Zuordnungstabelle
Zuordnung ISO/IEC 27001 zum IT-Grundschutz

IT-Grundschutz beschreibt mit Hilfe der BSI-Standards 200-1, 200-2 und 200-3 eine Vorgehensweise zum Aufbau und zur Aufrechterhaltung eines Managementsystems für Informationssicherheit (ISMS). Das IT-Grundschutz-Kompendium beschreibt die Umsetzung der damit einhergehenden Anforderungen. Das damit aufgebaute ISMS erfüllt die Anforderungen der ISO/IEC 27001 und verfügt über ein Äquivalent zu den Handlungsempfehlungen der ISO/IEC 27002.

Diese Gegenüberstellung dient der Zuordnung der Inhalte der ISO/IEC 27001:2022 zu den Inhalten des IT-Grundschutzes. So wird durch den IT-Grundschutz die Abdeckung der ISO/IEC 27001 deutlicher und eine komplementäre Anwendung des IT-Grundschutzes zu der Anwendung der ISO-Normen wird erleichtert.

Diese Gegenüberstellung basiert auf den folgenden Versionen der betrachteten Werke:

- BSI-Standard 200-1, Version 1.0 vom Oktober 2017
- BSI-Standard 200-2, Version 1.0 vom Oktober 2017
- BSI-Standard 200-3, Version 1.0 vom Oktober 2017
- BSI-Standard 200-4
- IT-Grundschutz-Kompendium, 6. Edition 2023
- ISO/IEC 27001:2022 und ISO/IEC 27002:2022

Für Themen, die in einem der BSI-Standards behandelt werden, wird das Kapitel des entsprechenden BSI-Standards angegeben. Das Kürzel (z. B. ISMS.1, ORP.1) weist auf den entsprechenden Baustein und "A" auf eine Anforderung im IT-Grundschutz-Kompendium hin. Wenn ein Thema aus den ISO-Normen 27001 bzw. 27002 in mehreren Bereichen im IT-Grundschutz behandelt wird, wird der primär relevante Bereich fett markiert.

Die Abschnitte dieses Dokuments, die sich auf die Maßnahmenziele und Maßnahmen des Anhangs A der ISO/IEC 27001 und auf die Empfehlungen der ISO/IEC 27002 beziehen, folgen aus Gründen der Übersichtlichkeit der Gliederung und den Bezeichnungen der ISO/IEC 27002. Es werden ausschließlich die Teile der ISO/IEC 27002 aufgeführt, die einen Bezug zum Anhang A der ISO/IEC 27001 haben.

ISO/IEC 27001:2022 und IT-Grundschutz

		ISO/IEC 27001:2022	IT-Grundschutz
1		Scope – Anwendungsbereich	BSI-Standard 200-2, Kapitel 1 Einleitung
2		Normative references – Normative Verweisungen	BSI-Standard 200-1, Kapitel 11.1 Literaturverzeichnis
3		Terms and definitions – Begriffe	Glossar IT-Grundschutz (siehe IT-Grundschutz-Kompendium) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html
4		**Context of the organization – Kontext der Organisation**	
	4.1	Understanding the organization and its context – Verstehen der Organisation und ihres Kontextes	**BSI-Standard 200-2, Kapitel 3.2.1 Ermittlung von Rahmenbedingungen** ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie ORP.5.A1 Identifikation der Rahmenbedingungen
	4.2	Understanding the needs and expectations of interested parties – Verstehen der Erfordernisse und Erwartungen interessierter Parteien	**BSI-Standard 200-2, Kapitel 3.2 Konzeption und Planung des Sicherheitsprozesses** **ORP.5.A1 Identifikation der Rahmenbedingungen**
	4.3	Determining the scope of the information security management system – Festlegen des Anwendungsbereichs des Informationssicherheits-managementsystems	**BSI-Standard 200-2, Kapitel 3.3.4 Festlegung des Geltungsbereichs und Kapitel 8 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise der Standard-Absicherung** ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit
	4.4	Information security management system – Informationssicherheits-managementsystem	**BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)** **BSI-Standard 200-2 IT-Grundschutz-Methodik** ISMS.1 Sicherheitsmanagement

		ISO/IEC 27001:2022	IT-Grundschutz
5		**Leadership – Führung**	
	5.1	Leadership and commitment – Führung und Verpflichtung	**BSI-Standard 200-2, Kapitel 3.1 Übernahme von Verantwortung durch die Leitungsebene** ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitung ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit ISMS.1.A9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse
	5.2	Policy – Politik	**BSI-Standard 200-2, Kapitel 3.4 Erstellung einer Leitlinie zur Informationssicherheit** **ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit**
	5.3	Organizational roles, responsibilities and authorities – Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	**BSI-Standard 200-2, Kapitel 4 Organisation des Sicherheitsprozesses** ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitung ISMS.1.A4 Benennung eines oder einer Informationssicherheitsbeauftragten ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit
6		**Planning – Planung**	
	6.1	Actions to address risks and opportunities – Maßnahmen zum Umgang mit Risiken und Chancen	
	6.1.1	General – Allgemeines	**BSI-Standard 200-2, Kapitel 3, 4, 8 und 9**
	6.1.2	Information security risk assessment – Informationssicherheits-risikobeurteilung	**BSI-Standard 200-2, Kapitel 3, 4 und 8** BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz Elementare Gefährdungen (G0-Gefährdungen) des IT-Grundschutz-Kompendiums
	6.1.3	Information security risk treatment – Informationssicherheits-risikobehandlung	**BSI-Standard 200-2, Kapitel 8 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise der Standard-Absicherung und Kapitel 9 Umsetzung der Sicherheitskonzeption** BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz IT-Grundschutz-Kompendium

		ISO/IEC 27001:2022	IT-Grundschutz
	6.2	Information security objectives and planning to achieve them – Informationssicherheitsziele und Planung zu deren Erreichung	**BSI-Standard 200-2, Kapitel 3 Initiierung des Sicherheitsprozesses**
7		**Support – Unterstützung**	
	7.1	Resources – Ressourcen	**BSI-Standard 200-1, Kapitel 5 Ressourcen für die Informationssicherheit** ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitung ISMS.1.A4 Benennung eines oder einer Informationssicherheitsbeauftragten ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit ISMS.1.A15 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit OPS.1.1.1.A4 Bereitstellen ausreichender Personal- und Sachressourcen
	7.2	Competence – Kompetenz	**BSI-Standard 200-2, Kapitel 4 Organisation des Sicherheitsprozesses** **ORP.2.A15 Qualifikation des Personals** ORP.2.A7 Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden
	7.3	Awareness – Bewusstsein	**BSI-Standard 200-1, Kapitel 6 Einbindung der Mitarbeiter in den Sicherheitsprozess** **ORP.3 Sensibilisierung und Schulung zur Informationssicherheit**
	7.4	Communication – Kommunikation	**BSI-Standard 200-2, Kapitel 5.2.4 Informationsfluss und Meldewege**
	7.5	Documented information – Dokumentierte Information	
	7.5.1	General – Allgemeines	**BSI-Standard 200-2, Kapitel 5 Dokumentation im Sicherheitsprozess** ISMS.1.A13 Dokumentation des Sicherheitsprozesses
	7.5.2	Creating and updating – Erstellen und Aktualisieren	**BSI-Standard 200-2, Kapitel 5.2 Informationsfluss im Informationssicherheitsprozess** ISMS.1.A13 Dokumentation des Sicherheitsprozesses
	7.5.3	Control of documented information – Lenkung dokumentierter Information	**BSI-Standard 200-1, Kapitel 4.2 Kommunikation und Wissen** **BSI-Standard 200-2, Kapitel 5.2 Informationsfluss im Informationssicherheitsprozess** ISMS.1.A13 Dokumentation des Sicherheitsprozesses

