Zuordnungstabelle
Zuordnung ISO/IEC 27001 sowie ISO/IEC 27002 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 27001:2013 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 100-4, Version 1.0 vom Dezember 2008
- IT-Grundschutz-Kompendium, 4. Edition 2021
- ISO/IEC 27001:2013 und ISO/IEC 27002:2013

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 27001:2013 und IT-Grundschutz

		ISO/IEC 27001:2013	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	BSI-Glossar der Cyber-Sicherheit, https://www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/cyber-glossar_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, Kapitel 3 ISMS-Definition und Prozessbeschreibung** **BSI-Standard 200-2, Kapitel 2 Informationssicherheitsmanagement mit IT-Grundschutz** ISMS.1 Sicherheitsmanagement
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

		ISO/IEC 27001:2013	IT-Grundschutz
			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.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 und 9** BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz IT-Grundschutz-Kompendium
	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**

		ISO/IEC 27001:2013	IT-Grundschutz
			ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitung ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit ISMS.1.A15 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit
	7.2	Competence – Kompetenz	**BSI-Standard 200-2, Kapitel 4.3 Aufgaben, Verantwortungen und Kompetenzen in der IS-Organisation** **ORP.2.A15 Qualifikation des Personals** ORP.2.A7 Überprüfung der Vertrauenswürdigkeit von Mitarbeitern
	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
8		**Operation – Betrieb**	
	8.1	Operational planning and control – Betriebliche Planung und Steuerung	**BSI-Standard 200-2, Kapitel 9 Umsetzung der Sicherheitskonzeption** ISMS.1.A13 Dokumentation des Sicherheitsprozesses SYS.1.1.A21 Betriebsdokumentation für Server

		ISO/IEC 27001:2013	IT-Grundschutz
	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 und 9** 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 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
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

		ISO/IEC 27001:2013	IT-Grundschutz
	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 27001:2013 Anhang A / ISO/IEC 27002:2013 und IT-Grundschutz			
		ISO/IEC 27002:2013	**IT-Grundschutz**
5		**Information security policies – Informationssicherheits-richtlinien**	
	5.1	Management direction for information security – Vorgaben der Leitung für Informationssicherheit	
	5.1.1	Policies for information security – Informationssicherheits-richtlinien	**ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit** BSI-Standard 200-2, Kapitel 3 Initiierung des Sicherheitsprozesses ISMS.1 Sicherheitsmanagement ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie ISMS.1.A16 Erstellung von zielgruppengerechten Sicherheitsrichtlinien
	5.1.2	Review of the policies for information security – Überprüfung der Informationssicherheits-richtlinien	**BSI-Standard 200-2, Kapitel 3.4.5 Aktualisierung der Sicherheitsleitlinie** ISMS.1 Sicherheitsmanagement ISMS.1.A11 Aufrechterhaltung der Informationssicherheit
6		**Organization of information security – Organisation der Informationssicherheit**	
	6.1	Internal organization –Interne Organisation	
	6.1.1	Information security roles and responsibilities – Informationssicherheits-	**BSI-Standard 200-2, Kapitel 4.2 Aufbau der Informationssicherheitsorganisation** **ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit**

		rollen und -verantwortlichkeiten	ORP.1.A1 Festlegung von Verantwortlichkeiten und Regelungen ORP.1.A2 Zuweisung der Zuständigkeiten ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT OPS.1.1.2.A7 Regelung der IT-Administrationstätigkeit OPS.1.1.3.A2 Festlegung der Zuständigkeiten DER.3.1.A1 Definition von Verantwortlichkeiten DER.3.2.A1 Benennung von Verantwortlichen für die IS-Revision IND.1.A1 Einbindung in die Sicherheitsorganisation
	6.1.2	Segregation of duties – Aufgabentrennung	**ORP.4.A4 Aufgabenverteilung und Funktionstrennung** ORP.1.A4 Funktionstrennung zwischen unvereinbaren Aufgaben
	6.1.3	Contact with authorities – Kontakt mit Behörden	**DER.4 Notfallmanagement** **DER 2.1 Behandlung von Sicherheitsvorfällen** **DER.2.1.A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen** DER.2.1.A3 Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle DER.2.1.A14 Eskalationsstrategie für Sicherheitsvorfälle
	6.1.4	Contact with special interest groups – Kontakt mit speziellen Interessensgruppen	**DER.1.A12 Auswertung von Informationen aus externen Quellen** ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit ISMS.1.A11 Aufrechterhaltung der Informationssicherheit IND.1.A12 Etablieren eines Schwachstellen-Managements
	6.1.5	Information security in project management – Informationssicherheit im Projektmanagement	**ISMS.1 Sicherheitsmanagement** **ISMS.1.A9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse**
	6.2	Mobile devices and teleworking – Mobilgeräte und Telearbeit	
	6.2.1	Mobile device policy – Richtlinie zu Mobilgeräten	**INF.9 Mobiler Arbeitsplatz** **INF.9.A2 Regelungen für mobile Arbeitsplätze** **INF.9.A8 Sicherheitsrichtlinie für mobile Arbeitsplätze**

			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 SYS.3.1.A1 Regelungen zur mobilen Nutzung von Laptops SYS.3.1.A14 Geeignete Aufbewahrung von Laptops SYS.3.2.1.A10 Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten SYS.3.2.2.A1 Festlegung einer Strategie für das Mobile Device Management SYS.3.2.2.A2 Festlegen erlaubter mobiler Endgeräte IND.1.A9 Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten in ICS-Umgebungen
	6.2.2	Teleworking – Telearbeit	**OPS.1.2.4 Telearbeit** **OPS.1.2.4.A1 Regelungen für Telearbeit**
7		**Human resource security – Personalsicherheit**	
	7.1	Prior to employment – Vor der Beschäftigung	
	7.1.1	Screening – Sicherheitsüberprüfung	**ORP.2.A7 Überprüfung der Vertrauenswürdigkeit von Mitarbeitern** **ORP.2.A13 Sicherheitsüberprüfung** ORP.2 Personal OPS.1.1.2.A14 Sicherheitsüberprüfung von Administratoren OPS.1.1.6.A16 Sicherheitsüberprüfung der Tester OPS.2.2.A19 Sicherheitsüberprüfung von Mitarbeitern OPS.3.1.A16 Sicherheitsüberprüfung von Mitarbeitern
	7.1.2	Terms and conditions of employment –	**ORP.2.A4 Festlegung von Regelungen für den Einsatz von Fremdpersonal**

