterpunkt: „+ Eine angemessene Überwachung und Aufzeichnung aller informationssicherheitsrelevanten Aktionen im Netzwerk sind etabliert“)*. Außerdem

stellt der Auditor fest, ob Sicherheitsrelevante Anforderungen an die Protokollierung der Aktivitäten von Systemadministratoren und Nutzern ermittelt sind und erfüllt werden *(Control 5.2.4; Anforderungen (muss); Zweiter Unterpunkt: „+ Sicherheitsrelevante Anforderungen an die Protokollierung der Aktivitäten von Systemadministratoren und Nutzern sind ermittelt und erfüllt“).* Er prüft weiterhin, dass eingesetzte IT-Systeme hinsichtlich der Protokollierung bewertet werden *(Control 5.2.4; Anforderungen (muss); Dritter Unterpunkt: „+ Die eingesetzten IT-Systeme werden hinsichtlich der Notwendigkeit der Protokollierung bewertet“)* und das speziell bei organisationsfremden IT-Diensten die Überwachungsmöglichkeiten bekannt sind und Berücksichtigung finden *(Control 5.2.4; Anforderungen (muss); Vierter Unterpunkt: „+ Bei der Nutzung organisationsfremder IT-Dienste werden Informationen zu den Überwachungsmöglichkeiten eingeholt und im Assessment berücksichtigt“).* Außerdem prüft er, dass die erfolgten Zugriffe beim Auf- und Abbau von organisationsfremden Netzwerkverbindungen protokolliert werden *(Control 5.2.4; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Zweiter Unterpunkt: „+ Zugriffe beim Auf- und Abbau von organisationsfremden Netzwerkverbindungen (z. B. Fernwartung) werden protokolliert. (C, I, A)“).* Der Auditor prüft ebenfalls das Vorhandensein von Nachweisen zur regelmäßigen Kontrolle von Ereignisprotokollen *(Control 5.2.4; Anforderungen (muss); Fünfter Unterpunkt: „+ Ereignisprotokolle werden regelmäßig auf Regelverstöße und Auffälligkeiten im Einklang mit den zulässigen gesetzlichen und betrieblichen Bestimmungen überprüft“)* und dass ein Eskalationsverfahren bei relevanten Ereignissen Anwendung findet *(Control 5.2.4; Anforderungen (sollte); Erster Unterpunkt: „+ Ein Verfahren zur Eskalation von relevanten Ereignissen an die zuständige Stelle (z. B. Sicherheitsvorfall-Meldung, Datenschutz, Unternehmenssicherheit, IT-Sicherheit) ist definiert und etabliert“).* Er kontrolliert weiter, dass die für die Sicherheit während der Handhabung relevanten Informationssicherheitsanforderungen definiert sind und eingehalten werden *(Control 5.2.4; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Informationssicherheitsanforderungen, die für die Sicherheit während der Handhabung von Ereignisprotokollen relevant sind, z. B. vertragliche Anforderungen, sind ermittelt und umgesetzt. (C, I, A)“)* und dass die Protokolle gegen Änderungen geschützt werden *(Control 5.2.4; Anforderungen (sollte); Zweiter Unterpunkt: „+ Ereignisprotokolle (Inhalte und Metadaten) sind gegen Änderungen geschützt. (z. B. durch eine dedizierte Umgebung)“)*.

5.2.5: „Inwieweit werden Schwachstellen erkannt und behandelt?“

In Bezug auf die Schwachstellenanalyse prüft der Auditor, dass Informationen über technische Schwachstellen gesammelt werden *(Control 5.2.5; Anforderungen (muss); Erster Unterpunkt: „+ Informationen über technische Schwachstellen zu den genutzten IT-Systemen werden gesammelt (z. B. Information vom Hersteller, System-Audits, CVS-Datenbank) und beurteilt (z. B. Allgemeines Bewertungssystem für Schwachstellen, en: Common Vulnerability Scoring System, CVSS)“)* und die erlangten Erkenntnisse zur Behandlung solcher eingesetzt werden *(Control 5.2.5; Anforderungen (muss); Zweiter Unterpunkt: „+ Potenziell betroffene IT-Systeme und Software werden identifiziert, bewertet und Schwachstellen behandelt“)* und dass Risiken auf ein Mindestmaß reduziert werden *(Control 5.2.4; Anforderungen (sollte); Zweiter Unterpunkt: „+ Maßnahmen zur Verringerung von Risiken auf ein Mindestmaß sind, soweit notwendig, umgesetzt “).* Der Auditor prüft außerdem das ein Patch-Management etabliert ist *(Control 5.2.5; Anforderungen (sollte); Erster Unterpunkt: „+ Ein angemessenes Patch-Management ist definiert und umgesetzt (z. B. Prüfung und Installation von Patches)“)* und das die erfolgreiche Installation verifiziert wird *(Control 5.2.5; Anforderungen (sollte); Dritter Unterpunkt: „+ Die erfolgreiche Installation von Patches ist in geeigneter Weise verifiziert“)*

5.2.6: „Inwieweit werden IT-Systeme und -Dienste technisch überprüft (System- und Dienst-Audit)?“

Zur Verifizierung der technischen Überprüfung von IT-Systemen und -Diensten prüft der Auditor, dass die Anforderungen an die Auditierung dieser Systeme und Dienste definiert sind *(Control 5.2.6; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen an die Auditierung von IT-Systemen oder -Diensten sind ermittelt“),* diese regelmäßig durchgeführt werden *(Control 5.2.6; Anforderungen (sollte); Zweiter Unterpunkt: „+ Regelmäßige System- oder Dienst-Audits werden durchgeführt – von Fachpersonal durchgeführt – geeignete Werkzeuge (z. B. Schwachstellen-Scanner) werden für System- und Dienst-Audits verwendet (sofern anwendbar) – vom Internet und dem internen Netzwerk durchgeführt“),* dass die Audits im Umfang festgelegt *(Control 5.2.6; Anforderungen (muss); Zweiter Unterpunkt: „+ Der Umfang des Systemaudits ist rechtzeitig festgelegt“* und im Hinblick auf die

entstehenden Sicherheitsrisiken bewertet werden. *(Control 5.2.6; Anforderungen (sollte); Erster Unterpunkt: „+ System- und Dienst-Audits werden unter Berücksichtigung aller Sicherheitsrisiken geplant, die dadurch hervorrufen werden, könnten (z. B. Störungen)“).* Weiter prüft der Auditor, dass sie den Betreibern und Nutzern bekannt gemacht werden *(Control 5.2.6; Anforderungen (muss); Dritter Unterpunkt: „+ System- oder Dienst-Audits sind mit dem Betreiber und den Nutzern der IT-Systeme oder -Dienste abgestimmt“).*

Die Prüfung beinhaltet auch die Kontrolle eines Nachweises zur Durchführung *(Control 5.2.6; Anforderungen (sollte); Dritter Unterpunkt: „+ Innerhalb eines angemessenen Zeitraums nach Abschluss des Audits wird ein Bericht erstellt)* sowie die Speicherung und die Weitermeldung der Ergebnisse an das Management *(Control 5.2.6; Anforderungen (muss); Vierter Unterpunkt: „+ Die Ergebnisse von System- oder Dienst-Audits werden rückverfolgbar gespeichert und an das zuständige Management berichtet“)* und das auf dem Bericht basierende Ableiten entsprechender Maßnahmen *(Control 5.2.6; Anforderungen (muss); Fünfter Unterpunkt: „+ Von den Ergebnissen werden Maßnahmen abgeleitet“).*

5.2.7: „Inwieweit wird das Netzwerk der Organisation verwaltet?“

Außerdem wird vom Auditor geprüft, ob die Anforderungen an die Steuerung und Segmentierung von Netzwerken umgesetzt ist *(Control 5.2.7; Anforderungen (muss); Erster Unterpunkt: „+ Anforderungen zur Verwaltung und Steuerung von Netzwerken sind ermittelt und erfüllt“* und ob die notwendigen Sicherheitsaspekte nach Stand der Technik umgesetzt sind *(Control 5.2.7; Anforderungen (sollte); Zweiter Unterpunkt: „+ Für eine risikobasierte Segmentierung des Netzwerks werden die folgenden Aspekte berücksichtigt: – Beschränkungen bei der Anbindung von IT-Systemen an das Netzwerk, – Anwendung von Sicherheitstechnologien, – Betrachtungen hinsichtlich Leistung, Vertrauen, Verfügbarkeit, Informationssicherheit und Funktionssicherheit – Begrenzung der Auswirkungen im Falle kompromittierter IT-Systeme – Erkennung möglicher Angriffe und der lateralen Bewegung von Angreifern – Trennung von Netzwerken mit unterschiedlichem Betriebszweck (z. B. Test- und Entwicklungsnetzwerke, Büronetzwerk, Produktionsnetzwerke) – Das erhöhte Risiko aufgrund von Netzwerkdiensten, die über das Internet zugänglich sind, – Technologiespezifische Trennungsmöglichkeit bei Nutzung externer IT-Dienste, – Angemessene Trennung zwischen den eigenen Netzwerken und Kundennetzwerken unter Berücksichtigung der Kundenanforderungen – Erkennung und Verhinderung von Datenverlust/Datenlecks“*.

