

Maßnahmen und zugeordnete Bausteine						
Maßnahme	Maßnahmentitel	Baustein	Alt	Zertifikat	Zyklus	Bausteinname
M 1.1	Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften	B 2.1	(4.1)	(A)	Umsetzg.	Gebäude
M 1.2	Regelungen für Zutritt zu Verteilern	B 2.1	(4.1)	(A)	Umsetzg.	Gebäude
M 1.3	Angepasste Aufteilung der Stromkreise	B 2.1	(4.1)	(A)	Planung	Gebäude
		B 2.4	(4.3.2)	(A)	Planung	Serverraum
		B 2.6	(4.3.4)	(A)	Planung	Raum für technische Infrastruktur
		B 2.9	(4.6)	(A)	Planung	Rechenzentrum
M 1.4	Blitzschutzeinrichtungen	B 2.1	(4.1)	(B)	Planung	Gebäude
M 1.5	Galvanische Trennung von Außenleitungen	B 2.1	(4.1)	(Z)	Planung	Gebäude
M 1.6	Einhaltung von Brandschutzvorschriften	B 2.1	(4.1)	(A)	Umsetzg.	Gebäude
		B 2.11	(4.8)	(A)	Umsetzg.	Besprechungs-, Veranstaltungs- und Schulungsräume
M 1.7	Handfeuerlöscher	B 2.1	(4.1)	(A)	Planung	Gebäude
		B 2.4	(4.3.2)	(A)	Planung	Serverraum
		B 2.5	(4.3.3)	(A)	Planung	Datenträgerarchiv
		B 2.6	(4.3.4)	(A)	Planung	Raum für technische Infrastruktur
		B 2.7	(4.4)	(B)	Planung	Schutzschrank
		B 2.9	(4.6)	(A)	Planung	Rechenzentrum
M 1.8	Raumbelegung unter Berücksichtigung von Brandlasten	B 2.1	(4.1)	(A)	Planung	Gebäude
M 1.9	Brandabschottung von Trassen	B 2.2	(4.2)	(A)	Umsetzg.	Verkabelung
M 1.10	Verwendung von Sicherheitstüren und -fenstern	B 2.1	(4.1)	(Z)	Planung	Gebäude
		B 2.4	(4.3.2)	(C)	Planung	Serverraum
		B 2.5	(4.3.3)	(C)	Planung	Datenträgerarchiv
		B 2.6	(4.3.4)	(Z)	Planung	Raum für technische Infrastruktur
		B 2.9	(4.6)	(C)	Planung	Rechenzentrum
M 1.11	Lagepläne der Versorgungsleitungen	B 2.1	(4.1)	(A)	Planung	Gebäude
M 1.12	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile	B 2.1	(4.1)	(A)	Planung	Gebäude
		B 2.9	(4.6)	(A)	Planung	Rechenzentrum

M 1.13	Anordnung schützenswerter Gebäudeteile	B 3.401	(8.1)	(B)	Planung	TK-Anlage
		B 2.1	(4.1)	(Z)	Planung	Gebäude
		B 2.9	(4.6)	(Z)	Planung	Rechenzentrum
		B 3.401	(8.1)	(Z)	Planung	TK-Anlage
M 1.14	Selbsttätige Entwässerung					
M 1.15	Geschlossene Fenster und Türen	B 2.1	(4.1)	(Z)	Planung	Gebäude
		B 2.1	(4.1)	(A)	Betrieb	Gebäude
		B 2.3	(4.3.1)	(A)	Betrieb	Bürraum
		B 2.4	(4.3.2)	(A)	Betrieb	Serverraum
		B 2.5	(4.3.3)	(A)	Betrieb	Datenträgerarchiv
		B 2.6	(4.3.4)	(A)	Betrieb	Raum für technische Infrastruktur
		B 2.7	(4.4)	(A)	Betrieb	Schutzschrank
		B 2.8	(4.5)	(A)	Betrieb	Häuslicher Arbeitsplatz
		B 2.9	(4.6)	(A)	Betrieb	Rechenzentrum
		B 2.10	(4.7)	(A)	Betrieb	Mobiler Arbeitsplatz
		B 2.11	(4.8)	(A)	Betrieb	Besprechungs-, Veranstaltungs- und Schulungsräume
M 1.16	Geeignete Standortauswahl					
M 1.17	Pfortnerdienst	B 2.1	(4.1)	(Z)	Planung	Gebäude
		B 2.1	(4.1)	(Z)	Umsetzg.	Gebäude
M 1.18	Gefahrenmeldeanlage	B 2.1	(4.1)	(Z)	Planung	Gebäude
		B 2.4	(4.3.2)	(Z)	Planung	Serverraum
		B 2.5	(4.3.3)	(Z)	Planung	Datenträgerarchiv
		B 2.6	(4.3.4)	(Z)	Planung	Raum für technische Infrastruktur
		B 2.7	(4.4)	(Z)	Planung	Schutzschrank
		B 2.9	(4.6)	(B)	Planung	Rechenzentrum
M 1.19	Einbruchschutz	B 2.1	(4.1)	(Z)	Planung	Gebäude
		B 2.8	(4.5)	(Z)	Planung	Häuslicher Arbeitsplatz
M 1.20	Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht					
M 1.21	Ausreichende Trassendimensionierung	B 2.2	(4.2)	(A)	Planung	Verkabelung
		B 2.2	(4.2)	(A)	Planung	Verkabelung
M 1.22	Materielle Sicherung von Leitungen und Verteilern					
M 1.23	Abgeschlossene Türen	B 2.2	(4.2)	(Z)	Planung	Verkabelung
		B 2.3	(4.3.1)	(A)	Betrieb	Bürraum

M 1.24	Vermeidung von wasserführenden Leitungen	B 2.4	(4.3.2)	(A)	Betrieb	Serverraum
		B 2.5	(4.3.3)	(A)	Betrieb	Datenträgerarchiv
		B 2.6	(4.3.4)	(A)	Betrieb	Raum für technische Infrastruktur
		B 2.8	(4.5)	(A)	Betrieb	Häuslicher Arbeitsplatz
		B 2.9	(4.6)	(A)	Betrieb	Rechenzentrum
M 1.25	Überspannungsschutz	B 2.10	(4.7)	(A)	Betrieb	Mobiler Arbeitsplatz
		B 2.4	(4.3.2)	(C)	Planung	Serverraum
		B 2.5	(4.3.3)	(Z)	Planung	Datenträgerarchiv
		B 2.6	(4.3.4)	(Z)	Planung	Raum für technische Infrastruktur
		B 2.7	(4.4)	(Z)	Planung	Schutzschrank
M 1.26	Not-Aus-Schalter	B 2.9	(4.6)	(C)	Planung	Rechenzentrum
		B 2.4	(4.3.2)	(B)	Planung	Serverraum
		B 2.6	(4.3.4)	(A)	Planung	Raum für technische Infrastruktur
		B 2.7	(4.4)	(B)	Planung	Schutzschrank
		B 2.9	(4.6)	(A)	Planung	Rechenzentrum
M 1.27	Klimatisierung	B 3.401	(8.1)	(B)	Planung	TK-Anlage
		B 4.3	(7.2)	(Z)	Planung	Modem
		B 4.5	(8.4)	(B)	Planung	LAN-Anbindung eines IT-Systems über ISDN
		B 2.4	(4.3.2)	(Z)	Planung	Serverraum
		B 2.6	(4.3.4)	(Z)	Planung	Raum für technische Infrastruktur
M 1.28	Lokale unterbrechungsfreie Stromversorgung	B 2.7	(4.4)	(A)	Planung	Schutzschrank
		B 2.9	(4.6)	(B)	Planung	Rechenzentrum
		B 2.4	(4.3.2)	(B)	Planung	Serverraum
		B 2.5	(4.3.3)	(Z)	Planung	Datenträgerarchiv
		B 2.6	(4.3.4)	(B)	Planung	Raum für technische Infrastruktur
M 1.29	Geeignete Aufstellung eines IT-Systems	B 2.7	(4.4)	(B)	Planung	Schutzschrank
		B 2.9	(4.6)	(B)	Planung	Rechenzentrum
		B 2.4	(4.3.2)	(B)	Planung	Serverraum
		B 2.7	(4.4)	(B)	Planung	Schutzschrank
		B 3.101	(6.1)	(B)	Planung	Allgemeiner Server
M 1.30	Absicherung der Datenträger mit TK-Gebührendaten	B 3.401	(8.1)	(B)	Planung	TK-Anlage
		B 1.9	(3.9)	(Z)	Umsetzg.	Hard- und Software-Management
		B 3.401	(8.1)	(A)	Umsetzg.	TK-Anlage
		B 1.9	(3.9)	(Z)	Umsetzg.	Hard- und Software-Management
		B 3.401	(8.1)	(A)	Umsetzg.	TK-Anlage
M 1.31	Fernanzeige von Störungen					

M 1.33	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz	B 2.4	(4.3.2)	(Z)	Planung	Serverraum
		B 2.6	(4.3.4)	(Z)	Planung	Raum für technische Infrastruktur
		B 2.7	(4.4)	(Z)	Planung	Schutzschrank
		B 2.9	(4.6)	(Z)	Planung	Rechenzentrum
M 1.34	Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz	B 3.203	(5.3)	(A)	Betrieb	Laptop
		B 3.405	(8.7)	(A)	Betrieb	PDA
M 1.35	Sammelaufbewahrung tragbarer IT-Systeme	B 3.203	(5.3)	(A)	Betrieb	Laptop
M 1.36	Sichere Aufbewahrung der Datenträger vor und nach Versand	B 3.203	(5.3)	(Z)	Betrieb	Laptop
M 1.37	Geeignete Aufstellung eines Faxgerätes	B 5.2	(7.1)	(A)	Betrieb	Datenträgeraustausch
M 1.38	Geeignete Aufstellung eines Modems	B 3.402	(8.2)	(A)	Umsetzg.	Faxgerät
M 1.39	Verhinderung von Ausgleichsströmen auf Schirmungen	B 4.3	(7.2)	(A)	Umsetzg.	Modem
M 1.40	Geeignete Aufstellung von Schutzschranken	B 2.2	(4.2)	(Z)	Umsetzg.	Verkabelung
M 1.41	Schutz gegen elektromagnetische Einstrahlung	B 2.7	(4.4)	(A)	Umsetzg.	Schutzschrank
M 1.42	Gesicherte Aufstellung von Novell Netware Servern	B 2.7	(4.4)	(Z)	Planung	Schutzschrank
M 1.43	Gesicherte Aufstellung aktiver Netzkomponenten	B 3.104	(6.5)	(A)	Umsetzg.	Server unter Novell Netware 3.x
		B 3.105	(6.6)	(A)	Umsetzg.	Server unter Novell Netware 4.x
M 1.44	Geeignete Einrichtung eines häuslichen Arbeitsplatzes	B 3.302	(7.11)	(A)	Umsetzg.	Router und Switches
		B 4.5	(8.4)	(A)	Umsetzg.	LAN-Anbindung eines IT-Systems über ISDN
M 1.45	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger	B 2.8	(4.5)	(A)	Planung	Häuslicher Arbeitsplatz
M 1.46	Einsatz von Diebstahl-Sicherungen	B 2.8	(4.5)	(A)	Betrieb	Häuslicher Arbeitsplatz
		B 2.10	(4.7)	(A)	Betrieb	Mobiler Arbeitsplatz
M 1.47	Eigener Brandabschnitt	B 1.9	(3.9)	(Z)	Betrieb	Hard- und Software-Management
		B 2.3	(4.3.1)	(Z)	Betrieb	Bürraum
		B 2.10	(4.7)	(Z)	Betrieb	Mobiler Arbeitsplatz
		B 3.203	(5.3)	(Z)	Betrieb	Laptop
		B 2.9	(4.6)	(B)	Planung	Rechenzentrum

M 1.48	Brandmeldeanlage						
M 1.49	Technische und organisatorische Vorgaben für das Rechenzentrum	B 2.9	(4.6)	(B)	Planung	Rechenzentrum	
M 1.50	Rauchschutz	B 2.9	(4.6)	(A)	Planung	Rechenzentrum	
M 1.51	Brandlastreduzierung	B 2.9	(4.6)	(C)	Planung	Rechenzentrum	
M 1.52	Redundanzen in der technischen Infrastruktur	B 2.9	(4.6)	(A)	Umsetzg.	Rechenzentrum	
M 1.53	Videoüberwachung	B 2.4	(4.3.2)	(Z)	Planung	Serverraum	
		B 2.9	(4.6)	(Z)	Planung	Rechenzentrum	
M 1.54	Brandfrühesterkennung / Löschtechnik	B 2.9	(4.6)	(Z)	Planung	Rechenzentrum	
M 1.55	Perimeterschutz	B 2.9	(4.6)	(Z)	Planung	Rechenzentrum	
M 1.56	Sekundär-Energieversorgung	B 2.9	(4.6)	(Z)	Planung	Rechenzentrum	
M 1.57	Aktuelle Infrastruktur- und Baupläne	B 2.9	(4.6)	(A)	Planung	Rechenzentrum	
M 1.58	Technische und organisatorische Vorgaben für Serverräume	B 2.9	(4.6)	(A)	Umsetzg.	Rechenzentrum	
M 1.59	Geeignete Aufstellung von Archivsystemen	B 2.4	(4.3.2)	(A)	Planung	Serverraum	
M 1.60	Geeignete Lagerung von Archivmedien	B 1.12	(9.5)	(B)	Umsetzg.	Archivierung	
M 1.61	Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes	B 1.12	(9.5)	(A)	Betrieb	Archivierung	
M 1.62	Brandschutz von Patchfeldern	B 2.10	(4.7)	(A)	Planung	Mobiler Arbeitsplatz	
M 2.1	Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz	B 2.4	(4.3.2)	(C)	Planung	Serverraum	
		B 2.9	(4.6)	(C)	Planung	Rechenzentrum	
M 2.2	Betriebsmittelverwaltung	B 1.1	(3.1)	(A)	Planung	Organisation	
M 2.3	Datenträgerverwaltung	B 1.1	(3.1)	(C)	Planung	Organisation	
M 2.4	Regelungen für Wartungs- und Reparaturarbeiten	B 1.9	(3.9)	(B)	Planung	Hard- und Software-Management	
		B 5.2	(7.1)	(B)	Planung	Datenträgeraustausch	
		B 1.1	(3.1)	(B)	Planung	Organisation	

M 2.5	Aufgabenverteilung und Funktionstrennung					
		B 1.1	(3.1)	(A)	Planung	Organisation
M 2.6	Vergabe von Zutrittsberechtigungen					
		B 1.1	(3.1)	(A)	Betrieb	Organisation
M 2.7	Vergabe von Zugangsberechtigungen					
		B 1.1	(3.1)	(A)	Betrieb	Organisation
M 2.8	Vergabe von Zugriffsrechten					
		B 1.1	(3.1)	(A)	Betrieb	Organisation
M 2.9	Nutzungsverbot nicht freigegebener Hard- und Software					
		B 1.9	(3.9)	(A)	Planung	Hard- und Software-Management
M 2.10	Überprüfung des Hard- und Software-Bestandes					
		B 1.9	(3.9)	(C)	Betrieb	Hard- und Software-Management
M 2.11	Regelung des Passwortgebrauchs					
		B 1.9	(3.9)	(A)	Planung	Hard- und Software-Management
		B 3.403	(8.3)	(A)	Planung	Anrufbeantworter
M 2.12	Betreuung und Beratung von IT-Benutzern					
		B 1.9	(3.9)	(C)	Planung	Hard- und Software-Management
M 2.13	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln					
		B 1.1	(3.1)	(A)	Aussnd.	Organisation
		B 2.8	(4.5)	(A)	Aussnd.	Häuslicher Arbeitsplatz
		B 2.10	(4.7)	(A)	Aussnd.	Mobiler Arbeitsplatz
M 2.14	Schlüsselverwaltung					
		B 1.1	(3.1)	(A)	Betrieb	Organisation
		B 2.1	(4.1)	(A)	Betrieb	Gebäude
M 2.15	Brandschutzbegehungen					
		B 2.1	(4.1)	(B)	Betrieb	Gebäude
M 2.16	Beaufsichtigung oder Begleitung von Fremdpersonen					
		B 1.1	(3.1)	(B)	Betrieb	Organisation
		B 2.11	(4.8)	(B)	Betrieb	Besprechungs-, Veranstaltungs- und Schulungsräume
M 2.17	Zutrittsregelung und -kontrolle					
		B 2.1	(4.1)	(A)	Umsetzg.	Gebäude
		B 2.3	(4.3.1)	(A)	Umsetzg.	Bürraum
		B 2.4	(4.3.2)	(A)	Umsetzg.	Serverraum
		B 2.5	(4.3.3)	(A)	Umsetzg.	Datenträgerarchiv
		B 2.6	(4.3.4)	(A)	Umsetzg.	Raum für technische Infrastruktur
		B 2.7	(4.4)	(C)	Umsetzg.	Schutzschrank
		B 2.9	(4.6)	(A)	Umsetzg.	Rechenzentrum
M 2.18	Kontrollgänge					
		B 1.1	(3.1)	(Z)	Betrieb	Organisation
M 2.19	Neutrale Dokumentation in den Verteilern					

M 2.20	Kontrolle bestehender Verbindungen	B 2.2	(4.2)	(B)	Umsetzg.	Verkabelung
M 2.21	Rauchverbot	B 2.2	(4.2)	(Z)	Betrieb	Verkabelung
		B 2.4	(4.3.2)	(A)	Umsetzg.	Serverraum
		B 2.5	(4.3.3)	(A)	Umsetzg.	Datenträgerarchiv
		B 2.6	(4.3.4)	(A)	Umsetzg.	Raum für technische Infrastruktur
		B 2.7	(4.4)	(A)	Umsetzg.	Schutzschrank
		B 2.9	(4.6)	(A)	Umsetzg.	Rechenzentrum
M 2.22	Hinterlegen des Passwortes	B 1.9	(3.9)	(Z)	Betrieb	Hard- und Software-Management
		B 3.101	(6.1)	(A)	Betrieb	Allgemeiner Server
		B 3.201	(5.99)	(A)	Betrieb	Allgemeiner Client
		B 3.202	(5.99)	(Z)	Betrieb	Allgemeines nicht vernetztes IT-System
M 2.23	Herausgabe einer PC-Richtlinie					
		B 3.201	(5.99)	(Z)	Planung	Allgemeiner Client
		B 3.202	(5.99)	(Z)	Planung	Allgemeines nicht vernetztes IT-System
M 2.25	Dokumentation der Systemkonfiguration					
		B 1.9	(3.9)	(A)	Umsetzg.	Hard- und Software-Management
		B 3.201	(5.99)	(A)	Umsetzg.	Allgemeiner Client
M 2.26	Ernennung eines Administrators und eines Vertreters					
M 2.27	Verzicht auf Fernwartung der TK-Anlage	B 1.9	(3.9)	(A)	Umsetzg.	Hard- und Software-Management
M 2.28	Bereitstellung externer TK-Beratungskapazität	B 3.401	(8.1)	(Z)	Planung	TK-Anlage
M 2.29	Bedienungsanleitung der TK-Anlage für die Benutzer	B 3.401	(8.1)	(Z)	Planung	TK-Anlage
M 2.30	Regelung für die Einrichtung von Benutzern / Benutzergruppen	B 3.401	(8.1)	(B)	Umsetzg.	TK-Anlage
		B 1.9	(3.9)	(A)	Planung	Hard- und Software-Management
		B 5.3	(7.4)	(A)	Planung	E-Mail
M 2.31	Dokumentation der zugelassenen Benutzer und Rechteprofile					
		B 3.101	(6.1)	(A)	Betrieb	Allgemeiner Server
		B 3.107	(6.10)	(B)	Planung	S/390- und zSeries-Mainframe
		B 3.204	(5.2)	(A)	Betrieb	Client unter Unix
		B 3.205	(5.5)	(B)	Betrieb	Client unter Windows NT
		B 3.207	(5.7)	(B)	Betrieb	Client unter Windows 2000
		B 5.7	(9.2)	(A)	Betrieb	Datenbanken
M 2.32	Einrichtung einer eingeschränkten Benutzerumgebung					
		B 3.101	(6.1)	(Z)	Umsetzg.	Allgemeiner Server
		B 3.204	(5.2)	(Z)	Umsetzg.	Client unter Unix

M 2.33	Aufteilung der Administrationstätigkeiten unter Unix	B 3.205	(5.5)	(Z)	Umsetzg.	Client unter Windows NT
		B 3.207	(5.7)	(Z)	Umsetzg.	Client unter Windows 2000
		B 3.209	(5.9)	(Z)	Umsetzg.	Client unter Windows XP
M 2.34	Dokumentation der Veränderungen an einem bestehenden System	B 3.102	(6.2)	(C)	Planung	Server unter Unix
		B 3.204	(5.2)	(Z)	Planung	Client unter Unix
M 2.35	Informationsbeschaffung über Sicherheitslücken des Systems	B 1.9	(3.9)	(A)	Betrieb	Hard- und Software-Management
		B 5.7	(9.2)	(A)	Betrieb	Datenbanken
M 2.36	Geregelte Übergabe und Rücknahme eines tragbaren PC	B 1.9	(3.9)	(B)	Betrieb	Hard- und Software-Management
		B 3.101	(6.1)	(B)	Betrieb	Allgemeiner Server
M 2.37	"Der aufgeräumte Arbeitsplatz"	B 3.203	(5.3)	(B)	Betrieb	Laptop
M 2.38	Aufteilung der Administrationstätigkeiten	B 1.1	(3.1)	(Z)	Betrieb	Organisation
		B 2.8	(4.5)	(C)	Betrieb	Häuslicher Arbeitsplatz
		B 2.10	(4.7)	(C)	Betrieb	Mobiler Arbeitsplatz
M 2.39	Reaktion auf Verletzungen der Sicherheitspolitik	B 1.9	(3.9)	(B)	Umsetzg.	Hard- und Software-Management
M 2.40	Rechtzeitige Beteiligung des Personal-/Betriebsrates	B 1.1	(3.1)	(B)	Betrieb	Organisation
M 2.41	Verpflichtung der Mitarbeiter zur Datensicherung	B 1.1	(3.1)	(A)	Planung	Organisation
		B 1.11	(3.10)	(Z)	Planung	Outsourcing
M 2.42	Festlegung der möglichen Kommunikationspartner	B 1.4	(3.4)	(A)	Umsetzg.	Datensicherungskonzept
M 2.43	Ausreichende Kennzeichnung der Datenträger beim Versand	B 1.11	(3.10)	(A)	Planung	Outsourcing
		B 4.3	(7.2)	(B)	Planung	Modem
		B 4.5	(8.4)	(A)	Planung	LAN-Anbindung eines IT-Systems über ISDN
		B 5.2	(7.1)	(B)	Planung	Datenträgeraustausch
		B 5.3	(7.4)	(B)	Planung	E-Mail
M 2.44	Sichere Verpackung der Datenträger	B 5.2	(7.1)	(A)	Betrieb	Datenträgeraustausch
M 2.45	Regelung des Datenträgeraustausches	B 5.2	(7.1)	(A)	Betrieb	Datenträgeraustausch
M 2.46	Geeignetes Schlüsselmanagement	B 5.2	(7.1)	(A)	Planung	Datenträgeraustausch
		B 1.7	(3.7)	(A)	Umsetzg.	Kryptokonzept



		B 4.3	(7.2)	(Z)	Planung	Modem
		B 4.5	(8.4)	(Z)	Planung	LAN-Anbindung eines IT-Systems über ISDN
		B 5.2	(7.1)	(Z)	Planung	Datenträgeraustausch
		B 5.3	(7.4)	(Z)	Planung	E-Mail
M 2.47	Ernennung eines Fax-Verantwortlichen					
		B 3.402	(8.2)	(B)	Umsetzg.	Faxgerät
M 2.48	Festlegung berechtigter Faxbediener					
		B 3.402	(8.2)	(Z)	Betrieb	Faxgerät
M 2.49	Beschaffung geeigneter Faxgeräte					
		B 3.402	(8.2)	(A)	Beschaff.	Faxgerät
M 2.50	Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen					
		B 3.402	(8.2)	(B)	Aussnd.	Faxgerät
M 2.51	Fertigung von Kopien eingehender Faxesendungen					
		B 3.402	(8.2)	(Z)	Betrieb	Faxgerät
M 2.52	Versorgung und Kontrolle der Verbrauchsgüter					
		B 3.402	(8.2)	(C)	Betrieb	Faxgerät
M 2.53	Abschalten des Faxgerätes außerhalb der Bürozeiten					
		B 3.402	(8.2)	(Z)	Betrieb	Faxgerät
M 2.54	Beschaffung geeigneter Anrufbeantworter					
		B 3.403	(8.3)	(A)	Beschaff.	Anrufbeantworter
M 2.55	Einsatz eines Sicherungscodes					
		B 3.403	(8.3)	(Z)	Umsetzg.	Anrufbeantworter
M 2.56	Vermeidung schutzbedürftiger Informationen auf dem Anrufbeantworter					
		B 3.403	(8.3)	(A)	Betrieb	Anrufbeantworter
M 2.57	Regelmäßiges Abhören und Löschen aufgezeichneter Gespräche					
		B 3.403	(8.3)	(A)	Betrieb	Anrufbeantworter
M 2.58	Begrenzung der Sprechdauer					
		B 3.403	(8.3)	(Z)	Umsetzg.	Anrufbeantworter
M 2.59	Auswahl eines geeigneten Modems in der Beschaffung					
		B 4.3	(7.2)	(A)	Beschaff.	Modem
M 2.60	Sichere Administration eines Modems					
		B 4.3	(7.2)	(A)	Betrieb	Modem
M 2.61	Regelung des Modem-Einsatzes					
		B 4.3	(7.2)	(A)	Planung	Modem
M 2.62	Software-Abnahme- und Freigabe-Verfahren					
		B 1.9	(3.9)	(B)	Beschaff.	Hard- und Software-Management
M 2.63	Einrichten der Zugriffsrechte					
		B 3.202	(5.99)	(A)	Planung	Allgemeines nicht vernetztes IT-System
		B 3.206	(5.6)	(A)	Planung	Client unter Windows 95
M 2.64	Kontrolle der Protokolldateien					
		B 1.9	(3.9)	(A)	Betrieb	Hard- und Software-Management

M 2.65	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System	B 4.5	(8.4)	(A)	Betrieb	LAN-Anbindung eines IT-Systems über ISDN
		B 1.9	(3.9)	(C)	Betrieb	Hard- und Software-Management
		B 3.206	(5.6)	(Z)	Betrieb	Client unter Windows 95
		B 5.7	(9.2)	(B)	Betrieb	Datenbanken
M 2.66	Beachtung des Beitrags der Zertifizierung für die Beschaffung					
M 2.67	Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste	B 1.10	(9.1)	(Z)	Beschaff.	Standardsoftware
M 2.68	Sicherheitskontrollen durch die Benutzer beim Einsatz von Peer-to-Peer-Diensten	B 5.1	(6.3)	(A)	Planung	Peer-to-Peer-Dienste
M 2.69	Einrichtung von Standardarbeitsplätzen	B 5.1	(6.3)	(B)	Betrieb	Peer-to-Peer-Dienste
		B 1.9	(3.9)	(B)	Umsetzg.	Hard- und Software-Management
		B 2.11	(4.8)	(B)	Umsetzg.	Besprechungs-, Veranstaltungs- und Schulungsräume
M 2.70	Entwicklung eines Konzepts für Sicherheit Gateways					
M 2.71	Festlegung einer Policy für ein Sicherheit Gateway	B 3.301	(7.3)	(A)	Planung	Sicherheit Gateway (Firewall)
M 2.73	Auswahl geeigneter Grundstrukturen für Sicherheit Gateways	B 3.301	(7.3)	(A)	Planung	Sicherheit Gateway (Firewall)
M 2.74	Geeignete Auswahl eines Paketfilters	B 3.301	(7.3)	(A)	Beschaff.	Sicherheit Gateway (Firewall)
M 2.75	Geeignete Auswahl eines Application-Level-Gateways	B 3.301	(7.3)	(A)	Beschaff.	Sicherheit Gateway (Firewall)
M 2.76	Auswahl und Einrichtung geeigneter Filterregeln	B 3.301	(7.3)	(A)	Beschaff.	Sicherheit Gateway (Firewall)
M 2.77	Integration von Servern in das Sicherheit Gateway	B 3.301	(7.3)	(A)	Umsetzg.	Sicherheit Gateway (Firewall)
M 2.78	Sicherer Betrieb eines Sicherheit Gateways	B 3.301	(7.3)	(A)	Umsetzg.	Sicherheit Gateway (Firewall)
M 2.79	Festlegung der Verantwortlichkeiten im Bereich Standardsoftware	B 3.301	(7.3)	(A)	Betrieb	Sicherheit Gateway (Firewall)
M 2.80	Erstellung eines Anforderungskatalogs für Standardsoftware	B 1.10	(9.1)	(A)	Planung	Standardsoftware
		B 1.10	(9.1)	(A)	Planung	Standardsoftware
		B 5.7	(9.2)	(A)	Planung	Datenbanken
M 2.81	Vorauswahl eines geeigneten Standardsoftwareproduktes					
M 2.82	Entwicklung eines Testplans für Standardsoftware	B 1.10	(9.1)	(A)	Beschaff.	Standardsoftware
M 2.83	Testen von Standardsoftware	B 1.10	(9.1)	(B)	Planung	Standardsoftware

M 2.84	Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware	B 1.10	(9.1)	(B)	Umsetzg.	Standardsoftware
M 2.85	Freigabe von Standardsoftware	B 1.10	(9.1)	(A)	Umsetzg.	Standardsoftware
M 2.86	Sicherstellen der Integrität von Standardsoftware	B 1.10	(9.1)	(A)	Umsetzg.	Standardsoftware
M 2.87	Installation und Konfiguration von Standardsoftware	B 1.10	(9.1)	(B)	Umsetzg.	Standardsoftware
M 2.88	Lizenzverwaltung und Versionskontrolle von Standardsoftware	B 1.10	(9.1)	(A)	Umsetzg.	Standardsoftware
M 2.89	Deinstallation von Standardsoftware	B 1.10	(9.1)	(A)	Betrieb	Standardsoftware
M 2.90	Überprüfung der Lieferung	B 1.10	(9.1)	(C)	Aussnd.	Standardsoftware
M 2.91	Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz	B 1.10	(9.1)	(A)	Umsetzg.	Standardsoftware
M 2.92	Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz	B 3.103	(6.4)	(A)	Planung	Server unter Windows NT
M 2.93	Planung des Windows NT Netzes	B 3.103	(6.4)	(B)	Betrieb	Server unter Windows NT
M 2.94	Freigabe von Verzeichnissen unter Windows NT	B 3.103	(6.4)	(A)	Planung	Server unter Windows NT
M 2.95	Beschaffung geeigneter Schutzschranke	B 3.103	(6.4)	(B)	Umsetzg.	Server unter Windows NT
		B 5.1	(6.3)	(B)	Umsetzg.	Peer-to-Peer-Dienste
M 2.96	Verschluss von Schutzschranken	B 2.7	(4.4)	(A)	Beschaff.	Schutzschrank
M 2.97	Korrektur Umgang mit Codeschlössern	B 2.7	(4.4)	(A)	Betrieb	Schutzschrank
M 2.98	Sichere Installation von Novell Netware Servern	B 2.7	(4.4)	(A)	Betrieb	Schutzschrank
M 2.99	Sichere Einrichtung von Novell Netware Servern	B 3.104	(6.5)	(A)	Umsetzg.	Server unter Novell Netware 3.x
M 2.100	Sicherer Betrieb von Novell Netware Servern	B 3.104	(6.5)	(A)	Planung	Server unter Novell Netware 3.x
M 2.101	Revision von Novell Netware Servern	B 3.104	(6.5)	(A)	Betrieb	Server unter Novell Netware 3.x
M 2.102	Verzicht auf die Aktivierung der Remote Console	B 3.104	(6.5)	(B)	Betrieb	Server unter Novell Netware 3.x
		B 3.104	(6.5)	(Z)	Umsetzg.	Server unter Novell Netware 3.x
		B 3.105	(6.6)	(Z)	Umsetzg.	Server unter Novell Netware 4.x

M 2.103	Einrichten von Benutzerprofilen unter Windows 95	B 3.206	(5.6)	(A)	Planung	Client unter Windows 95
M 2.104	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95	B 3.206	(5.6)	(Z)	Planung	Client unter Windows 95
M 2.105	Beschaffung von TK-Anlagen	B 3.401	(8.1)	(A)	Beschaff.	TK-Anlage
M 2.106	Auswahl geeigneter ISDN-Karten in der Beschaffung	B 4.5	(8.4)	(A)	Beschaff.	LAN-Anbindung eines IT-Systems über ISDN
M 2.107	Dokumentation der ISDN-Karten-Konfiguration	B 4.5	(8.4)	(A)	Umsetzg.	LAN-Anbindung eines IT-Systems über ISDN
M 2.108	Verzicht auf Fernwartung der ISDN-Netzkoppelelemente	B 4.5	(8.4)	(Z)	Planung	LAN-Anbindung eines IT-Systems über ISDN
M 2.109	Rechtevergabe für den Fernzugriff	B 4.5	(8.4)	(A)	Umsetzg.	LAN-Anbindung eines IT-Systems über ISDN
M 2.110	Datenschutzaspekte bei der Protokollierung	B 1.9	(3.9)	(A)	Betrieb	Hard- und Software-Management
M 2.111	Bereithalten von Handbüchern	B 1.9	(3.9)	(A)	Umsetzg.	Hard- und Software-Management
M 2.112	Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution	B 2.8	(4.5)	(A)	Umsetzg.	Häuslicher Arbeitsplatz
M 2.113	Regelungen für Telearbeit	B 5.8	(9.3)	(A)	Planung	Telearbeit
M 2.114	Informationsfluss zwischen Telearbeiter und Institution	B 5.8	(9.3)	(A)	Planung	Telearbeit
M 2.115	Betreuungs- und Wartungskonzept für Telearbeitsplätze	B 5.8	(9.3)	(B)	Planung	Telearbeit
M 2.116	Geregelte Nutzung der Kommunikationsmöglichkeiten	B 5.8	(9.3)	(A)	Planung	Telearbeit
M 2.117	Regelung der Zugriffsmöglichkeiten des Telearbeiters	B 5.8	(9.3)	(A)	Planung	Telearbeit
M 2.118	Konzeption der sicheren E-Mail-Nutzung	B 5.3	(7.4)	(A)	Planung	E-Mail
M 2.119	Regelung für den Einsatz von E-Mail	B 5.3	(7.4)	(A)	Planung	E-Mail
M 2.120	Einrichtung einer Poststelle	B 5.3	(7.4)	(A)	Umsetzg.	E-Mail
M 2.121	Regelmäßiges Löschen von E-Mails	B 5.3	(7.4)	(B)	Betrieb	E-Mail
M 2.122	Einheitliche E-Mail-Adressen	B 5.3	(7.4)	(B)	Planung	E-Mail

M 2.123	Auswahl eines Mailproviders						
		B 5.3	(7.4)	(B)	Beschaff.	E-Mail	
M 2.124	Geeignete Auswahl einer Datenbank-Software						
		B 5.7	(9.2)	(A)	Beschaff.	Datenbanken	
M 2.125	Installation und Konfiguration einer Datenbank						
		B 5.7	(9.2)	(A)	Umsetzg.	Datenbanken	
M 2.126	Erstellung eines Datenbanksicherheitskonzeptes						
		B 5.7	(9.2)	(A)	Planung	Datenbanken	
M 2.127	Inferenzprävention						
		B 5.7	(9.2)	(B)	Umsetzg.	Datenbanken	
M 2.128	Zugangskontrolle einer Datenbank						
		B 5.7	(9.2)	(A)	Umsetzg.	Datenbanken	
M 2.129	Zugriffskontrolle einer Datenbank						
		B 5.7	(9.2)	(A)	Umsetzg.	Datenbanken	
M 2.130	Gewährleistung der Datenbankintegrität						
		B 5.7	(9.2)	(A)	Betrieb	Datenbanken	
M 2.131	Aufteilung von Administrationstätigkeiten bei Datenbanksystemen						
		B 5.7	(9.2)	(C)	Planung	Datenbanken	
M 2.132	Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen						
		B 5.7	(9.2)	(A)	Planung	Datenbanken	
M 2.133	Kontrolle der Protokolldateien eines Datenbanksystems						
		B 5.7	(9.2)	(A)	Betrieb	Datenbanken	
M 2.134	Richtlinien für Datenbank-Anfragen						
		B 5.7	(9.2)	(B)	Planung	Datenbanken	
M 2.135	Gesicherte Datenübernahme in eine Datenbank						
		B 5.7	(9.2)	(C)	Umsetzg.	Datenbanken	
M 2.136	Einhaltung von Regelungen bzgl. Arbeitsplatz und Arbeitsumgebung						
		B 2.8	(4.5)	(A)	Betrieb	Häuslicher Arbeitsplatz	
		B 2.10	(4.7)	(A)	Betrieb	Mobiler Arbeitsplatz	
M 2.137	Beschaffung eines geeigneten Datensicherungssystems						
		B 1.4	(3.4)	(A)	Beschaff.	Datensicherungskonzept	
M 2.138	Strukturierte Datenhaltung						
		B 1.9	(3.9)	(B)	Umsetzg.	Hard- und Software-Management	
		B 3.101	(6.1)	(B)	Umsetzg.	Allgemeiner Server	
M 2.139	Ist-Aufnahme der aktuellen Netzsituation						
		B 4.1	(6.7)	(A)	Planung	Heterogene Netze	
M 2.140	Analyse der aktuellen Netzsituation						
		B 4.1	(6.7)	(Z)	Planung	Heterogene Netze	
M 2.141	Entwicklung eines Netzkonzeptes						
		B 4.1	(6.7)	(B)	Planung	Heterogene Netze	
M 2.142	Entwicklung eines Netz-Realisierungsplans						

M 2.143	Entwicklung eines Netzmanagementkonzeptes	B 4.1	(6.7)	(B)	Planung	Heterogene Netze
M 2.144	Geeignete Auswahl eines Netzmanagement-Protokolls	B 4.2	(6.8)	(A)	Planung	Netz- und Systemmanagement
M 2.145	Anforderungen an ein Netzmanagement-Tool	B 4.2	(6.8)	(A)	Planung	Netz- und Systemmanagement
M 2.146	Sicherer Betrieb eines Netzmanagementsystems	B 4.2	(6.8)	(B)	Beschaff.	Netz- und Systemmanagement
M 2.147	Sichere Migration von Novell Netware 3.x Servern in Novell Netware 4.x Netze	B 4.2	(6.8)	(A)	Betrieb	Netz- und Systemmanagement
M 2.148	Sichere Einrichtung von Novell Netware 4.x Netzen	B 3.105	(6.6)	(A)	Umsetzg.	Server unter Novell Netware 4.x
M 2.149	Sicherer Betrieb von Novell Netware 4.x Netzen	B 3.105	(6.6)	(A)	Planung	Server unter Novell Netware 4.x
M 2.150	Revision von Novell Netware 4.x Netzen	B 3.105	(6.6)	(A)	Betrieb	Server unter Novell Netware 4.x
M 2.151	Entwurf eines NDS-Konzeptes	B 3.105	(6.6)	(B)	Betrieb	Server unter Novell Netware 4.x
M 2.152	Entwurf eines Zeitsynchronisations-Konzeptes	B 3.105	(6.6)	(A)	Planung	Server unter Novell Netware 4.x
M 2.153	Dokumentation von Novell Netware 4.x Netzen	B 3.105	(6.6)	(B)	Planung	Server unter Novell Netware 4.x
M 2.154	Erstellung eines Computer-Virenschutzkonzepts	B 3.105	(6.6)	(A)	Planung	Server unter Novell Netware 4.x
M 2.155	Identifikation potentiell von Computer-Viren betroffener IT-Systeme	B 1.6	(3.6)	(A)	Planung	Computer-Virenschutzkonzept
M 2.156	Auswahl einer geeigneten Computer-Virenschutz-Strategie	B 1.6	(3.6)	(A)	Planung	Computer-Virenschutzkonzept
M 2.157	Auswahl eines geeigneten Computer-Viren-Suchprogramms	B 1.6	(3.6)	(A)	Planung	Computer-Virenschutzkonzept
M 2.158	Meldung von Computer-Virusinfektionen	B 1.6	(3.6)	(A)	Beschaff.	Computer-Virenschutzkonzept
M 2.159	Aktualisierung der eingesetzten Computer-Viren-Suchprogramme	B 1.6	(3.6)	(A)	Betrieb	Computer-Virenschutzkonzept
M 2.160	Regelungen zum Computer-Virenschutz	B 1.6	(3.6)	(A)	Betrieb	Computer-Virenschutzkonzept
M 2.161	Entwicklung eines Kryptokonzepts	B 1.6	(3.6)	(A)	Planung	Computer-Virenschutzkonzept
M 2.162	Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte	B 1.7	(3.7)	(A)	Planung	Kryptokonzept
		B 1.7	(3.7)	(A)	Planung	Kryptokonzept

M 2.163	Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte						
		B 1.7	(3.7)	(A)	Planung	Kryptokonzept	
M 2.164	Auswahl eines geeigneten kryptographischen Verfahrens						
		B 1.7	(3.7)	(A)	Planung	Kryptokonzept	
M 2.165	Auswahl eines geeigneten kryptographischen Produktes						
		B 1.7	(3.7)	(A)	Beschaff.	Kryptokonzept	
M 2.166	Regelung des Einsatzes von Kryptomodulen						
		B 1.7	(3.7)	(A)	Planung	Kryptokonzept	
M 2.167	Sicheres Löschen von Datenträgern						
		B 1.9	(3.9)	(B)	Aussnd.	Hard- und Software-Management	
M 2.168	IT-System-Analyse vor Einführung eines Systemmanagementsystems						
		B 4.2	(6.8)	(A)	Planung	Netz- und Systemmanagement	
M 2.169	Entwickeln einer Systemmanagementstrategie						
		B 4.2	(6.8)	(A)	Planung	Netz- und Systemmanagement	
M 2.170	Anforderungen an ein Systemmanagementsystem						
		B 4.2	(6.8)	(A)	Beschaff.	Netz- und Systemmanagement	
M 2.171	Geeignete Auswahl eines Systemmanagement-Produktes						
		B 4.2	(6.8)	(A)	Beschaff.	Netz- und Systemmanagement	
M 2.172	Entwicklung eines Konzeptes für die WWW-Nutzung						
		B 5.4	(7.5)	(A)	Planung	Webserver	
M 2.173	Festlegung einer WWW-Sicherheitsstrategie						
		B 5.4	(7.5)	(A)	Planung	Webserver	
M 2.174	Sicherer Betrieb eines WWW-Servers						
		B 5.4	(7.5)	(A)	Betrieb	Webserver	
M 2.175	Aufbau eines WWW-Servers						
		B 5.4	(7.5)	(A)	Planung	Webserver	
M 2.176	Geeignete Auswahl eines Internet Service Providers						
		B 5.4	(7.5)	(B)	Beschaff.	Webserver	
M 2.177	Sicherheit bei Umzügen						
		B 1.1	(3.1)	(Z)	Betrieb	Organisation	
M 2.178	Erstellung einer Sicherheitsleitlinie für die Faxnutzung						
		B 5.6	(8.5)	(A)	Planung	Faxserver	
M 2.179	Regelungen für den Faxserver-Einsatz						
		B 5.6	(8.5)	(A)	Planung	Faxserver	
M 2.180	Einrichten einer Fax-Poststelle						
		B 5.6	(8.5)	(A)	Umsetzg.	Faxserver	
M 2.181	Auswahl eines geeigneten Faxservers						
		B 5.6	(8.5)	(A)	Beschaff.	Faxserver	
M 2.182	Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen						
		B 1.9	(3.9)	(A)	Betrieb	Hard- und Software-Management	
M 2.183	Durchführung einer RAS-Anforderungsanalyse						