		ISO/IEC 27001:2022	IT-Grundschutz
8		**Operation – Betrieb**	
	8.1	Operational planning and control – Betriebliche Planung und Steuerung	**BSI-Standard 200-2, Kapitel 9 Umsetzung der Sicherheitskonzeption**
	8.2	Information security risk assessment – Informationssicherheits-risikobeurteilung	**BSI-Standard 200-2, Kapitel 3, 4 und 8** BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz Elementare Gefährdungen (G0-Gefährdungen) des IT-Grundschutz-Kompendiums
	8.3	Information security risk treatment – Informationssicherheits-risikobehandlung	**BSI-Standard 200-2, Kapitel 8 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise der Standard-Absicherung und Kapitel 9 Umsetzung der Sicherheitskonzeption** BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz IT-Grundschutz-Kompendium
9		**Performance evaluation – Bewertung der Leistung**	
	9.1	Monitoring, measurement, analysis and evaluation – Überwachung, Messung, Analyse und Bewertung	**BSI-Standard 200-2, Kapitel 10 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit** ISMS.1.A11 Aufrechterhaltung der Informationssicherheit
	9.2	Internal audit – Internes Audit	**BSI-Standard 200-2, Kapitel 10.1 Überprüfung des Informationssicherheitsprozesses auf allen Ebenen** **DER.3.1 Audits und Revisionen** **DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision** ISMS.1.A11 Aufrechterhaltung der Informationssicherheit
	9.3	Management review – Managementbewertung	**BSI-Standard 200-2, Kapitel 5.2.1 Berichte an die Leitungsebene** **BSI-Standard 200-2, Kapitel 10.1 Überprüfung des Informationssicherheitsprozesses auf allen Ebenen** **BSI-Standard 200-2, Kapitel 10.2 Eignung der Informationssicherheitsstrategie** ISMS.1.A11 Aufrechterhaltung der Informationssicherheit ISMS.1.A12 Management-Berichte zur Informationssicherheit

		ISO/IEC 27001:2022	IT-Grundschutz
10		**Improvement – Verbesserung**	
	10.1	Nonconformity and corrective action – Nichtkonformität und Korrekturmaßnahmen	**BSI-Standard 200-2, Kapitel 10.1 Überprüfung des Informationssicherheitsprozesses auf allen Ebenen und Kapitel 10.3 Übernahme der Ergebnisse in den Informationssicherheitsprozess** ISMS.1.A11 Aufrechterhaltung der Informationssicherheit
	10.2	Continual improvement – Fortlaufende Verbesserung	**BSI-Standard 200-2, Kapitel 10 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit** ISMS.1.A11 Aufrechterhaltung der Informationssicherheit DER.3.1.A1 Definition von Verantwortlichkeiten DER.3.2.A9 Integration in den Informationssicherheitsprozess

ISO/IEC 27001:2022 Anhang A und IT-Grundschutz			
		ISO/IEC 27002	**IT-Grundschutz**
5		**Organizational controls – Organisatorische Maßnahmen**	
	A.5.1	Policies for information security – Informationssicherheits-richtlinien	**ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit** **ORP.1.A1 Festlegung von Verantwortlichkeiten und Regelungen** ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitung ISMS.1.A16 Erstellung von zielgruppengerechten Sicherheitsrichtlinien ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT
	A.5.2	Information security roles and responsibilities – Informationssicherheits-rollen und -verantwortlichkeiten	**ISMS.1.A4 Benennung eines oder einer Informationssicherheitsbeauftragten** **ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit** **ORP.1.A1 Festlegung von Verantwortlichkeiten und Regelungen** **ORP.1.A2 Zuweisung der Zuständigkeiten**
	A.5.3	Segregation of duties – Aufgabentrennung	**ORP.1.A4 Funktionstrennung zwischen unvereinbaren Aufgaben** ORP.4.A4 Aufgabenverteilung und Funktionstrennung
	A.5.4	Management responsibilities – Verantwortlichkeiten der Leitung	**ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitung** **ISMS.1.A8 Integration der Mitarbeitenden in den Sicherheitsprozess** **ORP.3.A1 Sensibilisierung der Institutionsleitung für Informationssicherheit** ORP.2.A14 Aufgaben und Zuständigkeiten von Mitarbeitenden
	A.5.5	Contact with authorities – Kontakt mit Behörden	**DER.2.1.A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen** DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle DER.2.1.A14 Eskalationsstrategie für Sicherheitsvorfälle
	A.5.6	Contact with special interest groups – Kontakt mit speziellen Interessensgruppen	**DER.1.A12 Auswertung von Informationen aus externen Quellen** IND.1.A12 Etablieren eines Schwachstellen-Managements

	A.5.7	Threat intelligence – Bedrohungsintelligenz	**DER.1.A12 Auswertung von Informationen aus externen Quellen** OPS.1.1.1.A10 Führen eines Schwachstelleninventars OPS.1.1.1.A20 Prüfen auf Schwachstellen OPS.1.1.1.A22 Automatisierte Tests auf Schwachstellen OPS.1.1.1.A23 Durchführung von Penetrationstests DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle IND.1.A12 Etablieren eines Schwachstellen-Managements
	A.5.8	Information security in project management – Informationssicherheit im Projektmanagement	**ISMS.1.A9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse**
	A.5.9	Inventory of information and other associated assets – Inventar der Informationen und anderen damit verbundenen Werten	**BSI-Standard 200-2, Kapitel 8.1 Strukturanalyse** ORP.1.A2 Zuweisung der Zuständigkeiten ORP.1.A8 Betriebsmittel- und Geräteverwaltung OPS.1.1.1.A6 Durchführung des IT-Asset-Managements APP.6.A9 Inventarisierung von Software IND.1.A4 Dokumentation der OT-Infrastruktur NET.1.1.A2 Dokumentation des Netzes INF.11.A5 Erstellung einer Inventarliste
	A.5.10	Acceptable use of information and other associated assets – Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	**ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie** **ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT** CON.9 Informationsaustausch CON.7.A2 Sensibilisierung der Mitarbeitenden zur Informationssicherheit auf Auslandsreisen
	A.5.11	Return of assets – Rückgabe von Werten	**ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitenden** **ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen** ORP.2.A4 Festlegung von Regelungen für den Einsatz von Fremdpersonal
	A.5.12	Classification of information – Klassifizierung von	**BSI-Standard 200-2, Kapitel 5.1 Klassifikation von Informationen**

		Information	**BSI-Standard 200-2, Kapitel 8.2 Schutzbedarfsfeststellung** ISMS.1.A10 Erstellung eines Sicherheitskonzepts
	A.5.13	Labelling of information – Kennzeichnung von Information	**BSI-Standard 200-2, Kapitel 5.1 Klassifikation von Informationen**
	A.5.14	Information transfer – Informationsübertragung	**CON.9 Informationsaustausch** **CON.1 Kryptokonzept** APP.1.2 Webbrowser APP.5.3 Allgemeiner E-Mail-Client und -Server SYS.3.2.1 Allgemeine Smartphones und Tablets SYS.4.5 Wechseldatenträger CON.7.A9 Sicherer Umgang mit mobilen Datenträgern APP.5.3.A6 Festlegung einer Sicherheitsrichtlinie für E-Mail SYS.4.1.A5 Erstellung von Nutzungsrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten SYS.4.1.A15 Verschlüsselung von Informationen bei Druckern, Kopierern und Multifunktionsgeräten
	A.5.15	Access control – Zugangssteuerung	**ORP.4 Identitäts- und Berechtigungsmanagement** APP.2.1 Allgemeiner Verzeichnisdienst APP.2.2 Active Directory Domain Services APP.2.3 OpenLDAP NET.1.1 Netzarchitektur und -design NET.1.2 Netzmanagement NET.2.1 WLAN-Betrieb NET.2.2 WLAN-Nutzung NET.3.2 Firewall NET.3.3 VPN NET.3.4 Network Access Control INF.1.A7 Zutrittsregelung und -kontrolle
	A.5.16	Identity management – Identitätsmanagement	**ORP.4 Identitäts- und Berechtigungsmanagement**