5.2.8: „Inwieweit ist eine Kontinuitätsplanung für IT-Dienste vorhanden?“

Der Auditor prüft, ob eine Kontinuitätsplanung für IT-Dienste *(Control 5.2.8; Anforderungen (muss); Erster Unterpunkt: „+ Kritische IT-Dienste werden identifiziert, und die geschäftlichen Auswirkungen werden betrachtet“)* und IT-Systeme *(Control 5.2.8; Anforderungen (sollte); Erster Unterpunkt: „Kritische IT-Systeme werden identifiziert – die maßgeblichen Systeme sind nach dem entsprechenden Schutzbedarf klassifiziert – angemessene und geeignete Sicherheitsmaßnahmen werden umgesetzt)* besteht, die auf einer Bewertung der Kritikalität der vorhandenen Dienste bzw. Systeme beruht und die den maßgeblichen Verantwortlichen bekannt ist *(Control 5.2.8; Anforderungen (muss); Zweiter Unterpunkt: „+ Anforderungen und Verantwortlichkeiten für die Kontinuität und Wiederherstellung dieser IT-Dienste sind den maßgeblichen Beteiligten bekannt und werden erfüllt“)*.

Außerdem prüft das Audit das Vorhandensein von Spezifikationen zu unterschiedlichen Szenarien *(Control 5.2.8; Anforderungen (sollte); Zweiter Unterpunkt: „+ Die Kontinuitätsplanung schließt mindestens die folgenden Szenarien ein, welche kritische IT-Systeme betreffen: – (Distributed) Denial-of-Service-Angriffe – Erfolgreiche Ransomware-Angriffe und andere Sabotageaktivitäten – Systemausfall – Naturkatastrophe* und Backupstrategien *(Control 5.2.8; Anforderungen (sollte); Dritter Unterpunkt: „+ Bei der Kontinuitätsplanung werden die folgenden Fälle berücksichtigt: – Alternative Kommunikationsstrategien, falls primäre Kommunikationsmittel nicht verfügbar sind – Alternative Speicherungsstrategien, falls primäre Mittel zur Speicherung nicht verfügbar sind – Alternative Energieversorgung und alternatives Netzwerk*“) deren Aktualität anhand von Überprüfungsprotokollen geprüft wird *(Control 5.2.8; Anforderungen (sollte); Vierter Unterpunkt: „+ Die Kontinuitätsplanung wird regelmäßig überprüft und aktualisiert“).*

Ein weiterer Teil der Prüfung dient der Sicherstellung, dass sich Backups in einem wiederherstellungsfähigen Zustand befinden *(Control 5.2.8; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Fünfter*

Unterpunkt: „+ Eine Sicherungs- und Wiederherstellungsstrategie für kritische IT-Dienste und Informationen ist definiert und umgesetzt. Die folgenden Aspekte werden berücksichtigt: – Backups sind vor unbefugter Änderung oder Löschung durch Schadsoftware geschützt. (I, A) -Backups sind vor unbefugtem Zugriff durch Schadsoftware oder deren Betreiber geschützt (C, I)“) und die im Backup befindlichen Daten nicht korrupt sind und über den gesamten Zeitraum der Vorhaltung vor Manipulation geschützt werden.

5.2.9: „Inwieweit wird die Sicherung und Wiederherstellung von Daten und IT-Diensten sichergestellt?“

Zur Sicherstellung von Sicherungen und Wiederherstellungsfähigkeit von Daten und IT-Diensten prüft der Auditor das Vorhandensein von Backupkonzepten für maßgebliche Systeme *(Control 5.2.9; Anforderungen (muss); Erster Unterpunkt: „+ Für die maßgeblichen IT-Systeme sind Backup-Konzepte vorhanden. Die folgenden Aspekte werden berücksichtigt: – Entsprechende Schutzmaßnahmen, um die Vertraulichkeit, Integrität und Verfügbarkeit für Daten-Backups sicherzustellen. Integrität und Verfügbarkeit für Daten-Backups sicherzustellen“)* und Wiederherstellungskonzepten für maßgebliche IT-Dienste, *(Control 5.2.9; Anforderungen (muss); Zweiter Unterpunkt: „+ Für die maßgeblichen IT-Dienste sind Wiederherstellungs-Konzepte vorhanden“)* die die Abhängigkeiten bei der Wiederherstellung berücksichtigen. *(Control 5.2.9; Anforderungen (sollte); Erster Unterpunkt: „+ Für jeden maßgeblichen IT-Dienst ist ein Sicherungs- und Wiederherstellungs-Konzept vorhanden. – Abhängigkeiten zwischen IT-Diensten und die Reihenfolge für die Wiederherstellung werden berücksichtigt“).* Weiter prüft der Auditor für Unternehmen bei denen Verfügbarkeit eine erhöhte Relevanz hat, Nachweise, dass methodische Überprüfungen der Konzepte Stattfinden, *(Control 5.2.9; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Sicherungs- und Wiederherstellungskonzepte werden in regelmäßigen Abständen methodisch überprüft. (A)“)* die allgemeine Wiederherstellungskapazität berücksichtigt und geprüft wird *(Control 5.2.9; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Zweiter Unterpunkt: „+ Die allgemeine Wiederherstellungskapazität wird berücksichtigt und geprüft (z. B. Stichprobenprüfung, Prüfsysteme) (I, A)“)* und dass folgende Aspekte Berücksichtigt werden *(Control 5.2.9; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Dritter Unterpunkt: „+ Sicherungs- und Wiederherstellungskonzepte berücksichtigen die folgenden Aspekte: (A) - Zielsetzung für den Wiederherstellungspunkt (RPO, en Recovery Point Objective). – Zeitvorgabe für die Wiederherstellung (RTO, en: Recovery Time Objective). – Erforderliche Ressourcen für die Wiederherstellung (unter Berücksichtigung der Kapazität und Leistung einschließlich Personal und Hardware). – Vermeidung von Überlastungsszenarien während der Wiederherstellung. – Angemessene räumliche Redundanz (z. B. separater Raum, separater Brandabschnitt, separates Rechenzentrum, separater Standort)“).*

4.11.4 Resümee

Die Anforderungen der NIS-2 Artikel 21 (1) i), Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen, sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments durch den Auditor auf Vorhandensein und Umsetzung geprüft.

4.12 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 21 (2) j)

4.12.1 Anforderung aus der NIS-2

NIS-2 Artikel 21 (2) Unterpunkt j) fordert die Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

4.12.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls die Erfüllung der Forderung nach NIS-2 Artikel 21 (2) j) geprüft:

- 1.6.3: „In welchem Maße ist die Organisation vorbereitet, mit Krisensituationen umzugehen?“
- 4.1.2: „Inwieweit wird der Zugang von Benutzern zu IT-Diensten und IT-Systemen gesichert?“
- 4.1.3: „Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewendet?“
- 5.1.2: „Inwieweit werden Informationen während der Übertragung geschützt?“
- 5.2.8: „Inwieweit ist eine Kontinuitätsplanung für IT-Dienste vorhanden?“

4.12.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.6.3: „In welchem Maße ist die Organisation vorbereitet, mit Krisensituationen umzugehen?“

Zur Sicherstellung einer Notfallkommunikation prüft der Auditor das Vorhandensein einer Krisenplanung, die die Kommunikationsmittel und eine Fallback-Ebene berücksichtigt *(Control 1.6.3; Anforderungen (sollte); Fünfter Unterpunkt: + Krisenmaßnahmen und -verfahren sind definiert und genehmigt. Die folgenden Aspekte werden berücksichtigt: – Ausnahmebefugnisse und Entscheidungsfindungsprozesse über den Krisenstab hinaus – Primäres und Backup-Kommunikationsmittel – Notfallbetriebsverfahren – Außergewöhnliche Organisationsstrukturen (z. B. Melden, Informationen sammeln, Entscheidungsfindung) – Außergewöhnliche Funktionsbereiche, Verantwortlichkeiten und Befugnisse (einschließlich Melden) – Außergewöhnliche Werkzeuge“)*.