		Beschäftigungs- und Vertragsbedingungen	**ORP.2.A14 Aufgaben und Zuständigkeiten von Mitarbeitern** ORP.2 Personal ORP.2.A1 Geregelte Einarbeitung neuer Mitarbeiter
	7.2	During employment – Während der Beschäftigung	
	7.2.1	Management responsibilities – Verantwortlichkeiten der Leitung	**ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitung** ORP.3 Sensibilisierung und Schulung zur Informationssicherheit ORP.2.A4 Festlegung von Regelungen für den Einsatz von Fremdpersonal ORP.3.A1 Sensibilisierung der Institutionsleitung für Informationssicherheit ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT ORP.3.A4 Konzeption eines Sensibilisierungs-und Schulungsprogramms zur Informationssicherheit
	7.2.2	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 Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit ORP.3.A6 Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit ORP.3.A8 Messung und Auswertung des Lernerfolgs
	7.2.3	Disciplinary process – Maßregelungsprozess	**DER.2.1 Behandlung von Sicherheitsvorfällen** **ISMS.1.A8 Integration der Mitarbeiter in den Sicherheitsprozess** ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT IND.1.A7 Etablieren einer übergreifenden Berechtigungsverwaltung zwischen der OT und in der Office-IT

	7.3	Termination and change of employment – Beendigung und Änderung der Beschäftigung	
	7.3.1	Termination or change of employment responsibilities – Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	**ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitern** **ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen** ORP.2 Personal ORP.2.A4 Festlegung von Regelungen für den Einsatz von Fremdpersonal ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen
8		**Asset management – Verwaltung der Werte**	
	8.1	Responsibility for assets – Verantwortlichkeit für Werte	
	8.1.1	Inventory of assets – Inventarisierung der Werte	**BSI-Standard 200-2, Kapitel 8.1 Strukturanalyse** **ORP.1.A8 Betriebsmittel- und Geräteverwaltung** ISMS.1 Sicherheitsmanagement ORP.1 Organisation 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
	8.1.2	Ownership of assets – Zuständigkeit für Werte	**ORP.1.A2 Zuweisung der Zuständigkeiten**
	8.1.3	Acceptable use of assets – Zulässiger Gebrauch von Werten	**BSI-Standard 200-2, Kapitel 5.1 Klassifikation von Informationen** **ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT** ORP.2.A4 Festlegung von Regelungen für den Einsatz von Fremdpersonal CON.9.A4 Vereinbarungen zum Informationsaustausch mit Externen SYS.3.1.A14 Geeignete Aufbewahrung von Laptops

			SYS.4.5.A5 Regelung zur Mitnahme von Wechseldatenträgern INF.7.A7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger INF.9.A2 Regelungen für mobile Arbeitsplätze INF.9.A8 Sicherheitsrichtlinie für mobile Arbeitsplätze
	8.1.4	Return of assets –Rückgabe von Werten	**ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitern** **ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen** ORP.2.A4 Festlegung von Regelungen für den Einsatz von Fremdpersonal OPS.2.1.A15 Geordnete Beendigung eines Outsourcing-Verhältnisses OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses
	8.2	Information classification – Informationsklassifizierung	
	8.2.1	Classification of information – Klassifizierung von Information	**BSI-Standard 200-2, Kapitel 5.1 Klassifikation von Informationen** **BSI-Standard 200-2, Kapitel 8.2 Schutzbedarfsfeststellung** ISMS.1 Sicherheitsmanagement ISMS.1.A10 Erstellung eines Sicherheitskonzepts OPS.3.1.A3 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben
	8.2.2	Labelling of information – Kennzeichnung von Information	**BSI-Standard 200-2, Kapitel 5.1 Klassifikation von Informationen** ISMS.1 Sicherheitsmanagement
	8.2.3	Handling of assets – Handhabung von Werten	**BSI-Standard 200-2, Kapitel 5.1 Klassifikation von Informationen** **BSI-Standard 200-2, Kapitel 8.2 Schutzbedarfsfeststellung** **ISMS.1.A9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse** SYS.4.5.A13 Angemessene Kennzeichnung der Datenträger beim Versand
	8.3	Media handling – Handhabung von Datenträgern	
	8.3.1	Management of removable media – Handhabung von Wechseldatenträgern	**SYS.4.5 Wechseldatenträger** **SYS.4.5.A4 Erstellung einer Richtlinie zum sicheren Umgang mit Wechseldatenträgern** SYS.2.1.A24 Umgang mit externen Medien und Wechseldatenträgern

			SYS.4.5.A1 Sensibilisierung der Mitarbeiter zum sicheren Umgang mit Wechseldatenträgern SYS.4.5.A5 Regelung zur Mitnahme von Wechseldatenträgern SYS.4.5.A6 Datenträgerverwaltung SYS.4.5.A10 Datenträgerverschlüsselung
	8.3.2	Disposal of media – Entsorgung von Datenträgern	**CON.6 Löschen und Vernichten**
	8.3.3	Physical media transfer – Transport von Datenträgern	**SYS.4.5.A14 Sichere Versandart und Verpackung** SYS.4.5 Wechseldatenträger SYS.4.5.A5 Regelung zur Mitnahme von Wechseldatenträgern SYS.4.5.A6 Datenträgerverwaltung INF.8.A2 Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz
9		**Access control – Zugangssteuerung**	
	9.1	Business requirements of access control – Geschäftsanforderungen an die Zugangssteuerung	
	9.1.1	Access control policy – Zugangssteuerungsrichtlinie	**CON.4 Identitäts- und Berechtigungsmanagement** APP.2.1 Allgemeiner Verzeichnisdienst APP.2.2 Active Directory APP.2.3 OpenLDAP ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen ORP.4.A4 Aufgabenverteilung und Funktionstrennung ORP.4.A5 Vergabe von Zutrittsberechtigungen ORP.4.A6 Vergabe von Zugangsberechtigungen ORP.4.A7 Vergabe von Zugriffsrechten ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle

	9.1.2	Access to networks and network services – Zugang zu Netzwerken und Netzwerkdiensten	**CON.4 Identitäts- und Berechtigungsmanagement** APP.2.1 Allgemeiner Verzeichnisdienst APP.2.2 Active Directory 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.1.1.A4 Netztrennung in Zonen NET.1.1.A18 P-A-P-Struktur für die Internet-Anbindung NET.1.1.A22 Spezifikation des Segmentierungskonzepts NET.1.2.A11 Festlegung einer Sicherheitsrichtlinie für das Netzmanagement NET.1.2.A13 Erstellung eines Netzmanagement-Konzepts NET.3.1.A24 Einsatz von Netzzugangskontrollen NET.3.2.A1 Erstellung einer Sicherheitsrichtlinie NET.3.2.A2 Festlegen der Firewall-Regeln INF.10.A6 Einrichtung sicherer Netzzugänge
	9.2	User access management – Benutzerzugangsverwaltung	
	9.2.1	User registration and de-registration – Registrierung und Deregistrierung von Benutzern	**ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen** CON.4 Identitäts- und Berechtigungsmanagement ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitern ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen ORP.4.A3 Dokumentation der Benutzerkennungen und Rechteprofile ORP.4.A15 Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement OPS.1.1.2.A4 Beendigung der Tätigkeit als IT-Administrator
	9.2.2	User access provisioning – Zuteilung von	**ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle** ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen

		Benutzerzugängen	ORP.4.A6 Vergabe von Zugangsberechtigungen ORP.4.A7 Vergabe von Zugriffsrechten
	9.2.3	Management of privileged access rights – Verwaltung privilegierter Zugangsrechte	**ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle** OPS.1.1.2 Ordnungsgemäße IT-Administration OPS.1.1.2.A4 Beendigung der Tätigkeit als IT-Administrator OPS.1.1.2.A5 Nachweisbarkeit von administrativen Tätigkeiten OPS.1.1.2.A6 Schutz administrativer Tätigkeiten OPS.1.1.2.A15 Aufteilung von Administrationstätigkeiten OPS.1.1.2.A16 Zugangsbeschränkungen für administrative Zugänge OPS.1.1.2.A17 IT-Administration im Vier-Augen-Prinzip OPS.1.1.2.A18 Durchgängige Protokollierung administrativer Tätigkeiten APP.2.1.A12 Überwachung von Verzeichnisdiensten SYS.2.2.3.A20 Einsatz der Benutzerkontensteuerung UAC für privilegierte Konten
	9.2.4	Management of secret authentication information of users – Verwaltung geheimer Authentisierungsinformation von Benutzern	**ORP.4.A8 Regelung des Passwortgebrauchs** ORP.4.A11 Zurücksetzen von Passwörtern ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme
	9.2.5	Review of user access rights – Überprüfung von Benutzerzugangsrechten	**ORP.4.A3 Dokumentation der Benutzerkennungen und Rechteprofile** ORP.4.A6 Vergabe von Zugangsberechtigungen ORP.4.A7 Vergabe von Zugriffsrechten
	9.2.6	Removal or adjustment of access rights – Entzug oder Anpassung von Zugangsrechten	**ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen** ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitern ORP.2.A4 Festlegung von Regelungen für den Einsatz von Fremdpersonal ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle
	9.3	User responsibilities – Benutzerverantwortlich-keiten	

	9.3.1	Use of secret authentication information – Gebrauch geheimer Authentisierungsinformation	**ORP.4.A8 Regelung des Passwortgebrauchs** **ORP.4.A19 Einweisung aller Mitarbeiter in den Umgang mit Authentisierungsverfahren und -mechanismen**
	9.4	System and application access control – Zugangssteuerung für Systeme und Anwendungen	
	9.4.1	Information access restriction – Informationszugangs-beschränkung	**ORP.4.A7 Vergabe von Zugriffsrechten** ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle NET.1.1.A4 Netztrennung in Zonen NET.1.1.A22 Spezifikation des Segmentierungskonzepts NET.1.1.A23 Trennung von Netzsegmenten NET.1.1.A24 Sichere logische Trennung mittels VLAN
	9.4.2	Secure log-on procedures – Sichere Anmeldeverfahren	**ORP.4.A8 Regelung des Passwortgebrauchs** **ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme** ORP.4.A10 Schutz von Benutzerkennungen mit weitreichenden Berechtigungen 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 Benutzertrennung am IT-System bzw. an der Anwendung ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle CON.7.A5 Verwendung der Bildschirm-/Code-Sperre OPS.1.1.2.A16 Zugangsbeschränkungen für administrative Zugänge SYS.2.1.A1 Sichere Benutzerauthentisierung SYS.2.1.A37 Verwendung von Mehr-Faktor-Authentisierung SYS.3.2.1.A4 Verwendung eines Zugriffsschutzes
	9.4.3	Password management system – System zur Verwaltung von Kennwörtern	**ORP.4.A8 Regelung des Passwortgebrauchs** **ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme**

			ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen
	9.4.4	Use of privileged utility programs – Gebrauch von Hilfsprogrammen mit privilegierten Rechten	**CON.4 Identitäts- und Berechtigungsmanagement** ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen SYS.2.3.A7 Restriktive Rechtevergabe auf Dateien und Verzeichnisse SYS.4.4.A15 Restriktive Rechtevergabe
	9.4.5	Access control to program source code – Zugangssteuerung für Quellcode von Programmen	**ORP.4 Identitäts- und Berechtigungsmanagement** **CON.8 Software-Entwicklung** **CON.8.A10 Versionsverwaltung des Quellcodes** OPS.1.1.6.A7 Personalauswahl der Software-Tester OPS.1.1.6.A13 Trennung der Testumgebung von der Produktivumgebung SYS.2.3.A5 Sichere Installation von Software-Paketen SYS.4.4.A15 Restriktive Rechtevergabe
10		**Cryptography – Kryptographie**	
	10.1	Cryptographic controls – Kryptographische Maßnahmen	
	10.1.1	Policy on the use of cryptographic controls – Richtlinie zum Gebrauch von kryptographischen Maßnahmen	**CON.1 Kryptokonzept** CON.1.A7 Erstellung einer Sicherheitsrichtlinie für den Einsatz kryptografischer Verfahren und Produkte CON.1.A10 Entwicklung eines Kryptokonzepts
	10.1.2	Key management – Schlüsselverwaltung	**CON.1 Kryptokonzept** CON.1.A1 Auswahl geeigneter kryptografischer Verfahren CON.1.A2 Datensicherung bei Einsatz kryptografischer Verfahren CON.1.A4 Geeignetes Schlüsselmanagement CON.1.A5 Sicheres Löschen und Vernichten von kryptografischen Schlüsseln CON.1.A9 Auswahl eines geeigneten kryptografischen Produkts

