

TISAX[®] Assessment Bericht

Follow-Up

Carl Zeiss QEC GmbH

S2ZM0Z

AX6C8T-3

07.06.2023

Version 1.0

Anfangsbemerkungen

Dieser Bericht und die zugrundeliegende Prüfung wurde von entsprechend qualifizierten Prüfern eines für den Trusted Information Security Assessment Exchange (TISAX) freigegebenen Prüfdienstleisters erstellt. Hierbei wird die Wirksamkeit der Steuerungsprozesse und deren derzeitige Umsetzung auf Basis der in den TISAX „Audit Criteria and Assessment Requirements“ (ACAR), wie zum Zeitpunkt der Berichtserstellung von ENX veröffentlicht, spezifizierten Vorgehensweise eingeschätzt.

TISAX wird von der ENX Association betrieben und verantwortet. TISAX dient allgemein anerkannten, von vertrauenswürdigen und im Wettbewerb stehenden Prüfdienstleistern auf Basis des ISA Prüfkataloges durchgeführten Prüfungen. Detaillierte Informationen zu TISAX finden sich auf <http://www.enx.com/tisax/>.

Dieser Assessment Report ist zur ausschließlichen Nutzung innerhalb von TISAX bestimmt. Eine Weiterleitung der TISAX Assessment Ergebnisse oder die Kommunikation ihrer Inhalte muss entsprechend den in den anwendbaren TISAX Vereinbarungen und Richtlinien für TISAX Teilnehmer bzw. TISAX Prüfdienstleister für eine Kommunikation entsprechender Inhalte festgelegten Vorgaben erfolgen.

Eine Kommunikation der TISAX Assessment Ergebnisse außerhalb der definierten TISAX Verfahren für einen Austausch entsprechender Informationen sowie jeglicher Austausch entsprechender Informationen mit Dritten außerhalb von TISAX ist nicht zulässig. Es wird darauf hingewiesen, dass bestimmte, sich aus dem anwendbaren TISAX Rechtsrahmen ergebende Rechte ggf. nicht bestehen, wenn die Kommunikation der TISAX Assessment Ergebnisse nicht entsprechend den TISAX Richtlinien erfolgt.

Auch wenn die diesem Bericht zugrundeliegende Prüfung mit aller gebotenen Sorgfalt durchgeführt wurde, handelt es sich lediglich um eine Momentaufnahme auf Basis einer stichprobenhaften Prüfung. Diese ist grundsätzlich nicht geeignet, alle Schwachstellen der geprüften Prozesse und Verfahren zu identifizieren.

Zudem geben TISAX Assessment Ergebnisse ausschließlich eine Aussage zum Zeitpunkt der Bewertung. Jegliche möglichen Änderungen nach dem Prüfungszeitraum wurden nicht bei der Bewertung berücksichtigt. Es wird ausdrücklich darauf hingewiesen, dass bei einer Projektion der Ergebnisse auf einen späteren Zeitpunkt inhärent die Gefahr besteht, dass die in diesem Bericht beschriebenen Ergebnisse durch geänderte Voraussetzungen oder über die Zeit nachlassende Umsetzung der Richtlinien, Prozesse und Verfahrensweisen an Aussagekraft verlieren können.

Struktur des Berichts

Dieser Bericht ist wie folgt aufgebaut:

- A. Informationen zum Assessment (Assessment Related Information)
- B. Gesamtübersicht Prüfergebnisse (Summarized Results)
- C. Zusammenfassung der Ergebnisse des Assessments (Assessment Result Summary)
- D. Reifegrade gem. ISA (Ergebnis-Tab des ISA) (Maturity Levels of ISA (Result Tab))
- E. Detaillierte Ergebnisse zum Assessment (Detailed Assessment Results)

Die Struktur und die Überschriften entsprechen den möglichen Freigabestufen von Prüfergebnissen für andere TISAX Teilnehmer, die englischen Originalnamen werden aus Gründen der Transparenz in Klammern genannt.

Der Bericht beginnt mit allgemeinen Informationen über die Bewertung (A. Informationen zum Assessment). In den nächsten Abschnitten wird der Detailgrad von abstrakten Gesamtbewertungen (B. Gesamtübersicht Prüfergebnisse und C. Zusammenfassung der Ergebnisse des Assessments) bis hin zu den Einzelfeststellungen (D. Reifegrade gemäß ISA und E. Detaillierte Ergebnisse zum Assessment) kontinuierlich gesteigert.

A. Informationen zum Assessment (Assessment Related Information)

A.1 Prüfscope

TISAX® Scope-ID	S2ZM0Z
Scope-Typ	<input checked="" type="checkbox"/> Standard Scope 2.0 <i>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.</i> <i>Die Bewertung wird mindestens im höchsten Assessment-Level durchgeführt, das in einem der aufgeführten Prüfungsziele gefordert ist. Alle in den aufgelisteten Prüfungszielen geforderten Kriterien sind Gegenstand der Beurteilung.</i> <input type="checkbox"/> Erweiterter benutzerdefinierter Scope <input type="checkbox"/> Vollständig benutzerdefinierter Scope
Prüfziele	<input type="checkbox"/> Umgang mit Informationen von hohem Schutzbedarf <input type="checkbox"/> Hohe Verfügbarkeit <input checked="" type="checkbox"/> Umgang mit Informationen von sehr hohem Schutzbedarf <input type="checkbox"/> Sehr hohe Verfügbarkeit <input checked="" type="checkbox"/> Umgang mit schutzbedürftigen Prototypenkomponenten/-bauteilen <input type="checkbox"/> Umgang mit schutzbedürftigen Prototypenfahrzeugen <input type="checkbox"/> Nutzung von Erprobungsfahrzeugen <input type="checkbox"/> Events und Bildaufnahmen mit schutzbedürftigen Objekten <input type="checkbox"/> Umgang mit personenbezogenen Daten gemäß Artikel 28 DSGVO (Auftragsverarbeiter) <input type="checkbox"/> Umgang mit besonderen Kategorien (Artikel 9 DSGVO) personenbezogener Daten gemäß Artikel 28 DSGVO (Auftragsverarbeiter)
Prüfanforderungen	ACAR – TISAX Specification of Assessment Version 2.1: Family-ID: ISA, Version 5.1

A.2 Geprüfte Standorte

Firmenname	Anschrift	Location-ID	Ansprechpartner
Carl Zeiss QEC GmbH	Ruhrstr. 5a. 86633 Neuburg a.d. Donau Deutschland	L53HTM	Mayer, Katharina katharina.mayer@zeiss.com
Carl Zeiss QEC GmbH	Ruth-Hallensleben-Str.6 50739 Köln Deutschland	L8ZHVT	Mayer, Katharina katharina.mayer@zeiss.com

Der Auditor bestätigt, dass alle oben genannten Informationen auf ihre Richtigkeit hin überprüft wurden.

A.2.1 Erstprüfung

TISAX® Assessment-ID	AX6C8T-1
Assessment Level	AL3
Prüfmethode	<input type="checkbox"/> Plausibilisierung der Selbstauskunft auf der Grundlage von bereitgestellten Dokumenten und anderen Nachweisen <input checked="" type="checkbox"/> Detaillierte Überprüfung der Nachweise <input checked="" type="checkbox"/> Interviews mit prozessbeteiligten Personen <input checked="" type="checkbox"/> Vor-Ort-Prüfung <input type="checkbox"/> Videobasierte Standortprüfung (Remote)
Datum Kick-Off Meeting	16.12.2022
Datum Opening Meeting	06.02.2023
Datum Closing Meeting (Stichtag Gültigkeit)	09.02.2023
Zustimmung des Geprüften	Der Geprüfte <input checked="" type="checkbox"/> stimmt der sachlichen Korrektheit der Feststellungen zu. <input type="checkbox"/> stimmt den Feststellungen mit Einschränkungen zu (Anmerkungen wurden in den Berichtstext aufgenommen und sind als solche gekennzeichnet).

A.2.2 Prüfung des Maßnahmenplans

TISAX® Assessment-ID	AX6C8T-2
Prüfungszeitraum	09.02.2023
Zustimmung des Geprüften	Der Geprüfte <input checked="" type="checkbox"/> stimmt der sachlichen Korrektheit der Feststellungen zu. <input type="checkbox"/> stimmt den Feststellungen mit Einschränkungen zu (Anmerkungen wurden in den Berichtstext aufgenommen und sind als solche gekennzeichnet).

A.2.3 1. Follow-Up

TISAX® Assessment-ID	AX6C8T-3
Prüfmethode	<input type="checkbox"/> Auf Basis von vorliegender Dokumentation <input type="checkbox"/> Auf Basis von Interviews mit Prozessbeteiligten Personen <input checked="" type="checkbox"/> Vor-Ort-Prüfung
Prüfungszeitraum	07.06.2023
Zustimmung des Geprüften	Der Geprüfte <input checked="" type="checkbox"/> stimmt der sachlichen Korrektheit der Feststellungen zu. <input type="checkbox"/> stimmt den Feststellungen mit Einschränkungen zu (Anmerkungen wurden in den Berichtstext aufgenommen und sind als solche gekennzeichnet).

Autoren

Auditor
Götze, Tim
Qualitätssicherung
Klose, Isabel

B. Gesamtübersicht Prüfergebnisse (Summarized Results)

B.1 Erstprüfung

Nach der Erstprüfung errechnet sich ein durchschnittlicher Gesamtreifegrad von 2,91.

B.2 Prüfung des Maßnahmenplans

Basierend auf der Erstbewertung und der Prüfung des Maßnahmenplanes ist die Gesamtbewertung des Scopes:

- Nebenabweichend (es existieren ausschließlich Abweichungen, die keine unmittelbar kritischen Risiken erzeugen)
 - Es existieren Nebenabweichungen ohne definierte Korrekturmaßnahmen.
 - Alle Nebenabweichungen haben definierte Korrekturmaßnahmen. Die letzte Korrekturmaßnahme ist am 30.06.2023 fällig (bis zu diesem Datum können temporäre Labels vergeben werden).
 - Der Gesamtreifegrad liegt mehr als 10% unter dem Zielreifegrad (<2,7).
- Hauptabweichend
 - Einige der Abweichungen erzeugen unmittelbar kritische Risiken, es müssen mindestens kompensierende Sofortmaßnahmen umgesetzt werden, um den Status auf „Nebenabweichend“ zu ändern.
 - Der Gesamtreifegrad liegt mehr als 30% unter dem Zielreifegrad (<2,1).

Es wurden insgesamt vier Nebenabweichungen zu den geprüften Anforderungen identifiziert.

Ein Maßnahmenplan wurde vom Auditee dem Auditor vorgelegt während der Erstprüfung.

Die vom Auditee geplanten Korrekturmaßnahmen, die zeitliche Planung und die geplante Umsetzung von Kompensationsmaßnahmen im Zeitplan wurden als angemessen beurteilt.

B.3 1. Follow-Up

Basierend auf der Erstbewertung und dem Follow-Up am 7.06.2023 ist die Gesamtbewertung des Scopes:

- Konform
- Nebenabweichend (es existieren ausschließlich Abweichungen, die keine unmittelbar kritischen Risiken erzeugen)
 - Es existieren Nebenabweichungen ohne definierte Korrekturmaßnahmen.
 - Alle Nebenabweichungen haben definierte Korrekturmaßnahmen.
 - Der Gesamtreifegrad liegt mehr als 10% unter dem Zielreifegrad (<2,7).
- Hauptabweichend
 - Einige der Abweichungen erzeugen unmittelbar kritische Risiken, es müssen mindestens kompensierende Sofortmaßnahmen umgesetzt werden, um den Status auf „Nebenabweichend“ zu ändern.
 - Der Gesamtreifegrad liegt mehr als 30% unter dem Zielreifegrad (<2,1).