			OPS.1.1.2.A4 Beendigung der Tätigkeit in der IT-Administration
	A.5.17	Authentication information – Informationen zur Authentifizierung	**ORP.4 Identitäts- und Berechtigungsmanagement**
	A.5.18	Access rights – Zugangsrechte	**ORP.4 Identitäts- und Berechtigungsmanagement** OPS.1.1.1.A2 Festlegung von Rollen und Berechtigungen für den IT-Betrieb OPS.1.1.2.A21 Regelung der IT-Administrationsrollen
	A.5.19	Information security in supplier relationships – Informationssicherheit in Lieferantenbeziehungen	**OPS.2.3 Nutzung von Outsourcing** CON.9.A9 Vertraulichkeitsvereinbarungen
	A.5.20	Addressing information security within supplier agreements – Behandlung von Informationssicherheit in Lieferantenvereinbarungen	**ISMS.1.A5 Vertragsgestaltung bei Bestellung eines oder einer externen Informationssicherheitsbeauftragten** **OPS.2.3.A4 Grundanforderungen an Verträge mit Anbietenden von Outsourcing** **OPS.2.3.A6 Festlegung von Sicherheitsanforderungen und Erstellung eines Sicherheitskonzeptes für das Outsourcing-Vorhaben** **OPS.2.3.A13 Bereitstellung der erforderlichen Kompetenzen bei der Vertragsgestaltung** **OPS.2.3.A14 Erweiterte Anforderungen an Verträge mit Anbietenden von Outsourcing** **OPS.2.3.A21 Abschluss von ESCROW-Verträgen bei softwarenahen Dienstleistungen** **OPS.2.3.A24 Sicherheits- und Eignungsüberprüfung von Mitarbeitenden** **DER.2.2.A13 Rahmenverträge mit externen Dienstleistenden** OPS.3.2.A2 Grundanforderungen an Verträge mit Nutzenden von Outsourcing OPS.3.2.A3 Weitergabe der vertraglich geregelten Bestimmungen mit Nutzenden von Outsourcing an Sub-Dienstleistende OPS.3.2.A16 Transparenz über die Outsourcing-Kette der ausgelagerten Kundenprozesse
	A.5.21	Managing information security in the ICT supply chain – Umgang mit der Informationssicherheit in der IKT-Lieferkette	**OPS.2.3 Nutzung von Outsourcing**

	A.5.22	Monitoring, review and change management of supplier services – Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	**OPS.2.3.A18 Überprüfung der Vereinbarungen mit Anbietenden von Outsourcing** OPS.3.2.A9 Überprüfung der Vereinbarung mit Nutzenden von Outsourcing
	A.5.23	Information security for use of cloud services – Informationssicherheit für die Nutzung von Cloud-Diensten	**OPS.2.2 Cloud-Nutzung**
	A.5.24	Information security incident management planning and preparation – Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	**DER.2.1 Behandlung von Sicherheitsvorfällen** DER.1 Detektion von sicherheitsrelevanten Ereignissen
	A.5.25	Assessment and decision on information security events – Beurteilung und Entscheidung über Informationssicherheits-ereignisse	**DER.1 Detektion von sicherheitsrelevanten Ereignissen** **DER.2.1 Behandlung von Sicherheitsvorfällen**
	A.5.26	Response to information security incidents – Reaktion auf Informationssicherheits-vorfälle	**DER.2.1 Behandlung von Sicherheitsvorfällen**
	A.5.27	Learning from information security incidents – Erkenntnisse aus Informationssicherheits-	**DER.2.1 Behandlung von Sicherheitsvorfällen** DER.2.1.A17 Nachbereitung von Sicherheitsvorfällen DER.2.1.A18 Weiterentwicklung der Prozesse durch Erkenntnisse aus Sicherheitsvorfällen und

		vorfällen	Branchenentwicklungen DER.2.1.A22 Überprüfung der Effizienz des Managementsystems zur Behandlung von Sicherheitsvorfällen
	A.5.28	Collection of evidence – Sammeln von Beweismaterial	**DER.2.2 Vorsorge für die IT-Forensik**
	A.5.29	Information security during disruption – Informationssicherheit bei Störungen	DER.4 Notfallmanagement DER.2.1 Behandlung von Sicherheitsvorfällen DER.2.2 Vorsorge für die IT-Forensik DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle BSI-Standard 200-4
	A.5.30	ICT readiness for business continuity – IKT-Bereitschaft für Business Continuity	**DER.4 Notfallmanagement** BSI-Standard 200-4
	A.5.31	Legal, statutory, regulatory and contractual requirements – Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	**ORP.5 Compliance Management (Anforderungsmanagement)**
	A.5.32	Intellectual property rights – Geistige Eigentumsrechte	**ORP.5 Compliance Management (Anforderungsmanagement)** APP.3.2.A7 Rechtliche Rahmenbedingungen für Webangebote APP.6.A9 Inventarisierung von Software
	A.5.33	Protection of records – Schutz von Aufzeichnungen	BSI-Standard 200-2, Kapitel 5 Dokumentation im Sicherheitsprozess ISMS.1.A13 Dokumentation des Sicherheitsprozesses
	A.5.34	Privacy and protection of PII – Datenschutz und Schutz personenbezogener Daten (pbD)	**ORP.5 Compliance Management (Anforderungsmanagement)** **CON.2 Datenschutz** CON.1.A9 Festlegung von Kriterien für die Auswahl von Hard- oder Software mit kryptografischen Funktionen OPS.1.1.5.A5 Einhaltung rechtlicher Rahmenbedingungen OPS.1.1.6.A11 Verwendung von anonymisierten oder pseudonymisierten Testdaten DER.1.A2 Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokollierungsdaten

			DER.1.A10 Einsatz von TLS-/SSL-Proxies DER.2.2.A1 Prüfung rechtlicher und regulatorischer Rahmenbedingungen zur Erfassung und Auswertbarkeit APP.1.2.A11 Überprüfung auf schädliche Inhalte SYS.2.1.A42 Nutzung von Cloud- und Online-Funktionen SYS.2.2.3.A4 Telemetrie und Datenschutzeinstellungen unter Windows
	A.5.35	Independent review of information security – Unabhängige Überprüfung der Informationssicherheit	**ISMS.1.A11 Aufrechterhaltung der Informationssicherheit** **DER.3.1 Audits und Revisionen** **DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision** BSI-Standard 200-2, Kapitel 10 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit OPS.1.1.1.A22 Automatisierte Tests auf Schwachstellen OPS.1.1.1.A23 Durchführung von Penetrationstests
	A.5.36	Compliance with policies, rules and standards for information security – Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	**BSI-Standard 200-2, Kapitel 10 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit** **DER.3.1 Audits und Revisionen** **DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision** **ISMS.1.A11 Aufrechterhaltung der Informationssicherheit**
	A.5.37	Documented operating procedures – Dokumentierte Betriebsabläufe	**OPS.1.1.1.A3 Erstellen von Betriebshandbüchern für die betriebene IT** **OPS.1.1.2.A11 Dokumentation von IT-Administrationstätigkeiten** **OPS.1.1.3.A11 Kontinuierliche Dokumentation der Informationsverarbeitung** BSI-Standard 200-2, Kapitel 5.2.2 Dokumentation im Informationssicherheitsprozess ISMS.1.A13 Dokumentation des Sicherheitsprozesses CON.8.A12 Ausführliche Dokumentation OPS.1.2.5.A7 Dokumentation bei der Fernwartung DER.2.1.A16 Dokumentation der Behebung von Sicherheitsvorfällen SYS.1.1.A21 Betriebsdokumentation für Server SYS.2.1.A40 Betriebsdokumentation NET.3.1.A9 Betriebsdokumentationen NET.3.2.A14 Betriebsdokumentationen