4.1.2: „Inwieweit wird der Zugang von Benutzern zu IT-Diensten und IT-Systemen gesichert?“

Teil des Audits ist auch, dass der Auditor prüft, dass das Verfahren zur Benutzerauthentifizierung auf Basis einer Risikobewertung getroffen wurde, die unterschiedliche Angriffsszenarien berücksichtigt *(Control 4.1.2; Anforderungen (muss); Erster Unterpunkt: „+ Die Auswahl der Verfahren zur Benutzerauthentifizierung wurde auf Basis einer Risikobewertung getroffen. Mögliche Angriffsszenarien wurden berücksichtigt (z. B. direkte Zugänglichkeit über das Internet)“)* und das auf dem aktuellen Stand der Technik basiert *(Control 4.1.2; Anforderungen (muss); Zweiter Unterpunkt: „+ Für die Benutzerauthentifizierung werden Verfahren auf dem aktuellen Stand der Technik angewendet“)*. Außerdem wird geprüft, dass die Verfahren auf Grundlage der geschäftsbezogenen und sicherheitsrelevanten Anforderungen festgelegt und umgesetzt *(Control 4.1.2; Anforderungen (sollte); Erster Unterpunkt: „ + Die Verfahren zur Benutzerauthentifizierung werden auf der Grundlage der geschäftsbezogenen und sicherheitsrelevanten Anforderungen festgelegt und umgesetzt: – Benutzer werden mindestens mittels starker Passwörter entsprechend dem aktuellen Stand der Technik authentifiziert“),* der Kritikalität der Konten angepasst *(Control 4.1.2; Anforderungen (sollte); Zweiter Unterpunkt: „+ Es werden höherwertige Verfahren zur Authentifizierung von privilegierten Benutzerkonten angewendet (z. B. Privilegiertes Zugangsmanagement, 2-Faktor-Authentifizierung)“)* und nach Bedarf durch weitere Maßnahmen ergänzt wurden *(Control 4.1.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Abhängig von der Risikobewertung wurden das Authentifizierungsverfahren und die Zugriffskontrolle durch ergänzende Maßnahmen verstärkt (z. B. dauerhafte Zugriffsüberwachung hinsichtlich Unregelmäßigkeiten oder Einsatz einer starken Authentifizierung, automatische Abmeldung, Sperrung bei Inaktivität oder Schutz vor Brute-Force-Angriffen). (C, I, A)“)*.

4.1.3. „Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewendet?“

Weiterer Teil des Assessments ist die Prüfung, dass der Zugang zu Informationen und IT-Systemen über validierte Benutzerkonten erfolgt und dass Anmeldeinformationen geschützt werden und die Rückverfolgbarkeit von Transaktionen und Zugriffen sichergestellt wird. Hierzu prüft der Auditor, dass Benutzerkonten über ihren Lebenszyklus verwaltet werden *(Control 4.1.3; Anforderungen (muss); Erster Unterpunkt: „+ Die Erstellung,*

Änderung und Löschung von Benutzerkonten wird durchgeführt"), (Control 4.1.3; Anforderungen (muss); Vierter Unterpunkt: „+ Benutzerkonten werden unmittelbar nachdem der Benutzer aus der Organisation ausgeschieden ist oder diese verlassen hat (z. B. bei Beendigung des Arbeitsverhältnisses) gesperrt") und dass eine regelmäßige Überprüfung auf Aktualität der Zuteilung stattfindet *(Control 4.1.3; Anforderungen (muss); Fünfter Unterpunkt: „+ Benutzerkonten werden in regelmäßigen Abständen überprüft")*. Weiter prüft der Auditor, dass die Konten personalisiert werden *(Control 4.1.3; Anforderungen (muss); Zweiter Unterpunkt: „+ Es werden eindeutige und personalisierte Benutzerkonten verwendet")* oder im Bedarfsfall die Vergabe von Sammelkonten einer Regelung unterliegt *(Control 4.1.3; Anforderungen (muss); Dritter Unterpunkt: „+ Die Nutzung von „Sammel-Konten" ist geregelt (z. B. auf Fälle beschränkt, bei denen die Rückverfolgbarkeit von Aktionen verzichtbar ist)")*. Die sichere Übermittlung der Konteninformationen *(Control 4.1.3; Anforderungen (muss); Sechster Unterpunkt: „+ Es erfolgt eine sichere Zustellung der Anmeldeinformationen an den Benutzer"),* die Sicherstellung der Geheimhaltung der Anmeldeinformation *(Control 4.1.3; Anforderungen (muss); Achter Unterpunkt: „+ Die Anmeldeinformationen (z. B. Passwörter) eines personalisierten Benutzerkontos dürfen nur dem zugeordneten Benutzer bekannt sein")* und die zugehörigen Verhaltensweisen *(Control 4.1.3; Anforderungen (muss); Siebter Unterpunkt: „+ Eine Richtlinie zum Umgang mit Anmeldeinformationen ist definiert und umgesetzt. Die folgenden Aspekte werden berücksichtigt: – 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)")* werden vom Auditor ebenfalls geprüft.

In Bezug auf Benutzerprofile prüft der Auditor, dass ein Standardprofil besteht *(Control 4.1.3; Anforderungen (sollte); Erster Unterpunkt: „+ Ein Basis-Benutzerprofil mit minimalen Zugriffsrechten und Funktionalitäten ist vorhanden und wird angewendet")*. Außerdem prüft er, dass Herstellerseitige Standardkonten deaktiviert werden *(Control 4.1.3; Anforderungen (sollte); Zweiter Unterpunkt: „+ Herstellerseitig vorgegebene Standardkonten und -Passwörter werden deaktiviert (z. B. durch Sperrung oder Änderung des Passworts)")*, dass es einen definierten Prozess zur Erstellung von Konten gibt *(Control 4.1.3; Anforderungen (sollte); Vierter Unterpunkt: „+ Die Einrichtung von Benutzerkonten unterliegt einem Genehmigungsprozess (4-Augen-Grundsatz)")* und dass die Einrichtung von Konten durch eine autorisierte Stelle erfolgt *(Control 4.1.3; Anforderungen (sollte); Dritter Unterpunkt: „+ Die Einrichtung von Benutzerkonten erfolgt durch die verantwortliche Stelle oder wird durch diese autorisiert")*. Er prüft weiterhin, dass Sperr- und Löschfristen definiert *(Control 4.1.3; Anforderungen (sollte); Sechster Unterpunkt: „+ Sperr- und Löschfristen für Benutzerkonten sind definiert")* und auch bei Dienstleisterkonten umgesetzt werden *(Control 4.1.3; Anforderungen (sollte); Fünfter Unterpunkt: „+ Benutzerkonten von Dienstleistern werden nach Abschluss von deren Aufgabe gesperrt")*. Der Auditor prüft auch, dass die Verwendung von Standard-Passwörtern verhindert wird *(Control 4.1.3; Anforderungen (sollte); Siebter Unterpunkt: „+ Die Verwendung von Standard-Passworten wird technisch verhindert")*, dass die interaktive Anmeldung bei Dienste-Konten technisch verhindert wird, *(Control 4.1.3; Anforderungen (sollte); Zehnter Unterpunkt: „+ Die interaktive Anmeldung bei Dienstkonten (technischen Konten) wird technisch verhindert"),* dass beim Einsatz starker Authentifizierung das Medium sicher verwendet wird *(Control 4.1.3; Anforderungen (sollte); Achter Unterpunkt: „+ Beim Einsatz einer starken Authentifizierung wird das Medium (z. B. Faktor Besitz) sicher verwendet")* und schließlich, dass eine regelmäßige Überprüfung der Konten stattfindet *(Control 4.1.3; Anforderungen (sollte); Neunter Unterpunkt: „+ Es findet eine Überprüfung der Benutzerkonten in regelmäßigen Abständen statt. Dazu gehören auch Benutzerkonten in IT-Systemen von Kunden")*.

5.1.2 „Inwieweit werden Informationen während der Übertragung geschützt?"

Zur Sicherstellung des Schutzes von Informationen bei deren Übertragung prüft der Auditor, dass zur Übertragung genutzten Netzwerkdienste identifiziert und dokumentiert sind *(Control 5.1.2; Anforderungen (muss); Erster Unterpunkt: + Die zur Übertragung von Informationen genutzten Netzwerkdienste sind identifiziert und*

dokumentiert“), dass Richtlinien und Verfahren zur Nutzung von Netzwerkdiensten definiert und umgesetzt sind *(Control 5.1.2; Anforderungen (muss); Zweiter Unterpunkt: „+ Richtlinien und Verfahren entsprechend den Klassifizierungsvorgaben zur Nutzung von Netzwerkdiensten sind definiert und umgesetzt“)* und dass Maßnahmen zum Schutz übertragener Inhalte umgesetzt sind *(Control 5.1.2; Anforderungen (muss); Dritter Unterpunkt: + Maßnahmen zum Schutz von übertragenen Inhalten vor unberechtigtem Zugriff sind umgesetzt“)*. Außerdem ist Teil der Prüfung, dass Informationen in verschlüsselter Form transportiert oder übertragen werden *(Control 5.1.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: + Informationen werden in verschlüsselter Form transportiert oder übertragen: (C) - Wenn eine Verschlüsselung nicht möglich ist, müssen Informationen durch ähnlich wirksame Maßnahmen geschützt werden“) (Control 5.1.2; Anforderungen (sollte); Zweiter Unterpunkt: „+ Der elektronische Datenaustausch erfolgt entsprechend der jeweiligen Klassifizierung durch Inhalts- oder Transportverschlüsselung“)* und dass sichergestellt ist, dass die verwendeten Adressen korrekt sind *(Control 5.1.2; Anforderungen (sollte); Erster Unterpunkt: „+ Maßnahmen zur Sicherstellung der korrekten Adressen und des korrekten Transports von Informationen sind umgesetzt“).* Weiter wird vom Auditor geprüft, dass Fernzugriffsverbindungen über angemessene Sicherheitsmerkmale und -fähigkeiten verfügen *(Control 5.1.2; Anforderungen (sollte); Dritter Unterpunkt: „+ Fernzugriffsverbindungen werden dahingehend verifiziert, dass sie über angemessene Sicherheitsmerkmale (z. B. Verschlüsselung, Gewähren und Beenden des Zugriffs) und -fähigkeiten verfügen“).*

5.2.8: „Inwieweit ist eine Kontinuitätsplanung für IT-Dienste vorhanden?“

Der Auditor prüft, ob eine Kontinuitätsplanung für IT-Dienste *(Control 5.2.8; Anforderungen (muss); Erster Unterpunkt: „+ Kritische IT-Dienste werden identifiziert, und die geschäftlichen Auswirkungen werden betrachtet“)* und IT Systeme *(Control 5.2.8; Anforderungen (sollte); Erster Unterpunkt: „Kritische IT-Systeme werden identifiziert – die maßgeblichen Systeme sind nach dem entsprechenden Schutzbedarf klassifiziert – angemessene und geeignete Sicherheitsmaßnahmen werden umgesetzt)* besteht, die Backupstrategien berücksichtigt *(Control 5.2.8; Anforderungen (sollte); Dritter Unterpunkt: „+ Bei der Kontinuitätsplanung werden die folgenden Fälle berücksichtigt: – Alternative Kommunikationsstrategien, falls primäre Kommunikationsmittel nicht verfügbar sind – Alternative Speicherungsstrategien, falls primäre Mittel zur Speicherung nicht verfügbar sind – Alternative Energieversorgung und alternatives Netzwerk*“).