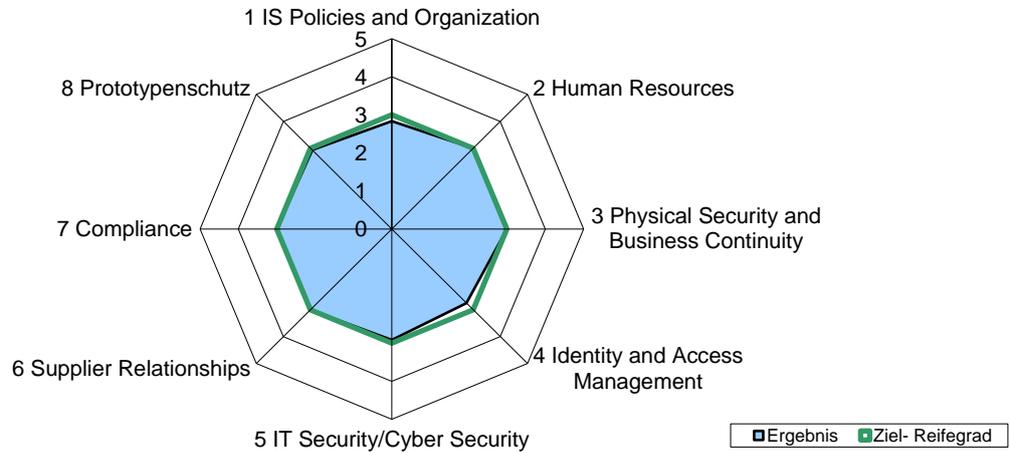
Es liegen keine Abweichungen mehr zu den Anforderungen vor.

Nach dem Follow-Up errechnet sich ein durchschnittlicher Reifegrad von 3,0.

C. Zusammenfassung der Ergebnisse des Assessments (Assessment Result Summary)

C.1 Erstprüfung

Die einzelnen Bereiche des Reifegradniveaus werden wie folgt im Spinnennetzdiagramm dargestellt.



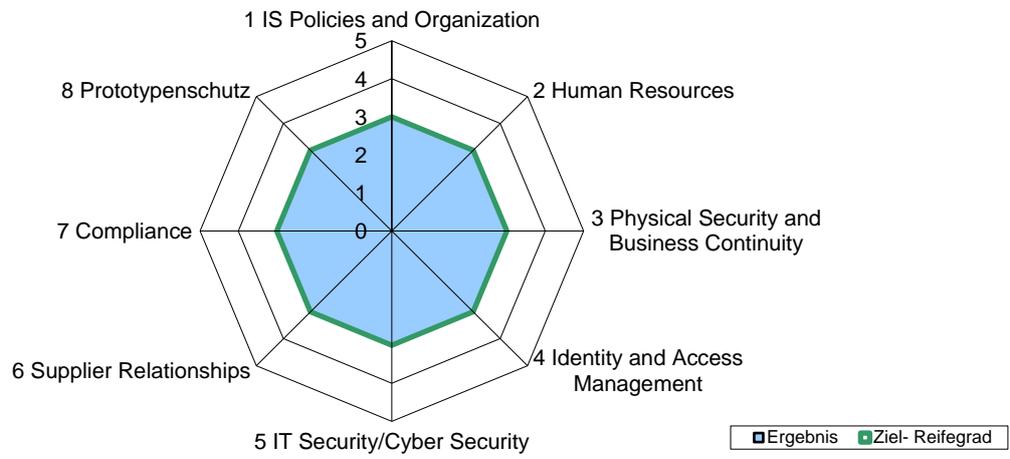
C.2 Prüfung des Maßnahmenplans

Für die einzelnen Bereiche ergeben sich die folgenden Haupt- (HA)- und Nebenabweichungen (NA):

Lfd. Nr.	Bereich	Anzahl HA	Anzahl NA
1	IS Policies and Organization	0	1
2	Human Ressources	0	0
3	Physical Security and Business Continuity	0	0
4	Identity and Access Management	0	1
5	IT Security / Cyber Security	0	1
6	Supplier Relationships	0	0
7	Compliance	0	0
8	Prototypenschutz	0	1
9	Datenschutz	N/A	N/A

C.3 1. Follow-Up

Die einzelnen Bereiche des Reifegradniveaus werden wie folgt im Spinnennetzdiagramm dargestellt.



D. Reifegrade gem. ISA (Ergebnis-Tab des ISA) (Maturity Levels of ISA)

D.1 ISMS

Basierend auf dem aktuellen Stand der Umsetzung ergeben sich für die einzelnen Prüfpunkte aus dem Bereich ISMS die nachfolgenden Reifegrade:

Nr.	Thema	Ziel- Reifegrad	Ergebnis
1	IS Policies and Organization		
1.1	Information Security Policies		
1.1.1	Inwieweit sind Richtlinien zur Informationssicherheit vorhanden?	3	3
1.2	Organization of Information Security		
1.2.1	Inwieweit wird in der Organisation Informationssicherheit gemanagt?	3	3
1.2.2	Inwieweit sind die Verantwortlichkeiten für Informationssicherheit organisiert?	3	3
1.2.3	Inwieweit werden Informationssicherheitsanforderungen in Projekten berücksichtigt?	3	3
1.2.4	Inwieweit sind die Verantwortlichkeiten zwischen Organisations-fremden IT-Service-Anbietern und der eigenen Organisation definiert?	3	3
1.3	Asset Management		
1.3.1	Inwieweit werden Informationswerte (Assets) identifiziert und erfasst?	3	3
1.3.2	Inwieweit werden Informationswerte hinsichtlich ihres Schutzbedarfs klassifiziert und gemanagt?	3	3
1.3.3	Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene organisationsfremde IT-Dienste zum Verarbeiten von Informationswerten der Organisation eingesetzt werden?	3	3
1.4	IS Risk Management		
1.4.1	Inwieweit werden Informationssicherheitsrisiken gemanagt?	3	3
1.5	Assessments		
1.5.1	Inwieweit wird die Einhaltung der Informationssicherheit in Verfahren und Prozessen sichergestellt?	3	3
1.5.2	Inwieweit wird das ISMS von einer unabhängigen Instanz überprüft?	3	3
1.6	Incident Management		
1.6.1	Inwieweit werden Informationssicherheitsereignisse verarbeitet?	3	3

Nr.	Thema	Ziel- Reifegrad	Ergebnis
2	Human Ressources		
2.1.1	Inwieweit wird die Eignung von Mitarbeitern für sensible Tätigkeitsbereiche sichergestellt?	3	3
2.1.2	Inwieweit werden alle Mitarbeiter zur Einhaltung der Informationssicherheit verpflichtet?	3	3
2.1.3	Inwieweit werden Mitarbeiter über die Risiken beim Umgang mit Informationen geschult und sensibilisiert?	3	3
2.1.4	Inwieweit ist mobiles Arbeiten geregelt?	3	3
3	Physical Security and Business Continuity		
3.1.1	Inwieweit werden Sicherheitszonen für den Schutz von Informationswerten gemanagt?	3	3
3.1.2	Inwieweit ist in Ausnahmesituationen die Informationssicherheit sichergestellt?	3	3
3.1.3	Inwieweit ist der Umgang mit Informationsträgern gemanagt?	3	3
3.1.4	Inwieweit ist der Umgang mit mobilen IT-Geräten und mobilen Datenträgern gemanagt?	3	3
4	Identity and Access Management		
4.1	Identity Management		
4.1.1	Inwieweit ist der Umgang mit Identifikationsmitteln gemanagt?	3	3
4.1.2	Inwieweit wird der Zugang von Benutzern zu Netzwerkdiensten, IT-Systemen und IT-Anwendungen gesichert?	3	3
4.1.3	Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewandt?	3	3
4.2	Access Management		
4.2.1	Inwieweit werden Zugriffsberechtigungen vergeben und gemanagt?	3	3
5	IT Security / Cyber Security		
5.1	Cryptography		
5.1.1	Inwieweit wird die Nutzung kryptografischer Verfahren gemanagt?	3	3
5.1.2	Inwieweit werden Informationen während der Übertragung geschützt?	3	3

Nr.	Thema	Ziel- Reifegrad	Ergebnis
5.2	Operations Security		
5.2.1	Inwieweit werden Änderungen gesteuert?	3	3
5.2.2	Inwieweit sind die Entwicklungs- und Testumgebungen von den Produktumgebungen getrennt?	3	N/A
5.2.3	Inwieweit werden IT-Systeme vor Schadsoftware geschützt?	3	3
5.2.4	Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert?	3	3
5.2.5	Inwieweit werden Schwachstellen erkannt und behandelt?	3	3
5.2.6	Inwieweit werden IT-Systeme technisch überprüft (Systemaudit)?	3	3
5.2.7	Inwieweit wird das Netzwerk der Organisation gemanagt?	3	3
5.3	System acquisitions, requirement management and development		
5.3.1	Inwieweit wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt?	3	3
5.3.2	Inwieweit sind Anforderungen an Netzwerkdienste definiert?	3	3
5.3.3	Inwieweit ist die Rückgabe und das sichere Entfernen von Informationswerten aus Organisationsfremden IT-Diensten geregelt?	3	3
5.3.4	Inwieweit sind Informationen in gemeinsam genutzten organisationsfremden IT-Diensten geschützt?	3	3
6	Supplier Relationships		
6.1.1	Inwieweit wird die Informationssicherheit bei Auftragnehmern und Kooperationspartnern sichergestellt?	3	3
6.1.2	Inwieweit ist Geheimhaltung beim Austausch von Informationen vertraglich vereinbart?	3	3
7	Compliance		
7.1.1	Inwieweit wird die Einhaltung regulatorischer und vertraglicher Bestimmungen sichergestellt?	3	3
7.1.2	Inwieweit wird der Schutz von personenbezogenen Daten bei der Umsetzung der Informationssicherheit berücksichtigt?	3	3

D.2 Umgang mit Prototypen

Basierend auf dem aktuellen Stand der Umsetzung ergeben sich für die einzelnen Prüfpunkte aus dem Bereich Prototypenschutz die nachfolgenden Reifegrade:

Nr.	Thema	Ziel- Reifegrad	Ergebnis
8.1	<i>Physische und umgebungsbezogene Sicherheit</i>		
8.1.1	Sicherheitskonzept	3	3
8.1.2	Perimetersicherung	3	N/A
8.1.3	Stabilität der Außenhaut	3	3
8.1.4	Sicht- und Einblickschutz	3	3
8.1.5	Schutz vor unbefugtem Betreten und Kontrolle des Zugangs	3	3
8.1.6	Einbruch Überwachung	3	3
8.1.7	Besuchermanagement	3	3
8.1.8	Mandantentrennung	3	3
8.2	<i>Organisatorische Anforderungen</i>		
8.2.1	Geheimhaltungsverpflichtungen	3	3
8.2.2	Unterauftragnehmer	3	3
8.2.3	Sensibilisierung	3	3
8.2.4	Sicherheitseinstufung	3	3
8.2.5	Zutrittsregelung	3	3
8.2.6	Foto- und Filmregelung	3	3
8.2.7	Mobile film- und fotofähige Endgeräte	3	3
8.3	<i>Umgang mit Fahrzeugen, Komponenten und Bauteilen</i>		
8.3.1	Transport	3	3
8.3.2	Abstellen und Lagerung	3	3
8.4	<i>Anforderungen für Erprobungsfahrzeuge</i>		
8.4.1	Tarnung	3	N/A
8.4.2	Test- und Erprobungsgelände	3	N/A
8.4.3	Test- und Erprobungsfahrten auf öffentlichen Straßen	3	N/A
8.5	<i>Anforderungen für Veranstaltungen und Shootings</i>		

8.5.1	Ausstellungen und Veranstaltungen	3	N/A
8.5.2	Film- und Fotoshootings	3	N/A

D.3 Datenschutz

Das Datenschutzmodul wurde nicht geprüft.