			NET.4.1.A10 Dokumentation und Revision der TK-Anlagenkonfiguration
6		**People controls – Personenbezogene Maßnahmen**	
	A.6.1	Screening – Sicherheitsüberprüfung	**ORP.2.A7 Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden** **ORP.2.A13 Sicherheitsüberprüfung** OPS.1.1.6.A16 Sicherheitsüberprüfung der Testenden OPS.2.2.A19 Sicherheitsüberprüfung von Mitarbeitenden
	A.6.2	Terms and conditions of employment – Beschäftigungs- und Vertragsbedingungen	**ORP.2.A4 Festlegung von Regelungen für den Einsatz von Fremdpersonal** **ORP.2.A14 Aufgaben und Zuständigkeiten von Mitarbeitenden** ORP.2.A1 Geregelte Einarbeitung neuer Mitarbeitender ORP.2.A5 Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal
	A.6.3	Information security awareness, education and training – Informationssicherheits-bewusstsein, -ausbildung und -schulung	**ORP.3 Sensibilisierung und Schulung zur Informationssicherheit** ORP.3.A1 Sensibilisierung der Institutionsleitung für Informationssicherheit ORP.3.A4 Konzeption und Planung eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit ORP.3.A6 Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit ORP.3.A7 Schulung zur Vorgehensweise nach IT-Grundschutz ORP.3.A8 Messung und Auswertung des Lernerfolgs
	A.6.4	Disciplinary process – Maßregelungsprozess	**ISMS.1.A8 Integration der Mitarbeitenden in den Sicherheitsprozess** IND.1.A7 Etablieren einer übergreifenden Berechtigungsverwaltung zwischen der OT und in der Office-IT
	A.6.5	Responsibilities after termination or change of employment – Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	**ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitenden** **ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen** ISMS.1.A5 Vertragsgestaltung bei Bestellung eines oder einer externe Informationssicherheitsbeauftragten ORP.2.A14 Aufgaben und Zuständigkeiten von Mitarbeitenden OPS.1.1.2.A4 Beendigung der Tätigkeit in der IT-Administration

	A.6.6	Confidentiality or nondisclosure agreements – Vertraulichkeits- oder Geheimhaltungs-vereinbarungen	**CON.9.A9 Vertraulichkeitsvereinbarungen** **ORP.2.A5 Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal** OPS.3.2.A18 Regelungen für den Einsatz von Sub-Dienstleistenden SYS.4.1.A2 Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte
	A.6.7	Remote working – Telearbeit	**OPS.1.2.4 Telearbeit** **INF.8 Häuslicher Arbeitsplatz** **INF.9 Mobiler Arbeitsplatz** NET.3.3 VPN CON.7.A7 Sicherer Remote-Zugriff auf das Netz der Institution
	A.6.8	Information security event reporting – Meldung von Informationssicherheits-ereignissen	**DER.1.A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse** **DER.1.A4 Sensibilisierung der Mitarbeitenden** **DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle** **DER.2.1.A20 Einrichtung einer dedizierten Meldestelle für Sicherheitsvorfälle**
7		**Physical controls – Physische Maßnahmen**	
	A.7.1	Physical security perimeters – Physische Sicherheitsperimeter	**INF.1.A6 Geschlossene Fenster und Türen** **INF.1.A22 Sichere Türen und Fenster** **INF.1.A23 Bildung von Sicherheitszonen** **INF.1.A26 Pforten- oder Sicherheitsdienst** **INF.1.A27 Einbruchschutz** **INF.1.A34 Gefahrenmeldeanlage** **INF.1.A35 Perimeterschutz** **INF.2.A1 Festlegung von Anforderungen** **INF.2.A7 Verschließen und Sichern** **INF.2.A12 Perimeterschutz für das Rechenzentrum** **INF.2.A24 Einsatz von Videoüberwachungsanlagen** **INF.2.A28 Einsatz von höherwertigen Gefahrenmeldeanlagen** INF.1.A1 Planung der Gebäudeabsicherung INF.1.A9 Sicherheitskonzept für die Gebäudenutzung

	A.7.2	Physical entry – Physischer Zutritt	**INF.1.A7 Zutrittsregelung und -kontrolle** **INF.1.A12 Schlüsselverwaltung** **INF.1.A13 Regelungen für Zutritt zu Verteilern** **INF.2.A6 Zutrittskontrolle** **INF.2.A7 Verschließen und Sichern** **ORP.4.A5 Vergabe von Zutrittsberechtigungen** ORP.1.A3 Beaufsichtigung oder Begleitung von Fremdpersonen INF.1.A26 Pforten- oder Sicherheitsdienst
	A.7.3	Securing offices, rooms and facilities – Sichern von Büros, Räumen und Einrichtungen	**Bausteine der Schicht Infrastruktur, z. B. INF.7 Büroarbeitsplatz** **INF.1.A9 Sicherheitskonzept für die Gebäudenutzung** **INF.5.A1 Planung der Raumabsicherung** **INF.5.A2 Lage und Größe des Raumes für technische Infrastruktur** **INF.7.A1 Geeignete Auswahl und Nutzung eines Büroraumes** INF.1.A16 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile INF.2.A1 Festlegung von Anforderungen INF.5.A4 Schutz vor Einbruch
	A.7.4	Physical security monitoring – Physische Sicherheitsüberwachung	**INF.1.A26 Pforten- oder Sicherheitsdienst** **INF.1.A27 Einbruchschutz** **INF.1.A34 Gefahrenmeldeanlage** **INF.2.A13 Planung und Installation von Gefahrenmeldeanlagen** **INF.2.A24 Einsatz von Videoüberwachungsanlagen** **INF.2.A28 Einsatz von höherwertigen Gefahrenmeldeanlagen** INF.1.A35 Perimeterschutz
	A.7.5	Protecting against physical and environmental threats – Schutz vor physischen und umweltbedingten Bedrohungen	**Bausteine der Schicht Infrastruktur** INF.1.A1 Planung der Gebäudeabsicherung INF.1.A3 Einhaltung von Brandschutzvorschriften INF.1.A4 Branderkennung in Gebäuden INF.1.A5 Handfeuerlöscher INF.1.A8 Rauchverbot

