CGM Austria Information Security and Cybersecurity Controls

Datum der Veröffentlichung:	24.02.2025 / v3.0
Kontakt:	cybersecurity.at@cgm.com

Nr.	Titel	Zielsetzung / Inhalt	ISO 27001:2022 Referenz - Annex A	Anforderung erfüllt		Beschreibung der Maßnahmenumsetzung
1.	**Informationsrisikomanagement**	Durch ein Informationsrisikomanagement wird sichergestellt, dass alle Informationsrisiken (inkl. anderer Risiken wie z.B. IT-Sicherheitsrisiken, Cyber-Risiken und Non-IT-Sicherheitsrisiken) aller Informationen, IT-Anwendungen, IT- und Cloud-Systeme nachvollziehbar und reproduzierbar identifiziert, bewertet und einer Risikobehandlung (Risikovermeidung, Risikotransfer, Risikomitigation, und/oder Risikoakzeptanz) unterzogen werden.	A.5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten			
1.1	Anforderungen bei Nichteinhaltung bzw. Abweichungen von Sicherheitsvorgaben	Das beschriebene Risikkomanagement-Verfahren muss mindestens die folgenden Aspekte gewährleisten. • Die Informationsrisiken müssen strukturiert erfasst werden. • Die Analyse und Bewertung der Informationsrisiken muss nachvollziehbar dokumentiert werden. • Die Geschäftsleitung muss über die gesamte Risikosituation informiert werden.		Ja	✔	Eine Richltinie für das Management von Informationssicherheitsrisiken existiert und ist in bestehende Geschäftprozesse integriert. Informationssicherheitsrisiken werden identifziert, strukturiert erfasst und die Analyse und Bewertung der Risiken wird nachvollziehbar dokumentiert. Aus dem Risiko Assessment ergriffenen Maßnahmen werden im Maßnahmentracking des ISMS nachverfolgt und im Zuge der wiederholten Risikobewertung erneut bewertet und deren Umsetzung auf Wirksamkeit geprüft. Die Geschäftsleitung wird regelmäßig über die gesamte Risikosituation informiert.
2.	**Assetmanagement**	Durch ein Assetmanagement wird sichergestellt, dass verwendeten Informationen, IT-Anwendungen, IT- und Cloud-Systeme und somit die Werte der Organisation identifiziert und Verantwortlichkeiten zu ihrem Schutz festgelegt sind. Somit kann eine potenzielle Offenlegung, Veränderung, Entfernung oder Zerstörung von Information verhindert werden.	A.5.9 Inventar der Informationen und anderen damit verbundenen Werten A.5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten A.5.11 Rückgabe von Werten A.7.10 Speichermedien			
2.1	Inventarisierung von Werten (Assets)	Dokumentierte Prozesse stellen sicher, dass für Informationswerte (inklusive ihrer Schutzbedarfe) inventarisiert sind und aktuell gehalten werden. In diesem Sinne können Informationswerte Prozesse, Informationen, Anwendungen, IT-Systeme, Datenträger/Informationsspeicher, IT-Infrastruktur, Räumlichkeiten und Subunternehmer sein. Für die etablierten und dokumentierten Prozesse müssen Kontrollen vorhanden		Ja	✔	Ein zentrales Assetmanagement wurde aufgebaut und wird betrieben. Dabei werden verschieden Quellen herangezogen um neue Assets automatisch zu identifzieren und zum Assetregister hinzuzufügen.
2.2	Konfigurationsmanagement	Das Konfigurationsmanagement soll sicherstellen, dass in Bezug auf Anwendungen/Verfahren, IDV/EUC System-/Systemnahe-/Sonstige-Software, konfigurierbare Informationsspeicher (z.B. Cloud-Dienste) und IT-Infrastruktur dokumentierte Prozesse implementiert sind. Bei diese Verfahrensweise müssen mindestens folgende Aspekte sicherstellt werden: • Eingesetzte Configuration Items (CI) sind zu verwalten und zu dokumentieren. • Es muss ein Kontrollprozess vorhanden sein, welcher die Datenbank, z.B. CMDB, im regelmäßigen Turnus auf Richtigkeit und Vollständigkeit überprüft		Ja	✔	Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken werden festgelegt, in verschiedenen Systemen (z.B. Assetmanagement, Endpoint-Management, GIT, etc.) dokumentiert, umgesetzt, überwacht und überprüft. Zur Umsetzung dieser Anforderungen werden zT auch Checklisten eingesetzt und zur Kontrolle durch Schwachstellenscans unterstützt. Es werden „Good Practice“ Vorgaben als Grundlage für die Konfiguration von Betriebssystemen und Anwendungen herangezogen und entsprechende Sicherheitsüberprüfungen mit den vorhandenen Schwachstellenscannern durchgeführt. Des Weiteren werden regelmäßige Compliance-Überprüfungen bei ausgewählten Endgeräten stichprobenartig durchgeführt.
2.3	Handhabung, Nutzung, Transport und Entsorgung von Datenträgern	Für die Verwendung von Datenträgern sind Prozesse zu implementieren, welche eine sichere Handhabung von Datenträgern regeln, sodass die Vertraulichkeit der Informationen sichergestellt wird. Die Regelungen müssen die Ausgabe, den Transport, das Löschen und die Entsorgung von Datenträgern umfassen. Es müssen dabei folgende Aspekte sichergestellt werden:		Ja	✔	Es existiert eine Richtlinie zur Klassifizierung, Kennzeichnung, Handhabung und Entsorgung von Informationen und Werten der CGM AT. Darin sind Vorgaben und Regelungen zur zulässigen Handhabung, Nutzung, Transport und Entsorgung von Datenträgern enthalten. Die Nutzung von externen Speichermedien wird durch eine USB-Port Restriktion technisch unterbunden. Ausnahmen dazu unterliegen einem Genehmigungsverfahren, wobei immer die Vorgaben der o.a. Richtlinie gelten.
2.4	Zuständigkeit für Werte	Jedes Asset bzw. Wert muss einem Verantwortlichen wie z.B. Informationseigentümer, Prozesseigentümer, Anwendungseigentümer, etc. zugeordnet sein.		Ja	✔	Zuständigkeiten und Verantwortlichkeiten werden für jedes Asset und Service im zentralgen Assetregister definiert und festgelegt. Aufgaben der Asset Owner bestehen aus • Aktualisierung und regelmäßige Prüfung des Inventars • Klassifizierung und etwaige Kennzeichnung von Werten • Genehmigung und Prüfung von Zugriffen • Patch- und Changemanagement
2.5	Rückgabe von Werten	Bei Austritt oder internem Wechsel von Mitarbeitenden, muss sichergestellt werden, dass nicht mehr benötigte Werte des Unternehmens (Geräte und Betriebsmittel, Informationen, etc.) zurück gegeben werden.		Ja	✔	Die Rückgabe von Werten und IT Equipment ist durch den Austrittsprozess der HR Abteilung geregelt und wird mithilfe einer Checkliste dokumentiert. Dabei dient das Assetregister als Grundlage. Externe Lieferantinnen und Lieferanten und Dienstleistende werden vertraglich zur Rückgabe bzw. Vernichtung von nicht mehr benötigten Werten und Informationen des Unternehmens nach Beendigung des Vertragsverhältnisses verpflichtet. Nach dem Austritt eines Mitarbeitenden (entweder nach Kündigungsfrist od. auch bei sofortigem Austritt) werden alle zugehörigen Accounts gesperrt, wodurch der Zugriff auf und ein Kopieren von Unternehmensinformationen weitestgehend vermieden werden kann.
3.	**Berechtigungsmanagement (Zutritt, Zugang, Zugriff)**	Durch ein Berechtigungsmanagement soll sichergestellt werden, dass der Zutritt zu Gebäuden und Räumen, der Zugang zu informationsverarbeitenden Einrichtungen und der Zugriff auf Informationen auf den betrieblich erforderlichen Zweck eingeschränkt ist. Unbefugte Zutritte, Zugänge und Zugriffe sind unterbunden.	A.5.3 Aufgabentrennung A.5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten A.5.15 Zugangssteuerung A.5.16 Identitätsmanagement A.5.18 Zugangsrechte A.8.2 Privilegierte Zugangsrechte A.8.3 Informationszugangsbeschränkung A.8.4 Zugriff auf den Quellcode			
3.1	Funktionstrennung	Funktionen und Rollen sind zu trennen, wenn eine gemeinsame Ausübung durch eine Person zu Interessenskonflikten führt, das Risiko schädlicher Handlungen erhöht , das Risiko des Missbrauchs und unberechtigter Manipulationen von Unternehmenswerten steigert oder das Ergebnis des Gesamtprozesses beeinträchtigt. In diesem Sinne erarbeitete Funktionstrennungsgebote sind bei der Vergabe von		Ja	✔	Mögliche Rollenkonflikte werden bereits bei der Defintion von Rollen- und Jobbeschreibungen berücksichtigt und bewertet. Sensible Rollen und Tätigkeiten (z.B. Banktransaktionen, Vertragszeichnungen, etc.) unterliegen einem mehrstufigen Verfahren oder dem Vier-Augen-Prinzip.

3.2	Berechtigungsverwaltung	Es müssen dokumentierte Prozesse zur Vergabe (Antrag und Freigabe), Änderung, Entzug (Sperrung, Deaktivierung, Löschung, Rückgabe) und Reaktivierung von Benutzerkonten und Berechtigungen (Zutritt, Zugang, Zugriff) inkl. Notfallberechtigungen und technischer User mit Vorgaben zu Verantwortlichkeiten, Dokumentationspflichten und Nachvollziehbarkeit existieren. Es muss sichergestellt werden, dass zeitnah die Berechtigungen eines Benutzers vollständig berichtbar sind. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Benutzer dürfen nur Berechtigungen besitzen, die zur Aufgabenerfüllung (Need-to-know Prinzip) benötigt werden. • Die Benutzerverwaltung einer Anwendung darf nicht durch ein darunterliegendes bzw. unterstützendes IT-System außer Kraft gesetzt werden. Der Mitarbeiter darf nicht die Möglichkeit haben, die an ihn vergebenen Rechte zu überschreiben, oder über einen direkten Zugriff (z. B. auf eine Datenbank) die auf Anwendungsebene vergebenen Rechte zu umgehen. • Berechtigungen insbesondere auch von technischen und nicht personalisierten Benutzerkonten müssen einer natürlichen Person verantwortlich zugeordnet werden. • Benutzerkonten und Berechtigungen müssen durch etablierte Kontrollen aktuell gehalten werden. • Vergabe, Änderung und Entzug von Berechtigungen inklusive der entsprechenden Genehmigungsvorgänge sind nachvollziehbar zu dokumentieren. • Der Empfänger der Legitimationsmedien muss eindeutig identifiziert werden.		Ja	✔	In der CGM AT gilt das Least Privilege Prinzip für den physischen und logischen Zugang zu Informationen und informationsverarbeitenden Einrichtungen. Somit wird der Zugang für Benutzerinnen und Benutzer nur zu jenen Informationen, Einrichtungen und IT-Systemen erteilt, welche für die Ausübung der jeweiligen Tätigkeit, Aufgabe oder Funktion benötigt werden. Dies wird durch formale und getrennte Genehmigungsverfahren unterstützt und dokumentiert. Die technische Umsetzung des Berechtigungskonzeptes erfolgt über Zero-Trust. Ferner verfügen einzelne Systeme über zusätzliche Konfigurationsmöglichkeiten, welche eine granularere Zugangssteuerung zulassen, obwohl immer das Least Privilege Prinzip einzuhalten ist. Erweiterte oder zusätzliche Rechte werden ausschließlich über das Genehmigungsverfahren gem. Zugangssteuerungsrichtlinie erteilt und dokumentiert.
3.3	Verwaltung privilegierter Berechtigungen	Der Berechtigungsprozess muss zur Verwaltung von privilegierten Berechtigungen mindestens folgendes sicherstellen: • Privilegierte Berechtigungen, die zu administrativen Zwecken verwendet werden, dürfen nicht mit fachlichen Berechtigungen in einer Rolle zusammengefasst werden um Funktionstrennungskonflikte zu vermeiden. • Nicht personalisierte Benutzerkonten mit privilegierten Berechtigungen dürfen ausschließlich für administrative Aufgaben genutzt werden, die nur mit diesem Benutzerkonto durchgeführt werden können. • Privilegierte Berechtigungen (z.B. fachlich umfangreiche Rechte oder Administratorenrechte) müssen bei der Einrichtung und Nutzung protokolliert und gesondert überwacht werden. • Die Nutzung von Notfall- bzw. Superusern ist nur dann zulässig, wenn besondere Eingriffe bzw. Administrationst		Ja	✔	Für privilegierte Zugangsrechte werden gesonderte, personalisierte Benutzerzugänge vergeben. Ausnahmen für Clients können für lokale Administratorrechte für Endbenutzergeräte erfolgen, welche aber einem gesonderten und formalen Genehmigungsprozess unterliegen und nur zeitlich begrenzt gültig sind. Die Vergabe privilegierte Zugangsrechte wird dokumentiert. Wartungszugänge und deren Verwendung werden protokolliert.
3.4	Überprüfung von Berechtigungen (Rezertifizierung)	Es sind dokumentierte Prozesse (Rezertifizierung) zu implementieren, die Berechtigungen für Zutritt, Zugang oder Zugriff mindestens jährlich, kritische Berechtigungen (privilegierte Benutzerkonten) mindestens halbjährlich überprüfen. Diese Prozesse müssen mindestens folgendes sicherstellen: • Alle Zuordnungen von Einzelrechten zu Rollen sowie alle Zuordnungen von Rollen zu Benutzern müssen den fachlichen Anforderungen entsprechen und sind auf Aktualität zu prüfen. • Es ist zu prüfen, dass die tatsächlich in den IT-Systemen und Anwendungen hinterlegten Berechtigungen dem Soll gemäß der Berechtigungskonzepte (Soll-Ist-Abgleich) entsprechen. • Die Zuordnung der nicht personalisierten Benutzerkonten zu den Verantwortlichen inkl. des zur Nutzung berechtigten Personenkreises ist auf Aktualität zu prüfen.		Ja	✔	Benutzerberechtigungen werden im Zuge des internen Kontrollsystems regelmäßig geprüft.