E. Detaillierte Ergebnisse zum Assessment (Detailed Assessment Results)

1 IS Policies and Organization

1.1 Information Security Policies

<p>1.1.1 Inwieweit sind Richtlinien zur Informationssicherheit vorhanden?</p>
<p>Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)</p> <p>Betrachtete Dokumente/Nachweise/Prüfungshandlung:</p> <ul style="list-style-type: none"> • SE.01 DE Management der Informationssicherheit • SE.02 DE Sicherheit für Endanwender • Einstieg MS über Mitarbeiterportal.png • Portal_Managementsysteme.jpeg • SE Guideline End User DE • PPT Business InfoSec IQS • SE.05 Informationssicherheitsrichtlinien <p>"Es gibt unternehmensweite Richtlinien und eine Organisation zur Informationssicherheit. Alle Richtlinien werden im Intranet zur Verfügung gestellt. Im Unternehmen ist ein umfassendes Regelwerk zur Informationssicherheit etabliert. Die Wichtigkeit und Bedeutung der Informationssicherheit für die Organisation ist im Regelwerk zur Informationssicherheit enthalten. Mitarbeiter erhalten über die Richtlinie „End User“ eine Zusammenfassung zum Thema Informationssicherheit."</p> <p>Vor Ort wurden diverse Richtlinien und begleitende Dokumente eingesehen. Das Regelwerk und seine Struktur wurden erläutert. Das Regelwerk definiert Ziele, die relevanten Anforderungen und die Verantwortlichkeiten. Die Ziele der Informationssicherheit wurden vor Ort erläutert. Das Regelwerk bzw. das ISMS wurden durch das ZEISS Executive Board freigegeben. Die SE.02 DE Sicherheit für Endanwender weist auf Konsequenzen bei Nichtbeachtung hin. Das gesamte Regelwerk wurde 2022 aktualisiert. Die Überarbeitung ist für 3 Jahre oder anlassbezogen in der SE.05 definiert. Das Regelwerk ist im Intranet unter „Managementsystem/Sicherheit“ veröffentlicht.</p>
<p>Feststellung</p> <p>Die Ziele könnten detailliert für die einzelnen Unternehmensbereiche definiert werden. Die Schutzziele der Informationssicherheit haben für unterschiedliche Bereiche eine unterschiedliche Wertigkeit. Für einzelne Unternehmensbereiche können andere Schutzziele als die Vertraulichkeit im Vordergrund stehen.</p> <p><input type="checkbox"/> Hauptabweichung <input type="checkbox"/> Nebenabweichung <input type="checkbox"/> Beobachtung <input checked="" type="checkbox"/> Identifiziertes Verbesserungspotential</p>

1.2 Organization of Information Security

1.2.1 Inwieweit wird in der Organisation Informationssicherheit gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- ZEISS Mitarbeiterportal als Einstieg in das ZEISS Management System.JPG
- SE.01 Management der Informationssicherheit
- Startseite des ZEISS Managementsystems mit Schnellzugriff auf Sicherheit-ISMS.JPG
- ZEISS CMM (ZEISS CMM DE.pdf) als übergeordnetes Dokument
- ZEISS ISMS.jpg
- WISA Report
- VDA ISA Excel (nur Reifegrad)
- Nachweisdokumentation VDA ISA 5.1_AL3-AL2.5.docx
- SE.06 Organisation der Informationssicherheit
- ZEISS Security Domain Structure based on ISO 27001

"Das ISMS ist in das ZEISS Management-System eingebunden. Auf das ZEISS Managementsystem haben alle ZEISS Mitarbeiter und Externe Zugriff, die einen ZEISS Account verfügen. Das ZEISS Management-System und somit auch das ISMS ist vom ZEISS Executive Board freigegeben. ISMS wird durch Interne Assessments alle 2 Jahr überprüft (WISA)"

Im Unternehmen ist ein ISMS etabliert. Die Carl Zeiss Coperate IT ist nach ISO 27001 zertifiziert. Der Scope für das ISMS ist für das gesamte Unternehmen definiert. Das ISMS wurde durch das ZEISS Executive Board freigegeben. Das lokale Management ist in die Informationssicherheitsprozesse eingebunden. Die anwendbaren Kontrollen wurden im Rahmen eines VDA ISA festgelegt. Die wenigen Ausschlüsse wurden plausibel vor Ort erläutert. Die Wirksamkeit wird im Rahmen von WISA überprüft (siehe 1.5.1).

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

1.2.2 Inwieweit sind die Verantwortlichkeiten für Informationssicherheit organisiert?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Präsentation Infosec_iqs_org 1.pdf
- SE.06 Organisation der Informationssicherheit

" Informationssicherheitsorganisation wurde 2022 neu aufgestellt (ISO / BISO); CISO der Organisation ist Oliver Ortlieb"

Die neue Sicherheitsorganisation wurde vor Ort erläutert. Es wurde eine neue Struktur geschaffen. Information Security (CIT-I) gehört jetzt Corporate (CIT). Es gibt ein neues Gremium (Security Council), um eine direkte Berichtslinie zum Management sicherzustellen. Die CIT-I unterteilt sich in Certification and Governance, Advisory Services und Business Information Security Enablement. Die einzelnen Bereiche wurden erläutert. Die CZ Corporate IT ist ISO 27001 zertifiziert. Das Global InfoSec Team in Business Information Security Officers (BISO), Regional Information Security Officer und Information Security Officer Germany. Die Verantwortlichkeiten und Aufgaben wurden erläutert. Daher ist eine angemessene organisatorische Trennung gegeben. Die notwendige Qualifikation wurde exemplarisch nachgewiesen.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

1.2.3 Inwieweit werden Informationssicherheitsanforderungen in Projekten berücksichtigt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- CSOP IT.01 EN IT Demand & Project Portfolio Management
- CSOP SE.20 DE Cloud Security
- SE Security Concept AD EN.docx
- Durchführung eines Auftrags.docx
- Informationssicherheit TISAX
- Laborhandbuch

"IT Projekte laufen bei ZEISS über den sogenannten IT-Demand-Prozess. Alle Segmente, Business-Groups und lokale Einheiten müssen sich an den Prozess halten. Des Weiteren wird seitens Corporate Security vorgegeben, wie Assets und neue Technologien zu bewerten und abzusichern sind. Im Demand-Prozess wird somit festgelegt, ob im Projekt nur ein einfaches oder ein erweitertes Security-Konzept zu erstellen ist. Dieses wird im Prozess abgenommen. Im Demand Prozess wird von jedem Projekt ein Security Concept eingefordert, ggf. ein erweitertes Security Concept eingefordert. Bei Cloud Projekten ist zusätzlich eine Cloud-Checkliste auszufüllen und Corporate Security prüft den CSP nach Bedarf. In Auftragsbestellung wird die Informationssicherheit bewertet und dokumentiert."

Im Laborhandbuch wird die Wichtigkeit vom vertraulichen Umgang mit Kundeninformationen betont. Die Vorgehensweise wurde vor Ort erläutert. Laut Aussage gelten Kundenprojekte grundsätzlich als vertraulich. Aktuell gibt es keine Projekte mit sehr hohem Schutzbedarf. Die Ausführungen in der Nachweisdokumentation beziehen sich ausschließlich auf IT-Projekte.

Feststellung

Die Festlegung, dass Kundenprojekte als vertraulich eingestuft sind, ist nicht im Laborhandbuch definiert.

Hauptabweichung Nebenabweichung Beobachtung Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)

Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft):

Projekte sind unter Berücksichtigung ihrer Anforderungen an die Informationssicherheit zu klassifizieren. Die Vorgehensweise und die Kriterien zur Klassifizierung von Projekten sind zu dokumentieren. In einer frühen Phase des Projektes ist eine Risikobewertung auf Basis einer definierten Vorgehensweise durchzuführen und bei Änderungen des Projektes zu wiederholen. Für identifizierte Informationssicherheitsrisiken sind Maßnahmen abzuleiten und im Projekt zu berücksichtigen. Es ist eine Prozessbeschreibung zu erstellen, welche die Vorgehensweise zur Klassifizierung sowie zur Durchführung einer Risikobewertung von Projekten beschreibt. Abgeleitete Maßnahmen sind im Verlauf des Projektes regelmäßig zu überprüfen und bei Änderungen der Bewertungskriterien neu zu bewerten.

Nachweis(e):

- Prozessbeschreibung zur Klassifizierung von Kunden-Projekten
- Prozessbeschreibung zur Risikobewertung von Projekten

Die Umsetzung wird gemäß Planung spätestens am 07.06.2023 abgeschlossen sein.

Bewertung nach Follow-Up

Nachweisprüfung am 07.06.2023

Bereitgestellte Nachweise:

- Ausschnitt aus_IQS LAB PL QEC 7 Erläuterungen zur Auftragsabwicklung
- Informationssicherheit TISAX
- TISAX_Routing_Info_V3

Es liegen keine Abweichungen mehr zu den Anforderungen vor.

1.2.4 Inwieweit sind die Verantwortlichkeiten zwischen Organisations-fremden IT-Service-Anbietern und der eigenen Organisation definiert?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- APP07 AT&T
- SE.20 Cloud Sicherheit
- IP4OP – Information Platform for Outsourcing Provider
- SE.20a Security Checklist for Cloud Platform
- SE.20b Sicherheitsanforderungen für Azure AD
- SE.20c Cloud Security Controls
- SE.20d Cloud Security Approval
- Request Security Assessment of cloud service Provider (onetrust)

"Auch bei externen Dienstleistern (z.B. Atos) wird vertraglich ein dedizierter Ansprechpartner für Information Security definiert, der in Projekten und im operativen Betrieb zuarbeitet und in „Emergency and Crisis Situations“ als Ansprechpartner beim IT-Dienstleister agiert."

Im Unternehmen werden eine Vielzahl von externen IT-Diensten eingesetzt. Die Dienste werden alle zentral verwaltet und gesteuert. Es existiert eine Übersicht in Form des IP4OP. In der Plattform LUY werden alle Applikationen erfasst. Dort werden jeweils die Verantwortlichen definiert. Die „onetrust“-Plattform wurde vor Ort eingesehen. SSO wird jeweils favorisiert. Die Cloud-Lösungen werden u. a. über ImmuniWeb überwacht.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

1.3 Asset Management

1.3.1 Inwieweit werden Informationswerte (Assets) identifiziert und erfasst?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.08 EN (Asset Management)
- Matrix 42 Portal / ITSM
- Informationssicherheit TISAX.docx
- Guideline Klassifizierung
- Prüfmittelliste

"ZEISS Assets werden zentral geführt. Neben den zentralen Verwaltungstools (Active Directory, MDM und ITSM Suite) gibt es auch lokale Verzeichnisse."

Es wurden die wesentlichen Informationswerte und Informationsträger ermittelt und deren Verantwortliche festgelegt. Vor Ort wurde die Prüfmittelliste eingesehen. Im Rahmen der Kalibrierung wird die Prüfmittelliste geprüft.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

1.3.2 Inwieweit werden Informationswerte hinsichtlich ihres Schutzbedarfs klassifiziert und gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.02 DE Sicherheit für Endanwender.
- SE.02k DE. (ZEISS Informationsklassifizierung)
- Guideline End User DE
- ZEISS Guideline Informationsklassifizierung DE

"Es gibt bei ZEISS per Policy 4 Klassifizierungsstufen. Umgesetzt wird die Vorgabe bisher v.a. in Bereichen, die mit kritischen / sensiblen Daten arbeiten. Informiert wurden die Mitarbeiter über Intranet/TEAM ZEISS, über Poster-Aktionen, Yammer-Beiträge, etc. Trainiert werden die Mitarbeiter über Schulungen in der eCademy/ CurioZ - CurioZ Übersicht über Security Schulung Daten und Informationen richtig klassifizieren Hardcopy. Zusätzlich wurde ein Tool zur technischen Klassifizierung (Azure Information Protection) weltweit ausgerollt."

Die Aussagen der Nachweisdokumentation wurden vor Ort verifiziert. Durch diverse Dokumente und deren Klassifizierung wurde die Umsetzung ebenfalls nachgewiesen. Das Regelwerk definiert den Umgang mit den Informationsträgern (Kennzeichnung, korrekte Handhabung, Transport, Speicherung, Rückgabe, Löschung / Entsorgung).

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

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

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- TEMPLATE_APP07_FWA_Security_v1.0.docx
- SE Guideline End User DE.docx
- Verbotene Software

"Der Freigabe-Prozess von externen Dienstleistern läuft federführend bei Corporate IT, wobei Corporate Security für den sicherheits-relevanten Vertragsbestandteil „Appendix 7 - Information Security, IT Security and Standards“."