11		**Physical and environmental security – Physische und umgebungsbezogene Sicherheit**	
	11.1	Secure areas – Sicherheitsbereiche	
	11.1.1	Physical security perimeter – Physischer Sicherheitsperimeter	**INF.1.A23 Bildung von Sicherheitszonen** INF.1 Allgemeines Gebäude INF.2 Rechenzentrum sowie Serverraum INF.1.A26 Pförtner- oder Sicherheitsdienst INF.1.A27 Einbruchsschutz INF.1.A35 Perimeterschutz INF.2.A1 Festlegung von Anforderungen INF.2.A12 Perimeterschutz für das Rechenzentrum INF.2.A24 Einsatz von Videoüberwachungsanlagen
	11.1.2	Physical entry controls – Physische Zutrittssteuerung	**INF.1.A7 Zutrittsregelung und -kontrolle** **INF.2.A6 Zutrittskontrolle** INF.1 Allgemeines Gebäude INF.2 Rechenzentrum sowie Serverraum INF.5 Raum sowie Schrank für technische Infrastruktur ORP.1.A3 Beaufsichtigung oder Begleitung von Fremdpersonen ORP.4.A5 Vergabe von Zutrittsberechtigungen INF.1.A12 Schlüsselverwaltung INF.5.A3 Zutrittsregelung und -kontrolle
	11.1.3	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.1.A16 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
	11.1.4	Protecting against external and environmental threats –	**Bausteine der Schicht Infrastruktur** INF.1.A3 Einhaltung von Brandschutzvorschriften

		Schutz vor externen und umweltbedingten Bedrohungen	INF.1.A4 Branderkennung in Gebäuden INF.1.A9 Sicherheitskonzept für die Gebäudenutzung INF.1.A10 Einhaltung einschlägiger Normen und Vorschriften INF.1.A25 Geeignete Standortauswahl INF.1.A34 Gefahrenmeldeanlage INF.1.A35 Perimeterschutz INF.2.A9 Einsatz einer Lösch- oder Brandvermeidungsanlage INF.2.A12 Perimeterschutz für das Rechenzentrum INF.2.A13 Planung und Installation von Gefahrenmeldeanlagen INF.2.A21 Ausweichrechenzentrum INF.2.A24 Einsatz von Videoüberwachungsanlagen INF.2.A28 Einsatz von höherwertigen Gefahrenmeldeanlagen INF.2.A30 Anlagen zur, Löschung oder Vermeidung von Bränden
	11.1.5	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
	11.1.6	Delivery and loading areas – Anlieferungs- und Ladebereiche	**INF.1.A7 Zutrittsregelung und -kontrolle** **INF.2.A6 Zutrittskontrolle** ORP.1.A3 Beaufsichtigung oder Begleitung von Fremdpersonen ORP.4.A5 Vergabe von Zutrittsberechtigungen INF.1.A9 Sicherheitskonzept für die Gebäudenutzung INF.1.A23 Bildung von Sicherheitszonen INF.1.A26 Pförtner- oder Sicherheitsdienst INF.1.A34 Gefahrenmeldeanlage INF.1.A35 Perimeterschutz INF.2.A1 Festlegung von Anforderungen INF.2.A12 Perimeterschutz für das Rechenzentrum INF.2.A24 Einsatz von Videoüberwachungsanlagen

	11.2	Equipment – Geräte und Betriebsmittel	
	11.2.1	Equipment siting and protection – Platzierung und Schutz von Geräten und Betriebsmitteln	**Bausteine der Schicht Infrastruktur** SYS.1.1.A1 Geeignete Aufstellung INF.7.A7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
	11.2.2	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
	11.2.3	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
	11.2.4	Equipment maintenance – Instandhaltung von Geräten und Betriebsmitteln	**OPS.1.1.2.A12 Regelungen für Wartungs- und Reparaturarbeiten** INF.2.A10 Inspektion und Wartung der Infrastruktur INF.5.A17 Inspektion und Wartung der Infrastruktur INF.11.A2 Wartung, Inspektion und Updates
	11.2.5	Removal of assets – Entfernen von Werten	**INF.9.A2 Regelungen für mobile Arbeitsplätze** CON.7.A13 Mitnahme notwendiger Daten und Datenträger SYS.4.5.A5 Regelung zur Mitnahme von Wechseldatenträgern
	11.2.6	Security of equipment and assets off-premises – Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten	**INF.9 Mobiler Arbeitsplatz** **INF.8 Häuslicher Arbeitsplatz** **OPS.1.2.4 Telearbeit** **CON.7 Informationssicherheit auf Auslandsreisen** SYS.3.1 Laptops CON.7.A10 Verschlüsselung tragbarer IT-Systeme und Datenträger SYS.3.1.A14 Geeignete Aufbewahrung von Laptops SYS.3.2.1.A1 Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets INF.8.A2 Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz INF.9.A1 Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes INF.9.A2 Regelungen für mobile Arbeitsplätze INF.9.A8 Sicherheitsrichtlinie für mobile Arbeitsplätze INF.9.A9 Verschlüsselung tragbarer IT-Systeme und Datenträger
	11.2.7	Secure disposal or re-use of equipment – Sichere	**CON.6 Löschen und Vernichten von Daten** CON.6.A1 Regelung für die Löschung und Vernichtung von Informationen

		Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	CON.6.A2 Ordnungsgemäßes Löschen und Vernichten von schützenswerten Betriebsmitteln und Informationen CON.6.A13 Vernichtung defekter digitaler Datenträger CON.6.A14 Vernichten von Datenträgern auf erhöhter Sicherheitsstufe 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
	11.2.8	Unattended user equipment – Unbeaufsichtigte Benutzergeräte	**SYS.2.1.A1 Sichere Benutzerauthentisierung** ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT ORP.4.A9 Identifikation und Authentisierung CON.7.A5 Verwendung der Bildschirm-/Code-Sperre CON.7.A11 Einsatz von Diebstahl-Sicherungen SYS.3.1.A18 Einsatz von Diebstahl-Sicherungen INF.7.A7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger INF.9.A3 Zutritts- und Zugriffsschutz
	11.2.9	Clear desk and clear screen policy – Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren	**INF.7.A6 Aufgeräumter Arbeitsplatz** SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte ORP.4.A9 Identifikation und Authentisierung SYS.2.1.A1 Sichere Benutzerauthentisierung
12		**Operations security – Betriebssicherheit**	
	12.1	Operational procedures and responsibilities – Betriebsabläufe und –verantwortlichkeiten	
	12.1.1	Documented operating procedures – Dokumentierte	**OPS.1.1.2.A11 Dokumentation von IT-Administrationstätigkeiten** **OPS.1.1.3.A11 Kontinuierliche Dokumentation der Informationsverarbeitung**