4.	**Verwaltung von Änderungen und Patches**	Durch ein Change- und Patchmanagement soll sichergestellt werden, dass Änderungenen an der IT-Systemlandschaft gesteuert erfolgen und der ordnungsgemäße und sichere Betrieb von informationsverarbeitenden Einrichtungen gewährleistet wird.	A.5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten A.8.32 Änderungssteuerung		
4.1	Kontrolle und Formalisierung von Änderungen	Änderungen an IT-Systemen sind auf Basis dokumentierter Prozesse zu kontrollieren. Zu den Verfahren der „Kontrolle“ gehören dabei Definition, Planung, Priorisierung, Test, Freigabe, Durchführung und Dokumentation der Änderung. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Identifikation und Aufzeichnung von signifikanten Änderungen, • Planung und Testen von Änderungen, • Bewertung der potenziellen Auswirkungen, einschließlich der Auswirkungen auf die Informationssicherheit, solcher Änderungen, • formales Genehmigungsverfahren für vorgeschlagene Änderungen, • Kommunikation von Änderungsdetails an alle relevanten Personen, insbesondere an Kunden, • Fall-Back-Verfahren, einschließlich Verfahren und Verantwortlichkeiten für den Abbruch und die Wiederherstellung nach erfolglosen Änderungen und unvorhergesehenen Ereignissen; • Bereitstellung eines Notfall-Änderungsprozesses, um eine schnelle und kontrollierte Implementierung von Änderungen zu ermöglichen die zur Behebung eines Vorfalls erforderlich sind		Ja	✔	Vorgaben zum IT-Änderungsmanagement sind in einer Richtlinie enthalten. Diese Richtlinie ist allen relevanten Stakeholdern bekannt und berücksichtigt Definition, Planung, Priorisierung, Test, Freigabe, Durchführung und Dokumentation von Änderung an der IT-Systemlandschaft. Durch Einhaltung dieser Richtlinie werden Änderungen gesteuert und negative Auswirkungen auf ein Minimum reduziert werden. OS-Patches werden als Standard-Changes betrachtet und dementsprechend regelmäßig behandelt.
5.	**Schwachstellenmanagement**	Durch ein Schwachstellenmanagement wird sichergestellt, dass Schwachstellen transparent werden und Gegenmaßnahmen zur Ausnutzung dieser Schwachstellen zielgerichtet umgesetzt werden.	A.5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten A.8.8 Handhabung von technischen Schwachstellen		
5.1	Schwachstellenmanagement und Soll-Ist-Abgleich	Über einen dokumentierten Prozess soll sichergestellt werden, dass technische Schwachstellen über technische Schwachstellentests, CERT-Meldungen und Herstellermeldungen identifiziert, bewertet und in einer dem Risiko angemessenen Zeit geschlossen werden, um Anwendungen und IT-Systeme unter Sicherheitsaspekten möglichst aktuell zu halten. Die Patches für Schwachstellen müssen gemäß dem Change-Management in die Produktion überführt werden. Bei Inbetriebnahme und im Anschluss muss ein Abgleich zwischen Soll- und Ist-Konfiguration erfolgen. Abweichungen müssen über das Change-Management behoben werden. Anwendungen und Systeme, die aus dem Internet erreichbar sind, müssen in höherer Frequenz überprüft werden.		Ja	✔	Eine Vulnerability Management Policy exisitert und wurde kommuniziert, welche Vorgaben und Regelungen zur Erkennung und Behandlung von Schwachstellen macht. Grundlage zur Schwachstellenerkennung ist das zentrale Assetregister mit Informationen zu eingesetzten Softwareprodukten und -versionen sowie Vorgaben aus dem Patchmanagement. Die Verantwortung der aktiven Schwachstellenerkennung, Beurteilung von Schwachstellen sowie die Behandlung und Nachverfolgung liegt bei den Produkt- bzw. Service-Ownern. Zudem sind die Produkt- bzw. Service-Owner für die Planung und Initiierung von laufenden Sicherheits-Patches verantwortlich. Zur Erkennung von potentiellen Schwachstellen werden unterschiedliche Tools eingesetzt. Erkannte Schwachstellen werden im zentralen Schwachstellen Register dokumentiert und nachverfolgt. Durch Penetration Tests identifizierte Schwachstellen in selbstentwickelten Softwareprodukten werden mit den jeweiligen Entwicklungsteams besprochen, bewertet und Gegen- oder Abhilfemaßnahmen eingeleitet.

5.2	Penetrationstests	Ergänzend zum Schwachstellenmanagement und zu Soll-Ist-Abgleichen sind für IT-Systeme mit Bezug zur vertragsgegenständlichen Leistung Penetrationstests durchzuführen. Penetrationstests sollen dabei versuchen, das Vorgehen von Angreifern nachzuempfinden und die Kombination mehrerer Schwachstellen eines Systemverbunds auszunutzen. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Die Penetrationstests sind risikoorientiert mit einem Planungshorizont von min. drei Jahren vorauszuplanen. Ergebnisse von vorhergehenden Penetrationstests sind bei der Planung zu berücksichtigen. Der Testplan ist schriftlich zu fixieren und anlassbezogen fortzuschreiben. • Es sind von der Implementierung und von der Betriebsverantwortung unabhängige Penetrationstester einzusetzen und die Penetrationstester bzw. die mit Penetrationstests beauftragte Unternehmen sind in angemessenen Abständen zu wechseln. Als Grundlage sind aktuelle Guidelines und Best Practices des Security Auditing and Testing zu berücksichtigen, wie beispielsweise: • OWASP Web Application Security Testing (WSTG) • Open Source Security Testing Methodology Manual (OSSTMM) • BSI-Studie „Durchführungskonzept für Penetrationstests“ • Ermitteln spezifischer Bedrohungen mit Threat Modeling (STRIDE Ansatz)		Ja	✔	Vorgaben hinsichtlich Penetration Tests werden in einen themenspezifischen Richtlinien geregelt. Vulnerability Assessments und Penetration Tests werden jährlich geplant und durch externe Partner durchgeführt. Zudem werden unsere Produkte teilweise auch durch Kundinnen und Kunden selbst auf technische Schwachstellen geprüft und die Ergebnisse sofern relevant an CGM AT mitgeteilt. Derartige Penetration Tests erfolgen aber immer erst nach Abstimmung mit dem Kunden und der CGM und werden in der Regel auf Testumgebungen gemacht.
6.	**Sicherheitsvorfall-Management**	Durch ein Security Incident Management wird sichergestellt, dass eine konsistente und wirksame Herangehensweise für die Handhabung von Informationssicherheitsvorfällen einschließlich der Benachrichtigung über Sicherheitsereignisse und Schwächen erfolgt.	A.5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten A.5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen A.6.8 Meldung von Informationssicherheitsereignissen A.5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse A.5.26 Reaktion auf Informationssicherheitsvorfälle A.5.27 Erkenntnisse aus Informationssicherheitsvorfällen A.5.28 Sammeln von Beweismaterial		
6.1	Umsetzung eines Sicherheitsvorfall-Management-Prozesses	Für eine organisierte und standardisierte Reaktion auf einen potenziellen Verstoß gegen die Informationssicherheit muss ein Security Incident Management (SIM) betrieben werden. Dieses Vorgehen muss mindestens folgendes sicherstellen: • folgende Ausprägungen von Ereignissen müssen bei der Definition des Security Incidents Management mindestens berücksichtigt werden: Allgemeiner Störfall, Security Event (Potenzieller Security Incident) und Security Incident • Das SIM muss dokumentierte Verfahren zur Überwachung, Erkennung, Analyse, Bewertung, Klassifizierung, Behebung sowie zur Berichterstattung über Security Incidents und Security Events umfassen. • Regelungen zur Initiierung der Beweissicherung inkl. forensischer Analysen sowie zur Protokollierung von Security Incidents sind zu etablieren. • Die Ergebnisse der Bewertung und Klassifizierung von Security Events und Security Incidents sind zu dokumentieren, um die Nachvollziehbarkeit zu gewährleisten.		Ja	✔	Ein Prozess und Kriterien zur Beurteilung von und Entscheidung über Informationssicherheitsereignisse ist vorhanden und im Group Security Operations Center (SOC) etabliert. Bei Informationssicherheitsereignissen, welche die CGM AT direkt betreffen, wird immer der Information Security Coordinator der CGM AT hinzugezogen. Für die Reaktion auf Informationssicherheitsvorfälle ist ein Prozess vorgegeben. Einzelne Vorfallsszenarien werden über sogenannten Runbooks dargestellt und werden bei der Behandlung von Sicherheitsvorfällen herangezogen. Erkenntnisse aus Informationssicherheitsvorfällen werden in regelmäßigen Jours Fixes mit allen Stakeholdern besprochen und fließen in die Risikobewertung ein, um erneute Vorfälle dieser Art zukünftig zu verhindern. Für forensische Tätigkeiten im Rahmen eines Sicherheitsvorfalls werden externe Partner hinzugezogen, mit denen Vertragsverhältnisse bestehen. Das Sammeln von Beweismitteln darf nur nach Freigabe durch die Geschäftsführung erfolgen.
6.2	Melden von Schwachstellen	Es müssen Prozesse zum organisierten und standardisierten Umgang mit Verstößen gegen die Informationssicherheit definiert und implementiert sein. Derartige Verstöße liegen vor, wenn Daten hinsichtlich ihrer Verfügbarkeit, Vertraulichkeit oder Integrität beeinträchtigt werden, beobachtete oder vermutete Schwachstellen vorhanden sind, oder ein entsprechender Verdachtsfall vorliegt. In der Prozessdefinition sind Verantwortlichkeiten, Meldepflichten und -wege, Bewertungsverfahren, Analyseverfahren, Reaktionszeiten, Dokumentations-, Informations- und Beweissicherungspflichten sowie Eskalationsverfahren zu regeln.		Ja	✔	Die Meldung von potenziellen Sicherheitsvorfällen erfolgt immer an das Security Operations Center (SOC), um dem Prinzip des Single Point of Contact zu folgen und somit Informationen für nachfolgende Risikoassessments oder Lessons Learned gesammelt verfügbar zu haben. Diese Meldestelle und Verhaltensregeln bei Sicherheitsvorfällen für Mitarbeitende wird geschult und per Plakate an den Standorten und Flyer für die einzelnen Mitarbeitenden veröffentlicht. Alle Mitarbeitenden werden laufend geschult bzw. informiert, um das Bewusstsein für die Meldung von Informationssicherheitsereignissen und potentiellen Schwachstellen zu steigern. Z.B. Metacompliance-Schulung: Meldung von Sicherheitsvorfällen Lieferantinnen und Lieferanten und Dienstleistende (Dritte) werden mit Vereinbarungen zum Datenschutz, Vertraulichkeit und zur Informationssicherheit ebenfalls zur Meldung von Informationssicherheitsereignissen und potentiellen Schwachstellen vertraglich verpflichtet. Im Zuge des Datenpannen - Notfallplan der BU AIS AT und Datenpannen - Notfallplan der BU CAT wird die verpflichtende Meldung von Informationssicherheitsvorfällen und Datenpannen an u.a. Geschäftsführung und die Informationssicherheits-Beauftragte/den -Beauftragten beschrieben.
7.	**Störfall- und Problemmanagement**	Durch das Problemmanagement wird sichergestellt, dass unbekannte Ursachen für tatsächliche und potentielle Störungen (Incidents) innerhalb der IT-Services reaktiv und proaktiv untersucht werden, die Behebung gesteuert und eine dauerhafte Problemlösung herbeigeführt wird.	A.5.29 Informationssicherheit bei Störungen A.5.30 IKT-Bereitschaft für Business Continuity		
7.1	Erkennung, Aufzeichnung, Kategorisierung, Priorisierung, Untersuchung und Lösung von Problemen	Die Prozesse müssen Regelungen zum Problemmanagement umfassen, um die Ursachen von Incidents sowie Schwachstellen in der Servicelandschaft zu identifizieren und deren Beseitigung zu initiieren. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Schnittstellen zum (Security) Incident Management, zum Kapazitäts- und Performancemanagement; zu Externen (z.B. Dienstleistern oder Herstellern) und zum Schwachstellenmanagement sind zu definieren. • Informationen aus dem Incident Management (z. B. Incident Reports) müssen regelmäßig analysiert werden. • Die für die Problembearbeitung relevanten Daten müssen dokumentiert (Problem Record) und während der Bearbeitung laufend aktualisiert werden (z. B. im Ticket-System zum Incident Management).		Ja	✔	Der etablierte Support-Prozess umfasst auch Regelungen und Vorgaben zum Problemmanagement, um die Ursachen von Incidents sowie Schwachstellen in der Servicelandschaft zu identifizieren und deren Beseitigung zu initiieren. Sofern der Verdacht eines Sicherheitsvorfalls besteht, wird der Security Incident Management Prozess aktiviert. Stör- und Problemfälle werden im bestehendne Ticketsystem dokumentiert und nachverfolgt. Geltende Sicherheitsanforderungen müssen auch während eines Störfalls eingehalten werden. Ausnahmen unterliegen einem Freigabeverfahren und werden dokumentiert.