Freigegebene Dienste sind über das IT4U bestellbar. Die entsprechende Applikationsliste wurde im Tool eingesehen. Es existiert auch eine Blacklist.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

1.4 IS Risk Management

1.4.1 Inwieweit werden Informationssicherheitsrisiken gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- AR.02 EN.docx (Risk Management)
- AR.02a EN.xlsm (Risk Management Tool)
- SE Information Security Risk Management
- 2021-11_Checklist_Risk Inventory_Carl_Zeiss_QEC_GmbH.pdf
- Management Review 21-22 QEC.pdf
- Infosec_Rismanagement CIT

"Informationssicherheits-Risiken werden von Corporate Security gesammelt und quartalsweise zentral an Corporate Risk Management gemeldet. Dazu wird ein standardisiertes Template (Risk Management Tool) verwendet. "

Im Unternehmen ist ein mehrstufiges Risikomanagement etabliert. Vor Ort wurde die lokale und globale Bewertung eingesehen. Risikobeurteilungen werden sowohl regelmäßig als auch anlassbezogen durchgeführt. Die Bewertung von Risiken wurde vor Ort erläutert. Die identifizierten Risiken werden einem Risikoeigner zugeordnet. Jedem Risiko werden, nach definierten Kriterien, Maßnahmen zur Kompensation zugeordnet. Die Umsetzung der definierten Maßnahmen wird überwacht. Signifikante Risiken werden im Rahmen des Management Review an das Management übermittelt.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

1.5 Assessments

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

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- ZEISS WISA-Live
- Interne_Audits_Managementreview_QEC_DE.docx
- Auditplan_von IQS QEC AP.xlsx
- Management Review CIT-I
- Final Audit Report (ISO 27001 CIT)
- InfoSec Security Dashboard (technische Themen)
- WISA Process

"Es werden alle 2 Jahre über WISA (Wordwide Information Security Assessments) die Umsetzung der Vorgaben in den Standorten bewertet und mit Tasks nachgehalten. CIT wird regelmäßig im Rahmen der 27001 Zertifizierung überprüft. CAR führt ebenfalls interne Audit durch, auch innerhalb der 9001 Zertifizierung werden relevante Prüfungen hinsichtlich Informationssicherheit vorgestellt "

Das WISA für die IQS wurde vor Ort eingesehen und erläutert. Dies wurde zuletzt 2021 durchgeführt. Für 2023 soll der Prozess inkl. RACI-Matrix angepasst werden. Die Verantwortlichkeiten für die Umsetzung von Maßnahmen aus dem WISA wurde definiert. Die Verantwortlichkeit für die Maßnahmen wird je nach Bereich festgelegt. Weiterhin wurde das Management Review für QEC und CIT-I eingesehen. Das interne Audit aus der ISO 27001 (CIT Scope) wurden nachgewiesen.

Feststellung

Maßnahmen, welche zentral gelöst wurden, sollten an die einzelnen Legal Entities im Tool Stream zurückgespielt werden. Diese Dokumentation im Stream könnte konsistenter gestaltet werden. Weiterhin sollten klare Vorgaben (z. B. nach Kritikalität) zur zeitlichen Behandlung von Abweichungen definiert werden.

Hauptabweichung Nebenabweichung Beobachtung Identifiziertes Verbesserungspotential

1.5.2 Inwieweit wird das ISMS von einer unabhängigen Instanz überprüft?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- ISO27001_CIT.pdf

"CIT ist 27001 geprüft (externe Überprüfung). QEC ist im TISAX-Assementprozess"

Neben dem TISAX Assessment durch die OS wurde noch die ISO 27001 Zertifizierung für die CIT nachgewiesen.

Feststellung

Es sollte ein detaillierter Auditplan erstellt werden. Dieser könnte genutzt werden, um sicherzustellen, dass jede Legal Entity bzw. Teilbereich unabhängig überprüft wird.

Hauptabweichung Nebenabweichung Beobachtung Identifiziertes Verbesserungspotential

1.6 Incident Management

<p>1.6.1 Inwieweit werden Informationssicherheitsereignisse verarbeitet?</p>
<p>Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)</p> <p>Betrachtete Dokumente/Nachweise/Prüfungshandlung:</p> <ul style="list-style-type: none"> • SE.02 DE.docx (Sicherheit für Endanwender) • SE.02k DE.pptx (ZEISS Informationsklassifizierung) • Guideline End User DE.docx (Punkt 23) • Live View IT4U • Yammer Info neuer Meldeweg • SE.16 Information Security Incident Management • Use Cases SOC • Live view Security Dashboard • Prototypen-Richtlinie_QEC_München.docx <p>"Security Incidents werden auf mannigfaltige Weise an Corporate Security gemeldet, z.B. per E-Mail an corporate-security@zeiss.com, Incident-Ticket IT4U, Telefon etc. Teilweise wird hier auch das Whistle-Blower-System von Corporate Compliance verwendet. Jeder Vorfall wird dokumentiert (meistens per Ticket) und abgearbeitet. Für Standard-Vorfälle aus unseren Monitoring-Systemen (z.B. SIEM) wurde ein 24x7 SOC (Security Operation Center) eingerichtet. Für Vorfälle, die als „secret“ eingestuft sind, wird die verschlüsselte Ablage (encrypted groupshare mit McAfee FRMP oder Brainloop) von Corporate Security zur Dokumentation verwendet. Ein Security-Dashboard für den Operativen Einsatz ist aktiv im Einsatz. Dabei werden messbare Compliance Verstöße größtenteils automatisiert adressiert. Die Fertigstellung der Entwicklung ist geplant bis 2023. In 2023 wird zusätzlich das Security Incident Modul implementiert. Ansprechpartner bei Auftraggebern sind dokumentiert."</p> <p>Der Prozess wurde vor Ort erläutert. Weiterhin wurden die Aussagen der Nachweisdokumentation validiert. Sicherheitsvorfälle werden zentral erfasst und bewertet. Dazu sind verschiedene Meldewege definiert und den Mitarbeitern bekannt.</p>
<p>Feststellung</p> <p>Die Anforderungen aus Geschäftsbeziehungen sollten erneut bewertet werden. Insbesondere der Feedbackweg zurück zum Business könnte eindeutiger definiert sein.</p> <p><input type="checkbox"/> Hauptabweichung <input type="checkbox"/> Nebenabweichung <input type="checkbox"/> Beobachtung <input checked="" type="checkbox"/> Identifiziertes Verbesserungspotential</p>

2 Human Resources

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

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.07 Personelle Sicherheit DE.docx
- Stellenbeschreibung_Anwendungstechnik_QEC_DE.docx
- Sensible Bereiche_Übersichtsliste.xlsx
- Recruiting Briefingbogen Überarbeitung
- Personalmanagement QEC

"Der Fachbereich teilt dem Recruiter bei der Besetzung einer Stelle mit, wenn es sich um einen sensiblen Tätigkeitsbereich handelt. In diesem Fall wird das Thema vom Recruiter und Hiring Manager im Briefing- und Bewerbungsgespräch berücksichtigt. Die Anforderungen an Mitarbeiter sind über die Stellenbeschreibung in der Personalanforderung, Briefinggespräch (siehe aufgeführten Briefingbogen rechts) und schließlich in der Ausschreibung definiert. Aufgrund der angeforderten Bewerbungsunterlagen und Bewerbungsgespräche wird die Eignung eingehend überprüft. In Bedarfsfällen werden beispielsweise auch Case Studies integriert. Für jeden externen Bewerbungskandidaten wird eine Compliance Überprüfung (Trade Compliance Management 4.0) vorgenommen und der Nachweis der Überprüfung an das Team Entry übergeben. Bei Mitarbeitern aus kritischen Ländern wird der Lebenslauf zur weiteren Überprüfung an die Abteilung Konzernsicherheit weitergeleitet. Persönliche Gespräche werden erst nach Freigabe durch die Konzernsicherheit geführt. Bei ausländischen Bewerbern wird vor Einstellung die Arbeits- und Aufenthaltserlaubnis eingefordert sofern erforderlich."

Im Regelwerk sind die Anforderungen beschrieben. Sensible Stellen sind definiert (z. B. IT oder BISO). Abhängig von der Stelle werden Überprüfungen durchgeführt. Die Identität von Bewerbern wird durch HR geprüft.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

2.1.2 Inwieweit werden alle Mitarbeiter zur Einhaltung der Informationssicherheit verpflichtet?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Verpflichtungserklärungen.PNG
- Arbeitsvertrag_QEC.pdf
- Austrittscheckliste.pdf
- Broschuere_DS_Informationssicherheit (002).pdf
- LP.04f Verpflichtungserklärung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes DE.docx
- SE.02 DE Sicherheit für Endanwender.docx

" Neue Mitarbeiter müssen im Rahmen der Unterzeichnung des Arbeitsvertrages auch eine Verpflichtungserklärung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes abgeben. Zugehörige Anlagen bilden die Datenschutzrichtlinie der ZEISS Gruppe sowie die Broschüre Datenschutz und Informationssicherheit bei ZEISS. Es wird darauf verwiesen, dass Verstöße bestraft werden können und auch arbeitsrechtliche Konsequenzen möglich sind. Die Verpflichtung gilt auch nach Beendigung des Arbeitsverhältnisses weiter."

Vor Ort wurden die genannten Dokumente eingesehen. Weiterhin wurde ein Beispiel für einen Arbeitsvertrag erläutert.

Feststellung

Die Broschüre Datenschutz und Informationssicherheit sollte aktualisiert werden (beispielsweise sind die Passwortanforderungen nicht aktuell).

Hauptabweichung Nebenabweichung Beobachtung Identifiziertes Verbesserungspotential

2.1.3 Inwieweit werden Mitarbeiter über die Risiken beim Umgang mit Informationen geschult und sensibilisiert?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Sicherheitsgrundsätze.pdf
- Verhaltenskodex.pdf
- Auswertung Phising-E-Mail Deutschland
- CurioZ Export

"Sicherheitsrelevante Pflichtschulungen werden im Einarbeitsungsplan aufgeführt. Die Schulung zu Informations- und IT Sicherheits-Themen ALLER Zeiss Mitarbeiter erfolgt durch die eCademy/CurioZ. Alle InfoSec Schulungen sind mandatory und müssen alle 2 Jahre absolviert werden. Die Schulungen werden in über 10 Sprachen weltweit zur Verfügung gestellt. Das System trackt automatisch, erinnert den Benutzer und informiert ggf den Vorgesetzten. Es erfolgen regelmäßige Testmails an Mitarbeiter, die einen möglichen Angriff von Schadsoftware simuliert. Bei Meldung solcher Testemails durch den Mitarbeiter über den sog. Pish Alert erhält der Mitarbeiter die Rückmeldung für sein korrektes Verhalten. Zur weiteren Sensibilisierung erhalten Mitarbeiter beim Eintritt Unterlagen zum Thema Compliance, Sicherheitsgrundsätze sowie eine Beschreibung des Verhaltenscodex bei ZEISS."

Die Mitarbeiter werden zur Informationssicherheit auf verschiedene Art geschult und sensibilisiert. Es werden verschiedene Broschüren bereitgestellt. Vor Ort wurde eine aktuelle Phishing-Kampagne erläutert und die Auswertung eingesehen. Die Schulungen finden jährlich oder bei Einstellung statt. Die Auswertung für die Standorte wurden vor Ort eingesehen. Die Schulung „Compliance“ wurde vor Ort eingesehen.

Feststellung

Eine Planung zu Schulungsinhalten (z. B. eine Roadmap) könnte die Transparenz bzgl. der zu schulenden Inhalte erhöhen. Diese könnte an aktuelle Erfordernisse angepasst werden.

