TISAX® Assessment Bericht

Erstprüfung

Carl Zeiss QEC GmbH

SMT12T

AXCH9W-1

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	SMT12T
Scope-Typ	☒ Standard Scope 2.0 *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 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.* ☐ Erweiterter benutzerdefinierter Scope ☐ Vollständig benutzerdefinierter Scope
Prüfziele	☒ Umgang mit Informationen von hohem Schutzbedarf ☐ Hohe Verfügbarkeit ☐ Umgang mit Informationen von sehr hohem Schutzbedarf ☐ Sehr hohe Verfügbarkeit ☐ Umgang mit schutzbedürftigen Prototypenkomponenten/ -bauteilen ☐ Umgang mit schutzbedürftigen Prototypenfahrzeugen ☐ Nutzung von Erprobungsfahrzeugen ☐ Events und Bildaufnahmen mit schutzbedürftigen Objekten ☐ Umgang mit personenbezogenen Daten gemäß Artikel 28 DSGVO (Auftragsverarbeiter) ☐ 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	Carl-Zeiss-Str. 8a 85748 Garching Deutschland	LHMCN1	Mayer, Katharina katharina.mayer@zeiss.com
Carl Zeiss QEC GmbH	Woltorfer Str.77d 31224 Peine Deutschland	L67NZX	Mayer, Katharina katharina.mayer@zeiss.com

Carl Zeiss QEC GmbH	Felix-Wankel-Str. 6 73760 Ostfildern Deutschland	LHX2TW	Mayer, Katharina katharina.mayer@zeiss.com
Carl Zeiss IMT Austria GmbH Magyarorszagl / Flöktelepe	Gyar u. 2, BITEP Ipari Park 2040 Budaörs Ungarn	LF17HR	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	AXCH9W-1
Assessment Level	AL2
Prüfmethode	☒ Plausibilisierung der Selbstauskunft auf der Grundlage von bereitgestellten Dokumenten und anderen Nachweisen ☒ Detaillierte Überprüfung der Nachweise ☒ Interviews mit prozessbeteiligten Personen ☐ Vor-Ort-Prüfung ☐ Videobasierte Standortprüfung (Remote)
Datum Kick-Off Meeting	17.02.2023
Datum Opening Meeting	11.05.2023
Datum Closing Meeting (Stichtag Gültigkeit)	11.05.2023
Zustimmung des Geprüften	Der Geprüfte ☒ stimmt der sachlichen Korrektheit der Feststellungen zu. ☐ 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

Basierend auf der Erstprüfung ist die Gesamtbewertung des Scopes:

☒ Konform

☐ Nebenabweichend (es existieren ausschließlich Abweichungen, die keine unmittelbar kritischen Risiken erzeugen)

☐ 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).

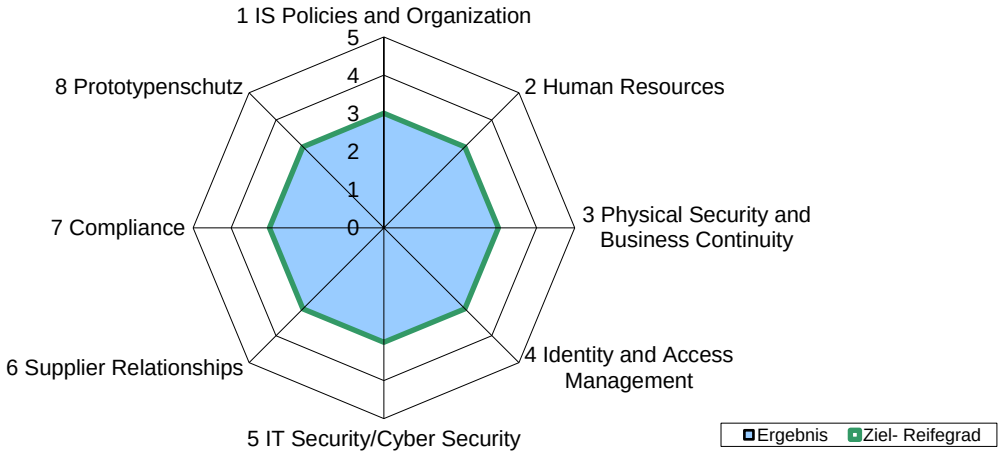
Nach der Erstprüfung errechnet sich ein durchschnittlicher Gesamtreifegrad von 3,0.