7.2	Störungserfassung, -dokumentation und -behandlung	Geschäftsprozesse müssen Regelungen zum Incidentmanagement umfassen, um Störungen mit dem Ziel der schnellstmöglichen Wiederherstellung der gestörten Dienste zu erfassen und zu behandeln. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Schnittstellen zum Security Incident Management, zum Kapazitäts- und Performancemanagement; zu Externen (z.B. Dienstleistern oder Herstellern), zum Schwachstellenmanagement, zum Business Continuity Management, zum Notfall- und Krisenmanagement sowie zum IT-Service Continuity Management sind zu definieren. • Der Incident Management Prozess muss mindestens Verfahren zur Identifikation, Nachverfolgung, Protokollierung, Klassifikation und Priorisierung von Vorfällen in Abhängigkeit zu Service-Vereinbarungen umfassen.		Ja	✔	
8.	**Kapazitäts- und Performancemanagement**	Durch das Kapazitäts- und Performancemanagementwird sichergestellt, dass für den Betrieb ausreichend technische Systemressourcen zur Verfügung stehen.	A.8.6 Kapazitätssteuerung		
8.1	Kapazitätsmanagement	Es sind dokumentierte Prozesse und Techniken zu implementieren, die die Bereitstellung ausreichender Systemressourcen und Kapazitäten für die Erbringung der vertragsgegenständlichen Dienstleistung gewährleisten. Dazu gehören Aufgaben der Bedarfserhebung, -planung und -überwachung. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Die Kapazitätsanforderungen müssen unter Berücksichtigung der Betriebswichtigkeit des betroffenen Systems festgestellt werden, um die Verfügbarkeit der Systeme sicherzustellen und ggf. zu verbessern. • Es müssen technische Überwachungssysteme und Kontrollen eingerichtet sein, mit denen Verfügbarkeits-, Kapazitäts- und Performanceengpässe rechtzeitig erkannt werden. • Es ist regelmäßig zu überprüfen, wie hoch die zukünftigen Kapazitätsanforderungen sind. Dabei sind neue geschäftliche und systembezogene Anforderungen sowie aktuelle und zukünftige Trends bezüglich der informationsverarbeitenden Einrichtungen des Unternehmens in Betracht zu ziehen.		Ja	✔	Zur Kapazitätssteuerung werden Daten und Informationen aus dem Monitoring herangezogen und reglemäßig bewertet. Daraus resultierende Ergebnisse sowie Geschäftsanforderungen werden für die Ressourcenplanung berücksichtigt. In Kundenprojekten werden Schwellenwerte mittels SLAs vereinbart und überwacht. Die Steuerung von Budget- und Personalressourcen erfolgt mind. jährlich durch die Geschäftsleitung, wobei Anforderungen und geplante Projekte aus IT und Informationssicherheit berücksichtigt werden. Regelmäßige Jours Fixes werden mit der Kundin/dem Kunden zur Überwachung und Steuerung von Kapazitäten abgehalten, sofern die Zuständigkeit der Betriebsführung bei der CGM liegt.
9.	**Informationssicherheitsaspekte im Notfallmanage**	Aufrechterhaltung der Informationssicherheit im Kontext des Business Continuity Managements (BCM), des IT-Service Continuity Managements (IT-SCM) und des Notfall- und Krisenmanagements (NuK). Dabei sind Risiken frühzeitig zu erkennen und geeignete Präventivmaßnahmen zu treffen, die die Ausfallsicherheit der wichtigen Geschäftsprozesse erhöhen sowie eine anforderungsgerechte Wiederaufnahme der Geschäftstätigkeiten in einem Not- oder Krisenfall ermöglichen.	A.5.29 Informationssicherheit bei Störungen A.5.30 IKT-Bereitschaft für Business Continuity A.8.14 Redundanz von informationsverarbeitenden Einrichtungen		
9.1	Berücksichtigung von Informationssicherheitsaspekten im Notfallmanagement	Die Prozesse müssen im Rahmen des BCM, IT-SCM und NuK auch Maßnahmen zur Wahrung der Informationssicherheit und zur Aufrechterhaltung des Informationssicherheitsmanagements im Not- und Krisenfall umfassen. Der Schutz von Informationen ist unverändert auch im Not- und Krisenfall durch entsprechende Maßnahmen kontinuierlich zu gewährleisten. Es soll dabei sichergestellt werden, dass die Verantwortlichen für das BCM, das IT-SCM und das NuK die Maßnahmen zur Aufrechterhaltung der Informationssicherheit mindestens jährlich auf Aktualität und Vollständigkeit kontrollieren. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Aspekte der Informationssicherheit müssen bereits während der Planungsphase bzw. bei der Aktualisierung der Prozesse berücksichtigt werden. • Die Auswirkungen eines Ausfalls sind in Bezug auf die Informationssicherheit zu beurteilen. • Benötigte Ressourcen müssen für die Durchführung eines Notbetriebs zur Gewährleistung des Informationsschutzes erhoben werden.		Ja	✔	Business Continuity Management ist Bestandteil der IS Policy und des Informationssicherheitsmanagements bei CGM. Ein ISM- und BCM Framework existiert, wodurch Aspkete der Informationssicherheit in die Geschäftskontinuität und Resilienz der CGM integriert sind. Dies wird bereits bei der Planung und Konzipierung neuer Geschäftsprozesse berücksichtigt. Bei der Erstellung von Business Continuity- und Notfallplänen werden Informationssicherheits-Risiken berücksichtigt und bewertet und Maßnahmen zur Durchführung eines Notbetriebs umgesetzt.
9.2	Verfügbarkeit und Redundanz für informationsverarbeitende Systeme	Es ist ein Redundanzkonzept zu definieren, das beschreibt, wie geforderte Verfügbarkeit (maximale Wiederherstellungszeit und maximaler Datenverlust) auch bei Ausfall von Komponenten aufrechterhalten werden kann. Die Maßnahmen sind mindestens jährlich zu testen. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Es ist eine Verfügbarkeitsübersicht mit folgenden Inhalten zu erstellen: o geforderte Verfügbarkeit je Anwendung und unterstützende IT-Systeme; o maximale Zeit bis zur vollständigen Wiederherstellung im Regelbetrieb (Recovery Time Objective, RTO) unter Berücksichtigung der maximal tolerierbaren Ausfallzeit; o maximal tolerierbarer Datenverlust im Regelbetrieb (Recovery Point Objective, RPO). • Soweit Assets hinsichtlich ihrer Funktionalität voneinander abhängen, sind erforderliche Verfügbarkeiten und Redundanzen in Korrelation zu wählen. Das Redundanzkonzept muss alle relevanten Bestandteile der Elementkette aus Anwendung, IT-System, weiteren IT-Komponenten und Daten berücksichtigen. Hierbei sind auch Kumulations- bzw. Verteilungseffekte zu berücksichtigen. • Redundanzen sind kontinuierlich zu überwachen. Die Verfügbarkeit der Schutzobjekte gemäß der Verfügbarkeitsliste ist zu messen und zu überwachen. Bei negativen Abweichungen von der geplanten Verfügbarkeit ist eine Prüfung der Redundanzspezifikation und der umgesetzten Maßnahmen vorzunehmen.		Ja	✔	Anforderungen an die Verfügbarkeit inkl. Wiederherstellungskriterien (MTDT, RTO, RPO) von Prozessen und Services, sowie von darunterliegenden Systemen werden anhand einer BIA festgelegt. Informationsverarbeitenden Einrichtungen und Systeme werden hinsichtlich ihrer Kritikalität und Verfügbarkeitsanforderungen redundant ausgelegt. Redundanzen werden regelmäßig auf deren Funktion getestet.
10.	**Sicherheit in Projekten**	Durch die Sicherheit in Projekten wird sichergestellt, dass die Umsetzung der Informationssicherheit in Projekten eingeleitet und gesteuert wird.	A.5.8 Informationssicherheit im Projektmanagement		
10.1	Informationssicherheit in Projekten	Ungeachtet der Art des Projekts, muss die Informationssicherheit im Projektmanagement berücksichtigt werden. Die Anforderungen an die Informationssicherheit in Projekten müssen daher bereits während der Erstellung der Projektauftragsbeschreibung ermittelt und in allen Phasen des Projektes beachtet werden.		Ja	✔	Informationssicherheit wird im Projektmanagement berücksichtigt, ungeachtet der Art des Projekts. Entweder wird bei Kundenprojekten/-programmen bereits in der Ausschreibungsphase der Informationssicherheitsbeauftragte (CISO) involviert oder bei internen Projekten im Zuge des Projekt-Kick-Offs. Bei Bedarf wird der Datenschutzbeauftragte konsolidierend hinzugezogen. Der Status zu Projekten sowie geplante Vorhaben werden auch in den regelmäßigen (quartalsweise) Management Meetings, bei denen auch der CISO ständiges Mitglied ist, vorgestellt und diskutiert.

11.	**Personalsicherheit**	Durch Personalsicherheit wird sichergestellt, dass interne und externe Beschäftigte ihre Verantwortlichkeiten bezüglich der Informationssicherheit verstehen, diesen nachkommen und für die für sie vorgesehenen Rollen geeignet sind. Ein angemessenes Bewusstsein für Informationssicherheit muss bei Führungskräften und Mitarbeitenden geschaffen und aufrechterhalten werden. Der Schutz der Interessen und Informationen des Unternehmens sind auch nach der Beendigung des Vertragsverhältnisses sichergestellt.	A.6.1 Sicherheitsüberprüfung A.6.2 Beschäftigungs- und Vertragsbedingungen A.5.4 Verantwortlichkeiten der Leitung A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.6.4 Maßregelungsprozess A.6.5 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung		
11.1	Personaleinstellungsprüfung	Um die Zuverlässigkeit des Personals zu gewährleisten, müssen unter Berücksichtigung einschlägiger Gesetze, Verordnungen und ethischer Grundsätze, während des Einstellungsverfahrens Hintergrundüberprüfungen durchgeführt werden. Dazu zählen die Überprüfungen von Leumundszeugnissen, Lebensläufen, akademischen und beruflichen Qualifikationen, den Identitäten sowie den Führungszeugnissen. Die Art und der Umfang der Überprüfungen haben sich nach den Bereichen, in denen die Bewerber beim Auftragnehmer eingesetzt werden sollen, zu richten. Die Überprüfung von Bewerbern muss einem definierten Ablauf folgen.		Ja	✔ Im Rahmen des Recruiting-Prozesses werden Lebensläufe auf Vollständigkeit und bei Bedarf auch auf Richtigkeit geprüft. Lücken im Lebenslauf werden im Falle eines Bewerbungsgespräches direkt mit dem Bewerber besprochen. Qualifikationen (vor allem hervorstechende) werden geprüft. Vor allem für Positionen, in denen mit sensiblen Daten gearbeitet wird, ist das Wissen bzw. die Einschätzung der Vertrauenswürdigkeit der potentiellen Kandidaten ein wichtiger Bewertungsfaktor. Je Kandidat erfolgt eine erste Sichtung auf Basis der schriftlichen Bewerbungsunterlagen, die im Regelfall aus Lebenslauf, Motivationsschreiben, Qualifikationsnachweise und Dienstzeugnisse bestehen. Diese Unterlagen werden akribisch und systematisch geprüft. Bei Managementpositionen (ab dem Seniority Level B3 (Senior Manager) und Mitarbeitenden, welche aufgrund ihres Jobprofils mit Kundendaten in Cloud-Services in Berührung kommen, erfolgt eine erweiterte Sicherheitsüberprüfung durch einen externen Partner.
11.2	Schulungen zur Informationssicherheit	In Bezug auf die Informationssicherheit sind interne und externe Mitarbeitende entsprechend dem jeweiligen Bedarf, der sich aus ihrem Aufgabenbereich ergibt, zu schulen. Die Mitarbeitenden sind in die Lage zu versetzen, die an sie gestellten Informationssicherheitsanforderungen zu kennen und zu beachten sowie Informationssicherheitsvorfälle zu erkennen und zu melden. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Schulungen sind bei Aufnahme der Tätigkeit durchzuführen und regelmäßig zu wiederholen. • Der jeweilige Schulungsbedarf ist risikoorientiert aus der Aufgabenstellung herzuleiten.		Ja	✔ Ein Security & Privacy Awareness Programm wird jährlich geplant und umgesetzt, welches Schulungen und Trainings in den Bereichen Informationssicherheit, Cyber Security und Datenschutz mithilfe eines Schulungsplattformen ausrollt. Anlassbezogen, z. B. nach Informationssicherheitsvorfällen oder Audits, werden im Zuge des kontinuierlichen Verbesserungsprozesses im Bedarfsfall ebenfalls Schulungen abgehalten. Grundsätzliche Sicherheitanforderungen und Verhaltensregelen werden im Rahmen eines On-Boarding Oline-Kurses, sowie eines Boarding Days geschult und durch ein Enduser Security Memo an neue Mitarbeitende kommuniziert. Fachspezifische Weiterbildungsmaßnahmen werden regelmäßig identifiziert, geplant und umgesetzt.
11.3	Verpflichtung der Mitarbeitenden auf die Einhaltung der Regelungen zur Informationssicherheit	Die Mitarbeitenden müssen auf die Einhaltung der Informationssicherheitsleitlinie verpflichtet werden. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Ein Prozess, der disziplinarische bzw. arbeitsrechtliche Maßnahmen für Mitarbeitende initiiert, die gegen Vorgaben der Informationssicherheit verstoßen haben, ist zu implementieren. • Die Mitarbeitenden sind darüber zu informieren, dass bei Zuwiderhandlungen Disziplinarmaßnahmen ergriffen werden können und dass bei vorsätzlichen oder grob fahrlässigen Verstößen auch strafrechtliche Maßnahmen eingeleitet werden können. • Alle Mitarbeitenden, die Zugang zu nicht öffentlichen Informationen des Unternehmens und desse Kunden erhalten, müssen eine Vertraulichkeitserklärung unterzeichnen, bevor sie Zugang zu Einrichtungen der Informationsverarbeitung erhalten.		Ja	✔ Bereits bei Eintritt in das Unternehmen verpflichten sich Mitarbeitende durch Unterzeichnung des Dienstvertrages zur Einhaltung der Regelungen zur Informationssicherheit und zum Datenschutz. Externe Mitarbeitende werden durch die Unterzeichnung eines NDA (siehe Vertraulichkeitsvereinbarungen) bzw. durch Sicherheitsunterweisungen (vgl. Zutrittsregelung RZ od. Besucherregelung) auf die Einhaltung von Sicherheitsrichtlinien verpflichtet. Bei Nichteinhaltung von Sicherheitsvorgaben und bei Verstößen gegen Sicherheitsrichtlinien, wird ein Maßregelungsprozess angestoßen.