Hauptabweichung Nebenabweichung Beobachtung Identifiziertes Verbesserungspotential

2.1.4 Inwieweit ist mobiles Arbeiten geregelt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- 2021-11_2021-11-09_KBV_Mobile_Arbeit.pdf
- SE.02 DE Sicherheit für Endanwender.docx
- SE.02 und dazugehörige Dokumente.PNG
- LP.04 DE Umgang mit personenbezogenen Daten.docx
- Sicherheits-Leitfaden für Endanwender

"In der Broschüre zum Datenschutz und zur Informationssicherheit und in den Sicherheitsgrundsätzen wird u.a. explizit auf die Verwendung von mobilen Endgeräten und die in diesem Zusammenhang zu beachtenden Regelungen eingegangen. Die Konzernbetriebsvereinbarung zum Moilen Arbeiten verweist in §6 ebenfalls auf diese Regelungen. Maßnahmen zu weiteren Schutzmaßnahmen werden beispielsweise im Rundschreiben vom 29.04.2021 wiederkehrend kommuniziert. Im Rahmen der Arbeitssicherheitsunterweisung und Gefährdungsbeurteilung stehen eine Unterweisungshilfe sowie eine standardisierte Gefährdungsbeurteilung für das mobile Arbeiten in Quentic zur Verfügung. Unterstützend ist über CuioZ z.B. das Training „Computer und Smartphones sicher nutzen“ verfügbar."

Die Anforderungen sind im Regelwerk abgebildet. Der externe Zugriff auf das Unternehmensnetz wird mit einer „zscaler“-Lösung abgesichert.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

3 Physical Security and Business Continuity

3.1.1 Inwieweit werden Sicherheitszonen für den Schutz von Informationswerten gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.11 Physische und umgebungsbezogene Sicherheit DE.docx
- SE.11a Vorgaben für Sicherheit von Liegenschaften und Rechenzentren DE.docx
- Neuburg:
 - Sicherheitszonenplan_NBG.pdf
 - Besuchermerkblatt
- Köln:
 - Sicherheitszonenplan_Köln.pdf
 - Besuchermerkblatt

"Alle schutzbedürftigen Informationen und Assets sind ermittelt. Sicherheitszonen sind entsprechend der ermittelten schutzbedürftigen Informationen bzw. Assets festgelegt worden. Es ist ein Lageplan erstellt mit Kennzeichnung und Beschreibung der einzelnen Zonen. Am Standort sind alle Räumlichkeiten einer Sicherheitszone zugeordnet. Die Anforderungen zum Schutz der Zone sind in der Richtlinie festgehalten. Alle Zugänge sind durch ein elektronisches Schließsystem (Interflex) gesichert. Sicherheitszonen sind durch Schutzmaßnahmen abgesichert worden. Für das Besuchermanagement wird eine Infolyer verwendet. Besucher tragen spezielle Ausweise "

Im Unternehmen sind Sicherheitszonen definiert. Für jede Zone sind Verhaltensregeln definiert. Es besteht ein Fotografierverbot. Besucher werden registriert und müssen begleitet werden.

Neuburg: Alle innenliegenden Bereiche sind der höchsten Sicherheitszone zugeordnet. Die Messräume und das Büro sind alarmgesichert. Diese Bereiche sind zusätzlich durch eine mechanische Schließanlage abgesichert. Es gibt nur eine Tür von außen, welche durch Interflex abgesichert ist. Weitere Türen zur Außenseite können nur von innen geöffnet werden. Es gibt am Standort einen Anlieferungs- und Versandbereich. Maßnahmen zum Schutz gegen einfaches Mithören und Einsichtnahme sind umgesetzt. Es gibt keine externen Liegenschaften am Standort. Die Netzwerkkomponenten sind vor unautorisiertem Zugang geschützt.

Köln: Am Standort ist eine Sicherheitszonenkonzept etabliert. Alle Bereiche sind mit einer Einbruchmeldeanlage ausgestattet. Zugänge sind entweder durch ein elektronisches (Interflex) oder ein mechanisches Schließsystem abgesichert. Alle relevanten Türen sind mit Türkontakten ausgestattet. Es gibt am Standort einen Anlieferungs- und Versandbereich. Maßnahmen zum Schutz gegen einfaches Mithören und Einsichtnahme sind umgesetzt. Es gibt keine externen Liegenschaften am Standort. Die Netzwerkkomponenten sind vor unautorisiertem Zugang geschützt.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

3.1.2 Inwieweit ist in Ausnahmesituationen die Informationssicherheit sichergestellt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Arbeitsumgebung_und_Notfallplanung_QEC_DE.docx
- Notfall-_und_Gefahrenabwehrplan_Carl Zeiss QEC GmbH.docx
- SE.11 Physische und umgebungsbezogene Sicherheit DE.docx
- SE.17 Business Continuity und Krisenmanagement DE.docx
- SE.02 DE Sicherheit für Endanwender.docx
- Informationssicherheit TISAX.docx
- EDV_und_Netzwerkarchitektur_QEC_München.docx
- SE.17 (Business Continuity and Crisis Management)

"Schutzmaßnahmen sind in der SE.11 definiert. Krisen- und Notfallsituationen und deren Handling sind in der SE.17 definiert. Lokaler Notfall und Gefahrenabwehrplan Backup & Archivierung ist zentral geregelt, wird je nach lokalen Anforderungen (Gesetzgebung) umgesetzt. Alle Mitarbeiter sind in der Lage remote/mobile zu arbeiten. Krisenfälle der IT werden durch zentrale Notfallstäben koordiniert."

Die genannten Dokumente wurden vor Ort eingesehen. Ein zentrales Backup ist vorhanden. Es werden keine weiteren Backups lokal angefertigt. Notfallpläne wurden vor Ort erläutert. In Köln wurde eine Evakuierungsübung (28.09.2022) durchgeführt. Es sind zentrale BCM-Prozesse definiert.

Feststellung

Der Netzwerkverteilteraum in Neuburg könnte mit einem Rauchmelder und Feuerlöscher ausgestattet werden. Zukünftig sollten Notfallübungen verstärkt unter Berücksichtigung von Informationssicherheitsaspekten durchgeführt werden.

Hauptabweichung Nebenabweichung Beobachtung Identifiziertes Verbesserungspotential

3.1.3 Inwieweit ist der Umgang mit Informationsträgern gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE Guideline End User DE.docx
- SE.02 DE Sicherheit für Endanwender.docx
- SE.08 DE Asset Management.docx
- Blancco Anweisung
- Rundgang Shredder
- Report Blancco

"Die Speicherung von Informationen auf mobilen Datenträgern ist nicht verboten, sondern soll bei ZEISS vermieden werden. Grundsätzlich sind verschlüsselte Datenträger (z.B. Kingston Sticks oder Bitlocker2Go) zu verwenden. Sichere Verwendung von Betriebsmitteln ist in der SE.02 und in der SE.08 definiert. Systeme werden mit aktuellen Standard Blancco gelöscht. Papierdokumente werden mit Shreddern der Klasse P4 oder höher entsorgt."

An den Standorten sind Shredder vorhanden (P5). Die genannten Nachweise wurden vor Ort eingesehen.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

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

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.12 Corporate Information Security DE.docx
- SE.08 DE Asset Management.docx
- SE.02k Informationsklassifizierung DE.pptx
- SE.02 DE Sicherheit für Endanwender.docx
- SE ZEISS Guideline Informationsklassifizierung DE.pptx
- SE Guideline End User DE.docx
- SE Electronical Handling of Information DE.pptx

"Die Speicherung von Informationen auf mobilen Datenträgern ist nicht verboten, sondern soll bei ZEISS vermieden werden. Grundsätzlich sind verschlüsselte Datenträger (z.B. Kingston Sticks oder Bitlocker2Go) zu verwenden. Alle mobilen Endgeräte werden über ein zentrales MDM (Mobile Device Management System/Airwatch Umstellung auf Intune läuft gerade) verwaltet. Über diese werden alle Sicherheitseinstellungen erzwungen."

Die Aussagen der Nachweisdokumentation wurden vor Ort validiert. Dazu wurden vor Ort Strichprobenprüfungen durchgeführt.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

4 Identity and Access Management

4.1 Identity Management

4.1.1 Inwieweit ist der Umgang mit Identifikationsmitteln gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- CSOP SE.09 EN "Access Control"
- SE.09a EN.xlsx (Authentification Policy Overview)
- Access Control Security Controls.docx
- Schlüsselliste_QEC_München
- Interflex-Zugang NBG
- Schlüsselliste Neuburg
- Schlüsselliste Köln
- SE Company IS Cards (SE.11)

"Ein weltweit gültiges Active Directory, an dem sich alle IT-Benutzer registrieren müssen. Pro User ist nur ein eindeutiger personalisierter Account zulässig
Im Unternehmen werden Mitarbeiterausweise eingesetzt. Diese werden u. a. für die Zutrittskontrollen (Interflex) genutzt. Die Beantragung bzw. Ausgabe der Ausweise werden durch HR verwaltet. Die Sperrung erfolgt im Bedarfsfall durch den Werkschutz. Vereinzelt werden auch Schlüssel eingesetzt."

Der Zutritt wird durch ein elektronisches Schließsystem sichergestellt. Die Mitarbeiterausweise dienen ebenfalls als Schlüsselkarte. Die Zutrittsberechtigungen können befristet werden. Der Beantragungsprozess und eine aktuelle Übersicht der Zutrittsberechtigungen wurden eingesehen. Zusätzlich existieren am Standort Neuburg physische programmierbare Schlüssel. Diese Schlüssel werden durch den Vermieter verwaltet. In Köln werden neben Interflex auch mechanische Schlüssel eingesetzt.

Feststellung

Aktuell ist kein Konzept bei Verlust von Schlüsseln für Neuburg definiert.

Hauptabweichung Nebenabweichung Beobachtung Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)

Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft):

Der Prozess zur (sofortigen) Sperrung ist festzulegen und zu beschreiben.

Nachweis(e):

- Prozessbeschreibung für Verhalten bei Verlust

Die Umsetzung wird gemäß Planung spätestens am 07.06.2023 abgeschlossen sein.

Bewertung nach Follow-Up

Nachweisprüfung am 07.06.2023

Bereitgestellte Nachweise:

- Prototypen-Richtlinie_QEC_München
- Schlüsselausgabe_NBG

Es liegen keine Abweichungen mehr zu den Anforderungen vor.

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

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.09 Zugriffskontrolle DE.docx
- SE.09a EN Authentication Policy Overview.xlsx
- SE.09b Access Control Security Controls EN.docx
- SE.02 DE Sicherheit für Endanwender.docx
- Befugnisse (SharePoint)
- Offboarding-Checkliste für Mitarbeiter
- Security Dashboard
- SE Passwort & PIN Policy
- When is MFA used?

"Jeder Mitarbeiter hat einen eigenen Account, mit dem er sich authentifizieren muss. Anschließend wird er autorisiert und je nach Berechtigung auf Informationen / Applikationen berechtigt. Authentifizierungsverfahren wurde durch die Konzern IT festgelegt. AD/AAD. Erkannte Sicherheitslücken werden gerade im Projekt BestAD bearbeitet. Im AAD wird Multifaktorauthentifizierung eingesetzt. Geräte sind Bitlocker verschlüsselt und benötigen eine PIN oder USB-Stick zum Starten. (2ter Faktor)"

Sammel-Konten werden für Messmaschinen an den Standorten eingesetzt. Diese besitzen restriktive Rechte und können beispielsweise nicht ins Internet. Benutzerkonten werden unmittelbar nach Verlassen der Organisation bzw. Ausscheiden aus der Organisation gesperrt. Die entsprechende Information wird durch HR an die IT gegeben. Die Prozesse sind alle im ServiceNow abgebildet. Eine starke Authentifizierung wird durch eine zusätzlichen persönlichen BitLocker-Pin und die Windows-Anmeldung sichergestellt. Der Zugriff auf Cloud-Dienste von Extern wird über Microsoft-Authenticator sichergestellt.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

4.1.3 Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewandt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE Guideline End User DE.docx
- SE.02 DE Sicherheit für Endanwender.docx
- SE.09 Zugriffskontrolle DE.docx
- SE.09b Access Control Security Controls EN.docx
- SE Password Policy DE.docx
- Live View Dashboard User-Kontrolle

"Ist in der CSOP SE.19 EN Network Security geregelt. Bei ZEISS ist weltweit ein Netzwerk-Standard etabliert, der auch Network Access Control beinhaltet. Somit können nur ZEISS Geräte sich am Netzwerk anmelden. Passwörter sind bei ZEISS als „secret“ eingestuft. Jede erkannte Übermittlung/Weitergabe wird angesprochen, verwarnt und ggf bei Wiederholung sanktioniert. Ein weltweit gültiges Active Directory, an dem sich alle IT-Benutzer registrieren müssen. Pro User ist nur ein eindeutiger personalisierter Account zulässig. Die Einrichtung des Users erfolgt im Onboarding. Die Rechtevergabe erfolgt durch den Vorgesetzten."