		Betriebsabläufe	OPS.1.1.2 Ordnungsgemäße IT-Administration OPS.1.2.5 Fernwartung ISMS.1.A13 Dokumentation des Sicherheitsprozesses ORP.1.A1 Festlegung von Verantwortlichkeiten und Regelungen 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
	12.1.2	Change management – Änderungssteuerung	**OPS.1.1.3 Patch- und Änderungsmanagement**
	12.1.3	Capacity management – Kapazitätssteuerung	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
	12.1.4	Separation of development, testing and operational environments – Trennung von Entwicklungs-, Test- und Betriebsumgebungen	**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
	12.2	Protection from malware – Schutz vor Schadsoftware	
	12.2.1	Controls against malware – Maßnahmen gegen Schadsoftware	**OPS.1.1.4 Schutz vor Schadprogrammen** DER.2.1 Behandlung von Sicherheitsvorfällen CON.7.A9 Sicherer Umgang mit mobilen Datenträgern DER.1.A12 Auswertung von Informationen aus externen Quellen APP.1.1.A3 Sicheres Öffnen von Dokumenten aus externen Quellen SYS.1.1.A31 Application Whitelisting IND.1.A3 Schutz vor Schadprogrammen IND.2.1.A8 Schutz vor Schadsoftware
	12.3	Backup – Datensicherung	
	12.3.1	Information backup – Sicherung von Information	**CON.3 Datensicherungskonzept** CON.3.A5 Regelmäßige Datensicherung CON.3.A6 Entwicklung eines Datensicherungskonzepts CON.3.A10 Verpflichtung der Mitarbeiter zur Datensicherung CON.3.A12 Geeignete Aufbewahrung der Datenträger von Datensicherungen
	12.4	Logging and monitoring – Protokollierung und Überwachung	
	12.4.1	Event logging – Ereignisprotokollierung	**OPS.1.1.5 Protokollierung** OPS.1.1.5.A1 Erstellung einer Sicherheitsrichtlinie für die Protokollierung OPS.1.1.5.A3 Konfiguration der Protokollierung auf System- und Netzebene OPS.1.1.5.A6 Aufbau einer zentralen Protokollierungsinfrastruktur OPS.1.1.5.A9 Bereitstellung von Protokollierungsdaten für die Auswertung

	12.4.2	Protection of log information – Schutz der Protokollinformation	**ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle** **OPS.1.1.5.A10 Zugriffsschutz für Protokollierungsdaten** **OPS.1.1.5.A12 Verschlüsselung der Protokollierungsdaten** OPS.1.1.5 Protokollierung OPS.1.1.5.A5 Einhaltung rechtlicher Rahmenbedingungen
	12.4.3	Administrator and operator logs – Administratoren- und Bedienerprotokolle	**OPS.1.1.5.A10 Zugriffsschutz für Protokollierungsdaten** **OPS.1.1.2.A18 Durchgängige Protokollierung administrativer Tätigkeiten** OPS.1.1.5 Protokollierung OPS.1.1.5.A5 Einhaltung rechtlicher Rahmenbedingungen
	12.4.4	Clock synchronisation – Uhrensynchronisation	**OPS.1.1.5.A4 Zeitsynchronisation der IT-Systeme**
	12.5	Control of operational software – Steuerung von Software im Betrieb	
	12.5.1	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 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
	12.6	Technical vulnerability management – Handhabung technischer Schwachstellen	
	12.6.1	Management of technical vulnerabilities – Handhabung von technischen Schwachstellen	**OPS.1.1.3.A16 Regelmäßige Suche nach Informationen zu Patches und Schwachstellen** **DER.1.A12 Auswertung von Informationen aus externen Quellen** OPS.1.1.3 Patch- und Änderungsmanagement IND.1.A12 Etablieren eines Schwachstellen-Managements

	12.6.2	Restrictions on software installation – Einschränkungen von Softwareinstallation	**OPS.1.1.3.A9 Test- und Abnahmeverfahren für neue Hardware** OPS.1.1.3 Patch- und Änderungsmanagement OPS.1.1.6 Software-Tests und -Freigaben APP.7 Entwicklung von Individualsoftware OPS.1.1.6.A4 Freigabe der Software SYS.2.3.A5 Sichere Installation von Software-Paketen
	12.7	Information systems audit considerations – Audit von Informationssystemen	
	12.7.1	Information systems audit controls – Maßnahmen für Audits von Informationssystemen	**DER.3.1 Audits und Revisionen** **DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision** ISMS.1.A11 Aufrechterhaltung der Informationssicherheit OPS.2.1.A4 Vertragsgestaltung mit dem Outsourcing-Dienstleister OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung
13		**Communications security – Kommunikationssicherheit**	
	13.1	Network security management – Netzwerksicherheits-management	
	13.1.1	Network controls – Netzwerksteuerungs-maßnahmen	**NET.1.1 Netzarchitektur und -design** **NET.1.2 Netzmanagement** CON.1 Kryptokonzept NET.1.1 Router und Switches NET.2.1 WLAN-Betrieb NET.2.2 WLAN-Nutzung NET.3.2 Firewall NET.3.3 VPN ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle

			DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokolldaten 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
	13.1.2	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 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
	13.1.3	Segregation in networks – Trennung in 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
	13.2	Information transfer – Informationsübertragung	
	13.2.1	Information transfer policies and procedures – Richtlinien und Verfahren zur Informationsübertragung	**CON.9.A2 Regelung des Informationsaustausches** CON.1 Kryptokonzept CON.9 Informationsaustausch APP.1.2 Web-Browser 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 CON.9.A4 Vereinbarungen zum Informationsaustausch mit Externen CON.9.A5 Beseitigung von Restinformationen vor Weitergabe APP.5.3.A6 Festlegung einer Sicherheitsrichtlinie für E-Mail SYS.4.1.A5 Erstellung von Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten
	13.2.2	Agreements on information transfer – Vereinbarungen zur Informationsübertragung	**CON.9.A4 Vereinbarungen zum Informationsaustausch mit Externen** CON.9 Informationsaustausch CON.7.A9 Sicherer Umgang mit mobilen Datenträgern CON.9.A2 Regelung des Informationsaustausches APP.5.3.A6 Festlegung einer Sicherheitsrichtlinie für E-Mail

	13.2.3	Electronic messaging – Elektronische Nachrichtenübermittlung	**Allgemeiner E-Mail-Client und -Server** CON.9 Informationsaustausch APP.1.2 Web-Browser APP.1.4 Mobile Anwendungen (Apps) CON.1.A3 Verschlüsselung der Kommunikationsverbindungen
	13.2.4	Confidentiality or nondisclosure agreements – Vertraulichkeits- oder Geheimhaltungs-vereinbarungen	**ORP.2.A5 Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal** **CON.9.A9 Vertraulichkeitsvereinbarungen** ORP.2 Personal ORP.2.A4 Festlegung von Regelungen für den Einsatz von Fremdpersonal OPS.3.1.A5 Regelungen für den Einsatz des Personals des Outsourcing-Dienstleisters
14		**System acquisition, development and maintenance – Anschaffung, Entwicklung und Instandhaltung von Systemen**	
	14.1	Security requirements of information systems – Sicherheitsanforderungen an Informationssysteme	
	14.1.1	Information security requirements analysis and specification – Analyse und Spezifikation von Informationssicherheits-anforderungen	**APP.6 Allgemeine Software** **APP.7 Entwicklung von Individualsoftware** CON.8 Software-Entwicklung OPS.1.1.6 Software-Tests und -Freigaben OPS.1.1.3.A9 Test- und Abnahmeverfahren für neue Hardware OPS.1.1.6.A4 Freigabe der Software APP.6.A2 Erstellung eines Anforderungskatalogs für Software APP.6.A3 Sichere Beschaffung von Software APP.6.A14 Nutzung zertifizierter Software

		SYS.4.4.A8 Beschaffungskriterien für IoT-Geräte
14.1.2	Securing application services on public networks – Sicherung von Anwendungsdiensten in öffentlichen Netzwerken	**APP.3.2 Webserver** **APP.3.1 Webanwendungen** CON.1 Kryptokonzept ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle CON.1.A1 Auswahl geeigneter kryptografischer Verfahren CON.1.A6 Bedarfserhebung für kryptografische Verfahren und Produkte APP.3.1.A1 Authentisierung bei Webanwendungen APP.3.2.A2 Schutz der Webserver-Dateien APP.3.2.A5 Authentisierung APP.3.2.A14 Integritätsprüfungen und Schutz vor Schadsoftware NET.1.1.A4 Netztrennung in Zonen NET.1.1.A16 Spezifikation der Netzarchitektur
14.1.3	Protecting application services transactions – Schutz der Transaktionen bei Anwendungsdiensten	**CON.1 Kryptokonzept** NET.3.3 VPN CON.1.A1 Auswahl geeigneter kryptografischer Verfahren CON.1.A6 Bedarfserhebung für kryptografische Verfahren und Produkte CON.9.A4 Vereinbarungen zum Informationsaustausch mit Externen APP.3.1.A1 Authentisierung bei Webanwendungen
14.2	Security in development and support processes – Sicherheit in Entwicklungs- und Unterstützungsprozessen	
14.2.1	Secure development policy – Richtlinie für sichere Entwicklung	**CON.8 Software-Entwicklung** CON.10 Entwicklung von Webanwendungen APP.7 Entwicklung von Individualsoftware CON.8.A11 Erstellung einer Richtlinie für die Software-Entwicklung APP.1.1.A10 Regelung der Software-Entwicklung durch Endbenutzer APP.3.1.A9 Beschaffung von Webanwendungen

			APP.4.3.A19 Schutz vor schädlichen Datenbank-Skripten APP.7.A5 Geeignete Steuerung der Anwendungsentwicklung IND.1.A11 Sichere Beschaffung und Systementwicklung
	14.2.2	System change control procedures – Verfahren zur Verwaltung von Systemänderungen	**OPS.1.1.3 Patch- und Änderungsmanagement** CON.8 Software-Entwicklung CON.8.A10 Versionsverwaltung des Quellcodes CON.10.A12 Verifikation essenzieller Änderungen OPS.1.1.3.A9 Test- und Abnahmeverfahren für neue Hardware OPS.1.1.3.A11 Kontinuierliche Dokumentation der Informationsverarbeitung OPS.1.1.6.A4 Freigabe der Software APP.6.A9 Inventarisierung von Software IND.1.A4 Dokumentation der OT-Infrastruktur
	14.2.3	Technical review of applications after operating platform changes – Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform	**OPS.1.1.3.A11 Kontinuierliche Dokumentation der Informationsverarbeitung** APP.7 Entwicklung von Individualsoftware OPS.1.1.3 Patch- und Änderungsmanagement OPS.1.1.6 Software-Tests und -Freigaben OPS.1.1.3.A1 Konzept für das Patch- und Änderungsmanagement OPS.1.1.3.A9 Test- und Abnahmeverfahren für neue Hardware OPS.1.1.6.A4 Freigabe der Software
	14.2.4	Restrictions on changes to software packages – Beschränkung von Änderungen an Softwarepaketen	**APP.6 Allgemeine Software** **APP.6.A5 Sichere Installation von Software** OPS.1.1.6 Software-Tests und -Freigaben OPS.1.1.3.A9 Test- und Abnahmeverfahren für neue Hardware OPS.1.1.6.A4 Freigabe der Software APP.6.A4 Regelung für die Installation und Konfiguration von Software APP.6.A10 Erstellung einer Sicherheitsrichtlinie für den Einsatz der Software
	14.2.5	Secure system engineering principles – Grundsätze für die Analyse, Entwicklung und	**CON.8 Software-Entwicklung** **APP.3.1 Webanwendungen** OPS.1.1.6 Software-Tests und -Freigaben

		Pflege sicherer Systeme	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
	14.2.6	Secure development environment – Sichere Entwicklungsumgebung	**CON.8 Software-Entwicklung** CON.8.A3 Auswahl einer Entwicklungsumgebung CON.8.A14 Schulung des Entwicklungsteams zur Informationssicherheit OPS.1.1.6.A13 Trennung der Testumgebung von der Produktivumgebung APP.7.A5 Geeignete Steuerung der Anwendungsentwicklung
	14.2.7	Outsourced development – Ausgegliederte Entwicklung	**OPS.2.1 Outsourcing für Kunden** **OPS.3.1 Outsourcing für Dienstleister** **APP.7 Entwicklung von Individualsoftware** OPS.2.1.A1 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben OPS.2.1.A3 Auswahl eines geeigneten Outsourcing-Dienstleisters OPS.2.1.A4 Vertragsgestaltung mit dem Outsourcing-Dienstleister OPS.2.1.A5 Festlegung einer Strategie zum Outsourcing OPS.2.1.A6 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben OPS.2.1.A11 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb APP.7.A2 Festlegung von Sicherheitsanforderungen an den Prozess der Software-Entwicklung
	14.2.8	System security testing – Testen der Systemsicherheit	**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
	14.2.9	System acceptance testing – Systemabnahmetest	**OPS.1.1.6 Software-Tests und -Freigaben** **OPS.1.1.3.A9 Test- und Abnahmeverfahren für neue Hardware** OPS.1.1.3 Patch- und Änderungsmanagement

			APP.7 Entwicklung von Individualsoftware ORP.1.A8 Betriebsmittel- und Geräteverwaltung OPS.1.1.6.A4 Freigabe der Software APP.7.A8 Frühzeitige Beteiligung des Fachverantwortlichen bei entwicklungsbegleitenden Software-Tests
	14.3	Test data – Testdaten	
	14.3.1	Protection of test data – Schutz von Testdaten	**CON.8.A7 Durchführung von entwicklungsbegleitenden Software-Tests** **OPS.1.1.6.A11 Verwendung von anonymisierten oder pseudonymisierten Testdaten** CON.8.A14 Schulung des Entwicklungsteams zur Informationssicherheit OPS.1.1.6.A1 Planung der Software-Tests OPS.1.1.6.A13 Trennung der Testumgebung von der Produktivumgebung
15		**Supplier relationships – Lieferantenbeziehungen**	
	15.1	Information security in supplier relationships – Informationssicherheit in Lieferantenbeziehungen	
	15.1.1	Information security policy for supplier relationships – Informationssicherheits-richtlinie für Lieferantenbeziehungen	**OPS.2.1 Outsourcing für Kunden** **OPS.2.2 Cloud-Nutzung** **OPS.3.1 Outsourcing für Dienstleister** OPS.1.1.2.A12 Regelungen für Wartungs- und Reparaturarbeiten OPS.2.1.A1 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben OPS.2.1.A5 Festlegung einer Strategie zum Outsourcing OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung OPS.3.1.A1 Erstellung eines Grobkonzeptes für die Outsourcing-Dienstleistung
	15.1.2	Addressing security within supplier agreements – Behandlung von Sicherheit in Lieferantenvereinbarungen	**OPS.2.1 Outsourcing für Kunden** **OPS.2.2 Cloud-Nutzung** **OPS.3.1 Outsourcing für Dienstleister** ISMS.1.A5 Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten

			OPS.1.2.5.A19 Fernwartung durch Dritte OPS.2.1.A4 Vertragsgestaltung mit dem Outsourcing-Dienstleister OPS.2.1.A6 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter OPS.3.1.A2 Vertragsgestaltung mit den Outsourcing-Kunden OPS.3.1.A7 Erstellung eines Mandantentrennungskonzeptes durch den Outsourcing-Dienstleister DER.2.2.A13 Rahmenverträge mit externen Dienstleistern APP.3.2.A10 Auswahl eines geeigneten Webhosters SYS.1.8.A9 Auswahl von Lieferanten für eine Speicherlösung IND.2.4.A2 Betrieb nach Ende der Gewährleistung
	15.1.3	Information and communication technology supply chain – Lieferkette für Informations- und Kommunikationstechnologie	**OPS.2.1 Outsourcing für Kunden** **OPS.2.2 Cloud-Nutzung** **OPS.3.1 Outsourcing für Dienstleister** CON.9.A9 Vertraulichkeitsvereinbarungen OPS.1.1.2.A12 Regelungen für Wartungs- und Reparaturarbeiten OPS.1.2.5.A19 Fernwartung durch Dritte DER.4.A16 Notfallvorsorge- und Notfallreaktionsplanung für ausgelagerte Komponenten
	15.2	Supplier service delivery management – Steuerung der Dienstleistungserbringung von Lieferanten	
	15.2.1	Monitoring and review of supplier services – Überwachung und Überprüfung von Lieferantendienstleistungen	**OPS.2.1.A11 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb** **OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb** **OPS.3.1.A10 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb** OPS.2.1 Outsourcing für Kunden OPS.2.2 Cloud-Nutzung OPS.3.1 Outsourcing für Dienstleister

			DER.3.1 Audits und Revisionen OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung
	15.2.2	Managing changes to supplier services – Handhabung der Änderungen von Lieferantendienstleistungen	**OPS.2.1 Outsourcing für Kunden** **OPS.2.2 Cloud-Nutzung** **OPS.3.1 Outsourcing für Dienstleister** OPS.1.1.3 Patch- und Änderungsmanagement OPS.1.1.3.A5 Umgang mit Änderungsanforderungen OPS.1.1.3.A11 Kontinuierliche Dokumentation der Informationsverarbeitung
16		**Information security incident management – Handhabung von Informationssicherheits-vorfällen**	
	16.1	Management of information security incidents and improvements – Handhabung von Informationssicherheits-vorfällen und Verbesserungen	
	16.1.1	Responsibility and procedures – Verantwortlichkeiten und Verfahren	**DER.2.1 Behandlung von Sicherheitsvorfällen** DER.2.1.A2 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen DER.2.1.A3 Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen DER.2.1.A7 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen
	16.1.2	Reporting information security events – Meldung von Informationssicherheits-ereignissen	**DER.2.1 Behandlung von Sicherheitsvorfällen** **DER.1 Detektion von sicherheitsrelevanten Ereignissen** DER.2.2 Vorsorge für die IT-Forensik DER.1.A1 Erstellung einer Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen DER.1.A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse DER.1.A4 Sensibilisierung der Mitarbeiter DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle

	16.1.3	Reporting information security weaknesses – Meldung von Schwächen in der Informationssicherheit	**DER.2.1 Behandlung von Sicherheitsvorfällen** OPS.1.1.3.A16 Regelmäßige Suche nach Informationen zu Patches und Schwachstellen DER.1.A12 Auswertung von Informationen aus externen Quellen DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle IND.1.A12 Etablieren eines Schwachstellen-Managements
	16.1.4	Assessment of and decision on information security events – Beurteilung von und Entscheidung über Informationssicherheits-ereignisse	**DER.1 Detektion von sicherheitsrelevanten Ereignissen** **DER.2.1 Behandlung von Sicherheitsvorfällen** DER.2.1.A1 Definition eines Sicherheitsvorfalls DER.2.1.A11 Einstufung von Sicherheitsvorfällen DER.2.1.A19 Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen
	16.1.5	Response to information security incidents – Reaktion auf Informationssicherheits-vorfälle	**DER.2.1 Behandlung von Sicherheitsvorfällen** DER.2.2 Vorsorge für die IT-Forensik DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle DER.2.1.A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen DER.2.1.A5 Behebung von Sicherheitsvorfällen DER.2.2.A11 Dokumentation der Beweissicherung
	16.1.6	Learning from information security incidents – Erkenntnisse aus Informationssicherheits-vorfällen	**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 Branchenentwicklungen DER.2.1.A22 Überprüfung der Effizienz des Managementsystems zur Behandlung von Sicherheitsvorfällen
	16.1.7	Collection of evidence – Sammeln von Beweismaterial	**DER.2.1 Behandlung von Sicherheitsvorfällen** **DER.2.2 Vorsorge für die IT-Forensik** DER.2.2.A5 Erstellung eines Leitfadens für Beweissicherungsmaßnahmen bei IT-Sicherheitsvorfällen DER.2.2.A9 Vorauswahl forensisch relevanter Daten DER.2.2.A11 Dokumentation der Beweissicherung DER.2.2.A14 Festlegung von Standardverfahren für die Beweissicherung

			DER.2.2.A15 Durchführung von Übungen zur Beweissicherung NET.1.2.A35 Festlegungen zur Beweissicherung
17		**Information security aspects of business continuity management – Informationssicherheits-aspekte beim Business Continuity Management**	
	17.1	Information security continuity – Aufrechterhalten der Informationssicherheit	
	17.1.1	Planning information security continuity – Planung zur Aufrechterhaltung der Informationssicherheit	**DER.4 Notfallmanagement** BSI-Standard 200-2, Kapitel 3 Initiierung des Sicherheitsprozesses BSI-Standard 100-4, Notfallmanagement DER.2.1 Behandlung von Sicherheitsvorfällen
	17.1.2	Implementing information security continuity – Umsetzung der Aufrechterhaltung der Informationssicherheit	**DER.4 Notfallmanagement** BSI-Standard 100-4, Notfallmanagement DER.2.1 Behandlung von Sicherheitsvorfällen
	17.1.3	Verify, review and evaluate information security continuity – Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit	**DER.4 Notfallmanagement** BSI-Standard 100-4, Notfallmanagement
	17.2	Redundancies – Redundanzen	
	17.2.1	Availability of information processing facilities – Verfügbarkeit von informationsverarbeitenden	**INF.2 Rechenzentrum sowie Serverraum** DER.4 Notfallmanagement OPS.1.1.2.A19 Berücksichtigung von Hochverfügbarkeitsanforderungen

		Einrichtungen	OPS.1.1.5.A13 Hochverfügbare Protokollierungsinfrastruktur APP.3.2.A15 Redundanz APP.3.3.A13 Replikation zwischen Standorten SYS.1.1.A28 Steigerung der Verfügbarkeit durch Redundanz SYS.1.2.2.A12 Redundanz und Hochverfügbarkeit bei Windows Server 2012 SYS.1.5.A20 Verwendung von hochverfügbaren Architekturen 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.1.1.A30 Schutz vor Distributed-Denial-of-Service NET.1.2.A30 Hochverfügbare Realisierung der Management-Lösung NET.3.1.A26 Hochverfügbarkeit INF.2.A21 Ausweichrechenzentrum INF.2.A25 Redundante Auslegung von unterbrechungsfreien Stromversorgungen INF.2.A26 Redundante Auslegung von Netzersatzanlagen
18		**Compliance – Compliance**	
	18.1	Compliance with legal and contractual requirements – Einhaltung gesetzlicher und vertraglicher Anforderungen	
	18.1.1	Identification of applicable legislation and contractual requirements – Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen	**ORP.5 Compliance Management (Anforderungsmanagement)** ORP.5.A1 Identifikation der Rahmenbedingungen ORP.5.A2 Beachtung der Rahmenbedingungen ORP.5.A4 Konzeption und Organisation des Compliance Managements ORP.2.A14 Aufgaben und Zuständigkeiten von Mitarbeitern
	18.1.2	Intellectual property rights – Geistige Eigentumsrechte	**ORP.5 Compliance Management (Anforderungsmanagement)** ORP.2.A14 Aufgaben und Zuständigkeiten von Mitarbeitern APP.3.2.A7 Rechtliche Rahmenbedingungen für Webangebote

	18.1.3	Protection of records – Schutz von Aufzeichnungen	**ORP.5 Compliance Management (Anforderungsmanagement)** ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT ISMS.1.A13 Dokumentation des Sicherheitsprozesses
	18.1.4	Privacy and protection of personally identifiable information – Privatsphäre und Schutz von personenbezogener Information	**ORP.5 Compliance Management (Anforderungsmanagement)** CON.2 Datenschutz ORP.2.A14 Aufgaben und Zuständigkeiten von Mitarbeitern
	18.1.5	Regulation of cryptographic controls – Regelungen bezüglich kryptographischer Maßnahmen	**ORP.5 Compliance Management (Anforderungsmanagement)** CON.1.A8 Erhebung der Einflussfaktoren für kryptografische Verfahren und Produkte CON.1.A9 Auswahl eines geeigneten kryptografischen Produkts
	18.2	Information security reviews – Überprüfungen der Informationssicherheit	
	18.2.1	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 ISMS.1 Sicherheitsmanagement
	18.2.2	Compliance with security policies and standards – Einhaltung von Sicherheitsrichtlinien und -standards	**ORP.5 Compliance Management (Anforderungsmanagement)** BSI-Standard 200-2, Kapitel 10.1 Überprüfung des Informationssicherheitsprozesses auf allen Ebenen ISMS.1.A11 Aufrechterhaltung der Informationssicherheit
	18.2.3	Technical compliance review – Überprüfung der Einhaltung von technischen Vorgaben	**ISMS.1.A11 Aufrechterhaltung der Informationssicherheit**