4.12.4 Resümee

Die Anforderungen der NIS-2 Artikel 21 (1) j), die Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments durch den Auditor auf Vorhandensein und Umsetzung geprüft.

4.13 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 21 (4)

4.13.1 Anforderung aus der NIS-2

NIS-2 Artikel 21 (4) fordert, dass eine Einrichtung, die feststsellt, dass sie den genannten Maßnahmen aus Artikel 21; Absatz 2; a bis j (Kapitel 4.3 bis 4.12 oben) nicht nachkommt, unverzüglich alle erforderlichen, angemessenen und verhältnismäßigen Korrekturmaßnahmen ergreift.

4.13.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls die Erfüllung der Forderung nach NIS-2 Artikel 21 (4) geprüft:

- 1.5.1: „Inwieweit wird die Einhaltung der Informationssicherheit in Verfahren und Prozessen sichergestellt?“
- 1.5.2: „Inwieweit wird das ISMS von einer unabhängigen Stelle überprüft?“

4.13.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.5.1 „Inwieweit wird die Einhaltung der Informationssicherheit in Verfahren und Prozessen sichergestellt?“

Im TISAX-Assessment prüft der Auditor die Einhaltung der Informationssicherheit in Verfahren und Prozessen *(Control 1.5.1; Anforderungen (muss); Erster Unterpunkt: + Die Einhaltung von Richtlinien wird organisationsweit überprüft)*. Er prüft weiterhin, dass die Kontrolle der Einhaltung der Informationssicherheit in Verfahren und Prozessen in regelmäßigen Abständen *(Control 1.5.1; Anforderungen (muss); Zweiter Unterpunkt: + Prüfungen von Richtlinien und Verfahren der Informationssicherheit werden regelmäßig durchgeführt)* nach einem definierten Plan *(Control 1.5.1; Anforderungen (sollte); Erster Unterpunkt: + Ein Plan über Inhalt und Rahmenbedingungen (Zeitplan, Umfang, Kontrollen) der durchzuführenden Überprüfungen liegt vor)* erfolgt und nachvollziehbar dokumentiert wird *(Control 1.5.1; Anforderungen (muss); Fünfter Unterpunkt: + Die Ergebnisse der durchgeführten Überprüfungen werden aufgezeichnet und aufbewahrt)*. Außerdem prüft er, dass die Einhaltung von Anforderungen der Informationssicherheit regelmäßig kontrolliert wird *(Control 1.5.1; Anforderungen (muss); Vierter Unterpunkt: „+ Die Einhaltung von Anforderungen der Informationssicherheit (z. B. technische Vorgaben) werden in regelmäßigen Abständen überprüft“)* und dass bei nicht-Konformitäten Korrekturmaßnahmen eingeleitet und verfolgt werden *(Control 1.5.1; Anforderungen (muss); Dritter Unterpunkt: „+ Korrekturmaßnahmen für mögliche Nicht-Konformitäten (Abweichungen) werden eingeleitet und verfolgt“).*

1.5.2 „Inwieweit wird das ISMS von einer unabhängigen Stelle überprüft?“

Der Auditor prüft ebenfalls, dass eine Prüfung durch eine unabhängige Stelle durchgeführt wird, die in regelmäßigen Abständen und bei wesentlichen Änderungen stattfindet *(Control 1.5.2; Anforderungen (muss); Erster Unterpunkt: + Prüfungen der Informationssicherheit werden von einer unabhängigen und sachkundigen Stelle in regelmäßigen Abständen und bei wesentlichen Änderungen durchgeführt)* und dass deren Ergebnisse dokumentiert und an die Organisationsleitung berichtet werden*(Control 1.5.2; Anforderungen (sollte); Erster Unterpunkt: + Die Ergebnisse der durchgeführten Prüfungen werden dokumentiert und an die Organisationsleitung berichtet)*. Teil seiner Prüfung ist auch, sicherzustellen, dass für mögliche Abweichungen Korrekturmaßnahmen eingeleitet und verfolgt werden (*Control 1.5.2; Anforderungen (muss); Zweiter Unterpunkt: + Korrekturmaßnahmen für mögliche Abweichungen werden eingeleitet und verfolgt).*

4.13.4 Resümee

Die Anforderungen der NIS-2 Artikel 21 (4), eine Einrichtung, die feststellt, dass sie den genannten Maßnahmen aus Artikel 21; Absatz 2; a bis j (Kapitel 4.3 bis 4.12 oben) nicht nachkommt, ergreift unverzüglich alle erforderlichen, angemessenen und verhältnismäßigen Korrekturmaßnahmen, sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments durch den Auditor auf Vorhandensein und Umsetzung geprüft.

Unter Berücksichtigung der Verpflichtung für die Betreiber Kritischer Infrastrukturen im Sinne des IT-Sicherheitsgesetzes gemäß BSI-Gesetz (BSIG) und BSI-Kritisverordnung, alle zwei Jahre einen Nachweis zur Erfüllung der

Anforderungen vorzulegen und dem Risikobasierten Ansatz der NIS-2-Richtlinie wird ein Dreijahreszyklus als angemessen angesehen.

5 NIS-2 Artikel 23

5.1 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 23 (1)

5.1.1 Anforderung aus der NIS-2

NIS-2 Artikel 23 (1) verlangt, dass wesentliche und wichtige Einrichtungen ihrem CSIRT oder gegebenenfalls ihrer zuständigen Behörde gemäß Absatz 4 unverzüglich über jeden Sicherheitsvorfall unterrichten, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste gemäß Absatz 3 (erheblicher Sicherheitsvorfall) hat. Gegebenenfalls unterrichten die betreffenden Einrichtungen die Empfänger ihrer Dienste unverzüglich über diese erheblichen Sicherheitsvorfälle, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten. Außerdem wird gefordert, dass unter anderem alle Informationen übermittelt werden, die es dem CSIRT oder gegebenenfalls der zuständigen Behörde ermöglichen zu ermitteln, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat.

5.1.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls die Erfüllung der Forderung nach NIS-2 Artikel 23 (1) geprüft:

- 1.6.1: „Inwieweit werden für die Informationssicherheit relevante Ereignisse oder Beobachtungen gemeldet?“
- 1.6.2: „Inwieweit werden gemeldete Sicherheitsereignisse verwaltet?“

5.1.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.6.1: „Inwieweit werden für die Informationssicherheit relevante Ereignisse oder Beobachtungen gemeldet?“

Der Auditor prüft, ob definiert ist, an welchen Parametern sich ein berichtspflichtiges Ereignis messen lässt *(Control 1.6.1; Anforderungen (muss); Erster Unterpunkt: „+ Es ist eine Definition für ein berichtspflichtiges Sicherheitsereignis oder eine berichtspflichtige sicherheitsrelevante Beobachtung vorhanden, die den Mitarbeitern und maßgeblichen Beteiligten bekannt ist. Die folgenden Aspekte werden berücksichtigt: –Ereignisse und Beobachtungen in Bezug auf Personal (z. B. Verfehlung/Fehlverhalten) – Ereignisse und Beobachtungen in Bezug auf die physische Sicherheit (z. B. Einbruch, Diebstahl, unbefugter Zugang zu Sicherheitszonen, Schwachstellen in den Sicherheitszonen) – Ereignisse und Beobachtungen in Bezug auf die IT und Cybersicherheit (z. B. anfällige IT-Systeme, erkannte erfolgreiche oder nicht erfolgreiche Angriffe) – Ereignisse und Beobachtungen in Bezug auf Lieferanten und andere Geschäftspartner (z. B. alle Vorfälle, die sich negativ auf die Sicherheit der eigenen Organisation auswirken können“)* und dass die der Schwere des Ereignisses angepassten Mechanismen zur Meldung bekannt sind *(Control 1.6.1; Anforderungen (muss); Zweiter Unterpunkt: + Es sind angemessene Mechanismen für die Meldung von Sicherheitsereignissen auf der Grundlage wahrgenommener Risiken festgelegt, die umgesetzt werden und allen maßgeblichen möglichen meldenden Personen bekannt sind“)*. Weiter wird geprüft, dass die dafür notwendigen Meldekanäle zur Verfügung stehen *(Control 1.6.1; Anforderungen (muss); Dritter Unterpunkt: „+ Es sind geeignete Kommunikationskanäle für die Ereignisse meldenden Personen vorhanden“).* Ein weiterer Teil der Prüfung ist die Sicherstellung, dass Meldewege zur Verfügung stehen, die sich am Schweregrad des Vorfalles orientieren *(Control 1.6.1; Anforderungen (sollte); Zweiter Unterpunkt: „+ Je nach dem*