Die Aussagen wurden vor Ort verifiziert und die entsprechenden Dokumente eingesehen. Die Anforderungen an Anmeldeinformationen sind entsprechend den Anforderungen des VDA ISA umgesetzt. An den Standorten werden keine Kundensysteme eingesetzt.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

4.2 Access Management

4.2.1 Inwieweit werden Zugriffsberechtigungen vergeben und gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Überprüfung Befugnisse.docx
- SE.09 Zugriffskontrolle DE.docx
- Personalmanagement_QEC_DE.docx
- Informationssicherheit TISAX.docx
- Befugnisse (SharePoint)
- EDV und Netzwerkarchitektur QEC
- SE.09a (Berechtigungskonzept)

" Sonderaccounts werden in der CSOP SE.09 betrachtet, je Sonderaccounttyp (Administratoren-, Service-, Gruppen-, Funktionsaccounts, etc) gelten besondere Regeln. Ein weltweit gültiges Active Directory, an dem sich alle IT-Benutzer registrieren müssen. Pro User ist nur ein eindeutiger personalisierter Account zulässig. Die Zugriffsrechte des Benutzerkontos eines Anwenders wird nach dessen Wechsel (z. B. in einen anderen Verantwortungsbereich) angepasst. Nachweis der Überprüfung nicht nur Rechte vergeben, sondern auch löschen. Jeder Mitarbeiter hat einen eigenen Account, mit dem er sich authentifizieren muss. Anschließend wird er autorisiert und je nach Berechtigung auf Informationen / Applikationen berechtigt"

Die Aussagen wurden vor Ort validiert und die genannten Dokumente eingesehen. Rechteüberprüfungen werden über einen automatischen Prozess im IT4U (ServiceNow) vorgenommen. Diese Überprüfung wird halbjährlich durchgeführt.

Feststellung

Aktuell gibt es keine Projekte mit sehr hohem Schutzbedarf. Daher werden bestehende Zugriffsberechtigungen nicht in kürzeren Abständen überprüft. Laut Aussage ist dies zukünftig vierteljährlich geplant, sofern derartige Daten vorhanden sind.

Hauptabweichung Nebenabweichung Beobachtung Identifiziertes Verbesserungspotential

5 IT Security / Cyber Security

5.1 Cryptography

5.1.1 Inwieweit wird die Nutzung kryptografischer Verfahren gemanagt?
Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)
<p>Betrachtete Dokumente/Nachweise/Prüfungshandlung:</p> <ul style="list-style-type: none">• SE.02 DE.docx (Sicherheit für Endanwender)• SE.02k DE.pptx (ZEISS Informationsklassifizierung)• SE Guideline End User DE.docx• ZEISS Guideline Informationsklassifizierung DE.pptx• SE.08 DE.docx (Asset Security)• SE.13 DE.docx (Communication Security)• SE.10 DE..docx (Cryptpgraphie)• SE.10a EN.docx (Cryptographic controls and Key Requirements)• SE Guideline Encryption.pptx• Prototypen-Richtlinie_QEC_München.docx• SE Baseline Crypto Requirements <p>" Es wird eine aktuelle „state of the art“ Verschlüsselung eingesetzt, z.B. auf Leitungsebene TLS (Transport Layer Encryption). Zusätzlich wird z.B. im E-Mail-Umfeld ZEISS-intern S/MIME, nach extern S/MIME, PGP, und ein WebMailer zur verschlüsselten E-Mail-Kommunikation eingesetzt. AIP (Azure Information Protect) ist verteilt und verfügbar. Bei der Datenablage werden verschlüsselte Groupshares (McAfee File & Removable Media Protection) eingesetzt. Alle Festplatten sind mit BitLocker (Windows) und FileVault (MAC) verschlüsselt."</p> <p>Die Vorgaben zur Verschlüsselung wurden vor Ort erläutert. Die Schlüsselhoheit wurde ebenfalls erörtert. Es gibt eine eigene PKI im Unternehmen (z. B. für NAC, S/MINE, SSL, iOS).</p>
Feststellung
Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.1.2 Inwieweit werden Informationen während der Übertragung geschützt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.02 DE.docx (Sicherheit für Endanwender)
- SE.02k DE.pptx (ZEISS Informationsklassifizierung)
- SE Guideline End User DE.docx
- SE.13 DE.docx (Communications Security)
- SE.13c EN.docx (Communication Security Controls)
- Prototypen-Richtlinie_QEC_München.docx

" Der elektronische Austausch von Informationen ist in der SE.13 generell definiert. Für den Endanwender sind alle notwendigen Informationen in der SE.02 zusammengefasst."

Die Umsetzung der Verschlüsselung für Speicherung und Transport wurde vor Ort erläutert. Im gesamten Unternehmen wird AIP und S/MINE eingesetzt. Für den Austausch wird ebenfalls Brainloop zur Verfügung gestellt. Weiterhin darf WinZip zur Verschlüsselung, z. B. in E-Mail Anhängen, genutzt werden. Im Regelwerk wird ein starkes Kennwort gefordert.

Feststellung

Für die Nutzung von WinZip sollte eine eindeutige Anleitung bzgl. der Verschlüsselung erstellt werden. Die Prototypen-Richtlinie_QEC_München sollte bzgl. der Übertragung mit den zentralen Vorgaben abglichen werden.

Hauptabweichung Nebenabweichung Beobachtung Identifiziertes Verbesserungspotential

5.2 Operations Security

5.2.1 Inwieweit werden Änderungen gesteuert?
Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)
Betrachtete Dokumente/Nachweise/Prüfungshandlung: <ul style="list-style-type: none">• IT.12 EN (IT Servicemanagement)• Process Handbook• MS.04 Auditing und Management Review• CP.09 Änderungen technischer Produktdokumenten• SE.11 physische Sicherheit <p>„Changemanagement ist ein zentraler IT-Prozess, der dem weltweiten ITIL Standard folgt. Changes werden im ServiceNow IT4U beantragt und bearbeitet.“</p> <p>Changemanagement für IT ist in ServiceNow abgebildet. Die Bewertung von Änderungen an Organisations- und Geschäftsprozesse werden durch die BISOs dokumentiert. Prozesse werden bei Änderungen ebenfalls geprüft.</p>
Feststellung
Die Bewertung bzgl. der Informationssicherheit im Changemanagement für Organisations- und Geschäftsprozesse wird aktuell nicht dokumentiert. <input type="checkbox"/> Hauptabweichung <input checked="" type="checkbox"/> Nebenabweichung <input type="checkbox"/> Beobachtung <input type="checkbox"/> Identifiziertes Verbesserungspotential
Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): Es ist zu dokumentieren, welche sicherheitsrelevanten Anforderungen bei Änderungen in der Organisation und Änderungen an kritischen Geschäftsprozessen, bestehen. Dazu ist ein formelles Änderungsverfahren zu definieren und einzuführen. Nachweis: - Dokumentation zur Ermittlung der sicherheitsrelevanten Anforderungen im Unternehmen Die Umsetzung wird gemäß Planung spätestens am 07.06.2023 abgeschlossen sein.

Bewertung nach Follow-Up

Nachweisprüfung am 07.06.2023

Bereitgestellte Nachweise:

- Agendapunkt_Informationssicherheit in Geschäftsprozessen
- Changemanagement Informationssicherheit

Es liegen keine Abweichungen mehr zu den Anforderungen vor.

5.2.2 Inwieweit sind die Entwicklungs- und Testumgebungen von den Produktivumgebungen getrennt?
Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)
Betrachtete Dokumente/Nachweise/Prüfungshandlung: <ul style="list-style-type: none">• SE.14d SAP-Sicherheitsrichtlinie <p>„Test und Entwicklungssystem werden im Prüfscope nicht eingesetzt (not applicable). Corporate IT: SAP 3 Systeme sind nach dem Schema Entwicklung – Test – Produktiv aufgesetzt. Im ZEISS Corporate Network gelten weltweit die gleichen Vorgaben zur Netzwerksegmentierung, die in einem einheitlichen VLAN-Konzept umgesetzt wurden. Dabei werden explizit Entwicklungs- und Produktionsumgebungen, die nicht den ZEISS Sicherheitsvorgaben entsprechen, durch Firewalls abgetrennt.“</p>
Feststellung
N/A – Vor wurde der Ausschluss für die Prüfscope plausibel erläutert. An den betrachteten Standorten werden keine Entwicklungs- oder Testumgebungen betrieben. Die Umsetzung aus der Nachweisdokumentation wurden in einem anderen Assessment nachgewiesen.

5.2.3 Inwieweit werden IT-Systeme vor Schadsoftware geschützt?
Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)
Betrachtete Dokumente/Nachweise/Prüfungshandlung: <ul style="list-style-type: none">• SE.12 DE.docx Operations security• Live view Defender und Info Sec Dashboard• SE.14 DE.docx (Application security) <p>"Endpoints und Server Systeme werden mit MS Defender und McAfee geschützt. Es externe Malwarescanstationen. Zusätzliche Systeme. System ohne aktuellen Schutz werden mit PDN Firewalls isoliert."</p> <p>Vor Ort wurde das Info Sec Dashboard eingesehen und erläutert. Die Umsetzung des Virenschutzes wurde vor Ort stichprobenartig überprüft.</p>
Feststellung
Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.2.4 Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.12 DE.docx Operations security
- SE.14 DE.docx (Application security)
- SOC Use Cases, Log quellen
- SE.14a Guideline for secure application Development

"Security Monitoring ist zentral geregelt und wird bei zentralen Systemen (z.B. Active Directory) zentral erzwungen. Logs werden durch ein SIEM Systeme verarbeitet und archiviert, Das SOC detektiert Anomalien und eskaliert 7/24."

Vor Ort wurden die Logquellen erläutert. Der Zugriff auf Daten mit sehr hohem Schutzbedarf wird entweder über Trellix bzw. AIP protokolliert.

Feststellung

Die regelmäßigen Auswertungen auf Regelverstöße und Auffälligkeiten bzgl. der Daten mit sehr hohem Schutzbedarf könnte erweitert werden. Aktuell werden keine entsprechenden Daten verarbeitet.

Hauptabweichung Nebenabweichung Beobachtung Identifiziertes Verbesserungspotential

5.2.5 Inwieweit werden Schwachstellen erkannt und behandelt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Schwachstellen report , weekly
- Live view Security Dashboard , Rapid 7
- SE.08 DE.docx (Asset Security)
- SE.12 DE.docx (Operations Security)
- SE.12a EN.docx (Vulnerability Management)

"Neben dem zentralen Security-Patching über SCCM und WSUS (Patch-Management) durch IT wird aktives Schwachstellen-Management (regelmäßige Discovery- und Schwachstellenscans) durch Corporate Security betrieben."

Vor Ort wurde das Vulnerability Management erläutert. Für die Clients wird der MS 365 Defender eingesetzt. Server werden mit RAPID7 überwacht. Weiterhin wurde vor Ort das InfoSec Dashboard eingesehen. Notwendige Patches sollen schnellstmöglich bzw. innerhalb von zwei Monaten geschlossen werden. Bei der stichprobenartigen Prüfung des InfoSec Dashboard und der MS Defender wurde keine älteren Patches identifiziert. Updates werden für Clients über das Softwarecenter verteilt.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.2.6 Inwieweit werden IT-Systeme technisch überprüft (Systemaudit)?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.20 DE.docx (Cloud Security)
- SE.20a EN.docx (Security Checklist for Cloud Platform)
- SE.12a EN.docx (Vulnerability Management)
- SE.23 DE.docx (Sicherheit digitaler Produkte)

"Eine Überprüfung von Informationssystemen findet vor Inbetriebnahme im Rahmen des IT Solution Management Prozesses (ehem. IT Demand Prozess), und fortlaufend während des IT-Projektes statt. Dabei wird ein Security Konzept gefordert. Bei weltweiten IT-Projekten ist vor Go-Live ein explizites Audit (meist durch Corporate Security) vorzunehmen. Je nach System werden hier Security Konzepte (z.B. Cloud Checkliste) geprüft, dedizierte Audits gemacht. Externe Systeme werden mit Immuniweb geprüft. Defender für Endpoint überprüft ständig die Einstellung und Patchzustand der Systeme. Rapid7 wird als Schwachstellenscanner unternehmensweit eingesetzt. Zusätzlich werden Pentester hinzugezogen."