			INF.1.A9 Sicherheitskonzept für die Gebäudenutzung INF.1.A10 Einhaltung einschlägiger Normen und Vorschriften INF.1.A14 Blitzschutzeinrichtungen INF.1.A15 Lagepläne der Versorgungsleitungen INF.1.A17 Baulicher Rauchschutz INF.1.A20 Alarmierungsplan und Brandschutzübungen INF.1.A24 Selbsttätige Entwässerung INF.1.A25 Geeignete Standortauswahl INF.1.A32 Brandschott-Kataster INF.2.A2 Bildung von Brandabschnitten INF.2.A5 Einhaltung der Lufttemperatur und -feuchtigkeit INF.2.A8 Einsatz einer Brandmeldeanlage INF.2.A9 Einsatz einer Lösch- oder Brandvermeidungsanlage INF.2.A15 Überspannungsschutzeinrichtung INF.2.A16 Klimatisierung im Rechenzentrum INF.2.A21 Ausweichrechenzentrum INF.2.A22 Durchführung von Staubschutzmaßnahmen INF.2.A30 Anlagen zur Löschung oder Vermeidung von Bränden
	A.7.6	Working in secure areas – Arbeiten in Sicherheitsbereichen	**Bausteine der Schicht Infrastruktur** **INF.1.A9 Sicherheitskonzept für die Gebäudenutzung** **INF.1.A23 Bildung von Sicherheitszonen** **INF.2.A1 Festlegung von Anforderungen** SYS.3.3.A15 Schutz vor Abhören der Raumgespräche über Mobiltelefone
	A.7.7	Clear desk and clear screen – Aufgeräumte Arbeitsumgebung und Bildschirmsperren	**SYS.2.1.A1 Sichere Authentisierung von Benutzenden** **SYS.3.2.1.A4 Verwendung eines Zugriffsschutzes** **INF.7.A6 Aufgeräumter Arbeitsplatz** SYS.4.5 Wechseldatenträger ORP.4.A9 Identifikation und Authentisierung INF.7.A7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger INF.7.A8 Einsatz von Diebstahlsicherungen

			INF.8.A1 Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz INF.8.A6 Umgang mit dienstlichen Unterlagen bei erhöhtem Schutzbedarf am häuslichen Arbeitsplatz
	A.7.8	Equipment siting and protection – Platzierung und Schutz von Geräten und Betriebsmitteln	**Bausteine der Schicht Infrastruktur** OPS.1.2.2.A3 Geeignete Aufstellung von Archivsystemen und Lagerung von Archivmedien SYS.1.1.A1 Zugriffsschutz und Nutzung INF.2.A5 Einhaltung der Lufttemperatur und -feuchtigkeit INF.7.A7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
	A.7.9	Security of assets off-premises – Sicherheit von Werten außerhalb der Räumlichkeiten	**OPS.1.2.4 Telearbeit** **INF.8 Häuslicher Arbeitsplatz** **INF.9 Mobiler Arbeitsplatz** **CON.7 Informationssicherheit auf Auslandsreisen** SYS.3.1 Laptops
	A.7.10	Storage media – Speichermedien	**SYS.4.5 Wechseldatenträger** **SYS.4.5.A5 Regelung zur Mitnahme von Wechseldatenträgern** CON.6 Löschen und Vernichten CON.3.A12 Sichere Aufbewahrung der Speichermedien für die Datensicherungen CON.6.A13 Vernichtung defekter digitaler Datenträger CON.6.A14 Vernichten von Datenträgern auf erhöhter Sicherheitsstufe CON.7.A10 Verschlüsselung tragbarer IT-Systeme und Datenträger CON.7.A13 Mitnahme notwendiger Daten und Datenträger OPS.1.2.2.A3 Geeignete Aufstellung von Archivsystemen und Lagerung von Archivmedien SYS.4.5.A13 Kennzeichnung der Wechseldatenträger beim Versand INF.7.A7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger INF.9.A9 Verschlüsselung tragbarer IT-Systeme und Datenträger
	A.7.11	Supporting utilities – Versorgungseinrichtungen	**INF.1 Allgemeines Gebäude** **INF.2 Rechenzentrum sowie Serverraum** **INF.5 Raum sowie Schrank für technische Infrastruktur** **INF.12 Verkabelung** INF.2.A3 Einsatz einer unterbrechungsfreien Stromversorgung

			INF.2.A4 Notabschaltung der Stromversorgung INF.2.A5 Einhaltung der Lufttemperatur und -feuchtigkeit INF.2.A10 Inspektion und Wartung der Infrastruktur INF.2.A11 Automatische Überwachung der Infrastruktur INF.2.A14 Einsatz einer Netzersatzanlage INF.2.A16 Klimatisierung im Rechenzentrum INF.2.A19 Durchführung von Funktionstests der technischen Infrastruktur INF.2.A25 Redundante Auslegung von unterbrechungsfreien Stromversorgungen INF.2.A26 Redundante Auslegung von Netzersatzanlagen INF.5.A9 Stromversorgung INF.5.A10 Einhaltung der Lufttemperatur und -feuchtigkeit INF.5.A11 Vermeidung von Leitungen mit gefährdenden Flüssigkeiten und Gasen INF.5.A16 Einsatz einer unterbrechungsfreien Stromversorgung INF.5.A17 Inspektion und Wartung der Infrastruktur INF.5.A24 Lüftung und Kühlung SYS.1.1.A15 Unterbrechungsfreie und stabile Stromversorgung SYS.2.1.A39 Unterbrechungsfreie und stabile Stromversorgung
	A.7.12	Cabling security – Sicherheit der Verkabelung	**INF.12 Verkabelung** INF.1.A13 Regelungen für Zutritt zu Verteilern INF.2.A23 Zweckmäßiger Aufbau der Verkabelung im Rechenzentrum INF.12.A2 Planung der Kabelführung INF.12.A5 Anforderungsanalyse für die Verkabelung INF.12.A10 Dokumentation und Kennzeichnung der Verkabelung INF.12.A11 Neutrale Dokumentation in den Verteilern INF.12.A15 Materielle Sicherung der Verkabelung INF.12.A17 Redundanzen für die IT-Verkabelung
	A.7.13	Equipment maintenance – Instandhaltung von Geräten und Betriebsmitteln	**OPS.1.1.1.A19 Regelungen für Wartungs- und Reparaturarbeiten** INF.2.A3 Einsatz einer unterbrechungsfreien Stromversorgung INF.2.A10 Inspektion und Wartung der Infrastruktur INF.2.A14 Einsatz einer Netzersatzanlage INF.2.A26 Redundante Auslegung von Netzersatzanlagen

			INF.5.A17 Inspektion und Wartung der Infrastruktur INF.5.A23 Netzersatzanlage INF.5.A24 Lüftung und Kühlung INF.11.A2 Wartung, Inspektion und Updates INF.13.A12 Sichere Konfiguration der TGM-Systeme INF.13.A17 Regelung von Wartungs- und Reparaturarbeiten im TGM INF.13.A18 Proaktive Instandhaltung im TGM
	A.7.14	Secure disposal or re-use of equipment – Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	**CON.6 Löschen und Vernichten** CON.6.A2 Ordnungsgemäßes Löschen und Vernichten von schützenswerten Betriebsmitteln und Informationen CON.6.A13 Vernichtung defekter digitaler Datenträger SYS.1.1.A25 Geregelte Außerbetriebnahme eines Servers SYS.1.8.A16 Sicheres Löschen in SAN-Umgebungen SYS.1.8.A25 Mehrfaches Überschreiben der Daten einer LUN SYS.2.1.A27 Geregelte Außerbetriebnahme eines Clients SYS.3.2.2.A22 Fernlöschung und Außerbetriebnahme von Endgeräten SYS.4.4.A20 Geregelte Außerbetriebnahme von IoT-Geräten NET.4.1.A11 Außerbetriebnahme von TK-Anlagen und -geräten NET.4.2.A12 Sichere Außerbetriebnahme von VoIP-Komponenten
8		**Technological controls – Technologische Maßnahmen**	
	A.8.1	User endpoint devices – Endpunktgeräte des Benutzers	**ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT** **Clients-Bausteine, z. B.** SYS.2.1 Allgemeiner Client SYS.3.1 Laptops SYS.3.2.1 Allgemeine Smartphones und Tablets SYS.3.2.2 Mobile Device Management (MDM) SYS.3.2.3 iOS (for Enterprise) SYS.3.2.4 Android SYS.3.3 Mobiltelefon