wahrgenommenen Schweregrad stehen unterschiedliche Meldewege zur Verfügung (d. h. Echtzeitkommunikation für signifikante Ereignisse/Notfälle zusätzlich zu asynchronen Mechanismen wie Tickets oder E-Mail).“) und dass die Meldeverfahren und -arten allen maßgeblich Meldenden zugänglich sind *(Control 1.6.1; Anforderungen (sollte); Fünfter Unterpunkt: „+ Verfahren zur Meldung von Vorfällen und Informationen darüber, wie diese zu melden sind, sind für alle maßgeblichen Meldenden zugänglich“).*

1.6.2: „Inwieweit werden gemeldete Sicherheitsereignisse verwaltet?“

Die Prüfung beinhaltet die Berücksichtigung von Kontaktverfahren auf der Grundlage der Art und Priorität *(Control 1.6.2; Anforderungen (sollte); Zweiter Unterpunkt: „+Verantwortlichkeiten für den Umgang mit Ereignissen sind auf der Grundlage der Ereigniskategorie definiert und zugewiesen. Die folgenden Aspekte werden berücksichtigt: – Koordinierung von Vorfällen und Schwachstellen über mehrere Kategorien – Qualifikation und Ressourcen – Kontaktverfahren auf der Grundlage der Art und Priorität (z. B. nicht-zeitkritische Kommunikation, zeitkritische Kommunikation, Notfallkommunikation) – Abwesenheits-management*“).

Außerdem wird geprüft, dass die Meldepflichten und die zugehörigen Kontaktinformationen bekannt sind *(Control 1.6.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Dritter Unterpunkt: „+ Gesetzliche, regulatorische und vertragliche Meldepflichten und entsprechende Kontaktinformationen sind bekannt. (C, I, A)“)* und eine Kommunikationsstrategie vorhanden ist, die die Adressaten, Meldezeiträume und Meldeform berücksichtigt *(Control 1.6.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Vierter Unterpunkt: „+ Eine Kommunikationsstrategie für sicherheitsbezogene Ereignisse ist vorhanden. Die folgenden Aspekte werden berücksichtigt: (C, I, A) – Mit wem zu kommunizieren ist (z. B. Gesellschafter, betroffene Geschäftspartner und Kunden, weitere Gesellschafter, allgemeine Öffentlichkeit) – Wann zu kommunizieren ist – Verantwortlichkeiten für die Kommunikation – Ermächtigung und Freigabe der Kommunikation – Gesetzliche und regulatorische Einschränkungen der Kommunikation – Was zu kommunizieren ist (z. B. vorbereitete Vorlagen und Bausteine für bestimmte Szenarien) – Wie zu kommunizieren ist (z. B. Kommunikationskanäle)“).*

5.1.4 Resümee

Die Anforderungen der NIS-2 Artikel 23 (1) zur unverzüglichen Unterrichtung über jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste (erheblicher Sicherheitsvorfall) hat und die unverzügliche Unterrichtung der Empfänger ihrer Dienste über diese erheblichen Sicherheitsvorfälle, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten, im Bedarfsfall, außerdem die Forderung, dass unter anderem alle Informationen übermittelt werden, die es dem CSIRT oder gegebenenfalls der zuständigen Behörde ermöglichen zu ermitteln, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat, werden durch den ISA6-Prüfstandard und die darin geprüften Controls nahezu voll erfüllt.
Eine Ausnahme bildet hier die Weitergabe zu grenzüberschreitenden Auswirkungen, die so explizit nicht innerhalb des ISA gefordert wird. Hier wurde bereits definiert, dass die Notfallkommunikation, um die Spezifikationen aus der NIS-2 zu erweitern ist. Nach Berücksichtigung dieser Erweiterung sind die Anforderungen voll erfüllt.

5.2 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 23 (2)

5.2.1 Anforderung aus der NIS-2

NIS-2 Artikel 23 (2) fordert, dass wesentliche und wichtige Einrichtungen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mitteilen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Einrichtungen informieren diese Empfänger gegebenenfalls auch über die erhebliche Cyberbedrohung selbst.

5.2.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls die Erfüllung der Forderung nach NIS-2 Artikel 23 (2) geprüft:

- 1.6.2: „Inwieweit werden gemeldete Sicherheitsereignisse verwaltet?“

5.2.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.6.2: „Inwieweit werden gemeldete Sicherheitsereignisse verwaltet?“

Die Prüfung des Umgangs mit Meldungen beinhaltet die Kategorisierung nach Klasse, Kategorie und Schweregrad *(Control 1.6.2; Anforderungen (sollte); Erster Unterpunkt: „+ Während der Bearbeitung werden gemeldete Ereignisse kategorisiert (z. B. nach der Verantwortung in das Personal, die physische Sicherheit und die Cybersicherheit betreffende Ereignisse), qualifiziert (z. B. nicht sicherheitsrelevant, Beobachtung, vorgeschlagene Verbesserung der Sicherheit, Sicherheitsschwachstelle, Sicherheitsvorfall) und priorisiert (z. B. niedriger, mittlerer, hoher, kritischer Schweregrad)“)* und die der Klasse zugewiesene Reaktion in einem definierten Zeitrahmen *(Control 1.6.2; Anforderungen (muss); Erste zwei Unterpunkte: „+ Gemeldete Ereignisse werden ohne unnötige Verzögerung bearbeitet. + Eine angemessene Reaktion auf gemeldete Sicherheitsereignisse ist sichergestellt“)* unter Einbeziehung der notwendigen Verantwortlichen *(Control 1.6.2; Anforderungen (sollte); Zweiter Unterpunkt: „+Verantwortlichkeiten für den Umgang mit Ereignissen sind auf der Grundlage der Ereigniskategorie definiert und zugewiesen. Die folgenden Aspekte werden berücksichtigt: – Koordinierung von Vorfällen und Schwachstellen über mehrere Kategorien – Qualifikation und Ressourcen – Kontaktverfahren auf der Grundlage der Art und Priorität (z. B. nicht-zeitkritische Kommunikation, zeitkritische Kommunikation, Notfallkommunikation) – Abwesenheits-management*“).

Außerdem wird geprüft, dass die Meldepflichten und die zugehörigen Kontaktinformationen bekannt sind *(Control 1.6.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Dritter Unterpunkt: „+ Gesetzliche, regulatorische und vertragliche Meldepflichten und entsprechende Kontaktinformationen sind bekannt. (C, I, A)“)* und eine Kommunikationsstrategie vorhanden ist, die die Adressaten, Meldezeiträume und Meldeform berücksichtigt *(Control 1.6.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Vierter Unterpunkt: „+ Eine Kommunikationsstrategie für sicherheitsbezogene Ereignisse ist vorhanden. Die folgenden Aspekte werden berücksichtigt: (C, I, A) – Mit wem zu kommunizieren ist (z. B. Gesellschafter, betroffene Geschäftspartner und Kunden, weitere Gesellschafter, allgemeine Öffentlichkeit) – Wann zu kommunizieren ist – Verantwortlichkeiten für die Kommunikation – Ermächtigung und Freigabe der Kommunikation – Gesetzliche und regulatorische Einschränkungen der Kommunikation – Was zu kommunizieren ist (z. B. vorbereitete Vorlagen und Bausteine für bestimmte Szenarien) – Wie zu kommunizieren ist (z. B. Kommunikationskanäle)“).*

5.2.4 Resümee

Die Anforderungen der NIS-2 Artikel 23 (2), das wesentliche und wichtige Einrichtungen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mitteilen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können und dass die Einrichtungen diese Empfänger gegebenenfalls auch über die erhebliche Cyberbedrohung selbst informieren, sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments durch den Auditor auf Vorhandensein und Umsetzung geprüft. Weiter beinhaltet die Prüfung des ISA-Anforderungskataloges durch den Auditor die Prüfung der Einhaltung von Meldezeiten und Meldewegen. Die expliziten Kontaktinformationen, Meldewege und -Sprachen müssen durch die Unternehmen nach deren Veröffentlichung durch die Mitgliedsstaaten der EU in das BCM aufgenommen werden. Die Prüfung dieser

Information auf Vorhandensein kann durch den Prüfer nicht gewährleitet werden, da die anzulegenden Informationen unternehmensspezifisch sind und sich dadurch in mannigfaltiger Ausprägung darstellen können.