Der Gesamtreifegrad ergibt sich aus den Reifegraden des bereits vollumfänglich geprüften Standortes der Firmengruppe (Assessment AX6C8T-2) sowie den Reifegraden der standortspezifisch ausgewählten Prüfpunkte (siehe Teil E).

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

C.1 Erstprüfung

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 Produktivumgebungen 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

Das Prototypenschutzmodul wurde nicht geprüft.

E.1 Datenschutz

Das Datenschutzmodul wurde nicht geprüft.

F. Detaillierte Ergebnisse zum Assessment (Detailed Assessment Results)

1 IS Policies and Organization

1.1 Information Security Policies

1.1.1 Inwieweit sind Richtlinien zur Informationssicherheit vorhanden?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- 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

"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."

Es 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 erläutert. Das Regelwerk bzw. das ISMS wurde 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.

Feststellung

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.

☐ Hauptabweichung ☐ Nebenabweichung ☐ Beobachtung ☒ Identifiziertes Verbesserungspotential

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 Corporate 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 erläutert. Die Wirksamkeit wird in 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
- 2020_02_07_DPC_Certificate_final_QEC.pdf
- Data Protection Coordinator_Certificate_IQS.pdf
- Organigramm_CZIMTA__Gesamt.pdf
- 20201209_Ernennung_MSB_Scheer.pdf
- 20170705_DPC_Certificate_Scheer.pdf
- Mindmap IQS Biso IT
- The Zeiss Security Engineer Programm

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

Die neue Sicherheitsorganisation wurde 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.

Im Interview wurden die lokalen Sicherheitsorganisationen erläutert. Die lokalen Ansprechpartner sind für die jeweiligen Ansprechpartner benannt. Alle BISO haben einen Regelaustausch. Es ist geplant Security Engineer für jeden Standort Ausbildung geplant. Die Planung und das Vorgehen wurden erläutert.

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

"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 erläutert. Kundenprojekte gelten grundsätzlich als vertraulich. Aktuell gibt es keine Projekte mit sehr hohem Schutzbedarf.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

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 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 Direktory, MDM und ITSM Suite) gibt es auch lokale Verzeichnisse."

Es wurden die wesentlichen Informationswerte und Informationsträger ermittelt und deren Verantwortliche festgelegt. Es 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 Sicherheitfür 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 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
- 20230315_IQS_Risk-Reporting_IMT_Austria_sent.xlsm
- CIT- Risk Report Auszug_Q1 _23.pdf

"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. Es wurden die lokale und globale Bewertung eingesehen. Risikobeurteilungen werden sowohl regelmäßig als auch anlassbezogen durchgeführt. Die Bewertung von Risiken wurde 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. Signifikate Risken 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
- audit_planning_IQS
- WISA_Status_IQS_31.05.23

"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 führ ebenfalls interne Audit durch, auch innerhalb der 9001 Zertifizierung werden relevante Prüfungen hinsichtlich Informationssicherheit vorgestellt "

Das WISA für die IQS wurde eingesehen und erläutert. Dies wurde zuletzt 2023 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) wurde nachgewiesen.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

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

1.6.1 Inwieweit werden Informationssicherheitsereignisse verarbeitet?

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 (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

"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."

Der Prozess wurde erläutert. Weiterhin wurden die Aussagen der Nachweisdokumentation validiert. Sicherheitsvorfälle werden zentral erfasst und bewertet. Dazu sind verschiedene Meldewege definiert und den Mitarbeitern bekannt.

Feststellung

Die Anforderungen aus Geschäftsbeziehungen sollten erneut bewertet werden. Insbesondere der Feedbackweg zurück zum Business könnte eindeutiger definiert sein.

☐ Hauptabweichung ☐ Nebenabweichung ☐ Beobachtung ☒ Identifiziertes Verbesserungspotential

2 Human Ressources

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
- Recruting 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 Briefung- 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."