			INF.9.A2 Regelungen für mobile Arbeitsplätze INF.9.A8 Sicherheitsrichtlinie für mobile Arbeitsplätze
	A.8.2	Privileged access rights – Privilegierte Zugangsrechte	**OPS.1.1.2 Ordnungsgemäße IT-Administration** **ORP.4.A10 Schutz von Benutzendenkennungen mit weitreichenden Berechtigungen** **ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle** ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen OPS.1.1.1.A2 Festlegung von Rollen und Berechtigungen für den IT-Betrieb OPS.1.1.2.A4 Beendigung der Tätigkeit in der IT-Administration OPS.1.1.2.A5 Nachweisbarkeit von administrativen Tätigkeiten OPS.1.1.2.A6 Schutz administrativer Tätigkeiten OPS.1.1.2.A16 Erweiterte Sicherheitsmaßnahmen für Administrationszugänge OPS.1.1.2.A17 IT-Administration im Vier-Augen-Prinzip OPS.1.1.2.A18 Durchgängige Protokollierung administrativer Tätigkeiten OPS.1.1.2.A21 Regelung der IT-Administrationsrollen APP.2.1.A12 Überwachung von Verzeichnisdiensten APP.2.2.A17 Anmelderestriktionen für hochprivilegierte Konten der Gesamtstruktur auf Clients und Servern APP.4.4.A9 Nutzung von Kubernetes Service-Accounts SYS.2.2.3.A20 Einsatz der Benutzerkontensteuerung UAC für privilegierte Konten IND.1.A14 Starke Authentisierung an OT-Komponenten
	A.8.3	Information access restriction – Informationszugangs-beschränkung	**ORP.4 Identitäts- und Berechtigungsmanagement** **ORP.4.A7 Vergabe von Zugriffsrechten** APP.2.1 Allgemeiner Verzeichnisdienst APP.2.2 Active Directory Domain Services APP.2.3 OpenLDAP ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzenden und Benutzendengruppen ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen ORP.4.A3 Dokumentation der Benutzendenkennungen und Rechteprofile ORP.4.A4 Aufgabenverteilung und Funktionstrennung ORP.4.A5 Vergabe von Zutrittsberechtigungen ORP.4.A6 Vergabe von Zugangsberechtigungen

			ORP.4.A15 Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle ORP.4.A19 Einweisung aller Mitarbeitenden in den Umgang mit Authentisierungsverfahren und -mechanismen OPS.1.1.2.A4 Beendigung der Tätigkeit in der IT-Administration
	A.8.4	Access to source code – Zugriff auf den Quellcode	**ORP.4 Identitäts- und Berechtigungsmanagement** **CON.8 Software-Entwicklung** **CON.8.A10 Versionsverwaltung des Quellcodes**
	A.8.5	Secure authentication – Sichere Authentifizierung	**ORP.4 Identitäts- und Berechtigungsmanagement** APP.2.1 Allgemeiner Verzeichnisdienst APP.2.2 Active Directory Domain Services APP.2.3 OpenLDAP NET.3.3 VPN ORP.4.A11 Zurücksetzen von Passwörtern ORP.4.A12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen ORP.4.A14 Kontrolle der Wirksamkeit der Benutzendentrennung am IT-System bzw. an der Anwendung OPS.1.1.2.A16 Erweiterte Sicherheitsmaßnahmen für Administrationszugänge SYS.2.1.A1 Sichere Authentisierung von Benutzenden SYS.2.1.A37 Verwendung von Mehr-Faktor-Authentisierung SYS.3.2.1.A4 Verwendung eines Zugriffsschutzes
	A.8.6	Capacity management – Kapazitätssteuerung	**OPS.1.1.1.A9 Durchführung von IT-Monitoring** OPS.1.2.2.A12 Überwachung der Speicherressourcen von Archivmedien DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten SYS.1.1.A12 Planung des Server-Einsatzes SYS.1.1.A23 Systemüberwachung und Monitoring von Servern SYS.1.5.A17 Überwachung des Betriebszustands und der Konfiguration der virtuellen Infrastruktur SYS.2.1.A29 Systemüberwachung und Monitoring der Clients NET.1.1.A13 Netzplanung NET.1.2.A25 Statusüberwachung der Netzkomponenten

			NET.3.2.A23 Systemüberwachung und -auswertung
	A.8.7	Protection against malware – Schutz gegen Schadsoftware	**OPS.1.1.4 Schutz vor Schadprogrammen** DER.2.1 Behandlung von Sicherheitsvorfällen CON.7.A2 Sensibilisierung der Mitarbeitenden zur Informationssicherheit auf Auslandsreisen CON.7.A9 Sicherer Umgang mit mobilen Datenträgern DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion DER.1.A12 Auswertung von Informationen aus externen Quellen APP.1.1.A3 Sicheres Öffnen von Dokumenten aus externen Quellen APP.1.2.A11 Überprüfung auf schädliche Inhalte APP.3.2.A14 Integritätsprüfungen und Schutz vor Schadsoftware APP.3.3.A12 Verschlüsselung des Datenbestandes APP.5.3.A1 Sichere Konfiguration der E-Mail-Clients SYS.1.1.A31 Einsatz von Ausführungskontrolle SYS.1.2.2.A5 Schutz vor Schadsoftware auf Windows Server 2012 SYS.2.2.3.A5 Schutz vor Schadsoftware unter Windows SYS.2.2.3.A13 Einsatz der SmartScreen-Funktion SYS.3.1.A7 Geregelte Übergabe und Rücknahme eines Laptops SYS.4.5.A12 Schutz vor Schadsoftware SYS.4.5.A16 Nutzung dedizierter IT-Systeme zur Datenprüfung IND.1.A3 Schutz vor Schadprogrammen IND.2.1.A8 Schutz vor Schadsoftware IND.3.2.A9 Sicherer Austausch von Dateien begleitend zur OT-Fernwartung NET.3.2.A21 Temporäre Entschlüsselung des Datenverkehrs INF.13.A15 Schutz vor Schadsoftware im TGM
	A.8.8	Management of technical vulnerabilities – Handhabung von technischen Schwachstellen	**OPS.1.1.3.A15 Regelmäßige Aktualisierung von IT-Systemen und Software** **DER.1.A12 Auswertung von Informationen aus externen Quellen** **OPS.1.1.1.A10 Führen eines Schwachstelleninventars** **OPS.1.1.1.A20 Prüfen auf Schwachstellen** **OPS.1.1.1.A22 Automatisierte Tests auf Schwachstellen** **OPS.1.1.1.A23 Durchführung von Penetrationstests** IND.1.A12 Etablieren eines Schwachstellen-Managements