Immuniweb wurde vor Ort eingesehen und erläutert. Laut Aussage gibt es keine lokalen Systeme, welche einen einzelnen Pen-Test gerechtfertigt hätten.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.2.7 Inwieweit wird das Netzwerk der Organisation gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.19 DE Network Security
- SE.19a EN (Firewall Rules Approval Criteria).docx
- SE19b EN (Rules for PDN Firewall Usage)
- SE.19c EN.docx (technical requirements)
- Live Demo Netzwerkmanagement

"Das ZEISS Netzwerk ist voll standardisiert und wird zentral durch den Provider „Orange“ betrieben. Das Netzwerk ist durch VLAN segmentiert und durch PDN Firewalls abgesichert. Z.B Produktion und Management VLAN NAC 802.1X ist im Einsatz."

Die Aufteilung der Netze und die Segmentierung wurde in der entsprechenden Verwaltungskonsole eingesehen. NAC ist im Einsatz. Die ITSM Verwaltung für Non-Standard-Clients wurde eingesehen. Diese funktioniert über MAC-Adressen. Für Standard-IT wird eine eigene PKI genutzt. An den Standorten besteht keine Anbindung an Kunden-netze.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.3. System acquisitions, requirement management and development

5.3.1 Inwieweit wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt?
Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)
Betrachtete Dokumente/Nachweise/Prüfungshandlung: <ul style="list-style-type: none">• IT Demand Management• IT 17 (Contract management)• SE.23 DE.docx Digital product security <p>"Die Beschaffung von IT-Systemen folgt einem definierten Vorgehen. Es dürfen generell nur Systeme aus dem IT-Warenkorb beschafft werden. In Demands bzw. daraus resultierenden Projekten werden neue Systeme durch Corporate Security geprüft."</p> <p>Für die Standorte werden keine Software-Lösungen entwickelt. Es werden nur zentrale bereitgestellte Dienste eingesetzt.</p>
Feststellung
Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.3.2 Inwieweit sind Anforderungen an Netzwerkdienste definiert?
Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)
Betrachtete Dokumente/Nachweise/Prüfungshandlung: <ul style="list-style-type: none">• CSOP SE.19 EN (Network Security) <p>" Alle Anforderungen werden in der CSOP SE.19 zusammengefasst. Orange betreibt das Netzwerk und die Standortverbindungen eine redundante Medienanbindung am Standort ist vorhanden. Monitoring ist vorhanden und erfolgt über die Corporate-IT."</p> <p>SD-WAN ist jeweils redundant angebunden. Das Monitoring wurde vor Ort eingesehen. Redundanzlösungen sind jeweils vorhanden.</p>
Feststellung
Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

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

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.20a: Security Checklist for Cloud Platform
- SE.20 DE.docx (Cloud Security)
- APP 07 AT&T
- APP08 Termination Assistance Service

"Das Entfernen von extern gespeicherten Informations-Assets ist vertraglich geregelt. Die Notwendigkeit einer Ausstiegsstrategie wird je IT-Dienstleistung evaluiert. Sollte eine Ausstiegsstrategie angemessen sein, wird ein möglicher Ausstieg aus der Dienstleistung beschrieben und dokumentiert. Dies wird in einem Anhang zum Dienstleistungsvertrag geregelt."

Ramp-Down-Anforderungen werden im Rahmen der Checkliste risikobasiert abgeprüft und ggf. vertraglich vereinbart.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

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

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Tenant Isolation Microsoft
- SE.20 DE.docx, Cloud Security
- SE.14 DE.docx (Application Security)

"Eine wirksame Trennung stellt sicher, dass Nutzer anderer Organisationen nicht auf eigene Informationen zugreifen können. Jeder Cloud Service und jede Cloud Hosted Application muss über ein dokumentiertes Sicherheitskonzept verfügen."

Die Aussagen aus der Nachweisdokumentation wurden vor Ort detailliert erläutert und die genannten Dokumente eingesehen.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

6 Supplier Relationships

6.1.1 Inwieweit wird die Informationssicherheit bei Auftragnehmern und Kooperationspartnern sichergestellt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Lieferantenbewertung SharePoint
- Zertifikate (Nerling Systemräume GmbH; ISO 9001)
- NDA
- CSOP SE.15 Lieferantenbeziehungen DE
- MS.21 Fremdfirmenrichtlinie
- SE.15“ – Supplier Management – Lieferantenbeziehungen (DE)
- Business-Partner-Vertrag - Anlage X – TISAX
- GS.05 Lieferantenmanagement (Auswahl)
- GS.06 Lieferantenbewertung und Controlling
- Beurteilungskriterien SAP-ACS (1-10)

"In den Verträgen sind SLAs definiert, die fortlaufend überwacht und regelmäßig geprüft werden. Zeiss Geheimhaltungsvertrag/-verpflichtung. Sub-Business Supporting Function Homepage (sharepoint.com). Eine Unterbeauftragung findet im Scope nicht statt. Eine Vertragserweiterung zur Umsetzung der TISAX® Anforderungen wurde erstellt."

An den Standorten spielen eigene Lieferanten eine untergeordnete Rolle. Lieferanten werden im Regelfall durch zentrale Prozesse bewertet. Die wenigen eigenen Lieferanten (Reinigung oder Klimawartung) wurden mit der MS.21 zur Informationssicherheit und auf Geheimhaltung verpflichtet.

Feststellung

Die Bewertungskriterien für die lokale Lieferantenbewertung sollten beschrieben werden.

Hauptabweichung Nebenabweichung Beobachtung Identifiziertes Verbesserungspotential

6.1.2 Inwieweit ist Geheimhaltung beim Austausch von Informationen vertraglich vereinbart?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.02 DE.docx (Sicherheit für Endanwender)
- SE.02k DE.pptx (ZEISS Informationsklassifizierung)
- Guideline End User DE.docx
- SE.13 EN.docx (Communications Security)
- MS. 21 Koordination von Tätigkeiten
- NDA deutsch beidseitig.dotx
- MS.21c (Hinweise zu Sicherheit) kann nach Aussage Head Legal als Vertraulichkeitsvereinbarung betrachtet werden.
- NDA Nerling (Klima)
- NDA Gegenbauer Service GmbH

"NDAs (Non Disclosure Agreements), also Geheimhaltungsvereinbarungen werden von „Corporate Legal“ zentral zu Verfügung gestellt und den Mitarbeitern über das ZEISS Managementsystem bereitgestellt."

Die Aussagen aus der Nachweisdokumentation wurden vor Ort validiert und die genannten Dokumente eingesehen.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

7 Compliance

7.1.1 Inwieweit wird die Einhaltung regulatorischer und vertraglicher Bestimmungen sichergestellt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.02 DE.docx (Sicherheit für Endanwender)
- SE.02 DE - Sicherheit für Endanwender und Applicable Documents.JPG
- Schulungen in Curioz
- Erfassungstemplate Compliancemeldungen (Excel)
- Code of Conduct Informationen im Managementsystem
- CM.01 EN WEB.docx
- CM.03 Compliance Management System EN.docx
- Compliance Officer Liste
- FAQ Hinweisgebersystem

"Zur weiteren Sensibilisierung erhalten Mitarbeiter beim Eintritt Unterlagen zum Thema Compliance, Sicherheitsgrundsätze sowie eine Beschreibung des Verhaltenscodex bei ZEISS. In allen Vorgabe Dokumenten werden gesetzliche Bestimmungen als „Input“ adressiert und in den CSOPs bzw. „Applicable Documents“ umgesetzt Pro Standort sind jeweilige Compliance Officer benannt."

Es existiert eine standortbezogene Liste der zuständigen Compliance Officer. Neben Schulungen werden im Intranet weitere Informationen bereitgestellt. Im Unternehmen ist ein Hinweisgebersystem etabliert.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

7.1.2 Inwieweit wird der Schutz von personenbezogenen Daten bei der Umsetzung der Informationssicherheit berücksichtigt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- 2020_02_07_DPC_Certificate_final_QEC.pdf
- LP.04 DE Datenschutzmanagement.
- Datenschutzwiki.jpeg
- LP.04e Template DE Datenschutzrechtliche Vereinbarung zur Auftragsverarbeitung

"ZEISS betreibt eine gruppenweite Datenschutzorganisation. ZEISS unterhält dazu ein einheitliches Datenschutzmanagementsystem. ZEISS strebt ein gruppenweit einheitliches Datenschutzlevel auf Basis der Vorgaben der EU-DSGVO an. Nationale Gesetze und Vorgaben werden dazu ergänzend überwacht und umgesetzt. ZEISS hat einen Konzerndatenschutzbeauftragten benannt und betreibt eine zentrale Datenschutzeinheit. Der zentrale Ansprechpartner ergänzen als Data Protection Coordinator (DPC) diese Strukturen. Die Verantwortung für Datenschutz liegt bei den Geschäftsführungen der Legal Einheiten, bzw. im Executive Management. Der Datenschutzbeauftragte wird aus dem Konzern gestellt."

Die Aussagen aus der Nachweisdokumentation wurden vor Ort validiert und die genannten Dokumente eingesehen.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

8 Prototypenschutz

8.1 Physische und umgebungsbezogene Sicherheit

8.1.1 Inwieweit ist ein Sicherheitskonzept vorhanden, das Mindestanforderungen zur physischen und umgebungsbezogenen Sicherheit für den Prototypenschutz beschreibt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Prototypen-Richtlinie_QEC_Köln.docx
- Zonenplan Köln und Neuburg siehe 3.1.1
- Prototypen-Richtlinie_QEC_München.docx,
- CSOP Prototypenschutz SE.26 DE
- SE.26a Sicherheitskonzept für Prototypen-Bereiche.pdf

Für den Standort wurde eine lokale Richtlinie zum Prototypenschutz erstellt. Diese beinhaltet neben allen relevanten Aspekten des Prototypenschutzes weitere Kunden- bzw. projekt-bezogene Schutzmaßnahmen.

Feststellung

Die Prototypen-Richtlinie sollte in Bezug auf notwendige Inhalte (z. B. Fax) überarbeitet werden.

Hauptabweichung Nebenabweichung Beobachtung Identifiziertes Verbesserungspotential

8.1.2 Inwieweit ist eine Perimetersicherung vorhanden, die einen unberechtigten Zutritt zu schützenden Objekten der Liegenschaften verhindert?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Prototypen-Richtlinie_QEC_Köln.docx
- Prototypen-Richtlinie_QEC_München.docx

Es gibt für die beiden Standorte jeweils eine Prototypen-Richtlinie. Das Gelände ist teilweise eingefriedet. Carl Zeiss ist nur Mieter der Immobilie. Neben Carl Zeiss befinden sich noch andere Mietparteien im Gebäude. Eine vollständige Einfriedung ist nicht angemessen, da nur nicht-designrelevante Komponenten gemessen werden. Diese werden nicht im Außenbereich gehandhabt.