5.3 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 23 (3)

5.3.1 Anforderung aus der NIS-2

NIS-2 Artikel 23 (3) beschreibt einen Sicherheitsvorfall als erheblich, wenn:

- er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann
- er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann

5.3.2 Resümee

Die Anforderungen der NIS-2 Artikel 23 (3) sind rein informativ zur Spezifikation eines erheblichen Sicherheitsvorfalls und stellen damit keinen prüfbaren Inhalt dar.

5.4 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 23 (4)

5.4.1 Anforderung aus der NIS-2

NIS-2 Artikel 23 (4) fordert, dass betreffende Einrichtungen dem CSIRT oder gegebenenfalls der zuständigen Behörde für die Zwecke der Meldung nach Absatz 1 Folgendes übermitteln:

a) unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Frühwarnung, in der gegebenenfalls angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;

b) unverzüglich, in jedem Fall aber innerhalb von 72 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Meldung über den Sicherheitsvorfall, in der gegebenenfalls die unter Buchstabe a genannten Informationen aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;

c) auf Ersuchen eines CSIRT oder gegebenenfalls der zuständigen Behörde einen Zwischenbericht über relevante Statusaktualisierungen;

d) spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Buchstabe b einen Abschlussbericht, das folgende Inhalte enthält:

   i) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;

ii) Angaben zur Art der Bedrohung bzw. zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;

iii) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;

iv) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls;

e) im Falle eines andauernden Sicherheitsvorfalls zum Zeitpunkt der Vorlage des Abschlussberichts gemäß Buchstabe d stellen die Mitgliedstaaten sicher, dass die betreffenden Einrichtungen zu diesem Zeitpunkt einen Fortschrittsbericht und einen Abschlussbericht innerhalb eines Monats nach Behandlung des Sicherheitsvorfalls vorlegen.

Abweichend von Unterabsatz 1 Buchstabe b unterrichtet ein Vertrauensdiensteanbieter das CSIRT oder gegebenenfalls die zuständige Behörde in Bezug auf erhebliche Sicherheitsvorfälle, die sich auf die Erbringung seiner Vertrauensdienste auswirken, unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls.

5.4.2 Anwendbare Kontrollfragen des ISA6

Im TISAX-Assessment nach dem aktuellen Standard ISA6 wird nach den folgenden Controls die Erfüllung der Forderung nach NIS-2 Artikel 23 (4) geprüft:

- 1.6.1: „Inwieweit werden für die Informationssicherheit relevante Ereignisse oder Beobachtungen gemeldet?“
- 1.6.2: „Inwieweit werden gemeldete Sicherheitsereignisse verwaltet?“
- 1.6.3: „In welchem Maße ist die Organisation vorbereitet, mit Krisensituationen umzugehen?“

5.4.3 Detaillierte Anforderungen innerhalb der Kontrollfragen des ISA6

1.6.1: „Inwieweit werden für die Informationssicherheit relevante Ereignisse oder Beobachtungen gemeldet?“

Der Auditor prüft, ob definiert ist, an welchen Parametern sich ein berichtspflichtiges Ereignis messen lässt *(Control 1.6.1; Anforderungen (muss); Erster Unterpunkt: „+ Es ist eine Definition für ein berichtspflichtiges Sicherheitsereignis oder eine berichtspflichtige sicherheitsrelevante Beobachtung vorhanden, die den Mitarbeitern und maßgeblichen Beteiligten bekannt ist. Die folgenden Aspekte werden berücksichtigt: –Ereignisse und Beobachtungen in Bezug auf Personal (z. B. Verfehlung/Fehlverhalten) – Ereignisse und Beobachtungen in Bezug auf die physische Sicherheit (z. B. Einbruch, Diebstahl, unbefugter Zugang zu Sicherheitszonen, Schwachstellen in den Sicherheitszonen) – Ereignisse und Beobachtungen in Bezug auf die IT und Cybersicherheit (z. B. anfällige IT-Systeme, erkannte erfolgreiche oder nicht erfolgreiche Angriffe) – Ereignisse und Beobachtungen in Bezug auf Lieferanten und andere Geschäftspartner (z. B. alle Vorfälle, die sich negativ auf die Sicherheit der eigenen Organisation auswirken können“)* und dass die der Schwere des Ereignisses angepassten Mechanismen zur Meldung bekannt sind *(Control 1.6.1; Anforderungen (muss); Zweiter Unterpunkt: + Es sind angemessene Mechanismen für die Meldung von Sicherheitsereignissen auf der Grundlage wahrgenommener Risiken festgelegt, die umgesetzt werden und allen maßgeblichen möglichen meldenden Personen bekannt sind“)*. Ein weiterer Teil der Prüfung ist die Sicherstellung, dass Meldewege zur Verfügung stehen, die sich am Schweregrad des Vorfalles orientieren *(Control 1.6.1; Anforderungen (sollte); Zweiter Unterpunkt: „+ Je nach dem wahrgenommenen Schweregrad stehen unterschiedliche Meldewege zur Verfügung (d. h. Echtzeitkommunikation für signifikante Ereignisse/Notfälle zusätzlich zu asynchronen Mechanismen wie Tickets oder E-Mail).“)*, dass die Meldeverfahren und -arten allen maßgeblich Meldenden zugänglich sind *(Control 1.6.1; Anforderungen (sollte); Fünfter Unterpunkt: „+ Verfahren zur Meldung von Vorfällen und Informationen darüber, wie diese zu melden sind, sind für alle*

maßgeblichen Meldenden zugänglich“) und dass eine Verpflichtung zur Meldung solcher Ereignisse besteht *(Control 1.6.1; Anforderungen (sollte); Dritter Unterpunkt: „+ Mitarbeiter sind verpflichtet, relevante Ereignisse zu melden und sind entsprechend geschult“)*. Außerdem wird geprüft, dass ein Verfahren für Rückmeldungen etabliert ist *(Control 1.6.1; Anforderungen (sollte); Sechter Unterpunkt: „+ Ein Verfahren für Rückmeldungen an die Meldenden ist etabliert“*.

1.6.2: „Inwieweit werden gemeldete Sicherheitsereignisse verwaltet?“

Die Prüfung des Umgangs mit Meldungen beinhaltet die Kategorisierung nach Klasse, Kategorie und Schweregrad *(Control 1.6.2; Anforderungen (sollte); Erster Unterpunkt: „+ Während der Bearbeitung werden gemeldete Ereignisse kategorisiert (z. B. nach der Verantwortung in das Personal, die physische Sicherheit und die Cybersicherheit betreffende Ereignisse), qualifiziert (z. B. nicht sicherheitsrelevant, Beobachtung, vorgeschlagene Verbesserung der Sicherheit, Sicherheitsschwachstelle, Sicherheitsvorfall) und priorisiert (z. B. niedriger, mittlerer, hoher, kritischer Schweregrad)“)* und die der Klasse zugewiesene Reaktion in einem definierten Zeitrahmen *(Control 1.6.2; Anforderungen (muss); Erste zwei Unterpunkte: „+ Gemeldete Ereignisse werden ohne unnötige Verzögerung bearbeitet. + Eine angemessene Reaktion auf gemeldete Sicherheitsereignisse ist sichergestellt“)* unter Einbeziehung der notwendigen Verantwortlichen *(Control 1.6.2; Anforderungen (sollte); Zweiter Unterpunkt: „+Verantwortlichkeiten für den Umgang mit Ereignissen sind auf der Grundlage der Ereigniskategorie definiert und zugewiesen. Die folgenden Aspekte werden berücksichtigt: – Koordinierung von Vorfällen und Schwachstellen über mehrere Kategorien – Qualifikation und Ressourcen – Kontaktverfahren auf der Grundlage der Art und Priorität (z. B. nicht-zeitkritische Kommunikation, zeitkritische Kommunikation, Notfallkommunikation) – Abwesenheits-management*“).