12.	**Überprüfung der Informationssicherheit durch Fachbereiche oder Prüfer**	Durch die Überprüfung der Informationssicherheit durch Fachbereiche oder Prüfer wird sichergestellt, dass Informationssicherheit in Übereinstimmung mit den Richtlinien und Verfahren der Organisation umgesetzt und angewendet wird, sodass insbesondere keine Unterbrechungen im Geschäftsbetrieb aufgrund einer Überprüfung erfolgen.	A.8.34 Schutz der Informationssysteme während der Überwachungsprüfung A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit		
12.1	Durchführung von Prüfungen und Audits für Informationssysteme	Prüfungs- und Audit-Aktivitäten, die eine technische Überprüfung von IT-Systemes beinhalten, müssen geplant werden. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Alle Aktivitäten sind so zu planen und durchzuführen, dass die Verfügbarkeit, Vertraulichkeit und Integrität der Daten gewährleistet bleiben. • Die sicherheitsgebenden Bereiche (z.B. IT, Infrastruktur- und Gebäudemanagement, Berechtigungsmanagement) müssen jährlich die von ihnen verantworteten Prozesse überprüfen bzw. durch externe Audits überprüfen lassen und dokumentieren, ob die aus den Sicherheitsvorgaben abgeleiteten Maßnahmen angemessen umgesetzt wurden.		Ja	✔ Prüfungen und Audits von Informationssystemen erfolgen einerseits automatisch mithilfe von diversen Tools und werden andererseits regelmäßig durch unabhängige Auditorinnen und Auditoren (intern und extern) durchgeführt. Audits werden dabei über einen Zyklus von drei Jahren in einem Auditprogramm geplant und nachverfolgt.
13.	**Sicherheit im Anwendungsbetrieb**	Durch die Sicherheit im Anwendungsbetrieb wird sichergestellt, dass Informationssicherheit ein fester Bestandteil über den gesamten Lebenszyklus von Informationssystemen ist. Dies beinhaltet auch die Anforderungen an Informationssysteme, die Dienste über öffentliche Netze bereitstellen.	A.8.26 Anforderungen an die Anwendungssicherheit		
13.1	Anforderungen an Internetapplikationen	Internetapplikationen müssen vor Angriffen geschützt werden. Dabei sind gängige Maßnahmen und Best Practices, die gegen entsprechende Bedrohungen wirken und dem Stand der Technik entsprechen (z.B. OWASP Top 10, BSI Leitfaden zur Entwicklung sicherer Webanwendungen), zu ergreifen.		Ja	✔ Eine Secure Software Development Lifecycle (SSDLC) ist implementiert. Dabei werden Sicherheitspraktiken und Best Practices (z.B. OWASP Top 10) in den täglichen Entwicklungsprozess integriert. Für Webanwendungen gelten verplichtende Sicherheitstests, welche erfolgreich absolviert werden müssen (Quality Gates) bevor diese zum Einsatz kommen.
13.2	Mehrmandantensysteme	Bei Anwendungen und IT-Systemen, auf die mehrere Mandanten Zugriff haben, müssen die Daten der Mandanten so getrennt und unabhängig voneinander verarbeitet werden, dass die Daten der Mandanten untereinander nicht einsehbar oder veränderbar sind (Mandantentrennung). Dieses Vorgehen muss mindestens folgendes sicherstellen: • Die Benutzer der Mandanten müssen sich bei der Anmeldung über eindeutige Merkmale authentisieren. • Sämtliche administrative Tätigkeiten und Verfahren (z. B. Konfiguration, Berechtigungs- und Benutzerverwaltung, Datensicherung, Datenrücksicherung, Wiederherstellung, Aktualisierung von Software und Hardware) müssen so ausgestaltet sein, dass zu jeder Zeit die Mandantentrennung aufrechterhalten bleibt.		Ja	✔ Durch den SSDLC werden auch Prinzipien der sicheren Softwarearchitektur angewendet, welche die Sicherheit von Mehrmandantensystemen gewährleisten.
14.	**Anwendungs- und Betriebsdokumentation**	Durch die Anwendungs- und Betriebsdokumentation wird sichergestellt, dass der ordnungsgemäße und sichere Betrieb von informationsverarbeitenden Einrichtungen dokumentiert ist und allen Benutzern, die sie benötigen, zugänglich sind.	A.5.37 Dokumentierte Betriebsabläufe		

14.1	Anwendungs- und Betriebsdokumentation	Für IT-Systeme und Anwendungen muss – für sachverständige Dritte verständliche – Dokumentationen erstellt werden und diese aktuell gehalten werden. Insbesondere sind folgende Dokumentationen vorzuhalten: • technische Betriebsdokumentation mit der Beschreibung von Installation und Konfiguration, Datensicherungs- und Wiederherstellungsverfahren, Batchläufen/Betriebsroutinen, Umgang mit Fehlersituationen, Anforderungen an System-Start und –Restart, Verfahren zum Logging und Monitoring sowie Anforderungen an RPO und RTO bei einem Systemausfall und/oder einem Datenverlust, • fachliche Dokumentation der fachlichen Funktionen mit dem Fokus auf Enduser, • eine Sicherheitsdokumentation mit der Beschreibung der Sicherheitsmaßnahmen zur Erreichung des erforderlichen Schutzniveaus (insbesondere Härtung) und der bekannten Abweichungen von Sicherheitsvorgaben und daraus resultierenden Restrisiken sowie • ein Berechtigungskonzept mit der Beschreibung der Rollen, Berechtigungen, Zuordnungen von Usern, Verfahren zur Berechtigungsvergabe und regelmäßigen Überprüfung.		Ja	✔	Interne IT-Prozesse sind in einem Betriebsführungshandbuch dokumentiert und mit Verantwortlichkeiten versehen. Für selbstentwickelte Anwendungen und Produkte werden Installationsanleitungen und Benutzerhandbücher bereitgestellt, welche auch Sicherheitsdokumentation enthalten. Notfall- und Wiederherstellungspläne sind Teil der Notfalldokumentation.
15.	**Informationsübertragung**	Durch die Sicherheitsvorgaben zur Informationsübertragung wird sichergestellt, dass die Vertraulichkeit, Integrität und Verfügbarkeit übertragener Information, sowohl innerhalb einer Organisation als auch mit jeglicher externer Stelle, aufrechterhalten wird.	A.5.14 Informationsübertragung A.5.23 Informationssicherheit für die Nutzung von Cloud-Diensten A.6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen			
15.1	Policies und Prozesse zur Informationsübertragung	Es müssen Regeln für die Nutzung von Kommunikationseinrichtungen und die Übertragung von Informationen etabliert werden. Diese Regeln müssen die Verantwortung der Mitarbeitenden bei der Übertragung unternehmenseigener und dienstleistungsbezogener Informationen, die erlaubten Kommunikationskanäle und -einrichtungen sowie die ergriffenen Maßnahmen zur Gewährleistung einer sicheren Informationsübertragung beinhalten. Nur genehmigte Kommunikationsmittel und -kanäle für die Informationsübertragung dürfen genutzt werden und ein unberechtigtes Abfangen, Kopieren, Verändern oder Zerstören von Informationen muss verhindert werden.		Ja	✔	Es gelten die in der Richtlinie zur Klassifizierung, Kennzeichnung, Handhabung und Entsorgung von Informationen und Werten definierten Anforderungen an die Informationsübertragung. Zur sicheren Kommunikation werden Kommunikationskanäle und Datenaustauschplattformen (File Sharing) genutzt. Anforderungen und Vereinbarungen zur Informationsübertragung sind im Dienstvertrag, in der Richtlinie zur Klassifizierung, Kennzeichnung, Handhabung und Entsorgung von Informationen und Werten und im Datenschutzmanagementsystem enthalten. Zudem werden mit externen Partnerinnen und Partnern Vereinbarungen hinsichtlich Vertraulichkeit und Informationssicherheit getroffen. Zum Schutz der Informationen während der Übertragung werden folgende Verfahren und Maßnahmen eingesetzt: • Verschlüsselte Netzwerkkommunikation (TLS), wo technisch umsetzbar • Einsatz von Software zur Erkennung und zum Schutz vor Schadsoftware • organisatorische Maßnahmen und Verfahren (Richtlinien, Prozessanweisungen) zur Festlegung von Anforderungen an die Informationsübermittlung • Awareness Schulungen aller Mitarbeitenden • elektronische Signatur bei Emails • geschützter Datenaustausch via File Sharing Plattformen
15.2	Sicherheit in E-Mail-Systemen	Bei der Nutzung von Systemen für den externen E-Mail-Verkehr über das Internet sind die folgenden Anforderungen zu beachten: • Das unmittelbare Ausführen von via E-Mail empfangenen Programmen ist zu verhindern. • Es sind Filtermechanismen zu etablieren, die potenziell schadhafte E-Mails in einem Quarantäneverzeichnis speichern (anstatt sie direkt dem Adressaten zuzustellen).		Ja	✔	Filtersysteme erkennen und blockieren böswillige Absender sowie schädliche Inhalte in E-Mails und Anhängen. Eingehende E-Mail-Anhänge werden sowohl auf dem E-Mail-Server als auch am Client-Endpunkt gescannt. Bei Erkennung von infizierten E-Mails oder Anhängen werden diese gelöscht oder in Quarantäne verschoben, und der Empfänger wird informiert. Wird Malware in ausgehenden E-Mails entdeckt, wird die Zustellung blockiert.
15.3	Sicherheit bei der Verwendung von Cloud-Services	Stellt die Dienstleistung selbst einen Cloud-Service dar oder wird die Dienstleistung unter Verwendung eines Cloud-Service erbracht, ist vom Auftragnehmer folgendes zu gewährleisten: • Die Dokumentation des Cloud-Services muss die eingesetzten IT-Komponenten, die Verantwortlichkeiten für dessen Betrieb, die zugrundeliegenden Service Level, die Funktionen, die auf Auftragnehmer verlagert sind, sowie die Verfahren bei unvorhergesehenen Situationen definieren. • Alle im Zusammenhang mit der Dienstleistungserbringung in dem Cloud-Service gespeicherten Informationen muss der Auftragnehmer bei einem kurzfristigen Vertragsende (z.B. auch bei Insolvenz) in einem allgemein als weiter verarbeitbar angesehenen elektronischen Format (z.B. csv, XML) bereitstellen. • Ein nachvollziehbares Backup-, Restore- und Löschkonzept für die Daten des Auftraggebers ist zu erstellen und kann auf Wunsch des Auftraggebers jederzeit angewandt werden. • Auf Wunsch des Auftraggebers können die Orte der Datenspeicherung eingeschränkt werden. • Daten müssen verschlüsselt übertragen werden. Als Grundlage sind aktuelle Guidelines und Best Practices zu berücksichtigen, wie beispielsweise: • ISO/IEC270017 - Cloud Security • ISO/IEC270018 - Datenschutz-Standard für Cloud-Dienste		Ja	✔	Es existiert eine Richtlinie zur sicheren Verwendung von Cloud-Diensten welche sich an der ISO/IEC 27017 und ISO/IEC 27018 orientiert. Vor der Nutzung von Cloud-Diensten erfolgt ein Risk Assessment, welches auch eine Datenschutzfolgenabschätzung beinhaltet. Zudem wird ein Sicherheitskonzept erstellt, welches Verantwortlichkeiten und Zuständigkeiten regelt, sowie Anforderungen der Datensicherheit und -verfügbarkeit adressiert.
15.4	Nutzung des Internet	Die Regeln zum Umgang der Mitarbeiter und Subunternehmer mit dem Internet sind vom Auftragnehmer zu kommunizieren und aktuell zu halten. Die Anforderungen sind abhängig von der Risikoeinschätzung des jeweiligen Arbeitsumfelds abzustufen. Die Regeln müssen sich insbesondere auf die folgenden Punkte beziehen: • zugelassene Programme für die Nutzung des Internets, • Herunterladen von Programmen und • Überwachung des Internetverkehrs, insbesondere Sperrung von Adressen und Protokollierung auf Proxy-Ebene. Der Auftragnehmer hat die Komponenten, die die Nutzung des Internets für Mitarbeiter des Auftragnehmers ermöglichen, nach aktuellem Stand der Technik zu schützen.		Ja	✔	Der Zugang zu externen Websites wird durch einen Internet Access Proxy geschützt, um die Gefährdung durch bösartige Inhalte zu verringern. Dabei wird der Zugriff auf Ressourcen im Internet überwacht und auf Bedrohungen reagiert. Alle installierten Softwareprogramme müssen einem legitimen Geschäftszweck dienen. Software ohne geschäftlichen Nutzen, wie z.B. Spotify, Tor Browser, Spiele-Launcher, Messenger-Clients und Torrent-Clients, ist strengstens verboten. Alle Mitarbeitenden werden gemäß der Software use Policy geschult.
16.	**Kryptographische Verfahren**	Durch kryptographische Verfahren wird sichergestellt, dass der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität und Integrität von Information erfolgt.	A.8.24 Verwendung von Kryptographie			

16.1	Auswahl und Einsatz kryptographischer Verfahren sowie Schlüsselerzeugung und –verwaltung	Sofern eine Verschlüsselung von Daten auf IT-Systemen aufgrund deren Vertraulichkeitsanforderungen erforderlich ist, müssen folgende Punkte gewährleistet werden: • Ein Kryptokonzept muss erstellt und gepflegt werden, das die Anwendungsbereiche und Verantwortlichkeiten regelt und sicherstellt, dass nur kryptographische Verfahren nach dem Stand der Technik eingesetzt werden, die nicht wesentlich geschwächt oder gebrochen sind. • Die Erzeugung, Verteilung, Installation und Verwaltung von Schlüsseln muss vertraulich, nach dem Stand der Technik und unter Nutzung zuverlässiger Hilfsmittel erfolgen. • Die jeweiligen Gesetze und ggf. existierende vertragliche Verpflichtungen mit Dritten müssen beachten werden. Insbesondere sind Gesetze zur Kryptographie in der jeweiligen Jurisdiktion zu berücksichtigen. • Für den Einsatz digitaler Signaturen müssen dokumentierte Prozesse etabliert sein.		Ja	✔	Eine Richtlinie Kryptographie, welche sich an der technischen Richtlinie BSI TR-02102 orientiert, ist erstellt und veröffentlicht. Die Entscheidung des Einsatzes sowie die Auswahl von kryptographischen Maßnahmen erfolgt basierend auf der Klassifizierung der Daten risikoorientiert. Die Einhaltung der kryptographischen Maßnahmen wird regelmäßig durch Schwachstellenscans überprüft. Anforderungen an die Schlüsselverwaltung sind ebenfalls in der Richtlinie enthalten. Kryptografisches Schlüsselmaterial wird entweder über eine Public Key Infrastructure verwaltet oder für öffentliche Dienste über vertrauenswürdige öffentliche Zertifikatsstellen ausgestellt. Der private Schlüssel verlässt dabei nie das anfragende System.
17.	**Datensicherung und Archivierung**	Durch die Datensicherung und Archivierung wird sichergestellt, dass Informationen und Daten vor Verlust geschützt sind. In IT-Systemen und Anwendungen verarbeitete Informationen sind zu speichern und aufzubewahren, sodass diese bei Bedarf jederzeit unter Berücksichtigung der Vertraulichkeits- und Integritätsanforderungen wiederhergestellt werden können.	A.8.13 Sicherung von Information		
17.1	Datensicherung und Datenhaltung	Es müssen dokumentierte Prozesse zur Datensicherung der Informationen, der verwendeten Software und der IT-Systeme etabliert sein. Insbesondere muss ein Datensicherungskonzept implementiert und dessen Einhaltung kontrolliert werden. Das Konzept muss insbesondere folgende Punkte regeln: • Häufigkeit, Ausprägung, Zeitpunkt und Aufbewahrungsdauer sowie Anzahl der Generationen der Sicherungen, • Zutritt-, Zugangs- und Zugriffskontrollen (inkl. Verschlüsselung) für die Datensicherungen sowie physische Trennung der Sicherungen vom betroffenen IT-System sowie • Testverfahren zur Überprüfung der Integrität und Wiederherstellbarkeit der Datensicherungen.		Ja	✔	Verantwortlichkeiten und Zuständigkeiten für die Datensicherung von Services sind definiert. Gesicherte Systeme, Zeiträume und Methoden sind in der jeweiligen Konfiguration der Backupumgebung vorhanden. Backups werden täglich auf Fehler geprüft. Restoretests werden bei Bedarf anhand von Echtfällen gemacht und protokolliert. Der Zugriff auf Backups ist gemäß dem Need2Know-Prinzip eingeschränkt und Backupmedien werden in getrennten Räumlichkeiten (off-site) sicher aufbewahrt.
17.2	Archivierung	Ein Archivierungskonzept muss implementieren und dessen Einhaltung kontrolliert werden. Das Konzept muss insbesondere folgende Punkte regeln: • Häufigkeit, Ausprägung und Zeitpunkt der Archivierung sowie Aufbewahrungsdauer der Archive, • Zutritt-, Zugangs- und Zugriffskontrollen (inkl. Verschlüsselung) für die Archive sowie physische Trennung der Archive vom betroffenen IT-System und Maßnahmen zum physischen Schutz der Archive sowie • Testverfahren zur Überprüfung der Integrität und Wiederherstellbarkeit der Archive.		Ja	✔	Verträge, Rechnungen und relevante Dokumente werden archiviert und entsprechend gesetzlicher Aufbewahrungspflichten gespeichert. Der Zugriff auf Archive wird gemäß dem Need2Know-Prinzip eingeschränkt. Für Archive existieren Löschkonzepte, deren Einhaltung regelmäßig im Rahmen von Datenschutzaudits überprüft wird.
18.	**Passwortmanagement und Authentisierung**	Durch das Passwortmanagement wird sichergestellt, dass Informationen durch befugte Benutzer nur nach Identitätsprüfung eingesehen und verarbeitet werden können.	A.5.17 Informationen zur Authentifizierung A.8.5 Sichere Authentifizierung		
18.1	Passwortkomplexität	Für die Authentifizierung von Benutzenden am Netzwerk und an IT-Systemen sind sichere Passwörter zu benutzen. Insbesondere sind die Mindestlänge, die Anzahl der zu nutzenden Zeichentypen, die maximale Gültigkeit und die Komplexität der Passwörter (z.B. keine Begriffe aus Wörterbüchern, keine einfachen Tastatur-Zeichenfolgen, keine Verwendung von Namen oder User-ID) zu regeln. Mit zunehmenden Privilegien des jeweiligen Kontotyps müssen auch die Anforderungen an das Passwort steigen.		Ja	✔	Anforderungen an die Passwortkomplexität sowie die Verwaltung und der Umgang mit Passwörtern sind in einer Password Management Richtlinie geregelt und kommuniziert. Diese Regeln gelten für alle Mitarbeitenden und IT-Systeme.
18.2	Passwortübermittlung/-speicherung	Es müssen Regeln zum Umgang mit Passwörtern/Authentisierungshilfsmitteln existieren, die z.B. die Erstellung und Übertragung vor erstmaliger Nutzung, die Speicherung/Aufbewahrung, die Dokumentation und den anlassbezogenen und regelmäßigen Passwortwechsel sowie die Sperrung von Benutzerkonten bei Überschreitung einer definierten Anzahl von falschen Passworteingaben beschreiben. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Es muss ein dokumentierter Prozess zur eindeutigen Identifizierung des Empfängers implementiert sein. • (Initial-)Passwörter müssen dem Benutzer auf sichere Art und Weise übergeben werden. • Passwörter dürfen nicht im Klartext gespeichert werden.		Ja	✔	Neuen Mitarbeitenden werden die initiale Zugangsdaten im Rahmen des Onboardings ausgehändigt, welche nach deren erstmaligen Nutzung geändert werden sowie ein zweiter Faktor aktiviert werden muss. Mitarbeitende dürfen keine Passwörter oder PIN-Codes mit anderen, einschließlich Vorgesetzten oder Kollegen, teilen – kein Passwortsharing. Unternehmenspasswörter müssen stets von privaten Passwörtern getrennt werden, und für unterschiedliche Systeme sind verschiedene Passwörter zu verwenden. Benutzer dürfen Passwörter oder PIN-Codes nicht in Computerdateien speichern, wie z.B. in Anmeldeskripten oder Programmen, es sei denn, sie sind sicher mit autorisierter Verschlüsselungssoftware verschlüsselt. Zur Verwaltung von Authentifzierungsinformationen werden Passwordmanager zur Verfügung gestellt. Systemadministratoren und technisches Personal dürfen niemals die Offenlegung persönlicher Passwörter oder PIN-Codes verlangen. Standardpasswörter werden bei der erstmaligen Konfiguration geändert.
19.	**Systemhärtung**	Durch die Systemhärtung wird sichergestellt, dass die vorhandenen Angriffsflächen durch die Grundkonfigurationen minimiert werden.	A.8.9 Konfigurationsmanagement		
19.1	Härtung von IT-Systemen	Für alle IT-Systeme sind Härtungsvorgaben zu pflegen, zu dokumentieren, anzuwenden und deren Einhaltung zu kontrollieren. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Nicht benötigte Komponenten, Module, Benutzer, Dienste, Schnittstellen, Diagnose- und Admin-Ports sowie temporäre Ablagen sind zu deaktivieren bzw. zu entfernen. • Systemeigene Sicherheitsparameter sind zu aktivieren. • Sicherheitsempfehlungen der Hersteller müssen geprüft und risikoorientiert umgesetzt werden. • Geräte mit Diagnose- und Konfigurationsports (z. B. Managementport bei aktiven Netzwerkkomponenten) sind gegen einen unberechtigten Zugang abzusichern. • Nach Stand der Technik unsichere Dienste müssen durch sichere Varianten ersetzt werden (z. B. ssh statt telnet, sftp oder ftps statt ftp).		Ja	✔	Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken werden festgelegt, in verschiedenen Systemen dokumentiert, umgesetzt, überwacht und überprüft. Zur Umsetzung dieser Anforderungen werden zT auch Checklisten eingesetzt und zur Kontrolle durch Schwachstellenscans unterstützt. Es werden „Good Practice“ Vorgaben als Grundlage für die Konfiguration von Betriebssystemen herangezogen und entsprechende Sicherheitsüberprüfungen mit dem vorhandenen Vulnerabilityscanner durchgeführt. Des Weiteren werden regelmäßige Compliance-Überprüfungen bei ausgewählten Endgeräten stichprobenartig durchgeführt.
20.	**Netzwerk- und Systemmanagement**	Durch das Netzwerk- und Systemmanagement wird sichergestellt, dass der Schutz von Information in Netzwerken und den unterstützenden informationsverarbeitenden Einrichtungen gewährleistet ist. Darüber hinaus wird sichergestellt, dass der kontrollierte Zugang zu Netzwerken im Unternehmen sowie der sichere Betrieb der Netzwerke und Netzwerkdienste im Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit durch Überwachung und Steuerung erfolgt.	A.5.15 Zugangssteuerung A.8.20 Netzwerksicherheit A.8.21 Sicherheit von Netzwerkdiensten A.8.22 Trennung von Netzwerken A.8.23 Webfilterung		

20.1	Zugang zu Netzwerken und Netzwerkdiensten	Es sind dokumentierte Prozesse zu implementieren, die eine kontrollierte Benutzung von Netzwerken und Netzwerkdiensten umfassen. Die Kontrollen stellen mindestens sicher, dass: • nur berechtigte und identifizierte Benutzer:innen über zugelassene Geräte Zugriff auf Netzwerkressourcen haben; • alle Netzwerkressourcen inventarisiert sind; • Fernzugriffe nur für definierte Anwendungsbereiche zugelassen sind, stets verschlüsselt und kontrolliert erfolgen; • Netzwerke und insbesondere Netzwerkübergänge mit Schutzmechanismen nach Stand der Technik ausgestattet sind und dauerhaft hinsichtlich sicherheitsrelevanter Ereignisse und Anomalien überwacht werden; • Alle Systeme zur Überwachung sicherheitsrelevanter Ereignisse strukturiert ausgewertet werden.	Ja	✔	Regelungen und Vorgaben zur Netzwerksicherheit sind in einer Network Security Policy enthalten. Bei der CGM wird eine Netzwerksicherheitsarchitektur nach dem Zero-Trust Model umgesetzt, wodurch jeder einzelne Zugriff auf Unternehmensressourcen geprüft und autorisiert wird. Perimeternetze sowie Netzübergänge sind mithilfe von Firewalls oder mindestens ACLs geschützt. Zur Überwachung werden alle sicherheitsrelevanten Ereignisse in einem SIEM gesammelt und auch Anomalien überprüft, wobei Alarmierungen gemäß dem Security Incident Response Prozess behandelt werden.
20.2	Netzwerksegmentierung	Das Netzwerk ist in separate Netzwerkdomänen (i.d.R. unterschiedliche IP-Adressbereiche) aufzuteilen. Die Vorgehensweise und die Kriterien zur Trennung sind zu dokumentieren und umzusetzen. Der Bereich der einzelnen Netzwerkdomänen muss definiert und dokumentiert werden.	Ja	✔	Eine Netzwerksegmentierung ist vorhanden und dokumentiert. Der Zugriff bzw. die Kommunikation zwischen den Netzwerksegmenten ist eingeschränkt und geregelt.
20.3	Sicherheit in Netzwerken	Firewalls haben eine besondere Funktion beim Schutz von Unternehmensnetzwerken. Folgende Anforderungen sind beim Betrieb von Firewalls zu berücksichtigen: • Grundsätzlich muss jeglicher Verbindungsaufbau gesperrt werden. Verbindungen dürfen nur nach erfolgter und dokumentierter Genehmigung in einem formalen Prozess freigegeben werden. • Zur Vermeidung des ungehinderten Ausbreitens von Schadsoftware oder nicht autorisierten Zugriffen ist das Netzwerk nach definierten Kriterien zu dokumentieren und zu segmentieren. Als trennende Verfahren zwischen den Segmenten sind filternde und protokollierende Mechanismen nach dem Stand der Technik einzusetzen.	Ja	✔	Durch die Zero-Trust Architektur ist vor jedem Netzwerkzugriff eine Autorisierung erforderlich. Der Netzwerkzugriff auf öffentlich zugängliche Services ist auf das notwendigste eingeschränkt und mittels Firewall bzw. Web Application Firewall (WAF) geschützt. Zudem werden Netzwerkkomponenten und -zugriffe zentral überwacht und protokolliert. Zentrale Knotenpunkte sind redundant ausgelegt. Anforderungen an die Servicequalität (SLAs) wurden mit den jeweiligen ISP getroffen und vertraglich vereinbart.