	A.8.9	Configuration management – Konfigurationsmanagement	**OPS.1.1.1.A5 Festlegen von gehärteten Standardkonfigurationen** **OPS.1.1.1.A7 Sicherstellung eines ordnungsgemäßen IT-Betriebs** **OPS.1.1.1.A8 Regelmäßiger Soll-Ist-Vergleich** **OPS.1.1.3.A11 Kontinuierliche Dokumentation der Informationsverarbeitung** CON.8.A12 Ausführliche Dokumentation OPS.1.1.1.A3 Erstellen von Betriebshandbüchern für die betriebene IT OPS.1.1.1.A25 Sicherstellen von autark funktionierenden Betriebsmitteln OPS.1.1.2.A11 Dokumentation von IT-Administrationstätigkeiten OPS.1.1.2.A26 Backup der Konfiguration APP.6.A4 Regelung für die Installation und Konfiguration von Software SYS.1.1.A21 Betriebsdokumentation für Server SYS.2.1.A40 Betriebsdokumentation NET.3.1.A9 Betriebsdokumentationen NET.3.2.A14 Betriebsdokumentationen NET.4.1.A10 Dokumentation und Revision der TK-Anlagenkonfiguration
	A.8.10	Information deletion – Löschung von Informationen	**CON.6 Löschen und Vernichten** CON.1.A5 Sicheres Löschen und Vernichten von kryptografischen Schlüsseln SYS.1.1.A25 Geregelte Außerbetriebnahme eines Servers SYS.2.1.A27 Geregelte Außerbetriebnahme eines Clients SYS.3.2.2.A22 Fernlöschung und Außerbetriebnahme von Endgeräten SYS.4.4.A20 Geregelte Außerbetriebnahme von IoT-Geräten NET.4.1.A11 Außerbetriebnahme von TK-Anlagen und -geräten NET.4.2.A12 Sichere Außerbetriebnahme von VoIP-Komponenten
	A.8.11	Data masking – Datenmaskierung	**OPS.1.1.6.A11 Verwendung von anonymisierten oder pseudonymisierten Testdaten** CON.2 Datenschutz
	A.8.12	Data leakage prevention – Verhinderung von Datenlecks	**SYS.2.1.A24 Umgang mit externen Medien und Wechseldatenträgern** **SYS.4.1.A20 Erweiterter Schutz von Informationen bei Druckern, Kopierern und Multifunktionsgeräten** **NET.1.1.A35 Einsatz von netzbasiertem DLP**
	A.8.13	Information backup –	**CON.3 Datensicherungskonzept**

		Sicherung von Information	CON.1.A2 Datensicherung beim Einsatz kryptografischer Verfahren
	A.8.14	Redundancy of information processing facilities – Redundanz von informationsverarbeitenden Einrichtungen	**INF.2 Rechenzentrum sowie Serverraum** **DER.4 Notfallmanagement** OPS.1.1.2.A19 Nutzung hochverfügbarer IT-Administrationswerkzeuge OPS.1.1.5.A13 Hochverfügbare Protokollierungsinfrastruktur OPS.1.2.5.A22 Redundante Kommunikationsverbindungen APP.3.2.A15 Redundanz APP.3.3.A13 Replikation zwischen Standorten APP.3.6.A2 Einsatz redundanter DNS-Server APP.5.3.A11 Einsatz redundanter E-Mail-Server SYS.1.1.A28 Steigerung der Verfügbarkeit durch Redundanz SYS.1.5.A20 Verwendung von hochverfügbaren Architekturen SYS.1.8.A2 Sichere Grundkonfiguration von Speicherlösungen SYS.1.8.A22 Einsatz einer hochverfügbaren SAN-Lösung NET.1.1.A28 Hochverfügbare Netz- und Sicherheitskomponenten NET.1.1.A29 Hochverfügbare Realisierung von Netzanbindungen NET.1.2.A30 Hochverfügbare Realisierung der Management-Lösung NET.4.1.A19 Redundanter Anschluss INF.2.A21 Ausweichrechenzentrum INF.2.A25 Redundante Auslegung von unterbrechungsfreien Stromversorgungen INF.2.A26 Redundante Auslegung von Netzersatzanlagen INF.5.A19 Redundanz des Raumes für technische Infrastruktur INF.12.A17 Redundanzen für die IT-Verkabelung
	A.8.15	Logging –Protokollierung	**OPS.1.1.5 Protokollierung** **DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten** **DER.1.A11 Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse** OPS.1.1.2.A18 Durchgängige Protokollierung administrativer Tätigkeiten DER.1.A2 Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokollierungsdaten DER.1.A14 Auswertung der Protokollierungsdaten durch spezialisiertes Personal APP.3.2.A4 Protokollierung von Ereignissen

			SYS.1.1.A10 Protokollierung SYS.1.1.A12 Planung des Server-Einsatzes SYS.1.5.A6 Protokollierung in der virtuellen Infrastruktur SYS.2.1.A45 Erweiterte Protokollierung SYS.2.2.3.A22 Verwendung der Windows PowerShell SYS.2.3.A1 Authentisierung von Administrierenden und Benutzenden SYS.4.3.A3 Protokollierung sicherheitsrelevanter Ereignisse bei eingebetteten Systemen SYS.4.4.A18 Protokollierung sicherheitsrelevanter Ereignisse bei IoT-Geräten IND.1.A10 Monitoring, Protokollierung und Detektion IND.1.A18 Protokollierung IND.1.A22 Zentrale Systemprotokollierung und -überwachung NET.1.2.A7 Grundlegende Protokollierung von Ereignissen NET.1.2.A26 Alarming und Logging NET.1.2.A35 Festlegungen zur Beweissicherung NET.1.2.A36 Einbindung der Protokollierung des Netzmanagements in eine SIEM-Lösung NET.3.1.A7 Protokollierung bei Routern und Switches NET.3.2.A9 Protokollierung NET.4.1.A5 Protokollierung bei TK-Anlagen NET.4.3.A9 Nutzung von Sende- und Empfangsprotokollen
	A.8.16	Monitoring activities – Überwachung von Aktivitäten	**OPS.1.1.1.A9 Durchführung von IT-Monitoring** OPS.1.1.7.A22 Einbindung des Systemmanagements in automatisierte Detektionssysteme OPS.1.1.7.A25 Protokollierung und Reglementierung von Systemmanagement-Sitzungen DER.1.A9 Einsatz zusätzlicher Detektionssysteme DER.1.A15 Zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen DER.1.A16 Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen SYS.1.1.A27 Hostbasierte Angriffserkennung SYS.1.9.A19 Erweitertes Monitoring des Terminalservers SYS.2.5.A17 Erweitertes Monitoring der virtuellen Clients SYS.2.6.A16 Integration der VDI in ein SIEM NET.2.1.A18 Einsatz von Wireless Intrusion Detection/Wireless Intrusion Prevention Systemen IND.3.2.A14 Technische Kontrolle von Fernwartungssitzungen

			INF.13.A29 Integration des TGM in ein SIEM
	A.8.17	Clock synchronization – Uhrensynchronisation	**OPS.1.1.5.A4 Zeitsynchronisation der IT-Systeme** **OPS.1.2.6 NTP-Zeitsynchronisation** OPS.1.1.7.A3 Zeitsynchronisation für das Systemmanagement OPS.1.1.7.A23 Standort-übergreifende Zeitsynchronisation für das Systemmanagement SYS.1.5.A7 Zeitsynchronisation in virtuellen IT-Systemen IND.2.2.A3 Zeitsynchronisation NET.1.2.A37 Standortübergreifende Zeitsynchronisation NET.3.2.A22 Sichere Zeitsynchronisation INF.14.A24 Zeitsynchronisation für die GA INF.14.A30 Bereitstellung eines GA-eigenen Zeitservers zur Zeitsynchronisation
	A.8.18	Use of privileged utility programs – Gebrauch von Hilfsprogrammen mit privilegierten Rechten	**ORP.4 Identitäts- und Berechtigungsmanagement** **OPS.1.1.2 Ordnungsgemäße IT-Administration** ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzenden und Benutzendengruppen ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen OPS.1.1.2.A22 Trennung von administrativen und anderen Tätigkeiten SYS.2.3.A7 Restriktive Rechtevergabe auf Dateien und Verzeichnisse SYS.4.4.A15 Restriktive Rechtevergabe
	A.8.19	Installation of software on operational systems – Installation von Software auf Systemen im Betrieb	**APP.6 Allgemeine Software** OPS.1.1.6 Software-Tests und -Freigaben OPS.1.1.3 Patch- und Änderungsmanagement APP.7 Entwicklung von Individualsoftware OPS.1.1.3.A9 Test- und Abnahmeverfahren für neue Hardware APP.6.A1 Planung des Software-Einsatzes APP.6.A4 Regelung für die Installation und Konfiguration von Software APP.6.A5 Sichere Installation von Software APP.6.A8 Regelung zur Verfügbarkeit der Installationsdateien
	A.8.20	Networks security – Netzwerksicherheit	**Bausteine der Schicht NET, z. B.** **NET.1.1 Netzarchitektur und -design** **NET.1.2 Netzmanagement**