Außerdem wird geprüft, dass die Meldepflichten und die zugehörigen Kontaktinformationen bekannt sind *(Control 1.6.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Dritter Unterpunkt: „+ Gesetzliche, regulatorische und vertragliche Meldepflichten und entsprechende Kontaktinformationen sind bekannt. (C, I, A)“)* und eine Kommunikationsstrategie vorhanden ist, die die Adressaten, Meldezeiträume und Meldeform berücksichtigt *(Control 1.6.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Vierter Unterpunkt: „+ Eine Kommunikationsstrategie für sicherheitsbezogene Ereignisse ist vorhanden. Die folgenden Aspekte werden berücksichtigt: (C, I, A) – Mit wem zu kommunizieren ist (z. B. Gesellschafter, betroffene Geschäftspartner und Kunden, weitere Gesellschafter, allgemeine Öffentlichkeit) – Wann zu kommunizieren ist – Verantwortlichkeiten für die Kommunikation – Ermächtigung und Freigabe der Kommunikation – Gesetzliche und regulatorische Einschränkungen der Kommunikation – Was zu kommunizieren ist (z. B. vorbereitete Vorlagen und Bausteine für bestimmte Szenarien) – Wie zu kommunizieren ist (z. B. Kommunikationskanäle)“).* Weiter wird geprüft, dass Höchstreaktionszeiten definiert *(Control 1.6.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Erster Unterpunkt: „+ Auf der Grundlage von Klasse, Kategorie und Schweregrad sind Höchstreaktionszeiten definiert. (C, I, A)“)* und deren Einhaltung kontrolliert und im Bedarfsfalle eskaliert wird *(Control 1.6.2; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Zweiter Unterpunkt: „+ Ereignisse, die nicht entsprechend ihrer Priorität angemessen bearbeitet wurden, werden eskaliert. (C, I, A) – Es sind Bedingungen und Schwellenwerte, wie z. B. Höchstreaktionszeiten, vor der Eskalation definiert – Mechanismen, Prozesse und Kontakte für die Eskalation sind festgelegt – Eskalationswege bis zur obersten Leitung der Organisation sind festgelegt“).*

1.6.3: „In welchem Maße ist die Organisation vorbereitet, mit Krisensituationen umzugehen?“

In Bezug auf Krisensituationen wird bei Organisationen, für die die Verfügbarkeit wesentlich ist, geprüft, dass notwendige Ressourcen zur Kommunikation identifiziert sind *(Control 1.6.3; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Zweiter Unterpunkt: „+ Notwendige Ressourcen und Informationen zur Bewältigung der Krise (z. B. Kommunikationsinfrastruktur, Verfügbarkeit notwendiger Informationen wie z. B. Kontaktinformationen und maßgebliche Risiken in verschiedenen Krisensituationen) sind identifiziert. (A) - Geeignete Maßnahmen zur Sicherstellung der Verfügbarkeit der Infrastruktur oder eine Ausweichplanung sowie Informationen, die verschiedene Krisenszenarien berücksichtigen, sind vorhanden“)* und eine Kommunikationsstrategie vorhanden ist *(Control 1.6.3; Anforderungen (Zusatzanforderungen bei hohem Schutzbedarf); Dritter Unterpunkt: „+ Es ist eine Kommunikationsstrategie für Krisensituationen vorhanden. Die folgenden Aspekte werden*

berücksichtigt: (A) – Mit wem zu kommunizieren ist (z. B. Gesellschafter, betroffene Geschäftspartner und Kunden, weitere Gesellschafter, allgemeine Öffentlichkeit – Wann zu kommunizieren ist – Verantwortlichkeiten für die Kommunikation – Ermächtigung und Freigabe der Kommunikation – Gesetzliche und regulatorische Einschränkungen der Kommunikation (z. B. aktienrechtliche Vorschriften) – Was zu kommunizieren ist (z. B. vorbereitete Vorlagen für Erklärungen, Kontaktinformationen und Bausteine für bestimmte Szenarien) – Kommunikationskanäle (z. B. Medienkanäle, soziale Medien) – Instrumente für die Überwachung der Kommunikation – Anweisungen und Verfahren für Mitarbeiter (im Falle direkter Kommunikationsansätze wie z. B. dem direkten Kontakt von Mitarbeitern durch Geschäftspartner)“).

5.4.4 Resümee

Die Anforderungen NIS-2 Artikel 23 (4), dass betreffende Einrichtungen dem CSIRT oder gegebenenfalls der zuständigen Behörde für die Zwecke der Meldung erheblicher Sicherheitsvorfälle die Meldewege und -zeiten einhalten und kennen, sind durch die im ISA6-Prüfstandard definierten Controls beschrieben und werden innerhalb eines TISAX-Assessments durch den Auditor auf Vorhandensein und Umsetzung geprüft. Der ISA-Standard fordert neben der Kenntnis und dem Vorhandensein der notwendigen Meldekanäle und -fristen auch die Einrichtung einer krisensicheren Kommunikation. Die Anforderungen des ISA gehen an dieser Stelle über die Anforderungen der NIS-2 hinaus.

Die expliziten Kontaktinformationen, Meldewege und -Sprachen müssen durch die Unternehmen nach deren Veröffentlichung durch die Mitgliedsstaaten der EU in das BCM aufgenommen werden. Die Prüfung dieser Information auf Vorhandensein erfolgt beim TISAX-Assessment nicht, da die anzulegenden Informationen unternehmensspezifisch sind und sich dadurch in mannigfaltiger Ausprägung darstellen können.

5.5 Bewertung des Erfüllungsgrades nach NIS-2 Artikel 23 (5-11)

5.5.1 Anforderung aus der NIS-2

NIS-2 Artikel 23 (5-11) stellt keine expliziten Forderungen an betroffene Unternehmen, die durch diese Vorbereitende Maßnahmen erfordern.

5.5.2 Resümee

Die Anforderungen der NIS-2 Artikel 23 (5 –11) ergeben keine zu prüfenden Maßnahmen und finden daher keine Berücksichtigung im ISA6 Anforderungskatalog.

6 NIS-2 Artikel 24

6.1.1 Anforderung aus der NIS-2

NIS-2 Artikel 24 (1) stellt keine expliziten Forderungen an betroffene Unternehmen, die durch diese Vorbereitende Maßnahmen erfordern.

6.1.2 Resümee

Die Anforderungen der NIS-2 Artikel 24 (1) ergeben keine zu prüfenden Maßnahmen und finden daher keine Berücksichtigung im ISA6 Anforderungskatalog.

7 NIS-2 Artikel 25

7.1.1 Anforderung aus der NIS-2

NIS-2 Artikel 25 befasst sich mit der Anwendung europäischer und internationaler Normen und technischer Spezifikationen für die Sicherheit von Netz- und Informationssystemen.

Expliziten Forderungen an betroffene Unternehmen, die vorbereitende Maßnahmen erfordern, werden nicht gestellt.

7.1.2 Resümee

Die Anforderungen der NIS-2 Artikel 25, europäische und internationale Normen und technische Spezifikationen für die Sicherheit von Netz- und Informationssystemen zur Sicherstellung der Umsetzung der aus der NIS-2 resultierenden Anforderungen an Unternehmen einzusetzen, werden durch eine nach TISAX durchgeführten Prüfung des ISMS einer Organisation eingehalten, was dieses Gutachten darlegt.

8 NIS-2 Artikel 22, 26-29

8.1.1 Anforderung aus der NIS-2

NIS-2 Artikel 22 setzt sich mit koordinierten Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten auf Ebene der Union auseinander.

NIS-2 Artikel 26 bis 28, die sich im Kapitel V zusammenfassen, befassen sich mit der Zuständigkeit und Territorialität (Artikel 26), dem Register der Einrichtungen (Artikel 27) und der Datenbank der Domänennamen-Registrierungsdaten (Artikel 28).

Explizite Forderungen an betroffene Unternehmen, die vorbereitende Maßnahmen erfordern, werden nicht gestellt.

NIS-2 Artikel 29 fordert den Austausch von Informationen zu Cybersicherheitsinformationen.

8.1.2 Resümee

NIS-2 Artikel 22 beinhaltet keine konkreten Anforderungen an Unternehmen. Daher findet dieser Artikel in diesem Gutachten keine weitere Berücksichtigung.

Die Anforderungen der NIS-2 Artikel 26 bis 28 ergeben keine zu prüfenden Maßnahmen und finden daher keine Berücksichtigung in diesem Dokument.

Die Anforderungen des NIS-2 Artikel 29 werden innerhalb des TISAX-Assessments nicht geprüft.

9 Gesamtergebnis

In der Automobilindustrie ist die Notwendigkeit branchenweiter Informations- und Cybersicherheit seit Jahren erkannt und wird strukturiert adressiert, u.a. durch die Etablierung des Prüfstandards TISAX in 2017 und den ihm zugrunde liegenden Anforderungskatalog ISA auf deren Basis derzeit bereits über 17.500 Standorte geprüft sind.

Nach Einschätzung der Experten der Automobilindustrie für Informations- und Cybersicherheit stellen ISA und TISAX-Standard den Stand der Technik nach der Spezifikation des Handbuchs der Rechtsförmlichkeit[4] dar:

„Als Stand der Technik gilt der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst in der Praxis mit Erfolg erprobt worden sein.“

Durch den Einsatz von TISAX durch hunderte Auditoren bei tausenden von Unternehmen, dem daraus resultierenden Erkenntnisgewinn und die kontinuierliche Weiterentwicklung und Integration neuster Erkenntnisse aus dem Bereich der Cybersicherheit durch das Expertengremium wird dies erreicht.

Nach Einschätzung der Experten der Automobilindustrie für Informations- und Cybersicherheit ist das TISAX-Label ein Nachweis, dass die Unternehmensführung eines TISAX-geprüften Unternehmens der in NIS-2 Artikel 20 geforderten Verantwortung gerecht wird und alle in Artikel 21 geforderten Risiko-Management-Maßnahmen nach Stand der Technik innerhalb des Unternehmens umgesetzt hat, sofern die Prüfziele das Gesamtrisiko reflektieren, dem sich das geprüfte Unternehmen ausgesetzt sieht und alle Unternehmensstandorte, die von den Anforderungen der NIS-2-Richtlinie betroffen sind, Teil der Prüfung waren.