20.4	Virtualisierung von Servern und Clients	Bei IT-Systemen in virtuellen Umgebungen, sind folgende Anforderungen zu erfüllen: • Das virtuelle System muss das Sicherheitsniveau des am höchsten eingestuften Gastsystems gewährleisten und • Über die Virtualisierung dürfen keine Netzsegmentierungen oder ähnliche filternde Komponenten unterlaufen werden. • Die Steuerung virtueller Systeme muss aus einem eigenen Netzsegment erfolgen, welches von den Segmenten der Gastsysteme getrennt ist.	Ja	✔	Virtualisierungsumgebungen werden in eigens dafür vorgesehenen Netzen betrieben, wobei Management-Komponenten davon segmentiert sind. Für virtuelle Systeme werden gehärtete und für den jeweiligen Zweck erforderliche Images verwendet. Es gelten die identen Sicherheitsanforderungen wie für alle IT-Systeme.
21.	**Protokollierung und Überwachung**	Durch die Protokollierung und Überwachung wird sichergestellt, dass eine zuverlässige und frühzeitige Erkennung von Störfällen der IT-Systeme und Angriffen gegen Informationen gewährleistet ist. Die Logdaten werden gegen Manipulationen und unberechtigte Zugriffe geschützt.	A.8.15 Protokollierung A.8.17 Uhrensynchronisation A.8.16 Überwachungstätigkeiten		
21.1	Dokumentationsanforderungen an die Protokollierung	Es ist eine Protokollierung und Überwachung zu etablieren und in den entsprechenden technischen Dokumentationen zu beschreiben. Dabei ist insbesondere zu regeln, was protokolliert wird, wer die Protokollierungskonfigurationen ändern kann, wo die Protokolldaten abgelegt werden, wie sie zugriffsgeschützt werden, wie lange die Daten aufbewahrt werden und wie häufig die Auswertung der Protokolle erfolgt.	Ja	✔	Anforderungen an die Ereignisprotokollierung werden mit der Monitoring and Log Policy geregelt und kommuniziert. Darin enthalten sind folgende Vorgaben: • Umfang und betroffene Systeme einer Protokollierung • Aufbewahrungsorte und -dauer von Protokollierungsinformationen • Anforderungen an den Zugriffsschutz
21.2	Protokollierung auf Netzwerk-, Betriebssystem-, Anwendungs-, Middleware- sowie Datenbankebene	Die Protokollierung muss sicherheitsrelevante Ereignisse auf allen Ebenen des IT-Systems, also der Anwendungs-, Datenbank-, Middleware-, Betriebssystem- und Netzinfrastrukturebene beinhalten. Aktivitäten von Benutzern mit technischen oder administrativen Berechtigungen (privilegierte Benutzer) müssen protokolliert und ausgewertet werden. In der Dokumentation der IT-Systeme und Anwendungen müssen alle Aspekte zur Protokollierung und Auswertung berücksichtigt und dokumentiert werden; dies umfasst u.a. Umfang der Protokollierung, Datenmanagement, Aufbewahrungsfristen sowie Details zur Auswertung von Protokolldaten. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Auf Betriebssystem-, Anwendungs-, Middleware-, sowie Datenbankebene sind mindestens Anmeldeversuche bzw. Anmeldungen von Nutzern, die Sperrung von Kennungen, das Beenden/der Neustart von Diensten bzw. Systemen sowie Änderungen an Sicherungsmechanismen und insbesondere administrative Tätigkeiten zu protokollieren. • Auf Sicherheitsgateways die an Schnittstellen zu nicht vertrauenswürdigen Netzen positioniert sind, müssen mindestens ausgehende Verbindungsversuche, die gegen die Filterregeln verstoßen und abgewiesen wurden, protokolliert werden. • Bei Sicherheitsgateways, welche an einem Netzübergang Einwahl- oder VPN-basierte oder ähnliche Zugangsmöglichkeiten in einen gesicherten Netzwerkbereich zur Verfügung stellen, sind darüber hinaus Zugriffsversuche mit Informationen zur Netzverbindung, die Sperrung von Kennungen, die Trennung von Sitzungen sowie Änderungen an Sicherungsmechanismen zu protokollieren. • Verändernde Eingriffe an den Protokollierungseinstellungen sind zu dokumentieren.	Ja	✔	Die Umsetzung der Monitoring und Log Policy erfolgt durch ein zentrales Logging, welches sicherheitsrelevante Ereignisse an ein SIEM weiterleitet. Dabei werden u.a. folgende Informationen protokolliert: • Benutzerkennungen • Systemaktivität/-ereignis inkl. Zeitpunkt (zB Anmeldung/Abmeldung) • Genutzte Anwendungen In den selbst entwickelten Software-Produkten der CGM sind ebenfalls konfigurierbare Protokollierungsmöglichkeiten enthalten. Der Zugang zum zentralen Logging ist nur ausgewählten Benutzerinnen und Benutzern gestattet (Need2Know-Prinzip) und wird ebenfalls protokolliert. Nur geschultes und berechtigtes Personal hat Zugang zu Protokollinformationen. Für administrative Tätigkeiten werden gesonderte, personalisierte Benutzeraccounts verwendet, die genau so protokolliert werden, wie von Systembenutzerinnen und -benutzer und sind im zentralen Logging bzw. SIEM zu finden.
22.	**Malwareschutz**	Durch den Malwareschutz wird sichergestellt, dass Information und informationsverarbeitende Einrichtungen vor Schadsoftware geschützt sind.	A.5.7 Bedrohungsintelligenz A.8.7 Schutz gegen Schadsoftware		
22.1	Schutz vor Schadsoftware	Alle IT-Systeme, die einer Bedrohung durch Malware unterliegen, sowie alle IT-Systeme die Schnittstellen zu nicht vertrauenswürdigen Netzen oder Quellen (z.B. externe Datenträger) haben, sind im Rahmen eines dokumentierten und strukturierten Vorgehens (z.B. Malwareschutzkonzept) gegen Schadsoftware abzusichern. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Die Mechanismen zur Schadsoftwareerkennung müssen dem Stand der Technik entsprechen. • Bekannte und potenzielle Schadsoftware ist bei den Gegenmaßnahmen zu berücksichtigen. • Bei Transfer und Zugriff auf Informationen sind diese – sofern technisch möglich – auf Schadsoftware zu prüfen. • Der Entdeckung von Schadsoftware muss mit zielgerichteten Maßnahmen zur Wiederherstellung des Normalbetriebs begegnet werden.	Ja	✔	Zum Schutz vor Schadsoftware sind Anforderungen und Regelungen in einer konzernweit gültigen Anti-Malware Richtlinie beschrieben. Es erfolgt ein zentrales Management aller Systeme, womit einerseits die zentrale Verwaltung der Endpoint-Protection erfolgt, Anomalien frühzeitig erkannt und Alerts erzeugt werden können und bei potentiellen Bedrohungen flächendeckende und automatisierte Gegenmaßnahmen (XDR) rasch eingeleitet werden können. Eine weitere technische Umsetzung zum Blocken potenzieller schädlicher Inhalte sind Secure Email Gateways und Web Proxies. Zudem werden alle Mitarbeitenden der CGM regelmäßig über die Gefahren und Risiken, welche von Schadsoftware ausgeht informiert und auf entsprechenden Verhaltensregeln geschult (Online-Schulung, Präsenzschulung, Simulationen, etc.). Schwachstellen Scanner werden zusätzlich zur Überprüfung eingesetzt sowie diverse Informationsquellen von Herstellerinnen und Hersteller und Foren regelmäßig herangezogen.

23.	**Sicherheit in der Anwendungs- und Systementwickl**	Durch die Sicherheit in der Anwendungs- und Systementwicklung wird sichergestellt, dass relevante Informationssicherheitsaspekte bei der Entwicklung von IT-Systemen und Anwendungen berücksichtigt und deren Einhaltung im Rahmen eines Systemabnahmetests überprüft werden. Der ordnungsgemäße und sichere Betrieb von informationsverarbeitenden Einrichtungen ist sichergestellt.	A.8.25 Lebenszyklus einer sicheren Entwicklung A.8.27 Sichere Systemarchitektur und technische Grundsätze A.8.28 Sicheres Coding A.8.29 Sicherheitsprüfung bei Entwicklung und Abnahme A.8.30 Ausgegliederte Entwicklung A.8.31 Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen A.8.32 Änderungssteuerung A.8.33 Prüfinformationen			
23.1	Trennung von Entwicklungs-, Test- und Produktionsumgebungen	Bei der Trennung der Umgebungen ist zu gewährleisten, dass auch für Entwicklungs- und Testumgebungen Maßnahmen entsprechend ihrem Schutzniveau umgesetzt werden. Durch Bereitstellung getrennter Umgebungen für die Entwicklung, die Tests (auch Abnahmeumgebung genannt) und die Produktion muss sichergestellt werden, dass das operative Geschäft frei von Entwickler- und Testtätigkeiten gehalten wird, um unnötige Gefährdungen in Bezug auf Vertraulichkeit, Verfügbarkeit und Integrität der Informationen durch einen unautorisierten Zugriff zu vermeiden.		Ja	✓	Entwicklungssysteme sind logisch und physisch von Test- und Produktivsystemen getrennt. Der Zugriff auf beide Umgebungen ist eingeschränkt und Änderungen am Produktivsystem werden gesteuert und kontrolliert. Kundenprojekte sind in der Regel in Staginginstanzen unterzeilt, wobei für den Entwicklungsbereich immer getrennte Test- bzw. QS-Systeme in Verwendung sind. Der Zugriff auf Entwicklungsumgebungen ist auf die Mitarbeitenden eingeschränkt, welche diesen zur Erfüllung ihrer Aufgaben benötigen und unterliegen dem Need2Know Prinzip.
23.2	Sichere Entwicklung von Software und IT-Systemen	Zu Beginn (Planungs- und Entwurfsphase) der Anwendungsentwicklung ist zu ermitteln welche Risiken/Bedrohungen im Zusammenhang mit den geplanten Anwendungsspezifikationen berücksichtigt werden müssen um Sicherheitslücken zu vermeiden. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Anforderungen an die Funktionalität der Anwendung (z. B. Fachkonzepte (Lastenheft), Technisches Fachkonzept (Pflichtenheft)) müssen ebenso erhoben, bewertet und dokumentiert werden wie nichtfunktionale Anforderungen (z. B. Ergebnisse der Schutzbedarfsfeststellung, Zugriffsregelungen, Ergonomie, Wartbarkeit, Antwortzeiten, Resilienz) werden erhoben. • Vorgaben und Prozesse zur sicheren Entwicklung von Software und IT-Systemen zum Aufbau eines sicheren Dienstes, einer sicheren Architektur sowie eines sicheren IT-Systems sind zu dokumentieren und zu implementieren. • Gegen Bedrohungen in Bezug auf Webanwendungen sind gängige Maßnahmen zu ergreifen, die dem Stand der Technik entsprechen (z.B. OWASP Top 10, ÖNORM A7700 - Sichere Webapplikatione, BSI Leitfaden zur Entwicklung sicherer Webanwendungen).		Ja	✓	Bei der Softwareentwicklung werden Grundsätze und Prinzipien der sicheren Sofwarearchitektur und Kodierung (Secure Coding(angewandt. Zu Beginn von Entwicklungstätigkeiten wird ein Threat Model zur Identifikation von möglichen Risiken und davon abgeleiteten Mindestsicherheitsmaßnahmen erstellt. Die Ergebnisse des Threat Models werden an den Informationssicherheitsverantwortlichen kommuniziert. Für die Umsetzung von erforderlichen Sicherheitsmaßnahmen im Rahmen der Entwicklung sowie die Einhaltung des sicheren Entwicklungsprozesses wurde eine eigene Checkliste (Security Konzept) erstellt. Es müssen alle Themen der Checkliste umgesetzt werden. Für offene Themenbereiche der Checkliste sind entsprechende Maßnahmen abzuleiten. Es existieren allgemeine Vorgaben für die Erstellung von sicheren Sourcecode. Darüber hinaus werden als Teil des Entwicklungsprozesses entsprechende Sourcecode Reviews durchgeführt. Es existiert ein Secure Software Development Lifecycle (SDLC) sowie ein Security Champion Program, mit dem Secure Coding Trainings regelmäßig durchgeführt werden.
23.3	Formelle Änderungskontrolle	Bei Anwendungs- und Systemänderungen (u. a. Patches, Service Packs und andere Aktualisierungen) sind zuvor festgelegte Sicherheitsfunktionen vor dem produktiven Einsatz technisch und fachlich zu testen. Die technischen und fachlichen Tests zur Überprüfung neuer oder geänderter Software müssen in separaten Umgebungen durchgeführt werden, die sowohl von der Produktions- als auch von der Entwicklungsumgebung getrennt sind. Die fachliche Testumgebung muss der Produktivumgebung - soweit möglich -, mindestens jedoch funktionell, entsprechen. Bevor neue oder geänderte Anwendungen/Programme in die Produktionsumgebung überführt werden, ist ein dokumentiertes Freigabeverfahren zu durchlaufen.		Ja	✓	Regelungen und Vorgaben für den Umgang mit IT-Changes werden in einer themenspezifischen Richtlinie beschrieben. Darin sind auch Vorgaben zum Testen der Systemsicherheit enthalten. Durch QA Teams in den unterschiedlichen Entwicklungsabteilungen werden neue und geänderte Entwicklungen vor deren Release in eigenen, von den Enwicklungs- und Produktivumgebungen getrennten Systemen getestet. Systemabnahmetest erfolgen ebenfalls auf Testumgebungen, werden dokumentiert und formal abgenommen.