Es 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. Es wurde eine aktuelle Phishing-Kampagne erläutert und die Auswertung eingesehen. Die Schulungen finden jährlich oder bei Einstellung statt. Die Auswertung für die Standorte wurden eingesehen. Die Schulung „Compliance“ wurde 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
- SE.11b DE.pdf Inteflex
- Budaörs:
    - Budaörs_Questionnaire for Physical Security.pdf
    - HUBUA01_Budaörs_Security_Zones.pdf
    - Budaörs.JPG
    - BÖRS-Z-KIV-120403-Földszinti_alaprajz-A0_20230328.pdf
    - HUBUA01_Budaörs_Visitors_Guideline.pdf
    - HUBUA01_Budaörs_Visitors_list_2023.xlsx
    - 20220908_NDA_Beke_Izabella_EV
    - Budaörs_Security
- Garching:
    - Fragebogen physische Sicherheit_2023_Garching.pdf
    - Raumzonenplan_Garching.pdf
- Ostfildern:
    - Fragebogen physische Sicherheit_2023_Ostfildern.pdf
    - Raumzonenplan_Ostfildern.pdf
- Peine:
    - Fragebogen physische Sicherheit_2023_Peine.pdf
    - Raumzonenplan_Peine.pdf
- CZ_QEC_BeBesucherflyer_ab 20220530.pdf
- Fotodoku_QEC Standorte

"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 Infoflyer 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. Für alle Standorte wurden die Schutzmaßnahmen (Zutrittskontrolle, Alarmabsicherung und Sichtschutz) durch Fotodokumentationen nachgewiesen.
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)
- Budaörs_emergency_evacuation_plan.pdf
- Emergency-and-Security_Plan_Carl Zeiss IMT Budaörs.pdf
- 20230109_Tuzvedelmi_Munkavedelmi_oktatas.pdf
- 03 Munka-es tuzvedelmi oktatasi tematikaka - 2022.06.pdf

"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 eingesehen. Ein zentrales Backup ist vorhanden. Es werden keine weiteren Backups lokal angefertigt. Notfallpläne wurden erläutert. Es sind zentrale BCM-Prozesse definiert.

Feststellung

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
- Budaörs:
    - Budaörs_Shredder.jpg
    - Budaörs_Shredder.pdf
    - Blancco-Report Beispiele
- Garching:
    - GBM_Datenschutztonne1.jpeg
    - GBM_Datenschutztonne2.jpeg
    - Zertifikat 20.11.2020 documentus Bayern Kundennr. 408193.pdf
- Ostfildern:
    - OFI_Shredder1.JPG
    - OFI_Shredder2.JPG
- Peine:
    - Peine_Shredder1.jpg
    - Peine_Shredder2.jpg

"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 oder Datenschutztonnen vorhanden. Die genannten Nachweise wurden 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 validiert. Dazu wurden 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
- Access Control Security Controls.docx
- SE Company IS Cards (SE.11)
- Budaörs:
    - HUBUA01_Budaörs_Key-Management.xlsx HUBUA01_Budaörs_Key-_Handover.pdf
- Garching:
    - Schlüssel Liste GBM und Neuburg_2023.pdf
    - Schlüsselausgabe_GBM.pdf
- Ostfildern:
    - Schlüssel Liste Ostfildern_2023.pdf
    - Schlüsselausgabe_OFI.pdf
- Peine:
    - Schlüssel Liste Peine_2023.pdf
    - Schlüsselausgabe_Peine.pdf
- SE.09 DE.pdf Zugriffskontrolle (Access Control)
- SE.11b DE.pdf Interflex Process

"Ein weltweit gültiges Active Directory, an dem sich alle IT-Benutzer registrieren müssen. Pro User ist nur ein eindeutiger personifizierter 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.
Feststellung
Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

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 Authentification 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 Konzert IT festgelegt. AD/AAD. Erkannte Sicherheitslücken werden gerade im Projekt BestAD bearbeitet. Im AAD wird Mulifaktorauthentifizierung eingesetzt. Geräte sind Bitlocker verlüsselt und benötigt 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 Sicherheitfür 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 personifizierter Account zulässig. Die Einrichtung des Users erfolgt im Onboarding. Die Rechtevergabe erfolgt durch den Vorgesetzen."