Feststellung

N/A

8.1.3 Inwieweit ist die Außenhaut der zu schützenden Gebäude in einer Form ausgeführt, die ein Entfernen oder Öffnen von Außenhautkomponenten mit handelsüblichen Werkzeugen nicht ermöglichen?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Prototypen-Richtlinie_QEC_Köln.docx
- Prototypen-Richtlinie_QEC_München.docx

Ein unberechtigter Zutritt zu den Räumlichkeiten der Carl Zeiss QEC GmbH ist nicht möglich. Fenster verfügen über eine Widerstandsklasse RC2. Die Gebäude an beiden Standorten sind in einer massiven Bauweise ausgeführt.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

8.1.4 Inwieweit ist ein Sicht- und Einblickschutz in definierte Sicherheitsbereiche gewährleistet?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Prototypen-Richtlinie_QEC_Köln.docx
- TISAX_Prototypen.pptx
- Prototypen-Richtlinie_QEC_München.docx
- Sichtschutz_Messraum.jpg

Sichtschutz ist an den Fenstern im Prototypenbereich angebracht. An beiden Standorten sind angemessene Maßnahmen bzgl. des Sichtschutzes umgesetzt.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

8.1.5 Inwieweit ist der Schutz vor unbefugtem Betreten in Form einer Zugangskontrolle geregelt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Schlüsselliste
- Alarmierungsplan_102766_20230110_111845.pdf
- Alarmprotokoll_20230110_114427.pdf
- EMA_Gebäudeplan_NBG_2.pdf
- Interlexzugänge
- TISAX_Prototypen.pptx

Die angemietete Räumlichkeit verfügt über elektronische bzw. mechanische Schließanlagen. Die Schließanlagen (Interflex) werden durch Carl Zeiss verwaltet. Ein unberechtigter Zutritt in Gebäude / Sicherheitsbereiche ist nicht möglich (Details siehe 3.1.1). Die Umsetzung der restriktiven Vergabe von Zutrittsberechtigungen wurden an beiden Standorten überprüft. Dazu wurde das Berechtigten im elektronischen Schließsystem und die Schlüssellisten eingesehen.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

<p>8.1.6 Inwieweit werden die zu sichernden Räumlichkeiten auf Einbruch überwacht?</p>
<p>Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)</p>
<p>Betrachtete Dokumente/Nachweise/Prüfungshandlung:</p> <ul style="list-style-type: none"> • Alarmierungsplan_102766_20230110_111845.pdf • Alarmprotokoll_20230110_114427.pdf • TISAX_Prototypen.pptx <p>Beide Standorte verfügen über eine Einbruchmeldeanlage. In Neuburg sind nur die Prototypenbereiche und ein Projektbüro in die Überwachung eingebunden. Der Standort in Köln ist vollständig überwacht. Die Einbruchmeldeanlagen sind auf lokale Sicherheitsdienstleister aufgeschaltet. Dies wurde u. a. durch entsprechende Verträge nachgewiesen. Die Einbruchmeldeanlagen werden jeweils durch den letzten Mitarbeiter aktiviert und am Morgen durch den ersten Mitarbeiter deaktiviert.</p>
<p>Feststellung</p>
<p>An beiden Standorten wird die Scharfschaltung nicht überwacht. Daher besteht das Risiko, das die Einbruchmeldeanlagen nicht zum Arbeitsende aktiviert werden.</p> <p><input type="checkbox"/> Hauptabweichung <input checked="" type="checkbox"/> Nebenabweichung <input type="checkbox"/> Beobachtung <input type="checkbox"/> Identifiziertes Verbesserungspotential</p>
<p>Geplante Maßnahmen (incl. Umsetzungszeitraum)</p>
<p>Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft):</p> <p>Die Scharfschaltung der Einbruchmeldeanlagen ist durch den Sicherheitsdienstleister aktiv zu überwachen.</p> <p>Nachweis(e):</p> <p>- Instruktionen für die Sicherheitsdienstleister</p> <p>Die Umsetzung wird gemäß Planung spätestens am 07.06.2023 abgeschlossen sein.</p>
<p>Bewertung nach Follow-Up</p>
<p>Nachweisprüfung am 07.06.2023</p> <p>Bereitgestellte Nachweise:</p> <ul style="list-style-type: none"> • AW_704584-Erweiterung und Optimierung des Sicherheitssystems <p>Es liegen keine Abweichungen mehr zu den Anforderungen vor.</p>

8.1.7 Inwieweit ist ein dokumentiertes Besuchermanagement vorhanden?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- CZ_QEC_Besucherflyer_ab 20220530.pdf
- Zonenplan Interflex_Köln.pptx
- 09_Sicherheitsgrundsätze.pdf
- Allgemeine_Broschuere_alle_Mitarbeiter.pdf
- Prototypen-Richtlinie_QEC_München.docx
- Prototypen-Richtlinie_QEC_Köln.docx

Der Umgang mit Besuchern ist geregelt, es herrscht eine Anmeldepflicht. Besucher müssen allgemeinen Verhaltensregeln unterschreiben. Generell liegt ein Fotografierverbot am Standort vor. Länderspezifische Vorgaben zum Datenschutz werden eingehalten. Eine Geheimhaltung ergibt sich aus Verträgen mit Kunden und Lieferanten. Am Standort Neuburg gibt es keinen Publikumsverkehr, in Köln gibt es einen Publikumsverkehr durch den Schulungsbetrieb. Bei entsprechenden Projekten haben diese keinen Zutritt zum relevanten Bereich.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

8.1.8 Inwieweit ist eine Mandantentrennung vor Ort gegeben?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Prototypen-Richtlinie_QEC_München.docx
- Prototypen-Richtlinie_QEC_Köln.docx
- Zonenplan Interflex_Köln.pptx
- Sicherheitszonenplan_NBG.pptx

Eine Mandantentrennung ist durch zwei getrennte Lager jederzeit möglich. Die Anforderungen sind im Regelwerk abgebildet.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

8.2 Organisatorische Anforderungen

8.2.1 Inwieweit liegen vertragsrechtlich gültige Geheimhaltungsvereinbarungen/ -verpflichtungen vor?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- 2016_GHV_Audi Sport_CZ3D München.pdf
- Prototypen-Richtlinie_QEC_München.docx
- 202_02_07_DPC_Certificate_final_QEC.pdf
- NDA 2020 deutsch beidseitig.dotx
- Prototypen-Richtlinie_QEC_Köln.docx
- NDA Nerling (Klima)
- NDA Gegenbauer Service GmbH
- NDA Sicherheitsdienstleister

Geheimhaltungsvereinbarungen werden zwischen den Auftragnehmern und der Carl Zeiss QEC GmbH abgeschlossen. Geheimhaltungsvereinbarungen zwischen Mitarbeitern / Projektbeteiligten und der Carl Zeiss QEC GmbH werden im Rahmen der Arbeitsverträge abgeschlossen. Zusätzlich wurden vor Ort Beispiele für abgeschlossene Geheimhaltungsvereinbarungen eingesehen.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

8.2.2 Inwieweit sind Vorgaben für die Beauftragung von Unterauftragnehmer bekannt und erfüllt?
Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)
Betrachtete Dokumente/Nachweise/Prüfungshandlung: <ul style="list-style-type: none">• Prototypen-Richtlinie_QEC_München.docx• Prototypen-Richtlinie_QEC_Köln.docx <p>Unterauftragnehmer werden zur Geheimhaltung verpflichtet. Derzeit sind keine Unterauftragnehmer am Standort Köln und Neuburg an der Donau im Einsatz.</p>
Feststellung
Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

8.2.3 Inwieweit werden Mitarbeiter und Projektbeteiligte über den Umgang mit Prototypen nachweislich geschult und sensibilisiert?
Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)
Betrachtete Dokumente/Nachweise/Prüfungshandlung: <ul style="list-style-type: none">• Prototypen-Richtlinie_QEC_München.docx• Prototypen-Richtlinie_QEC_Köln.docx• Teilnahmeprotokoll_Prototypenrichtlinie_NBG_2022.pdf <p>Mitarbeiter und Projektbeteiligte werden im Umgang mit Prototypen geschult. Die Schulung findet auf Basis der Richtlinie statt. Verständnisfragen werden am Ende der Schulung gestellt. Alle relevanten Mitarbeiter sind geschult. Ein digitaler Fragekatalog wird aktuell erstellt. Schulungsunterlagen wurden eingesehen. Die Schulung wird seit 2023 mit einem Fragebogen (MS Format) abgeschlossen.</p>
Feststellung
Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

8.2.4 Inwieweit sind die Sicherheitseinstufungen des Projekts und die daraus resultierenden Maßnahmen zur Absicherung bekannt?
Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)
Betrachtete Dokumente/Nachweise/Prüfungshandlung: <ul style="list-style-type: none">• CSOP SE.26 Prototype Protection• SE.26a DE.docx <p>Die Sicherheitseinstufung ist im Regelwerk verankert. Projektbeteiligten sind die Sicherheitseinstufungen bekannt.</p>
Feststellung
Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

8.2.5 Inwieweit ist ein Prozess zur Zutrittsvergabe in Sicherheitsbereiche definiert?
Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)
Betrachtete Dokumente/Nachweise/Prüfungshandlung: <ul style="list-style-type: none">• CSOP SE.26 Prototype Protection• SE.26a DE.docx• Tool – IT-SM• Überprüfung Befugnisse.docx• Überprüfung Befugnisse_MAYER_2022.pdf <p>Zutrittsberechtigungen werden zentral durch die Carl Zeiss AG verwaltet. Genehmigungsworkflow wurde eingesehen. Der Verlust der Schließmittel ist geregelt und dokumentiert. Es findet eine monatliche Prüfung der Zutrittsliste statt.</p>
Feststellung
Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

8.2.6 Inwieweit sind Regelungen zur Bildaufzeichnung und Umgang mit erstelltem Bildmaterial vorhanden?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Richtlinie Prototypenschutz
- CSOP SE.26 Prototype Protection
- Allgemeine Verhaltensregeln
- SE.02 DE.docx

Es gilt ein generelles Foto- und Filmverbot an den Standorten. Piktogramme finden sich auf den allgemeinen Verhaltensregeln und am strategischen Punkten wieder.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

8.2.7 Inwieweit existiert ein Prozess zur Einbringung und Nutzung von mobilen film- und fotofähigen Endgeräten in definierte Sicherheitsbereiche?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Prototypen-Richtlinie_QEC_Köln.docx
- Prototypen-Richtlinie_QEC_München.docx
- Verpflichtungserklärungen.PNG

Es gilt ein generelles Foto- und Filmverbot an den Standorten. Piktogramme finden sich auf den allgemeinen Verhaltensregeln und am strategischen Punkten wieder.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

8.3 Umgang mit Fahrzeugen, Komponenten und Bauteilen

8.3.1 Inwieweit werden Transporte von als schutzbedürftig klassifizierten Fahrzeugen, Komponenten oder Bauteilen nach den Vorgaben des Auftraggebers abgewickelt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Prototypen-Richtlinie_QEC_Köln.docx
- Prototypen-Richtlinie_QEC_München.docx
- SE.26 DE.docx
- SE.26a DE.docx

Die Anforderungen zum Transport von Prototypenteilen sind dokumentiert und geregelt. Es ist ein Prozess zur Meldung aller sicherheitsrelevanten Vorfälle an den Auftraggeber beschrieben und implementiert. Grundsätzlich wird der Transport über den Kunden geregelt.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

8.3.2 Inwieweit ist sichergestellt, dass als schutzbedürftig klassifizierte Fahrzeuge, Komponenten und Bauteile, den Vorgaben des Auftraggebers entsprechend abgestellt/gelagert werden?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Prototypen-Richtlinie_QEC_Köln.docx
- Prototypen-Richtlinie_QEC_München.docx
- SE.26 DE.docx
- SE.26a DE.docx

Die Anforderungen zur Lagerung und Abstellung sind dokumentiert und vorhanden.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

8.4 Anforderungen für Erprobungsfahrzeuge

8.4.1 Inwieweit werden die vorgegebenen Regelungen zur Tarnung von den Projektbeteiligten umgesetzt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

N/A

8.4.2 Inwieweit werden Schutzmaßnahmen freigegebener Test- und Erprobungsgelände eingehalten/umgesetzt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

N/A

8.4.3 Inwieweit werden die Schutzmaßnahmen für freigegebene Test- und Erprobungsfahrten in der Öffentlichkeit eingehalten/umgesetzt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

N/A

8.5 Anforderungen für Veranstaltungen und Shootings

8.5.1 Inwieweit sind die Sicherheitsvorgaben für Ausstellungen und Veranstaltungen mit als schutzbedürftig klassifizierten Fahrzeugen, Komponenten oder Bauteilen bekannt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

N/A

8.5.2 Inwieweit sind die Schutzmaßnahmen für Film- und Fotoshootings mit als schutzbedürftig klassifizierten Fahrzeugen, Komponenten oder Bauteilen bekannt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

N/A