			NET.2.1 WLAN-Betrieb **NET.2.2 WLAN-Nutzung** **NET.3.1 Router und Switches** **NET.3.2 Firewall** **NET.3.3 VPN** **NET.3.4 Network Access Control** **CON.1 Kryptokonzept** ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten NET.1.1.A4 Netztrennung in Zonen NET.1.1.A7 Absicherung von schützenswerten Informationen NET.1.1.A16 Spezifikation der Netzarchitektur NET.1.1.A22 Spezifikation des Segmentierungskonzepts NET.1.1.A23 Trennung von Netzsegmenten NET.1.1.A34 Einsatz kryptografischer Verfahren auf Netzebene NET.1.2.A7 Grundlegende Protokollierung von Ereignissen NET.1.2.A9 Absicherung der Netzmanagement-Kommunikation und des Zugriffs auf Netz-Management-Werkzeuge NET.1.2.A11 Festlegung einer Sicherheitsrichtlinie für das Netzmanagement NET.3.1.A24 Einsatz von Netzzugangskontrollen
	A.8.21	Security of network services – Sicherheit von Netzwerkdiensten	**NET.1.1 Netzarchitektur und -design** **NET.1.2 Netzmanagement** CON.1 Kryptokonzept NET.3.1 Router und Switches NET.3.2 Firewall NET.3.3 VPN NET.3.4 Network Access Control ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen NET.1.1.A34 Einsatz kryptografischer Verfahren auf Netzebene NET.3.1.A19 Sicherung von Switch-Ports

			NET.3.1.A24 Einsatz von Netzzugangskontrollen
	A.8.22	Segregation of networks – Trennung von Netzwerken	**NET.1.1 Netzarchitektur und -design** **NET.1.2 Netzmanagement** NET.1.1.A4 Netztrennung in Zonen NET.1.1.A5 Client-Server-Segmentierung NET.1.1.A6 Endgeräte-Segmentierung im internen Netz NET.1.1.A10 DMZ-Segmentierung für Zugriffe aus dem Internet NET.1.1.A18 P-A-P-Struktur für die Internet-Anbindung NET.1.1.A19 Separierung der Infrastrukturdienste NET.1.1.A21 Separierung des Management-Bereichs NET.1.1.A22 Spezifikation des Segmentierungskonzepts NET.1.1.A23 Trennung von Netzsegmenten NET.1.1.A24 Sichere logische Trennung mittels VLAN NET.1.1.A32 Physische Trennung von Management-Netzsegmenten NET.1.1.A33 Mikrosegmentierung des Netzes NET.1.1.A36 Trennung mittels VLAN bei sehr hohem Schutzbedarf NET.1.2.A32 Physische Trennung des Managementnetzes NET.1.2.A33 Physische Trennung von Management-Segmenten
	A.8.23	Web filtering – Webfilterung	**NET.3.2 Firewall**
	A.8.24	Use of cryptography – Verwendung von Kryptographie	**CON.1 Kryptokonzept**
	A.8.25	Secure development life cycle – Lebenszyklus einer sicheren Entwicklung	**CON.8 Software-Entwicklung** **APP.7 Entwicklung von Individualsoftware** CON.10 Entwicklung von Webanwendungen
	A.8.26	Application security requirements – Anforderungen an die Anwendungssicherheit	**CON.8 Software-Entwicklung** **APP.6 Allgemeine Software** **APP.7 Entwicklung von Individualsoftware** **OPS.1.1.6 Software-Tests und -Freigaben** **CON.10 Entwicklung von Webanwendungen**

			APP.3.1.A9 Beschaffung von Webanwendungen und Webservices APP.3.3.A6 Beschaffung eines Fileservers und Auswahl eines Dienstes
	A.8.27	Secure system architecture and engineering principles – Sichere Systemarchitektur und technische Grundsätze	**CON.8 Software-Entwicklung** **APP.6 Allgemeine Software** **APP.7 Entwicklung von Individualsoftware** OPS.1.1.6 Software-Tests und -Freigaben CON.8.A5 Sicheres Systemdesign CON.8.A12 Ausführliche Dokumentation CON.8.A22 Sicherer Software-Entwurf CON.10.A11 Softwarearchitektur einer Webanwendung SYS.4.3.A7 Hardware-Realisierung von Funktionen eingebetteter Systeme IND.1.A11 Sichere Beschaffung und Systementwicklung
	A.8.28	Secure coding – Sicheres Coding	**CON.8 Software-Entwicklung** **APP.7 Entwicklung von Individualsoftware** OPS.1.1.6 Software-Tests und -Freigaben CON.10 Entwicklung von Webanwendungen
	A.8.29	Security testing in development and acceptance – Sicherheitsprüfung in Entwicklung und Abnahme	**OPS.1.1.6 Software-Tests und -Freigaben** OPS.1.1.6.A5 Durchführung von Software-Tests für nicht funktionale Anforderungen OPS.1.1.6.A12 Durchführung von Regressionstests OPS.1.1.6.A14 Durchführung von Penetrationstests
	A.8.30	Outsourced development – Ausgegliederte Entwicklung	**OPS.2.3 Nutzung von Outsourcing** **APP.7 Entwicklung von Individualsoftware** OPS.3.2 Anbieten von Outsourcing
	A.8.31	Separation of development, test and production environments – Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen	**OPS.1.1.6.A13 Trennung der Testumgebung von der Produktivumgebung** CON.8 Software-Entwicklung OPS.1.1.6 Software-Tests und -Freigabe CON.8.A3 Auswahl einer Entwicklungsumgebung CON.8.A7 Durchführung von entwicklungsbegleitenden Software-Tests

			CON.8.A11 Erstellung einer Richtlinie für die Software-Entwicklung OPS.1.1.6.A1 Planung der Software-Tests OPS.1.1.6.A4 Freigabe der Software SYS.1.1.A30 Ein Dienst pro Server SYS.1.5.A10 Einführung von Verwaltungsprozessen für virtuelle IT-Systeme SYS.1.7.A33 Trennung von Test- und Produktionssystemen unter z/OS NET.1.1.A22 Spezifikation des Segmentierungskonzepts
	A.8.32	Change management – Änderungssteuerung	**OPS.1.1.3 Patch- und Änderungsmanagement**
	A.8.33	Test information – Prüfinformationen	**CON.8.A7 Durchführung von entwicklungsbegleitenden Software-Tests** **OPS.1.1.6.A11 Verwendung von anonymisierten oder pseudonymisierten Testdaten**
	A.8.34	Protection of information systems during audit testing – Schutz der Informationssysteme während der Überwachungsprüfung	**ISMS.1.A11 Aufrechterhaltung der Informationssicherheit** **DER.3.1 Audits und Revisionen** **DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision**