

Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz

IT-Grundschutz beschreibt mit Hilfe der BSI-Standards 100-1, 100-2 und 100-3 eine Vorgehensweise zum Aufbau und zur Aufrechterhaltung eines Managementsystems für Informationssicherheit (ISMS). Die IT-Grundschutz-Kataloge beschreiben die Umsetzung der damit einhergehenden Maßnahmenziele und Maßnahmen. Das damit aufgebaute ISMS erfüllt die Anforderungen der ISO 27001 und verfügt über ein Äquivalent zu den Handlungsempfehlungen der ISO 27002.

Diese Gegenüberstellung dient der Zuordnung der Inhalte der beiden Revisionen der beiden ISO-Normen von 2013 und 2005 zu den Inhalten von IT-Grundschutz. So wird die Abdeckung der ISO 27001 durch den IT-Grundschutz deutlicher und eine komplementäre Anwendung von IT-Grundschutz zu der Anwendung der ISO Normen wird erleichtert.

Diese Gegenüberstellung basiert auf den folgenden Versionen der betrachteten Werke:

- BSI-Standard 100-1, Version 1.5 vom Mai 2008
- BSI-Standard 100-2, Version 2.0 vom Mai 2008
- BSI-Standard 100-3, Version 2.5 vom Mai 2008
- Ergänzung zum BSI-Standard 100-3, Version 2.5 vom 3. August 2011
- BSI-Standard 100-4, Version 1.0 vom Dezember 2008
- IT-Grundschutz-Kataloge, 15. Ergänzungslieferung
- ISO/IEC 27001:2013 + Cor. 1:2014 und ISO/IEC 27002:2013 + Cor. 1:2014
- ISO/IEC 27001:2005 und ISO/IEC 27002:2005

Für Themen, die in einem der BSI-Standards behandelt werden, wird das Kapitel des entsprechenden BSI-Standards angegeben. Das Kürzel „B“ weist auf den entsprechenden Baustein und „M“ auf eine Maßnahme in den IT-Grundschutz-Katalogen hin. Wenn ein Thema aus den ISO-Standards 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 normativen Anhangs A der ISO 27001 und auf die Empfehlungen der ISO 27002 beziehen, folgen aus Gründen der Übersichtlichkeit der Gliederung und den Bezeichnungen der ISO 27002. Es werden ausschließlich die Teile der ISO 27002 aufgeführt, die einen Bezug zum Anhang A der ISO 27001 haben.

Eine tabellarische Gegenüberstellung der beiden Revisionen 2013 und 2005 der ISO 27001 und der ISO 27002 enthält das frei verfügbare Dokument „JTC 1/SC 27/SD3 – Mapping Old-New Editions of ISO/IEC 27001 and ISO/IEC 27002“ der ISO/IEC-Organisation (ISO/IEC JTC 1/SC 27).

ISO 27001:2013 und IT-Grundschutz

	ISO 27001:2013	IT-Grundschutz
1	Scope	BSI-Standard 100-2, Kapitel 1 Einleitung
2	Normative references	BSI-Standard 100-1, Kapitel 1.5 Literaturverzeichnis
3	Terms and definitions	IT-Grundschutz-Kataloge, Glossar
4	Context of the organization	
	4.1 Understanding the organization and its context	BSI-Standard 100-2, Kapitel 3.2.1 Ermittlung von Rahmenbedingungen M 2.335 Festlegung der Sicherheitsziele und -strategie
	4.2 Understanding the needs and expectations of interested parties	BSI-Standard 100-2, Kapitel 3.2 Konzeption und Planung des Sicherheitsprozesses
	4.3 Determining the scope of the information security management system	BSI-Standard 100-2, Kapitel 3.3.2 und Kapitel 4
	4.4 Information security management system	BSI-Standard 100-1, Kapitel 3 ISMS-Definition und Prozessbeschreibung BSI-Standard 100-2, Kapitel 2 Informationssicherheitsmanagement mit IT-Grundschutz B 1.0 Sicherheitsmanagement
5	Leadership	
	5.1 Leadership and commitment	BSI-Standard 100-2, Kapitel 3.1 Übernahme von Verantwortung durch die Leitungsebene M 2.336 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene
	5.2 Policy	BSI-Standard 100-2, Kapitel 2 und 3 M 2.192 Erstellung einer Leitlinie zur Informationssicherheit
	5.3 Organizational roles, responsibilities and authorities	BSI-Standard 100-2, Kapitel 3.4 Organisation des Sicherheitsprozesses M 2.193 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit
6	Planning	
	6.1 Actions to address risks and	

	ISO 27001:2013	IT-Grundschutz
	opportunities	
6.1.1	General	BSI-Standard 100-2, Kapitel 3, 4 und 5
6.1.2	Information security risk assessment	BSI-Standard 100-2, Kapitel 3 und 4 BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz Ergänzung zum BSI-Standard 100-3 Gefährdungskataloge der IT-Grundschutz-Kataloge
6.1.3	Information security risk treatment	BSI-Standard 100-2, Kapitel 4 und 5 BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz Ergänzung zum BSI-Standard 100-3 Maßnahmenkataloge der IT-Grundschutz-Kataloge
6.2	Information security objectives and planning to achieve them	BSI-Standard 100-2, Kapitel 3 Initiierung des Sicherheitsprozesses
7	Support	
7.1	Resources	BSI-Standard 100-2, Kapitel 3.5 Bereitstellung von Ressourcen für die Informationssicherheit M 2.339 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit
7.2	Competence	BSI-Standard 100-2, Kapitel 3.4.3 Aufgaben, Verantwortungen und Kompetenzen in der IS-Organisation
7.3	Awareness	BSI-Standard 100-2, Kapitel 3.6 Einbindung aller Mitarbeiter in den Sicherheitsprozess B 1.13 Sensibilisierung und Schulung zur Informationssicherheit
7.4	Communication	BSI-Standard 100-2, Kapitel 3.6 Einbindung aller Mitarbeiter in den Sicherheitsprozess
7.5	Documented information	
7.5.1	General	BSI-Standard 100-2, Kapitel 6.2 Informationsfluss im Informationssicherheitsprozess

	ISO 27001:2013	IT-Grundschutz
	7.5.2 Creating and updating	BSI-Standard 100-2, Kapitel 6.2 Informationsfluss im Informationssicherheitsprozess M 2.201 Dokumentation des Sicherheitsprozesses
	7.5.3 Control of documented information	BSI-Standard 100-1, Kapitel 4.3 Kommunikation und Wissen BSI-Standard 100-2, Kapitel 6.2 Informationsfluss im Informationssicherheitsprozess M 2.201 Dokumentation des Sicherheitsprozesses
8	Operation	
	8.1 Operational planning and control	BSI-Standard 100-2, Kapitel 5 Umsetzung der Sicherheitskonzeption
	8.2 Information security risk assessment	BSI-Standard 100-2, Kapitel 3 und 4 BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz Ergänzung zum BSI-Standard 100-3 Gefährdungskataloge der IT-Grundschutz-Kataloge
	8.3 Information security risk treatment	BSI-Standard 100-2, Kapitel 4 und 5 BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz Ergänzung zum BSI-Standard 100-3 Maßnahmenkataloge der IT-Grundschutz-Kataloge
9	Performance evaluation	
	9.1 Monitoring, measurement, analysis and evaluation	BSI-Standard 100-2, Kapitel 6 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit M 2.199 Aufrechterhaltung der Informationssicherheit
	9.2 Internal audit	BSI-Standard 100-2, Kapitel 6.1.1 Methoden zur Überprüfung des Informationssicherheitsprozesses M 2.199 Aufrechterhaltung der Informationssicherheit
	9.3 Management review	BSI-Standard 100-2, Kapitel 6.1 Überprüfung des Informationssicherheitsprozesses in allen

		ISO 27001:2013	IT-Grundschutz
			Ebenen
			M 2.199 Aufrechterhaltung der Informationssicherheit
10		Improvement	
	10.1	Nonconformity and corrective action	BSI-Standard 100-2, Kapitel 6.1 Überprüfung des Informationssicherheitsprozesses in allen Ebenen
			M 2.199 Aufrechterhaltung der Informationssicherheit
	10.2	Continual improvement	BSI-Standard 100-2, Kapitel 6 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit
			M 2.199 Aufrechterhaltung der Informationssicherheit

ISO 27001:2013 Anhang A / ISO 27002:2013 und IT-Grundschutz

	ISO 27002:2013	IT-Grundschutz
5	Information security policies	
	5.1 Management direction for information security	
	5.1.1 Policies for information security	M 2.192 Erstellung einer Leitlinie zur Informationssicherheit BSI-Standard 100-2, Kapitel 3 Initiierung des Sicherheitsprozesses B 1.0 Sicherheitsmanagement M 2.335 Festlegung der Sicherheitsziele und -strategie M 2.338 Erstellung von zielgruppengerechten Sicherheitsrichtlinien
	5.1.2 Review of the policies for information security	BSI-Standard 100-2, Kapitel 3.3.5 Aktualisierung der Sicherheitsleitlinie B 1.0 Sicherheitsmanagement M 2.199 Aufrechterhaltung der Informationssicherheit
6	Organization of information security	
	6.1 Internal organization	
	6.1.1 Information security roles and responsibilities	BSI-Standard 100-2, Kapitel 3.4.2 Aufbau der Informationssicherheitsorganisation M 2.193 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit M 2.1 Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten M 3.26 Einweisung des Personals in den sicheren Umgang mit IT
	6.1.2 Segregation of duties	M 2.5 Aufgabenverteilung und Funktionstrennung
	6.1.3 Contact with authorities	B 1.3 Notfallmanagement B 1.8 Behandlung von Sicherheitsvorfällen

	ISO 27002:2013	IT-Grundschutz
		M 6.59 Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen M 6.61 Eskalationsstrategie für Sicherheitsvorfälle M 6.65 Benachrichtigung betroffener Stellen
6.1.4	Contact with special interest groups	M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems M 2.199 Aufrechterhaltung der Informationssicherheit
6.1.5	Information security in project management	B 1.0 Sicherheitsmanagement M 2.337 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse M 2.550 Geeignete Steuerung der Anwendungsentwicklung
6.2	Mobile devices and teleworking	
6.2.1	Mobile device policy	M 2.309 Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung B 2.10 Mobiler Arbeitsplatz B 3.203 Laptop B 3.404 Mobiltelefon B 3.405 Smartphones, Tablets und PDAs M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten
6.2.2	Teleworking	B 5.8 Telearbeit
7	Human resource security	
7.1	Prior to employment	
7.1.1	Screening	M 3.33 Sicherheitsprüfung von Mitarbeitern B 1.2 Personal M 3.50 Auswahl von Personal
7.1.2	Terms and conditions of employment	M 2.226 Regelungen für den Einsatz von Fremdpersonal M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und

	ISO 27002:2013	IT-Grundschutz
		Regelungen B 1.2 Personal M 3.1 Geregelt Einarbeitung/Einweisung neuer Mitarbeiter
7.2	During employment	
7.2.1	Management responsibilities	M 2.336 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene B 1.13 Sensibilisierung und Schulung zur Informationssicherheit M 2.226 Regelungen für den Einsatz von Fremdpersonal M 3.5 Schulung zu Sicherheitsmaßnahmen M 3.96 Unterstützung des Managements für Sensibilisierung und Schulung
7.2.2	Information security awareness, education and training	B 1.13 Sensibilisierung und Schulung zur Informationssicherheit M 2.312 Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit M 3.5 Schulung zu Sicherheitsmaßnahmen M 3.96 Unterstützung des Managements für Sensibilisierung und Schulung
7.2.3	Disciplinary process	M 2.39 Reaktion auf Verletzungen der Sicherheitsvorgaben B 1.8 Behandlung von Sicherheitsvorfällen M 2.192 Erstellung einer Leitlinie zur Informationssicherheit M 3.26 Einweisung des Personals in den sicheren Umgang mit IT
7.3	Termination and change of employment	
7.3.1	Termination or change of employment responsibilities	M 3.6 Geregelt Verfahrensweise beim Ausscheiden von Mitarbeitern B 1.2 Personal M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen M 2.226 Regelungen für den Einsatz von Fremdpersonal

	ISO 27002:2013	IT-Grundschutz
8	Asset management	
8.1	Responsibility for assets	
8.1.1	Inventory of assets	BSI-Standard 100-2, Kapitel 4.2 Strukturanalyse B 1.0 Sicherheitsmanagement B 1.1 Organisation M 2.139 Ist-Aufnahme der aktuellen Netzsituation M 2.195 Erstellung eines Sicherheitskonzepts M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
8.1.2	Ownership of assets	M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten
8.1.3	Acceptable use of assets	M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz M 1.34 Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten M 2.226 Regelungen für den Einsatz von Fremdpersonal M 2.235 Richtlinien für die Nutzung von Internet-PCs M 2.309 Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung M 5.88 Vereinbarung über Datenaustausch mit Dritten
8.1.4	Return of assets	M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeiter M 2.226 Regelungen für den Einsatz von Fremdpersonal
8.2	Information classification	
8.2.1	Classification of information	BSI-Standard 100-2, Kapitel 4.3 Schutzbedarfsfeststellung B 1.0 Sicherheitsmanagement M 2.195 Erstellung eines Sicherheitskonzepts M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
8.2.2	Labelling of information	BSI-Standard 100-2, Kapitel 4.3 Schutzbedarfsfeststellung

	ISO 27002:2013	IT-Grundschutz
		B 1.0 Sicherheitsmanagement M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
8.2.3	Handling of assets	M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
8.3	Media handling	
8.3.1	Management of removable media	M 2.3 Datenträgerverwaltung B 5.14 Mobile Datenträger M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten
8.3.2	Disposal of media	B 1.15 Löschen und Vernichten von Daten M 2.431 Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen M 4.234 Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern
8.3.3	Physical media transfer	M 5.23 Auswahl einer geeigneten Versandart M 2.3 Datenträgerverwaltung M 2.4 Regelungen für Wartungs- und Reparaturarbeiten M 2.44 Sichere Verpackung der Datenträger M 2.45 Regelung des Datenträgeraustausches M 2.112 Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten
9	Access control	
9.1	Business requirements of access control	
9.1.1	Access control policy	B 1.18 Identitäts- und Berechtigungsmanagement B 5.15 Allgemeiner Verzeichnisdienst

	ISO 27002:2013	IT-Grundschutz
		M 2.5 Aufgabenverteilung und Funktionstrennung M 2.7 Vergabe von Zugangsberechtigungen M 2.8 Vergabe von Zugriffsrechten M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle
9.1.2	Access to networks and network services	B 1.18 Identitäts- und Berechtigungsmanagement B 4.4 VPN B 4.5 LAN-Anbindung eines IT-Systems über ISDN B 5.15 Allgemeiner Verzeichnisdienst M 2.71 Festlegung einer Policy für ein Sicherheitsgateway M 2.169 Entwickeln einer Systemmanagementstrategie M 2.214 Konzeption des IT-Betriebs M 2.457 Konzeption für die sichere Internet-Nutzung
9.2	User access management	
9.2.1	User registration and de-registration	M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen B 1.18 Identitäts- und Berechtigungsmanagement M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen
9.2.2	User access provisioning	M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.63 Einrichten der Zugriffsrechte M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen
9.2.3	Management of privileged access rights	M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.20 Kontrolle bestehender Verbindungen M 2.38 Aufteilung der Administrationstätigkeiten M 4.312 Überwachung von Verzeichnisdiensten
9.2.4	Management of secret	M 2.11 Regelung des Passwortgebrauchs

	ISO 27002:2013	IT-Grundschutz
	authentication information of users	M 2.22 Hinterlegen des Passwortes M 2.402 Zurücksetzen von Passwörtern M 4.7 Änderung voreingestellter Passwörter M 4.133 Geeignete Auswahl von Authentikationsmechanismen M 5.34 Einsatz von Einmalpasswörtern
9.2.5	Review of user access rights	M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile M 2.199 Aufrechterhaltung der Informationssicherheit
9.2.6	Removal or adjustment of access rights	M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.226 Regelungen für den Einsatz von Fremdpersonal
9.3	User responsibilities	
9.3.1	Use of secret authentication information	M 2.11 Regelung des Passwortgebrauchs M 2.22 Hinterlegen des Passwortes M 3.5 Schulung zu Sicherheitsmaßnahmen M 3.26 Einweisung des Personals in den sicheren Umgang mit IT M 4.7 Änderung voreingestellter Passwörter
9.4	System and application access control	
9.4.1	Information access restriction	M 2.8 Vergabe von Zugriffsrechten M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 5.61 Geeignete physikalische Segmentierung

	ISO 27002:2013	IT-Grundschutz
		M 5.62 Geeignete logische Segmentierung M 5.77 Bildung von Teilnetzen
9.4.2	Secure log-on procedures	M 4.15 Gesichertes Login M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.321 Planung des Einsatzes von Client-Server-Netzen M 2.322 Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz M 3.18 Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung M 4.2 Bildschirmsperre M 4.16 Zugangsbeschränkungen für Accounts und / oder Terminals M 4.41 Einsatz angemessener Sicherheitsprodukte für IT-Systeme M 4.133 Geeignete Auswahl von Authentikationsmechanismen
9.4.3	Password management system	M 2.11 Regelung des Passwortgebrauchs M 4.133 Geeignete Auswahl von Authentikationsmechanismen
9.4.4	Use of privileged utility programs	M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien
9.4.5	Access control to program source code	M 4.494 Sicherer Einsatz einer Entwicklungsumgebung M 2.378 System-Entwicklung M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien
10	Cryptography	
10.1	Cryptographic controls	
10.1.1	Policy on the use of cryptographic controls	B 1.7 Kryptokonzept M 2.161 Entwicklung eines Kryptokonzepts
10.1.2	Key management	B 1.7 Kryptokonzept M 2.46 Geeignetes Schlüsselmanagement M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens
11	Physical and	

	ISO 27002:2013	IT-Grundschutz
	environmental security	
11.1	Secure areas	
11.1.1	Physical security perimeter	M 1.79 Bildung von Sicherheitszonen B 2.1 Allgemeines Gebäude M 1.17 Pfortnerdienst M 1.53 Videoüberwachung M 1.19 Einbruchsschutz M 1.13 Anordnung schützenswerter Gebäudeteile M 1.55 Perimeterschutz
11.1.2	Physical entry controls	M 2.17 Zutrittsregelung und -kontrolle B 2.1 Allgemeines Gebäude M 1.80 Zutrittskontrollsystem und Berechtigungsmanagement M 2.6 Vergabe von Zutrittsberechtigungen M 2.16 Beaufsichtigung oder Begleitung von Fremdpersonen
11.1.3	Securing offices, rooms and facilities	Bausteine der Schicht 2 Infrastruktur , z. B. B 2.3 Büroraum / Lokaler Arbeitsplatz M 1.12 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile M 1.13 Anordnung schützenswerter Gebäudeteile M 1.78 Sicherheitskonzept für die Gebäudenutzung
11.1.4	Protecting against external and environmental threats	Bausteine der Schicht 2 Infrastruktur M 1.1 Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften M 1.6 Einhaltung von Brandschutzvorschriften M 1.13 Anordnung schützenswerter Gebäudeteile M 1.16 Geeignete Standortauswahl M 1.18 Gefahrenmeldeanlage M 1.55 Perimeterschutz M 1.75 Branderkennung in Gebäuden

	ISO 27002:2013	IT-Grundschutz
11.1.5	Working in secure areas	Bausteine der Schicht 2 Infrastruktur M 1.49 Technische und organisatorische Vorgaben für das Rechenzentrum M 1.58 Technische und organisatorische Vorgaben für Serverräume M 1.78 Sicherheitskonzept für die Gebäudenutzung M 1.79 Bildung von Sicherheitszonen M 2.18 Kontrollgänge
11.1.6	Delivery and loading areas	M 2.17 Zutrittsregelung und -kontrolle M 1.55 Perimeterschutz M 1.79 Bildung von Sicherheitszonen M 2.6 Vergabe von Zutrittsberechtigungen M 2.16 Beaufsichtigung oder Begleitung von Fremdpersonen M 2.90 Überprüfung der Lieferung
11.2	Equipment	
11.2.1	Equipment siting and protection	B 2.3 Büroraum / Lokaler Arbeitsplatz B 2.1 Allgemeines Gebäude M 1.29 Geeignete Aufstellung eines IT-Systems M 1.45 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
11.2.2	Supporting utilities	B 2.2 Elektrotechnische Verkabelung M 1.28 Lokale unterbrechungsfreie Stromversorgung M 1.56 Sekundär-Energieversorgung
11.2.3	Cabling security	B 2.2 Elektrotechnische Verkabelung B 2.12 IT-Verkabelung M 1.2 Regelungen für Zutritt zu Verteilern M 1.22 Materielle Sicherung von Leitungen und Verteilern M 5.4 Dokumentation und Kennzeichnung der Verkabelung M 5.5 Schadensmindernde Kabelführung

	ISO 27002:2013	IT-Grundschutz
11.2.4	Equipment maintenance	M 2.4 Regelungen für Wartungs- und Reparaturarbeiten
11.2.5	Removal of assets	M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten
11.2.6	Security of equipment and assets off-premises	B 2.10 Mobiler Arbeitsplatz B 3.203 Laptop B 5.8 Telearbeit M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz M 1.61 Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes M 2.112 Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten M 2.309 Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung M 4.29 Einsatz eines Verschlüsselungsproduktes für tragbare PCs
11.2.7	Secure disposal or re-use of equipment	B 1.15 Löschen und Vernichten von Daten M 2.431 Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen M 4.234 Geregeltete Außerbetriebnahme von IT-Systemen und Datenträgern
11.2.8	Unattended user equipment	M 4.2 Bildschirmsperre M 1.45 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger M 1.46 Einsatz von Diebstahl-Sicherungen M 2.37 Der aufgeräumte Arbeitsplatz M 3.26 Einweisung des Personals in den sicheren Umgang mit IT
11.2.9	Clear desk and clear screen policy	M 2.37 Der aufgeräumte Arbeitsplatz B 3.406 Drucker, Kopierer und Multifunktionsgeräte M 4.1 Passwortschutz für IT-Systeme M 4.2 Bildschirmsperre
12	Operations security	

	ISO 27002:2013	IT-Grundschutz
12.1	Operational procedures and responsibilities	
12.1.1	Documented operating procedures	M 2.219 Kontinuierliche Dokumentation der Informationsverarbeitung B 1.9 Hard- und Software-Management B 4.2 Netz- und Systemmanagement M 2.1 Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz M 2.201 Dokumentation des Sicherheitsprozesses
12.1.2	Change management	B 1.14 Patch- und Änderungsmanagement
12.1.3	Capacity management	M 2.214 Konzeption des IT-Betriebs
12.1.4	Separation of development, testing and operational environments	M 2.62 Software-Abnahme- und Freigabe-Verfahren M 2.9 Nutzungsverbot nicht freigegebener Software M 2.82 Entwicklung eines Testplans für Standardsoftware M 2.487 Entwicklung und Erweiterung von Anwendungen M 4.95 Minimales Betriebssystem
12.2	Protection from malware	
12.2.1	Controls against malware	B 1.6 Schutz vor Schadprogrammen B 1.8 Behandlung von Sicherheitsvorfällen M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems M 2.154 Erstellung eines Sicherheitskonzeptes gegen Schadprogramme M 6.23 Verhaltensregeln bei Auftreten von Schadprogrammen
12.3	Backup	
12.3.1	Information backup	B 1.4 Datensicherungskonzept M 6.20 Geeignete Aufbewahrung der Backup-Datenträger

	ISO 27002:2013	IT-Grundschutz
		M 6.32 Regelmäßige Datensicherung M 6.41 Übungen zur Datenrekonstruktion
12.4	Logging and monitoring	
12.4.1	Event logging	B 5.22 Protokollierung M 2.500 Protokollierung von IT-Systemen M 2.64 Kontrolle der Protokolldateien M 2.133 Kontrolle der Protokolldateien eines Datenbanksystems M 4.81 Audit und Protokollierung der Aktivitäten im Netz M 4.430 Analyse von Protokolldaten M 5.9 Protokollierung am Server
12.4.2	Protection of log information	M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle B 5.22 Protokollierung M 2.110 Datenschutzaspekte bei der Protokollierung M 2.500 Protokollierung von IT-Systemen M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen M 4.93 Regelmäßige Integritätsprüfung M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien
12.4.3	Administrator and operator logs	M 2.64 Kontrolle der Protokolldateien B 5.22 Protokollierung M 2.110 Datenschutzaspekte bei der Protokollierung M 2.133 Kontrolle der Protokolldateien eines Datenbanksystems M 2.500 Protokollierung von IT-Systemen M 4.5 Protokollierung der TK-Administrationsarbeiten M 4.25 Einsatz der Protokollierung im Unix-System
12.4.4	Clock synchronisation	M 4.227 Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation
12.5	Control of operational	

	ISO 27002:2013	IT-Grundschutz
	software	
12.5.1	Installation of software on operational systems	B 1.9 Hard- und Software-Management B 1.10 Standardsoftware B 5.25 Allgemeine Anwendungen M 2.62 Software-Abnahme- und Freigabe-Verfahren
12.6	Technical vulnerability management	
12.6.1	Management of technical vulnerabilities	M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
12.6.2	Restrictions on software installation	M 2.62 Software-Abnahme- und Freigabe-Verfahren B 1.14 Patch- und Änderungsmanagement B 5.25 Allgemeine Anwendungen M 2.85 Freigabe von Standardsoftware M 2.216 Genehmigungsverfahren für IT-Komponenten
12.7	Information systems audit considerations	
12.7.1	Information systems audit controls	M 2.64 Kontrolle der Protokolldateien M 2.199 Aufrechterhaltung der Informationssicherheit M 4.81 Audit und Protokollierung der Aktivitäten im Netz
13	Communications security	
13.1	Network security management	
13.1.1	Network controls	B 4.1 Lokale Netze B 4.4 VPN M 2.38 Aufteilung der Administrationstätigkeiten

		ISO 27002:2013	IT-Grundschutz
			M 2.141 Entwicklung eines Netzkonzeptes M 2.143 Entwicklung eines Netzmanagement-Konzeptes M 2.169 Entwickeln einer Systemmanagementstrategie M 2.279 Erstellung einer Sicherheitsrichtlinie für Router und Switches M 2.576 Erstellung einer Sicherheitsrichtlinie für den Einsatz von lokalen Netzen M 2.577 Auswahl geeigneter Kryptoverfahren für Netze M 2.579 Regelmäßige Audits des lokalen Netzes M 4.79 Sichere Zugriffsmechanismen bei lokaler Administration M 4.80 Sichere Zugriffsmechanismen bei Fernadministration M 4.81 Audit und Protokollierung der Aktivitäten im Netz M 4.82 Sichere Konfiguration der aktiven Netzkomponenten M 4.133 Geeignete Auswahl von Authentikationsmechanismen M 5.7 Netzverwaltung M 5.8 Regelmäßiger Sicherheitscheck des Netzes M 5.9 Protokollierung am Server M 5.68 Einsatz von Verschlüsselungsverfahren zur Netzkommunikation M 5.71 Intrusion Detection und Intrusion Response Systeme
13.1.2	Security of network services		B 4.1 Lokale Netze B 3.301 Sicherheitsgateway (Firewall) B 4.2 Netz- und Systemmanagement B 4.4 VPN B 4.5 LAN-Anbindung eines IT-Systems über ISDN M 2.577 Auswahl geeigneter Kryptoverfahren für Netze M 4.133 Geeignete Auswahl von Authentikations-Mechanismen M 5.68 Einsatz von Verschlüsselungsverfahren zur Netzkommunikation
13.1.3	Segregation in networks		M 5.77 Bildung von Teilnetzen M 5.61 Geeignete physikalische Segmentierung M 5.62 Geeignete logische Segmentierung
13.2	Information transfer		

	ISO 27002:2013	IT-Grundschutz
13.2.1	Information transfer policies and procedures	M 2.393 Regelung des Informationsaustausches B 3.402 Faxgerät B 3.403 Anrufbeantworter B 3.404 Mobiltelefon B 3.405 Smartphones, Tablets und PDAs B 5.2 Datenträgeraustausch B 5.3 Groupware B 5.14 Mobile Datenträger B 5.19 Internet-Nutzung M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 2.398 Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten M 5.88 Vereinbarung über Datenaustausch mit Dritten
13.2.2	Agreements on information transfer	M 5.88 Vereinbarung über Datenaustausch mit Dritten M 2.45 Regelung des Datenträgeraustausches M 2.393 Regelung des Informationsaustausches M 2.455 Festlegung einer Sicherheitsrichtlinie für Groupware
13.2.3	Electronic messaging	B 5.3 Groupware B 5.19 Internet-Nutzung M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 5.54 Umgang mit unerwünschten E-Mails M 5.56 Sicherer Betrieb eines Mailservers M 5.108 Kryptographische Absicherung von Groupware bzw. E-Mail
13.2.4	Confidentiality or nondisclosure agreements	M 3.55 Vertraulichkeitsvereinbarungen B 1.2 Personal M 2.226 Regelungen für den Einsatz von Fremdpersonal

	ISO 27002:2013	IT-Grundschutz
		M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
14	System acquisition, development and maintenance	
	14.1 Security requirements of information systems	
	14.1.1 Information security requirements analysis and specification	M 2.80 Erstellung eines Anforderungskataloges für Standardsoftware M 2.546 Analyse der Anforderungen an neue Anwendungen B 1.10 Standardsoftware B 1.9 Hard- und Software-Management B 5.25 Allgemeine Anwendungen B 5.27 Software-Entwicklung M 2.62 Software-Abnahme- und Freigabe-Verfahren M 2.66 Beachtung des Beitrags der Zertifizierung für die Beschaffung
	14.1.2 Securing application services on public networks	B 5.4 Webserver M 2.162 Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens M 2.172 Entwicklung eines Konzeptes für die Web-Nutzung M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 4.93 Regelmäßige Integritätsprüfung M 4.94 Schutz der Webserver-Dateien M 4.176 Auswahl einer Authentisierungsmethode für Webangebote M 5.87 Vereinbarung über die Anbindung an Netze Dritter M 5.88 Vereinbarung über Datenaustausch mit Dritten B 5.21 Webanwendungen B 5.24 Web-Services
14.1.3 Protecting application	B 1.7 Kryptokonzept	

	ISO 27002:2013	IT-Grundschutz
	services transactions	M 2.162 Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens M 4.176 Auswahl einer Authentisierungsmethode für Webangebote M 5.88 Vereinbarung über Datenaustausch mit Dritten
14.2	Security in development and support processes	
14.2.1	Secure development policy	B 5.27 Software-Entwicklung M 2.487 Entwicklung und Erweiterung von Anwendungen
14.2.2	System change control procedures	B 1.14 Patch- und Änderungsmanagement B 5.27 Software-Entwicklung M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software M 2.34 Dokumentation der Veränderungen an einem bestehenden System M 2.62 Software-Abnahme- und Freigabe-Verfahren
14.2.3	Technical review of applications after operating platform changes	M 4.78 Sorgfältige Durchführung von Konfigurationsänderungen B 1.14 Patch- und Änderungsmanagement B 5.25 Allgemeine Anwendungen M 2.62 Software-Abnahme- und Freigabe-Verfahren
14.2.4	Restrictions on changes to software packages	M 2.9 Nutzungsverbot nicht freigegebener Software
14.2.5	Secure system engineering principles	B 5.27 Software-Entwicklung B 5.21 Webanwendungen B 5.24 Web-Services
14.2.6	Secure development environment	M 4.494 Sicherer Einsatz einer Entwicklungsumgebung M 2.487 Entwicklung und Erweiterung von Anwendungen

	ISO 27002:2013	IT-Grundschutz
14.2.7	Outsourced development	B 5.25 Allgemeine Anwendungen B 1.11 Outsourcing M 2.251 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben M 2.252 Wahl eines geeigneten Outsourcing-Dienstleisters M 2.253 Vertragsgestaltung mit dem Outsourcing-Dienstleister M 2.254 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben M 2.256 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb
14.2.8	System security testing	M 2.568 Testverfahren für Software M 5.150 Durchführung von Penetrationstests
14.2.9	System acceptance testing	M 2.62 Software-Abnahme- und Freigabe-Verfahren B 1.14 Patch- und Änderungsmanagement B 5.25 Allgemeine Anwendungen M 2.85 Freigabe von Standardsoftware M 2.216 Genehmigungsverfahren für IT-Komponenten M 4.65 Test neuer Hard- und Software
14.3	Test data	
14.3.1	Protection of test data	M 2.568 Testverfahren für Software M 2.83 Testen von Standardsoftware
15	Supplier relationships	
15.1	Information security in supplier relationships	
15.1.1	Information security policy for supplier relationships	B 1.11 Outsourcing B 1.17 Cloud-Nutzung M 2.4 Regelungen für Wartungs- und Reparaturarbeiten M 2.250 Festlegung einer Outsourcing-Strategie

	ISO 27002:2013	IT-Grundschutz
		M 2.251 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben M 2.516 Bereitstellung von Sicherheitsrichtlinien für Cloud-Anwender
15.1.2	Addressing security within supplier agreements	B 1.11 Outsourcing B 1.17 Cloud-Nutzung M 2.253 Vertragsgestaltung mit dem Outsourcing-Dienstleister M 2.254 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben M 2.356 Vertragsgestaltung mit Dienstleistern für Speicherlösungen M 2.475 Vertragsgestaltung bei Bestellung eines externen IT-Sicherheitsbeauftragten M 2.517 Vertragsgestaltung mit Dritt-Dienstleistern M 2.539 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung M 2.541 Vertragsgestaltung mit dem Cloud-Diensteanbieter M 2.554 Geeignete Vertragsgestaltung bei Beschaffung, Entwicklung und Betriebsunterstützung für Anwendungen M 3.55 Vertraulichkeitsvereinbarungen M 5.87 Vereinbarung über die Anbindung an Netze Dritter M 5.88 Vereinbarung über Datenaustausch mit Dritten
15.1.3	Information and communication technology supply chain	B 1.11 Outsourcing M 2.4 Regelungen für Wartungs- und Reparaturarbeiten M 2.517 Vertragsgestaltung mit Dritt-Dienstleistern M 3.55 Vertraulichkeitsvereinbarungen M 5.33 Absicherung von Fernwartung
15.2	Supplier service delivery management	
15.2.1	Monitoring and review of supplier services	M 2.256 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb B 1.11 Outsourcing

		ISO 27002:2013	IT-Grundschutz
			B 1.17 Cloud-Nutzung
	15.2.2	Managing changes to supplier services	B 1.11 Outsourcing B 1.14 Patch- und Änderungsmanagement B 1.17 Cloud-Nutzung B 5.23 Cloud Management M 2.221 Änderungsmanagement M 2.34 Dokumentation der Veränderungen an einem bestehenden System
16		Information security incident management	
	16.1	Management of information security incidents and improvements	
	16.1.1	Responsibility and procedures	B 1.8 Behandlung von Sicherheitsvorfällen M 6.58 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen M 6.59 Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen M 6.121 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen
	16.1.2	Reporting information security events	B 1.8 Behandlung von Sicherheitsvorfällen M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern M 6.60 Festlegung von Meldewegen für Sicherheitsvorfälle
	16.1.3	Reporting information security weaknesses	B 1.8 Behandlung von Sicherheitsvorfällen M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems M 6.60 Festlegung von Meldewegen für Sicherheitsvorfälle
	16.1.4	Assessment of and decision on information security events	B 1.8 Behandlung von Sicherheitsvorfällen M 6.122 Definition eines Sicherheitsvorfalls
	16.1.5	Response to information	B 1.8 Behandlung von Sicherheitsvorfällen

	ISO 27002:2013	IT-Grundschutz
	security incidents	M 6.64 Behebung von Sicherheitsvorfällen M 6.65 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen
16.1.6	Learning from information security incidents	B 1.8 Behandlung von Sicherheitsvorfällen M 6.66 Nachbereitung von Sicherheitsvorfällen M 6.68 Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen
16.1.7	Collection of evidence	B 1.8 Behandlung von Sicherheitsvorfällen M 6.127 Etablierung von Beweissicherungsmaßnahmen bei Sicherheitsvorfällen
17	Information security aspects of business continuity management	
17.1	Information security continuity	
17.1.1	Planning information security continuity	B 1.3 Notfallmanagement BSI-Standard 100-2, Kapitel 3 Initiierung des Sicherheitsprozesses BSI-Standard 100-4, Notfallmanagement B 1.8 Behandlung von Sicherheitsvorfällen
17.1.2	Implementing information security continuity	B 1.3 Notfallmanagement BSI-Standard 100-4 Notfallmanagement B 1.8 Behandlung von Sicherheitsvorfällen
17.1.3	Verify, review and evaluate information security continuity	B 1.3 Notfallmanagement BSI-Standard 100-4 Notfallmanagement
17.2	Redundancies	
17.2.1	Availability of information	B 2.4 Serverraum

	ISO 27002:2013	IT-Grundschutz
	processing facilities	B 2.9 Rechenzentrum M 1.52 Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur M 6.18 Redundante Leitungsführung M 6.53 Redundante Auslegung der Netzkomponenten M 6.75 Redundante Kommunikationsverbindungen M 6.103 Redundanzen für die Primärverkabelung M 6.104 Redundanzen für die Gebäudeverkabelung M 6.157 Entwicklung eines Redundanzkonzeptes für Anwendungen
18	Compliance	
	18.1 Compliance with legal and contractual requirements	
	18.1.1 Identification of applicable legislation and contractual requirements	B 1.16 Anforderungsmanagement M 2.340 Beachtung rechtlicher Rahmenbedingungen M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
	18.1.2 Intellectual property rights	B 1.16 Anforderungsmanagement M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 2.10 Überprüfung des Software-Bestandes M 4.99 Schutz gegen nachträgliche Veränderungen von Informationen
	18.1.3 Protection of records	M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
	18.1.4 Privacy and protection of personally identifiable information	B 1.16 Anforderungsmanagement B 1.5 Datenschutz M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen M 2.10 Überprüfung des Software-Bestandes M 2.205 Übertragung und Abruf personenbezogener Daten
	18.1.5 Regulation of cryptographic	B 1.16 Anforderungsmanagement

	ISO 27002:2013	IT-Grundschutz
	controls	M 2.163 Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte
18.2	Information security reviews	
18.2.1	Independent review of information security	M 2.199 Aufrechterhaltung der Informationssicherheit BSI-Standard 100-2, Kapitel 6 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit B 1.0 Sicherheitsmanagement
18.2.2	Compliance with security policies and standards	B 1.16 Anforderungsmanagement M 2.199 Aufrechterhaltung der Informationssicherheit BSI-Standard 100-2, Kapitel 6.1.1 Methoden zur Überprüfung des Informationssicherheitsprozesses
18.2.3	Technical compliance review	M 2.199 Aufrechterhaltung der Informationssicherheit

ISO 27001:2005 und IT-Grundschutz

	ISO 27001:2005	IT-Grundschutz
1	Scope	BSI-Standard 100-2, Kapitel 1 Einleitung
2	Normative references	BSI-Standard 100-1, Kapitel 1.5 Literaturverzeichnis
3	Terms and definitions	IT-Grundschutz-Kataloge, Glossar
4	Information security management system	
	4.1 General requirements	BSI-Standard 100-1, Kapitel 3 ISMS-Definition und Prozessbeschreibung BSI-Standard 100-2, Kapitel 2 Informationssicherheitsmanagement mit IT-Grundschutz B 1.0 Sicherheitsmanagement
	4.2 Establishing and managing the ISMS	
	4.2.1 Establish the ISMS	BSI-Standard 100-2, Kapitel 3, 4 und 5 BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz Ergänzung zum BSI-Standard 100-3 B 1.0 Sicherheitsmanagement M 2.192 Erstellung einer Leitlinie zur Informationssicherheit M 2.335 Festlegung der Sicherheitsziele und -strategie
	4.2.2 Implement and operate the ISMS	BSI-Standard 100-2, Kapitel 5 M 2.195 Erstellung eines Sicherheitskonzepts
	4.2.3 Monitor and review the ISMS	BSI-Standard 100-2, Kapitel 6 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit M 2.199 Aufrechterhaltung der Informationssicherheit M 2.200 Management-Berichte zur Informationssicherheit
	4.2.4 Maintain and improve the ISMS	BSI-Standard 100-2, Kapitel 6 Aufrechterhaltung und kontinuierliche Verbesserung der

	ISO 27001:2005	IT-Grundschutz
		Informationssicherheit
		M 2.199 Aufrechterhaltung der Informationssicherheit M 2.200 Management-Berichte zur Informationssicherheit
	4.3	Documentation requirements
	4.3.1	General BSI-Standard 100-2, Kapitel 6.2 Informationsfluss im Informationssicherheitsprozess M 2.201 Dokumentation des Sicherheitsprozesses
	4.3.2	Control of documents BSI-Standard 100-1, Kapitel 4.3 Kommunikation und Wissen M 2.201 Dokumentation des Sicherheitsprozesses
	4.3.3	Control of records BSI-Standard 100-2, Kapitel 6.2 Informationsfluss im Informationssicherheitsprozess M 2.201 Dokumentation des Sicherheitsprozesses M 2.340 Beachtung rechtlicher Rahmenbedingungen
5	Management responsibility	
	5.1	Management commitment BSI-Standard 100-2, Kapitel 3.1 Übernahme von Verantwortung durch die Leitungsebene M 2.336 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene
	5.2	Resource management
	5.2.1	Provision of resources BSI-Standard 100-2, Kapitel 3.5 Bereitstellung von Ressourcen für die Informationssicherheit M 2.339 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit
	5.2.2	Training, awareness and competence B 1.13 Sensibilisierung und Schulung zur Informationssicherheit M 3.96 Unterstützung des Managements für Sensibilisierung und Schulung
6	Internal ISMS audits	BSI-Standard 100-2, Kapitel 6.1.1 Methoden zur Überprüfung des Informationssicherheitsprozesses M 2.199 Aufrechterhaltung der Informationssicherheit

		ISO 27001:2005	IT-Grundschutz
7		Management review of the ISMS	
	7.1	General	BSI-Standard 100-2, Kapitel 6.1 Überprüfung des Informationssicherheitsprozesses in allen Ebenen M 2.336 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene
	7.2	Review input	BSI-Standard 100-2, Kapitel 6.1 Überprüfung des Informationssicherheitsprozesses in allen Ebenen
	7.3	Review output	BSI-Standard 100-2, Kapitel 6.1 Überprüfung des Informationssicherheitsprozesses in allen Ebenen
8		ISMS Improvement	
	8.1	Continual improvement	BSI-Standard 100-2, Kapitel 6 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit M 2.199 Aufrechterhaltung der Informationssicherheit
	8.2	Corrective action	BSI-Standard 100-2, Kapitel 6 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit M 2.199 Aufrechterhaltung der Informationssicherheit
	8.3	Preventive action	BSI-Standard 100-2, Kapitel 6 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit M 2.199 Aufrechterhaltung der Informationssicherheit

ISO 27001:2005 Anhang A / ISO 27002:2005 und IT-Grundschutz

		ISO 27002:2005	IT-Grundschutz
5		Security policy	
	5.1	Information security policy	
	5.1.1	Information security policy document	M 2.192 Erstellung einer Leitlinie zur Informationssicherheit BSI-Standard 100-2, Kapitel 3 Initiierung des Sicherheitsprozesses B 1.0 Sicherheitsmanagement M 2.335 Festlegung der Sicherheitsziele und -strategie
	5.1.2	Review of the information security policy	BSI-Standard 100-2, Kapitel 3.3.5 Aktualisierung der Sicherheitsleitlinie B 1.0 Sicherheitsmanagement M 2.193 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit M 2.199 Aufrechterhaltung der Informationssicherheit M 2.200 Management-Berichte zur Informationssicherheit
6		Organizing information security	
	6.1	Internal organization	B 1.0 Sicherheitsmanagement
	6.1.1	Management commitment to information security	BSI-Standard 100-2, Kapitel 3.1 Übernahme von Verantwortung durch die Leitungsebene M 2.336 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene B 1.0 Sicherheitsmanagement M 2.192 Erstellung der Leitlinie zur Informationssicherheit M 2.200 Management-Berichte zur Informationssicherheit
	6.1.2	Information security coordination	M 2.193 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit BSI-Standard 100-2, Kapitel 3 Initiierung des Sicherheitsprozesses B 1.0 Sicherheitsmanagement

	ISO 27002:2005	IT-Grundschutz
		B 1.13 Sensibilisierung und Schulung zur Informationssicherheit
6.1.3	Allocation of information security responsibilities	BSI-Standard 100-2, Kapitel 3.4.2 Aufbau der Informationssicherheitsorganisation M 2.193 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten
6.1.4	Authorization process for information processing facilities	B 1.9 Hard- und Software-Management B 1.0 Sicherheitsmanagement M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software M 2.216 Genehmigungsverfahren für IT-Komponenten
6.1.5	Confidentiality agreements	M 3.55 Vertraulichkeitsvereinbarungen B 1.2 Personal M 2.226 Regelungen für den Einsatz von Fremdpersonal M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
6.1.6	Contact with authorities	B 1.3 Notfallmanagement B 1.8 Behandlung von Sicherheitsvorfällen M 6.59 Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen M 6.61 Eskalationsstrategie für Sicherheitsvorfälle M 6.65 Benachrichtigung betroffener Stellen
6.1.7	Contact with special interest groups	M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems M 2.199 Aufrechterhaltung der Informationssicherheit
6.1.8	Independent review of information security	M 2.199 Aufrechterhaltung der Informationssicherheit BSI-Standard 100-2, Kapitel 6 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit B 1.0 Sicherheitsmanagement M 2.200 Management-Berichte zur Informationssicherheit
6.2	External parties	

	ISO 27002:2005	IT-Grundschutz
6.2.1	Identification of risks related to external parties	B 1.11 Outsourcing B 1.9 Hard- und Software-Management B 1.17 Cloud-Nutzung B 4.4 VPN M 2.251 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben M 2.539 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung
6.2.2	Addressing security conditions when dealing with customers	M 5.88 Vereinbarung über Datenaustausch mit Dritten B 5.23 Cloud Management M 2.516 Bereitstellung von Sicherheitsrichtlinien für Cloud-Anwender M 5.87 Vereinbarung über die Anbindung an Netze Dritter
6.2.3	Addressing security in third party agreements	B 1.11 Outsourcing B 1.17 Cloud-Nutzung M 2.541 Vertragsgestaltung mit dem Cloud-Diensteanbieter M 5.87 Vereinbarung über die Anbindung an Netze Dritter M 5.88 Vereinbarung über Datenaustausch mit Dritten
7	Asset management	
7.1	Responsibility for assets	
7.1.1	Inventory of assets	BSI-Standard 100-2, Kapitel 4.2 Strukturanalyse B 1.0 Sicherheitsmanagement B 1.1 Organisation M 2.139 Ist-Aufnahme der aktuellen Netzsituation M 2.195 Erstellung eines Sicherheitskonzeptes M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
7.1.2	Ownership of assets	M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten

	ISO 27002:2005	IT-Grundschutz
7.1.3	Acceptable use of assets	M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz M 1.34 Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz M 2.455 Festlegung einer Sicherheitsrichtlinie für Groupware M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten M 2.226 Regelungen für den Einsatz von Fremdpersonal M 2.235 Richtlinien für die Nutzung von Internet-PCs M 2.309 Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung M 5.88 Vereinbarung über Datenaustausch mit Dritten
7.2	Information classification	
7.2.1	Classification guidelines	BSI-Standard 100-2, Kapitel 4.3 Schutzbedarfsfeststellung B 1.0 Sicherheitsmanagement M 2.195 Erstellung eines Sicherheitskonzepts M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
7.2.2	Information labelling and handling	BSI-Standard 100-2, Kapitel 4.3 Schutzbedarfsfeststellung B 1.0 Sicherheitsmanagement M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
8	Human resources security	
8.1	Prior to employment	
8.1.1	Roles and responsibilities	M 2.1 Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz B 1.1 Organisation B 1.2 Personal M 2.5 Aufgabenverteilung und Funktionstrennung M 2.193 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit M 2.198 Sensibilisierung der Mitarbeiter für Informationssicherheit M 3.1 Geregelt Einarbeitung/Einweisung neuer Mitarbeiter M 3.26 Einweisung des Personals in den sicheren Umgang mit IT

	ISO 27002:2005	IT-Grundschutz
8.1.2	Screening	M 3.33 Sicherheitsprüfung von Mitarbeitern B 1.2 Personal M 3.50 Auswahl von Personal
8.1.3	Terms and conditions of employment	M 2.226 Regelungen für den Einsatz von Fremdpersonal M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen B 1.2 Personal M 3.1 Geregelt Einarbeitung/Einweisung neuer Mitarbeiter
8.2	During employment	
8.2.1	Management responsibilities	M 2.198 Sensibilisierung der Mitarbeiter für Informationssicherheit B 1.13 Sensibilisierung und Schulung zur Informationssicherheit M 2.226 Regelungen für den Einsatz von Fremdpersonal M 3.5 Schulung zu Sicherheitsmaßnahmen
8.2.2	Information security awareness, education and training	B 1.13 Sensibilisierung und Schulung zur Informationssicherheit M 2.312 Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit M 3.5 Schulung zu Sicherheitsmaßnahmen M 3.96 Unterstützung des Managements für Sensibilisierung und Schulung
8.2.3	Disciplinary process	M 2.39 Reaktion auf Verletzungen der Sicherheitsvorgaben B 1.8 Behandlung von Sicherheitsvorfällen M 2.192 Erstellung einer Leitlinie zur Informationssicherheit M 3.26 Einweisung des Personals in den sicheren Umgang mit IT
8.3	Termination or change of employment	
8.3.1	Termination responsibilities	M 3.6 Geregelt Verfahrensweise beim Ausscheiden von Mitarbeitern B 1.2 Personal

	ISO 27002:2005	IT-Grundschutz
		M 2.226 Regelungen für den Einsatz von Fremdpersonal
8.3.2	Return of assets	M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeiter
		M 2.226 Regelungen für den Einsatz von Fremdpersonal
8.3.3	Removal of access rights	M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen
		M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern M 2.226 Regelungen für den Einsatz von Fremdpersonal
9	Physical and environmental security	
9.1	Secure areas	
9.1.1	Physical security perimeter	M 1.79 Bildung von Sicherheitszonen B 2.1 Allgemeines Gebäude M 1.17 Pförtnerdienst M 1.53 Videoüberwachung M 1.19 Einbruchschutz M 1.13 Anordnung schützenswerter Gebäudeteile M 1.55 Perimeterschutz
9.1.2	Physical entry controls	M 2.17 Zutrittsregelung und -kontrolle B 2.1 Allgemeines Gebäude M 1.80 Zutrittskontrollsystem und Berechtigungsmanagement M 2.6 Vergabe von Zutrittsberechtigungen M 2.16 Beaufsichtigung oder Begleitung von Fremdpersonen
9.1.3	Securing offices, rooms and facilities	Bausteine der Schicht 2 Infrastruktur , z. B. B 2.3 Büroraum / Lokaler Arbeitsplatz M 1.12 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile M 1.13 Anordnung schützenswerter Gebäudeteile

	ISO 27002:2005	IT-Grundschutz
		M 1.78 Sicherheitskonzept für die Gebäudenutzung
9.1.4	Protecting against external and environmental threats	Bausteine der Schicht 2 Infrastruktur M 1.1 Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften M 1.6 Einhaltung von Brandschutzvorschriften M 1.13 Anordnung schützenswerter Gebäudeteile M 1.16 Geeignete Standortauswahl M 1.18 Gefahrenmeldeanlage M 1.55 Perimeterschutz M 1.75 Branderkennung in Gebäuden
9.1.5	Working in secure areas	Bausteine der Schicht 2 Infrastruktur M 1.49 Technische und organisatorische Vorgaben für das Rechenzentrum M 1.58 Technische und organisatorische Vorgaben für Serverräume M 1.78 Sicherheitskonzept für die Gebäudenutzung M 1.79 Bildung von Sicherheitszonen M 2.18 Kontrollgänge
9.1.6	Public access, delivery and loading areas	M 2.17 Zutrittsregelung und -kontrolle M 1.55 Perimeterschutz M 1.79 Bildung von Sicherheitszonen M 2.6 Vergabe von Zutrittsberechtigungen M 2.16 Beaufsichtigung oder Begleitung von Fremdpersonen M 2.90 Überprüfung der Lieferung
9.2	Equipment security	
9.2.1	Equipment siting and protection	B 2.3 Büroraum / Lokaler Arbeitsplatz B 2.1 Allgemeines Gebäude M 1.29 Geeignete Aufstellung eines IT-Systems M 1.45 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
9.2.2	Supporting utilities	B 2.2 Elektrotechnische Verkabelung

	ISO 27002:2005	IT-Grundschutz
		M 1.28 Lokale unterbrechungsfreie Stromversorgung M 1.56 Sekundär-Energieversorgung
9.2.3	Cabling security	B 2.2 Elektrotechnische Verkabelung B 2.12 IT-Verkabelung M 1.2 Regelungen für Zutritt zu Verteilern M 1.22 Materielle Sicherung von Leitungen und Verteilern M 5.4 Dokumentation und Kennzeichnung der Verkabelung M 5.5 Schadensmindernde Kabelführung
9.2.4	Equipment maintenance	M 2.4 Regelungen für Wartungs- und Reparaturarbeiten
9.2.5	Security of equipment off-premises	B 2.10 Mobiler Arbeitsplatz B 3.203 Laptop B 5.8 Telearbeit M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz M 1.61 Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes M 2.309 Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten M 2.112 Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution M 4.29 Einsatz eines Verschlüsselungsproduktes für tragbare PCs
9.2.6	Secure disposal or re-use of equipment	B 1.15 Löschen und Vernichten von Daten M 2.431 Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen M 4.234 Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern
9.2.7	Removal of property	M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten

	ISO 27002:2005	IT-Grundschutz
10	Communications and operations management	
10.1	Operational procedures and responsibilities	
10.1.1	Documented operating procedures	M 2.219 Kontinuierliche Dokumentation der Informationsverarbeitung B 1.9 Hard- und Software-Management B 4.2 Netz- und Systemmanagement M 2.1 Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz M 2.201 Dokumentation des Sicherheitsprozesses
10.1.2	Change management	B 1.14 Patch- und Änderungsmanagement
10.1.3	Segregation of duties	M 2.5 Aufgabenverteilung und Funktionstrennung
10.1.4	Separation of development, test and operational facilities	M 4.494 Sicherer Einsatz einer Entwicklungsumgebung M 2.62 Software-Abnahme- und Freigabe-Verfahren M 2.9 Nutzungsverbot nicht freigegebener Software M 2.82 Entwicklung eines Testplans für Standardsoftware M 4.95 Minimales Betriebssystem
10.2	Third party service delivery management	
10.2.1	Service delivery	B 1.11 Outsourcing B 1.17 Cloud-Nutzung M 2.251 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben M 2.253 Vertragsgestaltung mit dem Outsourcing-Dienstleister M 2.254 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben M 2.539 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung M 2.541 Vertragsgestaltung mit dem Cloud-Diensteanbieter M 6.83 Notfallvorsorge beim Outsourcing

	ISO 27002:2005	IT-Grundschutz
		M 6.155 Erstellung eines Notfallkonzeptes für einen Cloud Service
10.2.2	Monitoring and review of third party services	M 2.256 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb B 1.11 Outsourcing B 1.17 Cloud-Nutzung M 2.543 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb
10.2.3	Managing changes to third party services	B 1.11 Outsourcing B 1.14 Patch- und Änderungsmanagement B 1.17 Cloud-Nutzung B 5.23 Cloud Management M 2.221 Änderungsmanagement M 2.34 Dokumentation der Veränderungen an einem bestehenden System
10.3	System planning and acceptance	
10.3.1	Capacity management	M 2.214 Konzeption des IT-Betriebs
10.3.2	System acceptance	M 2.62 Software-Abnahme- und Freigabe-Verfahren B 1.14 Patch- und Änderungsmanagement B 5.25 Allgemeine Anwendungen M 2.85 Freigabe von Standardsoftware M 2.216 Genehmigungsverfahren für IT-Komponenten M 4.65 Test neuer Hard- und Software
10.4	Protection against malicious and mobile software	
10.4.1	Controls against malicious software	B 1.6 Schutz vor Schadprogrammen B 1.8 Behandlung von Sicherheitsvorfällen

	ISO 27002:2005	IT-Grundschutz
		M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software M 2.10 Überprüfung des Software-Bestandes M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems M 2.154 Erstellung eines Sicherheitskonzeptes gegen Schadprogramme M 6.23 Verhaltensregeln bei Auftreten von Schadprogrammen
10.4.2	Controls against mobile code	M 5.69 Schutz vor aktiven Inhalten B 1.6 Schutz vor Schadprogrammen M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software M 2.198 Sensibilisierung der Mitarbeiter für Informationssicherheit M 4.23 Sicherer Aufruf ausführbarer Dateien M 4.100 Firewalls und aktive Inhalte M 4.199 Vermeidung gefährlicher Dateiformate
10.5	Back-up	
10.5.1	Information back-up	B 1.4 Datensicherungskonzept M 6.20 Geeignete Aufbewahrung der Backup-Datenträger M 6.32 Regelmäßige Datensicherung M 6.41 Übungen zur Datenrekonstruktion
10.6	Network security management	
10.6.1	Network controls	B 4.1 Lokale Netze B 4.4 VPN M 2.38 Aufteilung der Administrationstätigkeiten M 2.141 Entwicklung eines Netzkonzeptes M 2.143 Entwicklung eines Netzmanagement-Konzeptes M 2.169 Entwickeln einer Systemmanagementstrategie M 2.279 Erstellung einer Sicherheitsrichtlinie für Router und Switches M 2.576 Erstellung einer Sicherheitsrichtlinie für den Einsatz von lokalen Netzen M 2.577 Auswahl geeigneter Kryptoverfahren für Netze

	ISO 27002:2005	IT-Grundschutz
		<p>M 2.579 Regelmäßige Audits des lokalen Netzes M 4.79 Sichere Zugriffsmechanismen bei lokaler Administration M 4.80 Sichere Zugriffsmechanismen bei Fernadministration M 4.81 Audit und Protokollierung der Aktivitäten im Netz M 4.82 Sichere Konfiguration der aktiven Netzkomponenten M 5.7 Netzverwaltung M 5.8 Regelmäßiger Sicherheitscheck des Netzes M 5.9 Protokollierung am Server M 5.68 Einsatz von Verschlüsselungsverfahren zur Netzkommunikation M 5.71 Intrusion Detection und Intrusion Response Systeme</p>
10.6.2	Security of network services	<p>B 4.1 Lokale Netze</p> <p>B 3.301 Sicherheitsgateway (Firewall) B 4.2 Netz- und Systemmanagement B 4.4 VPN B 4.5 LAN-Anbindung eines IT-Systems über ISDN M 2.577 Auswahl geeigneter Kryptoverfahren für Netze M 4.133 Geeignete Auswahl von Authentikations-Mechanismen M 5.68 Einsatz von Verschlüsselungsverfahren zur Netzkommunikation</p>
10.7	Media handling	
10.7.1	Management of removable media	<p>M 2.3 Datenträgerverwaltung</p> <p>B 5.14 Mobile Datenträger M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten</p>
10.7.2	Disposal of media	<p>B 1.15 Löschen und Vernichten von Daten</p> <p>M 2.431 Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen M 4.234 Geregeltete Außerbetriebnahme von IT-Systemen und Datenträgern</p>
10.7.3	Information handling procedures	<p>M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen</p>

	ISO 27002:2005	IT-Grundschutz
		B 5.2 Datenträgeraustausch B 5.3 Groupware M 2.7 Vergabe von Zugangsberechtigungen M 2.42 Festlegung der möglichen Kommunikationspartner M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
10.7.4	Security of system documentation	M 2.25 Dokumentation der Systemkonfiguration M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
10.8	Exchanges of information	
10.8.1	Information exchange policies and procedures	M 2.393 Regelung des Informationsaustausches B 3.402 Faxgerät B 3.403 Anrufbeantworter B 3.404 Mobiltelefon B 3.405 Smartphones, Tablets und PDAs B 5.2 Datenträgeraustausch B 5.3 Groupware B 5.14 Mobile Datenträger B 5.19 Internet-Nutzung M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 2.398 Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten M 5.88 Vereinbarung über Datenaustausch mit Dritten
10.8.2	Exchange agreements	M 5.88 Vereinbarung über Datenaustausch mit Dritten M 2.45 Regelung des Datenträgeraustausches M 2.455 Festlegung einer Sicherheitsrichtlinie für Groupware M 2.393 Regelung des Informationsaustausches
10.8.3	Physical media in transit	M 5.23 Auswahl einer geeigneten Versandart M 2.3 Datenträgerverwaltung M 2.4 Regelungen für Wartungs- und Reparaturarbeiten

	ISO 27002:2005	IT-Grundschutz
		M 2.44 Sichere Verpackung der Datenträger M 2.45 Regelung des Datenträgeraustausches M 2.112 Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten
10.8.4	Electronic messaging	B 5.3 Groupware B 5.19 Internet-Nutzung M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 5.54 Umgang mit unerwünschten E-Mails M 5.56 Sicherer Betrieb eines Mailservers M 5.108 Kryptographische Absicherung von Groupware bzw. E-Mail
10.8.5	Business information systems	M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 2.1 Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz M 2.7 Vergabe von Zugangsberechtigungen M 2.8 Vergabe von Zugriffsrechten M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.338 Erstellung von zielgruppengerechten Sicherheitsrichtlinien
10.9	Electronic commerce services	
10.9.1	Electronic commerce	B 5.4 Webserver M 2.162 Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens M 2.172 Entwicklung eines Konzeptes für die Web-Nutzung M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 4.176 Auswahl einer Authentisierungsmethode für Webangebote M 5.87 Vereinbarung über die Anbindung an Netze Dritter M 5.88 Vereinbarung über Datenaustausch mit Dritten

	ISO 27002:2005	IT-Grundschutz
		B 5.21 Webanwendungen B 5.24 Web-Services
10.9.2	On-Line Transactions	B 1.7 Kryptokonzept M 2.162 Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens M 4.176 Auswahl einer Authentisierungsmethode für Webangebote M 5.88 Vereinbarung über Datenaustausch mit Dritten
10.9.3	Publicly available information	B 5.4 Webserver B 5.19 Internet-Nutzung M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 2.272 Einrichtung eines Internet-Redaktionsteams M 4.93 Regelmäßige Integritätsprüfung M 4.94 Schutz der Webserver-Dateien B 5.21 Webanwendungen B 5.24 Web-Services
10.10	Monitoring	
10.10.1	Audit logging	B 5.22 Protokollierung M 2.500 Protokollierung von IT-Systemen M 2.64 Kontrolle der Protokolldateien M 2.110 Datenschutzaspekte bei der Protokollierung M 4.81 Audit und Protokollierung der Aktivitäten im Netz M 5.9 Protokollierung am Server
10.10.2	Monitoring system use	B 5.22 Protokollierung M 2.500 Protokollierung von IT-Systemen M 2.64 Kontrolle der Protokolldateien

	ISO 27002:2005	IT-Grundschutz
		M 2.133 Kontrolle der Protokolldateien eines Datenbanksystems M 4.81 Audit und Protokollierung der Aktivitäten im Netz M 4.430 Analyse von Protokolldaten M 5.9 Protokollierung am Server
10.10.3	Protection of log information	M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle B 5.22 Protokollierung M 2.110 Datenschutzaspekte bei der Protokollierung M 2.500 Protokollierung von IT-Systemen M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen M 4.93 Regelmäßige Integritätsprüfung M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien
10.10.4	Administrator and operator logs	M 2.64 Kontrolle der Protokolldateien B 5.22 Protokollierung M 2.110 Datenschutzaspekte bei der Protokollierung M 2.133 Kontrolle der Protokolldateien eines Datenbanksystems M 2.500 Protokollierung von IT-Systemen M 4.5 Protokollierung der TK-Administrationsarbeiten M 4.25 Einsatz der Protokollierung im Unix-System
10.10.5	Fault logging	M 2.215 Fehlerbehandlung M 4.81 Audit und Protokollierung der Aktivitäten im Netz
10.10.6	Clock synchronisation	M 4.227 Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation
11	Access control	
11.1	Business requirement for access control	
11.1.1	Access control policy	B 1.18 Identitäts- und Berechtigungsmanagement B 5.15 Allgemeiner Verzeichnisdienst

	ISO 27002:2005	IT-Grundschutz
		M 2.5 Aufgabenverteilung und Funktionstrennung M 2.7 Vergabe von Zugangsberechtigungen M 2.8 Vergabe von Zugriffsrechten M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle
11.2	User access management	
11.2.1	User registration	M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen B 1.18 Identitäts- und Berechtigungsmanagement M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile M 2.63 Einrichten der Zugriffsrechte M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen M 3.6 Geregelter Verfahrensweise beim Ausscheiden von Mitarbeitern M 4.13 Sorgfältige Vergabe von IDs M 2.402 Zurücksetzen von Passwörtern
11.2.2	Privilege management	M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.20 Kontrolle bestehender Verbindungen M 2.38 Aufteilung der Administrationstätigkeiten M 4.312 Überwachung von Verzeichnisdiensten
11.2.3	User password management	M 2.11 Regelung des Passwortgebrauchs M 2.22 Hinterlegen des Passwortes M 4.7 Änderung voreingestellter Passwörter M 4.133 Geeignete Auswahl von Authentikationsmechanismen M 5.34 Einsatz von Einmalpasswörtern
11.2.4	Review of user access rights	M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile M 2.199 Aufrechterhaltung der Informationssicherheit

	ISO 27002:2005	IT-Grundschutz
		M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen
11.3	User responsibilities	
11.3.1	Password use	M 2.11 Regelung des Passwortgebrauchs M 2.22 Hinterlegen des Passwortes M 3.5 Schulung zu Sicherheitsmaßnahmen M 3.26 Einweisung des Personals in den sicheren Umgang mit IT M 4.7 Änderung voreingestellter Passwörter
11.3.2	Unattended user equipment	M 4.2 Bildschirmsperre M 1.45 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger M 1.46 Einsatz von Diebstahl-Sicherungen M 2.37 Der aufgeräumte Arbeitsplatz M 3.26 Einweisung des Personals in den sicheren Umgang mit IT
11.3.3	Clear desk and clear screen policy	M 2.37 Der aufgeräumte Arbeitsplatz B 3.406 Drucker, Kopierer und Multifunktionsgeräte M 4.1 Passwortschutz für IT-Systeme M 4.2 Bildschirmsperre
11.4	Network access control	
11.4.1	Policy on use of network services	M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle B 4.4 VPN M 2.71 Festlegung einer Policy für ein Sicherheitgateway M 2.169 Entwickeln einer Systemmanagementstrategie M 2.457 Konzeption für die sichere Internet-Nutzung M 2.214 Konzeption des IT-Betriebs
11.4.2	User authentication for external connections	B 4.4 VPN B 4.5 LAN-Anbindung eines IT-Systems über ISDN M 2.7 Vergabe von Zugangsberechtigungen

	ISO 27002:2005	IT-Grundschutz
		M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle
11.4.3	Equipment identification in the network	M 4.82 Sichere Konfiguration der aktiven Netzkomponenten M 4.133 Geeignete Auswahl von Authentikationsmechanismen
11.4.4	Remote diagnostic port protection	B 4.4 VPN M 4.80 Sichere Zugriffsmechanismen bei Fernadministration
11.4.5	Segregation in networks	M 5.77 Bildung von Teilnetzen M 5.61 Geeignete physikalische Segmentierung M 5.62 Geeignete logische Segmentierung
11.4.6	Network connection control	B 3.301 Sicherheitgateway (Firewall) B 4.4 VPN M 4.238 Einsatz eines lokalen Paketfilters M 5.13 Geeigneter Einsatz von Elementen zur Netzkopplung
11.4.7	Network routing control	B 3.301 Sicherheitgateway (Firewall) B 3.302 Router und Switches M 4.82 Sichere Konfiguration der aktiven Netzkomponenten M 5.61 Geeignete physikalische Segmentierung M 5.70 Adressumsetzung - NAT (Network Address Translation)
11.5	Operating system access control	
11.5.1	Secure log-on procedures	M 4.15 Gesichertes Login M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.321 Planung des Einsatzes von Client-Server-Netzen M 2.322 Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz M 4.133 Geeignete Auswahl von Authentikationsmechanismen
11.5.2	User identification and	B 1.18 Identitäts- und Berechtigungsmanagement