23.4	Grundsätze zur sicheren Systementwicklung	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme sind festzulegen, zu dokumentieren und für jedes Informationssystem anzuwenden. Für neue Informationssysteme, Upgrades und neue Versionen müssen Testpläne und dazugehörige Abnahmekriterien festgelegt sein. Es sind die jeweils aktuell geltenden Bestimmungen der europäischen Datenschutzgrundverordnung („DSGVO“) zum „Datenschutz durch Technikgestaltung” (Privacy by Design) und „Datenschutz durch datenschutzfreundliche Voreinstellungen“ (Privacy by Default) nach Art. 25 DSGVO im Entwicklungsprozess zu berücksichtigt. Relevante Sicherheitsanforderungen werden bereits in der Designphase des Entwicklungsprozesses nachweislich erhoben, im Zuge der Softwarearchitektur berücksichtigt und während der Implementierung nachweislich umgesetzt. Das Freigabeverfahren muss mindestens folgende Anforderungen erfüllen: • Für die eigentlichen Testverfahren müssen Pläne definiert werden, die Auskunft über die Testart, den Testumfang, die verwendeten Umgebungen und Testdaten, die Testabbruch- oder -endekriterien und den zeitlichen Ablauf geben, sowie Testdokumentationen, die Auskunft über die Durchführung der Tests geben. • Für den Systemabnahmetest sind automatische Tools wie z. B. Codeanalyse-Tools oder Schwachstellen-Scanner zu nutzen. Etwaige sicherheitsbezogene Defizite sind zu beheben und die Behebung ist zu kontrollieren.		Ja	✓	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme werden in einer themenspezifischen Secure Development Lifecycle Richtlinie beschrieben, welche unter anderem auch die Datenschutzprinzipien "Privacy by Default" und "Privacy by Design" berücksichtigen. Durch Anwendung eines agilen Softwareentwicklungsprozesses werden bereits in der Design- und Planungsphase von Entwicklungsprojekten Threat Models erstellt und dabei Sicherheitsanforderungen spezifiziert. Diese Anforderungen werden in den Entwicklungsprozess aufgenommen und somit auch Teil von Code Reviews und werden als Akzeptanzkriterien in einen Testplan integriert. In der Build Pipeline sind unterstützende Analyse-Tools zur statischen Code Analyse und zum Management von Third Party Components vorhanden. Zusätzlich werden in regelmäßigen Abständen oder anlassbezogen Penetration Tests durchgeführt.
23.5	Sichere Entwicklungsumgebung	Es ist eine sichere Entwicklungsumgebung für die spezifischen Systementwicklungsvorhaben unter Berücksichtigung der folgenden Punkte einzurichten und zu dokumentieren: • Es ist eine Trennung zwischen den Entwicklungsumgebungen unter Berücksichtigung der Sicherheitsvorgaben zur Trennung von Entwicklungs-, Test- und Produktionsumgebungen zu implementieren. • Der Datenverkehr aus der und in die Umgebungen ist zu kontrollieren. • Die Entwicklungsumgebung ist gemäß den Sicherheitsvorgaben zur Systemhärtung abzusichern.		Ja	✓	Für den Entwicklungsbereich sind getrennte Test- bzw. QS-Systeme in Verwendung. Die Entwicklungsumgebung ist physisch von Produktivumgebungen (Test-, Qualitäts-, Schulungs- und Produktivumgebung) getrennt. Der Zugriff auf Entwicklungsumgebungen ist auf die Benutzer eingeschränkt, welche diesen zur Erfüllung ihrer Aufgaben benötigen und unterliegen dem Need2Know Prinzip. Änderungen am Code werden dokumentiert und unterliegen einem vorhergehenden Code Review.
23.6	Software- und Systementwicklungen durch Dritte	Software, die im Auftrag des Unternehmens durch Dritte entwickelt wird, ist erst nach einem sorgfältigen Abnahme- und Freigabeprozess auf den produktiven IT-Systemen zu installieren. Daher müssen die Rahmenbedingungen bei an externe Dritte vergebene Anwendungs- und Systementwicklungstätigkeiten kontrolliert werden. Dabei sind interne Anforderungen an die Anwendungsentwicklung zu berücksichtigen.		Ja	✓	Externe Partner, welche für die Entwicklung von Software eingesetzt werden, unterliegen den gleichen Anforderungen der sicheren Softwareentwicklung (SSDLC), wie Mitarbeitende der CGM selbst und nutzen die gleichen Umgebungen.
23.7	Verwendung von Testdaten	Die fachlich verantwortlichen Mitarbeitenden sind beim Aufbau realistischer Testdatenbestände und Definition der Einsatzbedingungen zu beteiligen. Bei Verwendung von Echtdaten müssen die gleichen Sicherheitsmechanismen und Rahmenbedingungen gelten wie in der Produktion. Die Nutzung der Daten für Testzwecke ist zu dokumentieren. Ein Test mit vertraulichen Echtdaten ist grundsätzlich nicht zulässig. Sollte ein fachlicher Test mit selbst generierten Testdaten nicht möglich sein, ist die Notwendigkeit für die Nutzung von vertraulichen Echtdaten zu begründen (Nachvollziehbarkeit, Aufwand für die Testdatengenerierung, Qualitätssicherung) und mit dem Auftraggeber abzustimmen.		Ja	✓	Zum Testen von Software werden keine Echtdaten verwendet, sondern ausschließlich fiktive, automatisch generierte Daten. Sollte es zur Fehleranalyse unbedingt erforderlich sein, dass Echtdaten benötigt werden, so erfolgt dies bevorzugt auf Testsystemen beim Kunden oder nach einem definierten und gesicherten Datenimport-Prozess nach vorgehender schriftlicher Genehmigung durch die Kundin/den Kunden und Freigabe durch die Geschäftsleitung.

24.	**Einsatz von Software**	Durch Vorgaben zum Einsatz von Software wird sichergestellt, dass die korrekte Funktionalität der im Unternehmen eingesetzten Software sichergestellt ist und Anforderungen an die Installation von Software auf IT-Systemen im Rahmen geregelter Prozesse definiert sind.	A.8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten A.8.19 Installation von Software auf Systemen im Betrieb		
24.1	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	Die Verwendung von Dienst- oder Hilfsprogrammen, die in der Lage sein könnten, System- und Sicherheitsfunktionen zu umgehen, ist ausschließlich für administrative Zwecke in der IT-Organisation zulässig. Die Nutzung ist auf den berechtigten Personenkreis einzugrenzen.		Ja	✔	Standardmäßig haben Benutzer keine privilegierten Rechte auf deren Endgeräten. Lokale administrative Berechtigungen können entweder automatisiert und zeitlich eingeschränkt auf 3h oder längerfristig für 3 Monate über ein Support-Ticket beantragt werden. Zudem mit der Endpoint Protection eine Application Control auf Clients und Servern eingesetzt. Für administrative Tätigkeiten auf Serversystemen werden getrennte personalisierte Benutzeraccounts verwendet. Gebrauch von Hilfsprogrammen mit privilegierten Rechten durch Dritte (Support- und Wartungspersonal) wird gesondert protokolliert und im SIEM analysiert.
24.2	Installation von Software auf Systemen im Betrieb	Software und Anwendungen müssen vor Installation unter Berücksichtigung der Vorgaben zur sicheren Anwendungsentwicklung getestet werden. Neuinstallationen und Updates dürfen nur durch einen Administrator vorgenommen werden. Die Software ist so abzusichern, dass das automatisierte Ausführen oder Nachladen von Code aus nicht zugelassenen Quellen (z.B. Externes Office Dokument mit Makros) verhindert wird. Betriebliche Systeme enthalten nur freigegebenen ausführbaren Code und keinen Entwicklungscode oder Compiler.		Ja	✔	Die Softwareinstallation auf Servern erfolgt immer im Auftrag der Serviceowner und wird ausschließlich durch geschultes Personal durchgeführt, wobei dies anhand vorgegebenen Prozesse erfolgt. Dies Prozesse umfassen unter anderem Sicherungs- und Rollback-Vorkehrungen, Dokumentation und Abnahmetests. Aktualisierungen des Betriebssystems und vom Unternehmen bereitgestellter Software werden zentral gesteuert. Für die laufende Aktualisierung der individuell installierten Software, ist die Endbenutzerin/der Endbenutzer verantwortlich und wird über das zentrale Schwachstellenmanagement überwacht. Die automatische Installation von notwendiger Software auf Clients wird zentral gesteuert. Vorgaben hinsichtlich Installation und Nutzung von Software sind zudem im Dienstvertrag vorhanden und wird durch regelmäßige Schulungen übermittelt.
25.	**Sicherheit von Geräten und Betriebsmitteln**	Durch Vorgaben zur Sicherheit von Geräten und Betriebsmitteln wird sichergestellt, dass der Umgang mit diesen so gestaltet ist, dass das Risiko von Verlust, Beschädigung, Diebstahl oder die Gefährdung von Informationswerten minimiert ist.	A.7.13 Instandhaltung von Geräten und Betriebsmitteln A.7.10 Speichermedien A.7.9 Sicherheit von Werten außerhalb der Räumlichkeiten A.7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln A.8.1 Endpunktgeräte des Benutzers A.7.7 Aufgeräumte Arbeitsumgebung und Bildschirmsperren		
25.1	Instandhaltung von Geräten und Betriebsmitteln	Geräte und Betriebsmittel müssen entsprechend der Serviceintervalle und Spezifikationen der Hersteller durch autorisiertes Personal gewartet werden. Fernwartungen von IT-Geräten müssen autorisiert und mittels besonderer Schutzmaßnahmen wie starke Authentifizierung (Zwei-Faktor), Verschlüsselung sowie Logging und Monitoring abgesichert werden.		Ja	✔	Geräte und Betriebsmittel werden gemäß den von den Herstellern empfohlenen Wartungsintervallen und Spezifikationen gewartet. Nur autorisiertes und geschultes Wartungspersonal führt dokumentierte Reparaturen und Services an Geräten durch. Aufzeichnungen über alle vermuteten oder tatsächlichen Fehler sowie über alle vorbeugenden und korrigierenden Wartungsarbeiten werden geführt. Externes Wartungspersonal wird zuvor angemeldet und zu jederzeit begleitet. Falls erforderlich, werden vertrauliche Informationen vor einer Wartung durch externes Wartungspersonal, aus dem Gerät entfernt. Bevor das Gerät nach seiner Wartung wieder in Betrieb genommen wird, wird überprüft, ob das Gerät nicht manipuliert wurde und keine Fehlfunktion aufweist.
25.2	Mitnahme von Geräten, Betriebsmitteln und Dokumenten	Es sind für mindestens folgende Themenbereiche verbindliche Vorgaben zu etablieren, mit dem Ziel, den unbefugten Zugriff zu verhindern und damit die Vertraulichkeit, Verfügbarkeit und Integrität der Daten zu schützen: • für die Mitnahme und Außerhausnutzung von Geräten, Betriebsmitteln und Dokumenten, sowie den Umgang mit Kundendokumenten, • für die Löschung und Entsorgung von Geräten, Betriebsmitteln und Dokumenten und • für den Arbeitsplatz im engeren Sinne (z.B. „clear screen“ und „clear desk-Policy“)		Ja	✔	Anforderungen an die Verwendung von Geräten zur Speicherung und Verarbeitung von Informationen (Clients bzw. mobile Geräte) außerhalb des Unternehmensgeländes wird durch die IS Policy und eine themenspezifische Enduser Richtlinie geregelt. Dies gilt für Geräte, die im Eigentum der Organisation sind und für Geräte, die sich in Privatbesitz befinden und im Auftrag der Organisation verwendet werden. Geräte und Medien, die außerhalb des Betriebsgeländes verwendet werden, dürfen an öffentlichen Orten nicht unbeaufsichtigt bleiben und müssen besonders geschützt werden. Außerhalb der CGM Räumlichkeiten befinden sich keine stationären Geräte in Betrieb. Ersatzgeräte und -teile werden in eigens geschützten Lagerräumen aufbewahrt. Vor Reparaturen oder Wartungen von Geräten außer Haus, werden alle darin befindlichen Datenträger entfernt.
25.3	Sichere Entsorgung oder Weiterverwendung von Geräten und Betriebsmitteln	Alle Geräte und Betriebsmittel die Datenträger enthalten, auf denen firmeninterne Informationen gespeichert sind/waren, sind über einen definierten Prozess zu entsorgen. Das Löschen von Informationen auf Datenträgern muss mit geeigneten Löschtechniken erfolgen, die dem aktuellen Stand der Technik entsprechen, zertifiziert sind und das Risiko einer Wiederherstellung der Daten minimieren.		Ja	✔	Anforderungen und Regelungen zur sicheren Entsorgung sind in einer themenspezifischen Richtlinie enthalten. Speichermedien wie Festplatten werden vor der Entsorgung von Geräten entfernt und einer sicheren Entsorgung (z. B. mechanische Zerstörung) zugeführt. Vor einer Wiederverwendung werden Speichermedien wie Festplatten überschrieben.
26.	**Beschaffung von Hard- und Software**	Durch die Vorgaben zur Beschaffung von Hard- und Software wird sichergestellt, dass der sichere und reibungslose IT-Betrieb durch die geeignete Auswahl von Produkten, sowie der Berücksichtigung aller relevanten Anforderungen der Informationssicherheit in Beschaffungsprozessen von IT-Systemen, Anwendungen und Services gewährleistet ist.	A.5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten A.5.8 Informationssicherheit im Projektmanagement		

26.1	Sicherheitsanforderungen bei der Beschaffung von Anwendungen und IT-Systemen	Es ist ein dokumentierter Prozess für die Beschaffung von Anwendungen und IT-Systemen zu etablieren, der sicherstellt, dass Sicherheitsanforderungen an zu beschaffende Produkte erfüllt werden. Dieses Vorgehen muss mindestens folgendes sicherstellen: • Die Produkte müssen kompatibel mit der IT-(Sicherheits-)Architektur und den Update-, Wartungs- und Freigabeverfahren sein. • Die Bezugsquellen der Produkte müssen vertrauenswürdig sein.		Ja	✓	Für die Beschaffung von IT-Systemen wurde ein Prozess etabliert, durch den im Rahmen einer Anforderungsanalyse für ein IT-System in Bezug auf Informationssicherheit folgende Punkte berücksichtigt werden: • Anforderungen an die Einsatzumgebung • Performanceanforderungen • Interoperabilitätsanforderungen • Zuverlässigkeitsanforderungen • Konformität zu Standards • Einhaltung von internen Regelungen und gesetzlichen Vorschriften • Anforderungen an die Wartbarkeit • Anforderungen an die Dokumentation Zusätzlich zu den allgemeinen Anforderungen müssen die Anforderungen an die Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit und Authentizität von Informationswerten vorgegeben werden. Hierfür ist zunächst eine Risikoanalyse durchzuführen, indem relevante Bedrohungen ermittelt werden und Maßnahmen zu deren Behandlung abgeleitet werden. Zudem sind vorhandene Anforderungen aus dem ISMS und DSMS, beispielsweise Anforderungen an kryptographische Maßnahmen, Datenschutzprinzipien "privacy by default" und "privacy by design" sowie Kundenanforderungen und Auswertungen aus aufgetretenen Informationssicherheitsvorfällen zu beachten. Getroffene Bewertungen und Entscheidungen werden nachvollziehbar dokumentiert, sodass später eine effiziente Weiterentwicklung der Anwendung durch ausreichende Dokumentation gewährleistet ist.