Der benötigte Nachweis hierzu wird durch einen unabhängigen Auditor in einem Dreijahreszyklus bestätigt. Unter Berücksichtigung der Verpflichtung für die Betreiber kritischer Infrastrukturen im Sinne des IT-Sicherheitsgesetzes gemäß BSI-Gesetz (BSIG) und BSI-Kritisverordnung, alle zwei Jahre einen Nachweis zur Erfüllung der Anforderungen vorzulegen und dem risikobasierten Ansatz der NIS-2-Richtlinie wird der Dreijahreszyklus der TISAX-Prüfung nach Einschätzung der Experten der Automobilindustrie für Informations- und Cybersicherheit als angemessen angesehen.

Innerhalb des Dreijahreszyklus ist das Unternehmen dazu verpflichtet, die in der Prüfung angegebenen Maßnahmen weiter zu verfolgen und die Umsetzung zu dokumentieren. Außerdem muss das Unternehmen regelmäßig interne Prüfungen von Richtlinien und Verfahren der Informationssicherheit durchführen und die Ergebnisse der durchgeführten Überprüfungen aufzeichnen und aufbewahren. Diese Dokumente werden als Nachweis der aktiven Umsetzung in der nächsten Prüfung oder bei Zwischenprüfungen herangezogen.

Damit sind Unternehmen, die bereits über ein gültiges TISAX-Label verfügen oder sich zukünftig prüfen lassen, in diesen Bereichen gut aufgestellt, die Anforderungen der NIS-2-Richtlinie zu erfüllen.

Zusätzlich müssen NIS-2-Vorgaben zur Erfüllung des verpflichtenden Reporting an Behörden und Kunden an den passenden Stellen im Incident-Management verankert werden. TISAX erbringt den Nachweis, dass Mechanismen für die Erfüllung solcher Vorgaben etabliert sind. Durch den direkten Bezug des Dokuments auf die Forderungen der NIS-2-Richtlinie bleibt es im Verantwortungsbereich der geprüften Unternehmen sich über länderspezifische Zusatzanforderungen zu informieren und diese gegen die umgesetzten Maßnahmen zu prüfen.

[4] Bundesministerium der Justiz / 3.4.1 Generalklauseln > 122 Generalklausel „Stand der Technik“
https://www.bmj.de/SharedDocs/Publikationen/DE/Fachpublikationen/Handbuch_der_Rechtsfoermlichkeit.pdf

10 Danksagung

Die deutsche Automobilindustrie hat sich sehr früh und intrinsisch motiviert mit der ganzheitlichen Etablierung von Informations- und Cybersicherheit in den Organisationen der Branche befasst. Hieraus resultieren der in der Arbeitsgruppe ISA der ENX Association gepflegte und vom Verband der Automobilindustrie veröffentlichte Anforderungskatalog ISA und das weltweit genutzte Prüfprogramm TISAX.

Wie wir heute als Industrie aufgestellt sind, ist dem großen Einsatz der Experten in den beteiligten Häusern, beim Verband der Automobilindustrie und bei der ENX Association geschuldet. Für diesen Einsatz, der sich nicht zuletzt in der Arbeit an dieser Analyse wiederfindet, danken wir herzlich.

11 Anhang – Definition Prozessreifegrade gemäß ISA

	Reifegrad 0
Name	**Unvollständig**
Kurzbeschreibung	Es gibt keinen Prozess, es wird keinem Prozess gefolgt oder der Prozess ist nicht geeignet, um das Ziel zu erreichen.
Definition	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.

Tabelle 4 – Beschreibung des Reifegrads 0

	Reifegrad 1
Name	**Durchgeführt**
Kurzbeschreibung	Es wird einem nicht oder unvollständig dokumentierten Prozess gefolgt ("informeller Prozess") und es gibt Anzeichen, dass er sein Ziel erreicht.
Definition	– Der realisierte Prozess erfüllt seinen (Prozess-) Zweck. – Die beabsichtigten Basispraktiken werden nachweisbar durchgeführt.
Mögliche Nachweise (GWP)	+ Arbeitsergebnisse, die einen Nachweis für Prozessergebnisse liefern.

Tabelle 5 – Beschreibung des Reifegrads 1

	Reifegrad 2
Name	**Gesteuert**
Kurzbeschreibung	Es wird einem Prozess gefolgt, der seine Ziele erreicht. Prozessdokumentation und Prozessdurchführungsnachweise sind vorhanden.
Definition	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 der Planungen angepasst. – Verantwortlichkeiten und Befugnisse zur Durchführung des Prozesses sind definiert, zugewiesen und kommuniziert. – Für die Durchführung des Prozesses notwendige Ressourcen und Informationen sind ermittelt, bereitgestellt, zugewiesen und werden genutzt. – Schnittstellen zwischen den betroffenen Einheiten werden gemanagt, um eine effektive Kommunikation und eine klare Zuweisung von Verantwortlichkeiten sicherzustellen. Management der Arbeitsergebnisse (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.
Mögliche Nachweise (GWP)	+ Prozessdokumentation + Prozessplan + Qualitätsplan, -aufzeichnungen + Prozessdurchführungsaufzeichnungen

Tabelle 6 – Beschreibung des Reifegrads 2

	Reifegrad 3
Name	**Etabliert**
Kurzbeschreibung	Es wird einem Standardprozess gefolgt, der in das Gesamtsystem integriert ist. Abhängigkeiten von anderen Prozessen sind dokumentiert und geeignete Schnittstellen geschaffen. Es existieren Nachweise, dass der Prozess über einen längeren Zeitraum nachhaltig und aktiv genutzt wurde.
Definition	Prozessdefinition (PA 3.1): - Ein Standardprozess einschließlich in geeigneter Weise angepasste Vorgaben ist definiert, der die grundlegenden Elemente beschreibt, die ein definierter 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 zugeschnittenen Standardprozess basiert, ist ausgebracht/verbreitet. - Benötigte Rollen, Verantwortlichkeiten und Befugnisse zur Durchführung des definierten Prozesses sind zugewiesen und kommuniziert. - 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 Arbeitsumgebung, die zur Durchführung des definierten Prozesses erforderlich sind, sind verfügbar, werden gemanagt 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.
Mögliche Nachweise (GWP)	+ Prozessdokumentation + Prozessplan + Qualitätsaufzeichnungen + Richtlinien und Standards + Prozessdurchführungsaufzeichnungen

Tabelle 7 – Beschreibung des Reifegrads 3

	Reifegrad 4
Name	**Vorhersagbar**
Kurzbeschreibung	Es wird einem etablierten Prozess gefolgt. Die Wirksamkeit des Prozesses wird durch Erheben von Kennzahlen kontinuierlich überwacht. Es sind Grenzwerte definiert, bei denen der Prozess als nicht hinreichend wirksam angesehen wird und angepasst werden muss. (Key Performance Indicators)
Definition	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 bezüglich 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 bezüglich der Prozessdurchführung definiert. – Messergebnisse sind gesammelt, analysiert und werden berichtet, um den Grad der quantitativen Zielerreichung bezüglich der Prozessdurchführung zu überwachen. – Messergebnisse werden genutzt, um die Durchführung des Prozesses zu charakterisieren. Prozesssteuerung (PA 4.2): – Analyse- und Steuerungstechniken sind bestimmt und werden, wie jeweils zutreffend, angewendet. – Variable Steuerungsgrenzen sind zur gewöhnlichen Durchführung des Prozesses etabliert. – Messdaten für spezielle Varianten werden analysiert. – Korrekturmaßnahmen werden durchgeführt, um spezielle Varianten zu berücksichtigen. – Steuerungsgrenzen werden (falls erforderlich) im Anschluss an Korrekturmaßnahmen erneut etabliert.
Mögliche Nachweise (GWP)	+ Prozessdokumentation + Prozesssteuerungsplan + Prozessverbesserungsplan + Prozessmessplan + Prozessdurchführungsaufzeichnungen

Tabelle 8 – Beschreibung des Reifegrads 4

	Reifegrad 5
Name	**Optimierend**
Kurzbeschreibung	Es wird einem vorhersagbaren Prozess gefolgt, bei dem die kontinuierliche Verbesserung ein wesentliches Ziel ist. Die Verbesserung wird von dedizierten Ressourcen aktiv vorangetrieben.
Definition	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 Ursachen für Variationen bei der Durchführung von Prozessen zu identifizieren. – Geeignete Daten werden analysiert, um 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 Standardprozesses bewertet. – Die Umsetzung aller beschlossenen Änderungen wird gemanagt, um sicherzustellen, dass jegliche Unterbrechung der Durchführung eines Prozesses begriffen und darauf eingewirkt wird. – Die Wirksamkeit einer Prozessänderung wird auf Grundlage der tatsächlichen Leistung gegenüber definierten Prozessanforderungen und Prozesszielen beurteilt, um zu bestimmen, ob Ergebnisse mit allgemeinen oder speziellen Fällen übereinstimmen.
Mögliche Nachweise (GWP)	+ Prozessverbesserungsplan + Prozessmessplan + Prozessdurchführungsaufzeichnungen

Tabelle 9 – Beschreibung des Reifegrads 5

ENX Association
Bockenheimer Landstr. 97-99
60325 Frankfurt am Main
Germany
+49 69 9866927-0
info@enx.com