	ISO 27002:2005	IT-Grundschutz
	authentication	M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.585 Konzeption eines Identitäts- und Berechtigungsmanagements
11.5.3	Password management system	M 2.11 Regelung des Passwortgebrauchs M 4.133 Geeignete Auswahl von Authentikationsmechanismen
11.5.4	Use of system utilities	M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien
11.5.5	Session time-out	M 3.18 Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung M 4.2 Bildschirmsperre M 4.41 Einsatz angemessener Sicherheitsprodukte für IT-Systeme
11.5.6	Limitation of connection time	M 4.16 Zugangsbeschränkungen für Accounts und / oder Terminals M 4.133 Geeignete Auswahl von Authentikationsmechanismen
11.6	Application access control	
11.6.1	Information access restriction	M 2.8 Vergabe von Zugriffsrechten M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.555 Entwicklung eines Authentisierungskonzeptes für Anwendungen
11.6.2	Sensitive system isolation	M 5.77 Bildung von Teilnetzen M 5.61 Geeignete physikalische Segmentierung M 5.62 Geeignete logische Segmentierung
11.7	Mobile computing and teleworking	
11.7.1	Mobile computing	B 2.10 Mobiler Arbeitsplatz B 3.203 Laptop B 3.404 Mobiltelefon B 3.405 Smartphones, Tablets und PDAs

		ISO 27002:2005	IT-Grundschutz
			M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz M 2.309 Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten
	11.7.2	Teleworking	B 5.8 Telearbeit
12		Information systems acquisition, development and maintenance	
	12.1	Security requirements of information systems	
	12.1.1	Security requirements analysis and specification	M 2.80 Erstellung eines Anforderungskataloges für Standardsoftware M 2.546 Analyse der Anforderungen an neue Anwendungen B 1.10 Standardsoftware B 1.9 Hard- und Software-Management B 5.25 Allgemeine Anwendungen B 5.27 Software-Entwicklung M 2.62 Software-Abnahme- und Freigabe-Verfahren M 2.66 Beachtung des Beitrags der Zertifizierung für die Beschaffung M 2.83 Testen von Standardsoftware M 2.487 Entwicklung und Erweiterung von Anwendungen M 2.556 Planung und Umsetzung von Test und Freigabe von Anwendungen M 5.168 Sichere Anbindung von Hintergrundsystemen an Webanwendungen und Web-Services M 5.169 Systemarchitektur einer Webanwendung
	12.2	Correct processing in applications	
	12.2.1	Input data validation	B 5.21 Webanwendungen B 5.24 Web-Services M 2.363 Schutz gegen SQL-Injection M 4.393 Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services

	ISO 27002:2005	IT-Grundschutz
		M 2.83 Testen von Standardsoftware
12.2.2	Control of internal processing	M 2.378 System-Entwicklung M 2.82 Entwicklung eines Testplans für Standardsoftware M 2.83 Testen von Standardsoftware M 2.487 Entwicklung und Erweiterung von Anwendungen M 4.404 Sicherer Entwurf der Logik von Webanwendungen
12.2.3	Message integrity	M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen B 1.7 Kryptokonzept
12.2.4	Output data validation	B 5.21 Webanwendungen B 5.24 Web-Services M 4.393 Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services M 2.83 Testen von Standardsoftware
12.3	Cryptographic controls	
12.3.1	Policy on the use of cryptographic controls	B 1.7 Kryptokonzept M 2.161 Entwicklung eines Kryptokonzepts
12.3.2	Key management	B 1.7 Kryptokonzept M 2.46 Geeignetes Schlüsselmanagement M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens
12.4	Security of system files	
12.4.1	Control of operational software	B 1.9 Hard- und Software-Management B 1.10 Standardsoftware M 2.62 Software-Abnahme- und Freigabe-Verfahren M 2.85 Freigabe von Standardsoftware M 2.86 Sicherstellen der Integrität von Standardsoftware M 2.87 Installation und Konfiguration von Standardsoftware

	ISO 27002:2005	IT-Grundschutz
		M 2.88 Lizenzverwaltung und Versionskontrolle von Standardsoftware
12.4.2	Protection of system test data	M 2.83 Testen von Standardsoftware M 2.568 Testverfahren für Software
12.4.3	Access control to program source code	M 4.494 Sicherer Einsatz einer Entwicklungsumgebung M 2.378 System-Entwicklung M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien
12.5	Security in development and support processes	
12.5.1	Change control procedures	B 1.14 Patch- und Änderungsmanagement B 5.27 Software-Entwicklung M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software M 2.34 Dokumentation der Veränderungen an einem bestehenden System M 2.62 Software-Abnahme- und Freigabe-Verfahren
12.5.2	Technical review of applications after operating system changes	M 4.78 Sorgfältige Durchführung von Konfigurationsänderungen B 1.14 Patch- und Änderungsmanagement B 5.25 Allgemeine Anwendungen M 2.62 Software-Abnahme- und Freigabe-Verfahren
12.5.3	Restrictions on changes to software packages	M 2.9 Nutzungsverbot nicht freigegebener Software
12.5.4	Information leakage	M 4.345 Schutz vor unerwünschten Informationsabflüssen M 2.224 Vorbeugung gegen trojanische Pferde B 5.25 Allgemeine Anwendungen M 2.66 Beachtung des Beitrags der Zertifizierung für die Beschaffung M 2.87 Installation und Konfiguration von Standardsoftware M 2.214 Konzeption des IT-Betriebs M 3.10 Auswahl eines vertrauenswürdigen Administrators und Vertreters

	ISO 27002:2005	IT-Grundschutz
		M 4.35 Verifizieren der zu übertragenden Daten vor Versand
12.5.5	Outsourced software development	B 5.25 Allgemeine Anwendungen B 1.11 Outsourcing B 5.25 Allgemeine Anwendungen M 2.251 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben M 2.252 Wahl eines geeigneten Outsourcing-Dienstleisters M 2.253 Vertragsgestaltung mit dem Outsourcing-Dienstleister M 2.254 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben M 2.256 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb
12.6	Technical Vulnerability Management	
12.6.1	Control of technical vulnerabilities	M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
13	Information security incident management	
13.1	Reporting information security events and weaknesses	
13.1.1	Reporting information security events	B 1.8 Behandlung von Sicherheitsvorfällen M 3.6 Geregelt Verfahrensweise beim Ausscheiden von Mitarbeitern M 6.60 Festlegung von Meldewegen für Sicherheitsvorfälle
13.1.2	Reporting security weaknesses	B 1.8 Behandlung von Sicherheitsvorfällen M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems M 6.60 Festlegung von Meldewegen für Sicherheitsvorfälle
13.2	Management of information security incidents and improvements	

	ISO 27002:2005	IT-Grundschutz
	13.2.1 Responsibility and procedures	B 1.8 Behandlung von Sicherheitsvorfällen M 6.58 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen M 6.59 Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen M 6.121 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen
	13.2.2 Learning from information security incidents	B 1.8 Behandlung von Sicherheitsvorfällen M 6.66 Nachbereitung von Sicherheitsvorfällen M 6.68 Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen
	13.2.3 Collection of evidence	B 1.8 Behandlung von Sicherheitsvorfällen M 6.127 Etablierung von Beweissicherungsmaßnahmen bei Sicherheitsvorfällen
14	Business continuity management	
	14.1 Information Security Aspects of business continuity management	
	14.1.1 Including information security in the business continuity management process	B 1.3 Notfallmanagement BSI-Standard 100-2, Kapitel 3 Initiierung des Sicherheitsprozesses BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz BSI-Standard 100-4, Notfallmanagement B 1.8 Behandlung von Sicherheitsvorfällen
	14.1.2 Business continuity and risk assessment	B 1.3 Notfallmanagement BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz Ergänzung zum BSI-Standard 100-3 BSI-Standard 100-4, Notfallmanagement

	ISO 27002:2005	IT-Grundschutz
		B 1.8 Behandlung von Sicherheitsvorfällen
14.1.3	Developing and implementing continuity plans including information security	B 1.3 Notfallmanagement BSI-Standard 100-4, Notfallmanagement B 1.8 Behandlung von Sicherheitsvorfällen
14.1.4	Business continuity planning framework	B 1.3 Notfallmanagement BSI-Standard 100-4, Notfallmanagement B 1.8 Behandlung von Sicherheitsvorfällen
14.1.5	Testing, maintaining and re-assessing business continuity plans	B 1.3 Notfallmanagement BSI-Standard 100-4, Notfallmanagement B 1.8 Behandlung von Sicherheitsvorfällen
15	Compliance	
15.1	Compliance with legal requirements	
15.1.1	Identification of applicable legislation	B 1.16 Anforderungsmanagement M 2.340 Beachtung rechtlicher Rahmenbedingungen M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
15.1.2	Intellectual property rights (IPR)	B 1.16 Anforderungsmanagement M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen M 2.10 Überprüfung des Software-Bestandes M 4.99 Schutz gegen nachträgliche Veränderungen von Informationen
15.1.3	Protection of organizational records	M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
15.1.4	Data protection and privacy of personal information	B 1.16 Anforderungsmanagement

	ISO 27002:2005	IT-Grundschutz
		B 1.5 Datenschutz M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen M 2.10 Überprüfung des Software-Bestandes M 2.205 Übertragung und Abruf personenbezogener Daten
15.1.5	Prevention of misuse of information processing facilities	B 1.16 Anforderungsmanagement M 2.380 Ausnahmegenehmigungen B 1.13 Sensibilisierung und Schulung zur Informationssicherheit M 3.26 Einweisung des Personals in den sicheren Umgang mit IT
15.1.6	Regulation of cryptographic controls	B 1.16 Anforderungsmanagement M 2.163 Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte
15.2	Compliance with security policies and standards	
15.2.1	Compliance with security policies and standards	B 1.16 Anforderungsmanagement M 2.199 Aufrechterhaltung der Informationssicherheit BSI-Standard 100-2, Kapitel 3 Initiierung des Sicherheitsprozesses
15.2.2	Technical compliance checking	M 2.199 Aufrechterhaltung der Informationssicherheit
15.3	Information systems audit considerations	
15.3.1	Information systems audit controls	B 1.16 Anforderungsmanagement M 2.199 Aufrechterhaltung der Informationssicherheit M 2.64 Kontrolle der Protokolldateien M 4.81 Audit und Protokollierung der Aktivitäten im Netz
15.3.2	Protection of information systems audit tools	M 2.199 Aufrechterhaltung der Informationssicherheit