27.	**Physische Sicherheit**	Durch die physische Sicherheit in Bezug auf Standorte, Gebäude und Räume sowie Betriebsmittel mit denen Informationswerte verarbeitet werden wird sichergestellt, dass diese mittels geeigneter technischer und organisatorischer Maßnahmen vor physischen Schäden sowie der Beeinträchtigung von Informationswerten geschützt sind.	A.7.1 Physische Sicherheitsperimeter A.7.2 Physischer Zutritt A.7.3 Sichern von Büros, Räumen und Einrichtungen A.7.4 Physische Sicherheitsüberwachung A.7.5 Schutz vor physischen und umweltbedingten Bedrohungen A.7.6 Arbeiten in Sicherheitsbereichen A.7.8 Platzierung und Schutz von Geräten und Betriebsmitteln A.7.11 Versorgungseinrichtungen A.7.12 Sicherheit der Verkabelung			
27.1	Physische Sicherheitszonen	Die Ausgestaltung der Standorte und Gebäude stellt sicher, dass Sicherheitszonen hinsichtlich ihres Schutzbedarfes eingerichtet und Schutzmaßnahmen – insbesondere gegen unautorisierten Zutritt und standort- und gebäudespezifische Gefahren – etabliert sind. Dies gilt in besonderem Maße für den Übergang aus Anlieferungs- und Ladezonen und ähnlichen Bereichen, über die sich nicht autorisierte Mitarbeiternde Zutritt zu den Gebäuden verschaffen können. IT-Räume (Räume, in denen IKT-Komponenten untergebracht sind, die nicht nur Clients/Endgeräte darstellen) gelten als Sicherheitszonen und sind in besonderem Maße zu schützen.		Ja	✓	Sicherheitszonen sind festgelegt und Sicherheitsanforderungen dafür werden in einer themenspezifischen Richtlinie geregelt. Deren Einhaltung wirde im Rahmen von regelmäßigen Audits (Spotchecks) überwacht.
27.2	Zutrittskontrolle	Zutrittskontrollen müssen sicherstellen, dass für Mitarbeitende, Besucher und Lieferanten und sonstige Externe definierte Verfahren zur (De-)Autorisierung und Überwachung und Dokumentation des Zutritts eingehalten werden. Die Maßnahmen sind differenziert nach Sicherheitsanforderung auszugestalten.		Ja	✓	Eine elektronische Zutrittskontrolle ist an allen Standorten vorhanden. Durch eine allgemein gültige Besucherregelung werden Beuucher und derne Besuchszeiten dokumentiert. Besucher dürfen sich dabei nicht alleine in Gebäuden bewegen und werden zu jeder Zeit begleitet. Besucherinnen und Besucher sind verpflichtet, ihren Besucherausweis immer sichtbar zu tragen. Mitarbeitende sind darauf geschult, bei Nichteinhaltung dieser Regelung diese Person darauf aufmerksam zu machen und zum Empfang bzw. zur Standortverantwortlichen/zum Standortverantwortlichen zu begleiten. Mitarbeitenden wird nur Zutritt für zur Ausübung derer Tätigkeiten relevanten Bereiche und Standorte gewährt. Beispielsweise können nur bestimmte Mitarbeitende den Serverraum betreten. Zutrittsrechte zu sensiblen Bereichen werden regelmäßig überprüft und erforderlichenfalls widerrufen. Im Zuge des Austrittsprozesses werden alle erteilten Zutrittsberechtigungen ebenfalls widerrufen.
27.3	Schutz vor externen Einflüssen	Risiken, die aus extremen und umweltbedingten standortspezifischen Einflüssen entstehen, müssen analysiert werden und entsprechende Schutzmaßnahmen sind zu etablieren; dies gilt insbesondere für Überschwemmungen und Schutz vor Überspannung durch Blitze. Außerdem sind mindestens die standortrelevanten gesetzlichen behördlichen und versicherungstechnischen Brandschutzregelungen einzuhalten und eine lokale Brandschutzorganisation zu etablieren.		Ja	✓	Für die eigenen Rechenzentren wurden Bewertungen, sowie Sicherheitskonzepte nach dem BSI Grundschutz erstellt. Eine Neubewertung wird einmal jährlich durchgeführt. Eine Brandschutzorganistation mit benannten Zuständigkeiten wurde etabliert.
27.4	Sicherheitsanalyse	Risiken, die sich für Betriebsmittel und Versorgungseinrichtungen ergeben (insbesondere solche, mit denen sensible Informationen verarbeitet werden) müssen analysiert und entsprechende Schutzmaßnahmen etabliert werden. Die Risiken müssen u. a. umweltbezogene Bedrohungen, Störungen von Versorgungseinrichtungen, elektromagnetische Strahlung und Vandalismus umfassen.		Ja	✓	Elementare Gefährdungen, Störungen von Versorgungseinrichtungen, elektromagnetische Strahlung und Vandalismus wurden neben vielen weiteren Bedrohungen im IT-Risikomanagement der CGM berücksichtigt, analysiert, bewertet und Maßnahmen zur Risikobehandlung eingeleitet.
28.	**Rechenzentren**	Durch die Ausgestaltung der Rechenzentren wird sichergestellt, dass die Verfügbarkeit der Informationen bzw. informationsverarbeitenden IT-Systeme i.V.m. mit dem ordnungsmäßen Betrieb gewährleistet ist.	A.7.1 Physische Sicherheitsperimeter A.7.2 Physischer Zutritt A.7.3 Sichern von Büros, Räumen und Einrichtungen A.7.4 Physische Sicherheitsüberwachung A.7.5 Schutz vor physischen und umweltbedingten Bedrohungen A.7.6 Arbeiten in Sicherheitsbereichen A.7.8 Platzierung und Schutz von Geräten und Betriebsmitteln A.7.11 Versorgungseinrichtungen A.7.12 Sicherheit der Verkabelung A.7.13 Instandhaltung von Geräten und Betriebsmitteln			

28.1	Informationssicherheit im Rechenzentrum	Die zentralen IT-Systeme sind in einem Rechenzentrum unter Berücksichtigung der Informationssicherheitsvorgaben zur physischen Sicherheit zu betreiben. Die Maßnahmen müssen mindestens folgendes sicherstellen: • Risiken, die sich aus dem Standort selbst ergeben, z.B. geographische oder nachbarliche, müssen regelmäßig analysiert und entsprechende Schutzmaßnahmen etabliert werden. • Erdbeben- und Überflutungsbereiche müssen als Standort ausgeschlossen werden. Mindestabstände zu anderen Infrastrukturen, aus denen sich Risiken ergeben können wie z.B. Flughäfen, Autobahnen, Bahnstrecken, Wasserstraßen, Militärbasen und Kraftwerken, müssen definiert und eingehalten werden. • Versorgungsleitungen, Komponenten für die öffentliche Netzanbindung und Gebäudezugänge sind redundant auszulegen • Einrichtungen zur Informationsverarbeitung, die exklusiv dem Auftraggeber zur Verfügung stehen, sind physisch angemessen von solchen Einrichtungen zu trennen, die anderen Parteien zur Verfügung stehen. • Zugangspunkte wie Anlieferungs- und Ladezonen sowie andere Punkte, über die sich nicht-autorisierte Personen Zutritt zu den Betriebsgebäuden verschaffen könnten, sind zu kontrollieren und von informationsverarbeitenden Einrichtungen zu isolieren, um nicht autorisierten Zugang zu verhindern. • Gebäudestruktur, Raumaufteilung und Gebäudetechnik, ggf. Aufteilung der einzelnen Mieteinheiten auf Mieter sind vom Auftragnehmer zu dokumentieren und aktuell zu halten. Ist der Auftragnehmer nur Mieter in dem Rechenzentrum, ist ihm die ihn betreffende Dokumentation zugänglich zu machen. • Um Schäden aus Störungen und Notfällen zu minimieren, ist vom Auftragnehmer ein dokumentiertes Konzept zum Umgang mit Störungen und Notfällen zu erstellen. Dieses muss mindestens Eskalationspläne, die auch die Kundenkommunikation abdecken, enthalten. Die Pläne müssen regelmäßig getestet werden. • Zudem ist eine Liste mit allen Single Points of Failure dokumentiert und wird halbjährlich aktualisiert. Als Grundlage sind aktuelle Guidelines und Best Practices zur physischen Sicherheit und Verfügbarkeit von Rechenzentren zu berücksichtigen,		Ja	✔	Für die eigenen Rechenzentren wurden Bewertungen, sowie Sicherheitskonzepte nach dem BSI Grundschutz erstellt. Eine Neubewertung wird einmal jährlich durchgeführt. Zudem wurden Business Continuity und Notfallpläne für Rechenzentren erstellt.
29.	**Konfigurations- und Datenmanagement**	Durch die Ausgestaltung der Rechenzentren wird sichergestellt, dass die Verfügbarkeit der Informationen bzw. informationsverarbeitenden IT-Systeme sowie ein ordnungsmäßer Betrieb gewährleistet ist.	A.8.9 Konfigurationsmanagement A.8.10 Löschung von Informationen A.8.11 Datenmaskierung A.8.12 Verhinderung von Datenlecks		
29.1	Konfigurationsmanagement	Sicherstellen, dass alle Informationssysteme und IT-Ressourcen definiert und dokumentiert sind und ihre Konfiguration laufend aktualisiert wird, um sicherzustellen, dass die Systemintegrität und Verfügbarkeit gewährleistet sind. Dies umfasst die Verwaltung und Überwachung von Systemänderungen, um unerwünschte Änderungen oder Fehler zu vermeiden.		Ja	✔	Ein zentrales Assetmanagement wird betrieben, in dem alle IT-Assets und deren Konfigurationen dokumentiert sind. Durch die zentrale Verwaltung und Steuerung aller IT-Assets, werden auch Sicherheitskonfigurationen laufend überwacht und aktualisiert. Es werden Hersteller-Vorgaben und „Good Practices“ als Grundlage für die Konfiguration von Betriebssystemen herangezogen und entsprechende Sicherheitsüberprüfungen mit Schwachstellen-Scannern durchgeführt.
29.2	Löschung von Informationen	Sicherstellen, dass alle sensiblen Informationen, die nicht mehr benötigt werden, sicher und dauerhaft gelöscht werden. Dies umfasst sowohl elektronische Daten als auch physische Datenträger. Es wird gewährleistet, dass die Löschvorgänge dokumentiert werden und entsprechenden Richtlinien und gesetzlichen Anforderungen entsprechen.		Ja	✔	Informationen, die in Informationssystemen, Geräten oder auf anderen Speichermedien gespeichert sind, werden gelöscht, sofern sie nicht mehr benötigt werden. Vorgaben zur sicheren Löschung von Informationen befinden sich in einer themenspezifischen Richtlinie. Im Rahmen des Austrittprozesses werden persönlichen Daten der Mitarbeitenden durch den zentralen IKT-Dienstleister nach Ablauf definierter Aufbewahrungszeiten gelöscht. Für IT-Syteme existieren im Rahmen des DSMS Löchkonzepte, deren Einhaltung mind. 1x jährlich im Rahmen von DS-Audits überprüft wird.
29.3	Datenmaskierung	Anwenden von Techniken, um sensible Daten zu verbergen oder zu anonymisieren, um die Datensicherheit zu erhöhen. Dies dient insbesondere dem Schutz personenbezogener Daten und anderer vertraulicher Informationen vor unautorisiertem Zugriff, insbesondere in Test- und Entwicklungsumgebungen.		Ja	✔	Die Datenmaskierung wird in Übereinstimmung mit den themenspezifischen Richtlinien der Organisation zur Zugriffssteuerung und anderen damit zusammenhängenden themenspezifischen Richtlinien sowie den geschäftlichen Anforderungen und unter Berücksichtigung der geltenden Rechtsvorschriften eingesetzt.
29.4	Verhinderung von Datenlecks	Etablieren von Maßnahmen und Technologien, um das Risiko von Datenlecks zu minimieren. Dies kann die Implementierung von Data Loss Prevention (DLP)-Systemen, die Schulung von Mitarbeitenden zum sicheren Umgang mit Daten und das regelmäßige Überprüfen und Testen von Sicherheitsmaßnahmen umfassen, um sicherzustellen, dass schützenswerte Informationen nicht unautorisiert abfließen. Jede dieser Maßnahmen trägt dazu bei, dass die Konfigurations- und Datenmanagementpraktiken den Anforderungen der Informationssicherheit entsprechen und die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen gewährleistet werden.		Ja	✔	Maßnahmen zur Verhinderung von Datenlecks werden technisch auf Systemen, Netzwerken und alle anderen Geräten angewendet, die sensible Informationen verarbeiten, speichern oder übertragen. Es existieren unterschiedliche Maßnahmen zur Verhinderung von möglichen Datenlecks (z.B. Sperre von USB-Speichermedien, Vorgabe von Datenübermittlungs- und Speicherformen, EDR-Lösung zu Sicherstellung der Endgerätesicherheit, DLP usw.).