Die Aussagen wurden 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 personifizierter 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 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)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- 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 (Communicatiion Security)
- SE.10 DE..docx (Cryptpgraphie)
- SE.10a EN.docx (Cryptographic controls and Key Requirements)
- SE Guideline Encryption.pptx
- SE Baseline Crypto Requirements

" 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."

Die Vorgaben zur Verschlüsselung wurden erläutert. Die Schlüsselhoheit wurde ebenfalls erörtert. Es gibt eine eigene PKI im Unternehmen (z. B. für NAC, S/MINE, SSL, iOS).

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)

" 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 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.

☐ Hauptabweichung ☐ Nebenabweichung ☐ Beobachtung ☒ Identifiziertes Verbesserungspotential

5.2 Operations Security

5.2.1 Inwieweit werden Änderungen gesteuert?
Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)
Betrachtete Dokumente/Nachweise/Prüfungshandlung: • IT.12 EN (IT Servicemanagement) • Process Handbook • MS.04 Auditing und Management Review • CP.09 Änderungen technischer Produktdokumenten • SE.11 physische Sicherheit „Changemanagement ist ein zentraler IT-Prozess, der dem weltweiten ITIL Standard folgt. Changes werden im ServiceNow IT4U beantragt und bearbeitet.“ 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.
Feststellung
Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

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

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.14d SAP-Sicherheitsrichtlinie

„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.“

Feststellung

N/A – Der Ausschluss für den Prüfscope wurde plausibel erläutert. An den betrachteten Standorten werden keine Entwicklungs- oder Testumgebungen betrieben. Die Umsetzung aus der Nachweisdokumentation wurde in einem anderen Assessment nachgewiesen.

5.2.3 Inwieweit werden IT-Systeme vor Schadsoftware geschützt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SE.12 DE.docx Operations security
- Live view Defender und Info Sec Dashboard
- SE.14 DE.docx (Application security)

"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."

Das Info Sec Dashboard wurde eingesehen und erläutert. Die Umsetzung des Virenschutzes wurde stichprobenartig überprüft.

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."

Die Logquellen wurden 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.doxc (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."

Das Vulnerability Management wurde erläutert. Für die Clients wird der MS 365 Defender eingesetzt. Server werden mit RAPID7 überwacht. Weiterhin wurde 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 wurden 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 (Vulnerablity 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 Patchtzustand der Systeme. Rapid7 wird als Schwachstellenscanner unternehmensweit eingesetzt. Zusätzlich werden Pentester hinzugezogen."

Immuniweb wurde 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
- Budaörs:
  - Budaörs_IT-Rack.jpg
  - Technical_specifactions_Internet_Budaörs.pdf
  - BITEP_Kft_Carl_Zeiss_internet_1.sz._módosítás.pdf
  - VLAN_Budaörs.jpg
- Garching:
  - VLAN_Garching.jpg
- Ostfildern:
  - VLAN_Ostfildern.j.jpg
- Peine:
  - VLAN_Peine.jpg

"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 Kundennetze.

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:

- IT Demand Management
- IT 17 (Contract management)
- SE.23 DE.docx Digital product security

"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."

Für die Standorte werden keine Software-Lösungen entwickelt. Es werden nur zentrale bereitgestellte Dienste eingesetzt.

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:

- CSOP SE.19 EN (Network Security)

" 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."

SD-WAN ist jeweils redundant angebunden. Das Monitoring wurde eingesehen. Redundanzlösungen sind jeweils vorhanden.

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 wurde 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.
- NDAs in a nutshell_DE.pdf
- NDA 2020 English bilateral.pdf
- Anlage NDA TISISAX Vereinbarung 2021.pdf
- NDA Garching Reinigung (A.Greitner Gebäudereinigung+ Service GmbH) & Sommer Kompressoren GmbH
- NDA Peine PG Gruppe & Co KG
- Vertraulichkeitsformular_Putzfirma_Ostfildern
- 20220908_NDA_Beke_Izabella_EV.pdf

"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 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 Informartionen 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 Datenschutzbeauftrage wir aus dem Konzern gestellt."

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

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.