M 2.184	Entwicklung eines RAS-Konzeptes	B 4.4	(7.6)	(A)	Planung	Remote Access
M 2.185	Auswahl einer geeigneten RAS-Systemarchitektur	B 4.4	(7.6)	(A)	Planung	Remote Access
M 2.186	Geeignete Auswahl eines RAS-Produktes	B 4.4	(7.6)	(A)	Planung	Remote Access
M 2.187	Festlegen einer RAS-Sicherheitsrichtlinie	B 4.4	(7.6)	(A)	Beschaff.	Remote Access
M 2.188	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	B 4.4	(7.6)	(A)	Planung	Remote Access
M 2.189	Sperrung des Mobiltelefons bei Verlust	B 3.404	(8.6)	(A)	Planung	Mobiltelefon
M 2.190	Einrichtung eines Mobiltelefon-Pools	B 3.404	(8.6)	(A)	Betrieb	Mobiltelefon
M 2.192	Erstellung einer IT-Sicherheitsleitlinie	B 3.404	(8.6)	(Z)	Beschaff.	Mobiltelefon
M 2.193	Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit	B 1.0	(3.0)	(A)	Planung	IT-Sicherheitsmanagement
M 2.195	Erstellung eines IT-Sicherheitskonzeptes	B 1.0	(3.0)	(A)	Umsetzg.	IT-Sicherheitsmanagement
M 2.197	Integration der Mitarbeiter in den Sicherheitsprozess	B 1.0	(3.0)	(A)	Umsetzg.	IT-Sicherheitsmanagement
M 2.198	Sensibilisierung der Mitarbeiter für IT-Sicherheit	B 1.0	(3.0)	(A)	Umsetzg.	IT-Sicherheitsmanagement
M 2.199	Aufrechterhaltung der IT-Sicherheit	B 1.13	(3.11)	(A)	Betrieb	IT-Sicherheitssensibilisierung und -schulung
M 2.200	Managementreporte und -bewertungen der IT-Sicherheit	B 1.0	(3.0)	(A)	Betrieb	IT-Sicherheitsmanagement
M 2.201	Dokumentation des IT-Sicherheitsprozesses	B 1.0	(3.0)	(C)	Betrieb	IT-Sicherheitsmanagement
M 2.204	Verhinderung ungesicherter Netzzugänge	B 1.0	(3.0)	(C)	Betrieb	IT-Sicherheitsmanagement
M 2.205	Übertragung und Abruf personenbezogener Daten	B 1.9	(3.9)	(A)	Umsetzg.	Hard- und Software-Management
		B 2.11	(4.8)	(A)	Umsetzg.	Besprechungs-, Veranstaltungs- und Schulungsräume
		B 3.101	(6.1)	(A)	Betrieb	Allgemeiner Server
		B 3.201	(5.99)	(A)	Betrieb	Allgemeiner Client
		B 4.3	(7.2)	(A)	Umsetzg.	Modem
		B 4.5	(8.4)	(A)	Umsetzg.	LAN-Anbindung eines IT-Systems über ISDN
		B 4.4	(7.6)	(A)	Planung	Remote Access



M 2.206	Planung des Einsatzes von Lotus Notes	B 5.8	(9.3)	(C)	Planung	Telearbeit
M 2.207	Festlegen einer Sicherheitsrichtlinie für Lotus Notes	B 5.5	(7.7)	(A)	Planung	Lotus Notes
M 2.208	Planung der Domänen und der Zertifikathierarchie von Lotus Notes	B 5.5	(7.7)	(A)	Planung	Lotus Notes
M 2.209	Planung des Einsatzes von Lotus Notes im Intranet	B 5.5	(7.7)	(A)	Planung	Lotus Notes
M 2.210	Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff	B 5.5	(7.7)	(B)	Planung	Lotus Notes
M 2.211	Planung des Einsatzes von Lotus Notes in einer DMZ	B 5.5	(7.7)	(B)	Planung	Lotus Notes
M 2.212	Organisatorische Vorgaben für die Gebäudereinigung	B 5.5	(7.7)	(A)	Planung	Lotus Notes
M 2.213	Wartung der technischen Infrastruktur	B 2.9	(4.6)	(B)	Umsetzg.	Rechenzentrum
M 2.214	Konzeption des IT-Betriebs	B 2.9	(4.6)	(A)	Umsetzg.	Rechenzentrum
M 2.215	Fehlerbehandlung	B 1.9	(3.9)	(A)	Planung	Hard- und Software-Management
M 2.216	Genehmigungsverfahren für IT-Komponenten	B 1.9	(3.9)	(B)	Betrieb	Hard- und Software-Management
M 2.217	Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen	B 1.9	(3.9)	(C)	Planung	Hard- und Software-Management
M 2.218	Regelung der Mitnahme von Datenträgern und IT-Komponenten	B 1.9	(3.9)	(B)	Planung	Hard- und Software-Management
		B 1.9	(3.9)	(C)	Planung	Hard- und Software-Management
		B 2.10	(4.7)	(A)	Planung	Mobiler Arbeitsplatz
		B 3.203	(5.3)	(B)	Planung	Laptop
		B 3.405	(8.7)	(C)	Planung	PDA
M 2.219	Kontinuierliche Dokumentation der Informationsverarbeitung					
M 2.220	Richtlinien für die Zugriffs- bzw. Zugangskontrolle	B 1.9	(3.9)	(A)	Betrieb	Hard- und Software-Management
M 2.221	Änderungsmanagement	B 1.9	(3.9)	(A)	Planung	Hard- und Software-Management
		B 1.9	(3.9)	(B)	Planung	Hard- und Software-Management
M 2.223	Sicherheitsvorgaben für die Nutzung von Standardsoftware	B 1.11	(3.10)	(A)	Betrieb	Outsourcing
M 2.224	Vorbeugung gegen Trojanische Pferde	B 1.9	(3.9)	(B)	Planung	Hard- und Software-Management

M 2.225	Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten	B 1.6	(3.6)	(A)	Betrieb	Computer-Virenschutzkonzept
M 2.226	Regelungen für den Einsatz von Fremdpersonal	B 1.1	(3.1)	(B)	Planung	Organisation
M 2.227	Planung des Windows 2000 Einsatzes	B 1.9 B 1.11	(3.9) (3.10)	(A) (A)	Planung Planung	Hard- und Software-Management Outsourcing
M 2.228	Festlegen einer Windows 2000 Sicherheitsrichtlinie	B 3.106 B 3.207	(6.9) (5.7)	(A) (A)	Planung Planung	Server unter Windows 2000 Client unter Windows 2000
M 2.229	Planung des Active Directory	B 3.106 B 3.207	(6.9) (5.7)	(A) (A)	Planung Planung	Server unter Windows 2000 Client unter Windows 2000
M 2.230	Planung der Active Directory-Administration	B 3.106	(6.9)	(A)	Planung	Server unter Windows 2000
M 2.231	Planung der Gruppenrichtlinien unter Windows 2000	B 3.106	(6.9)	(A)	Planung	Server unter Windows 2000
M 2.232	Planung der Windows 2000 CA-Struktur	B 3.106 B 3.207	(6.9) (5.7)	(A) (A)	Planung Planung	Server unter Windows 2000 Client unter Windows 2000
M 2.233	Planung der Migration von Windows NT auf Windows 2000	B 3.106	(6.9)	(B)	Planung	Server unter Windows 2000
M 2.234	Konzeption von Internet-PCs	B 3.106	(6.9)	(B)	Planung	Server unter Windows 2000
M 2.235	Richtlinien für die Nutzung von Internet-PCs	B 3.208	(5.8)	(A)	Planung	Internet-PC
M 2.236	Planung des Einsatzes von Novell eDirectory	B 3.208	(5.8)	(A)	Planung	Internet-PC
M 2.237	Planung der Partitionierung und Replikation im Novell eDirectory	B 5.9	(9.4)	(A)	Planung	Novell eDirectory
M 2.238	Festlegung einer Sicherheitsrichtlinie für Novell eDirectory	B 5.9	(9.4)	(B)	Planung	Novell eDirectory
M 2.239	Planung des Einsatzes von Novell eDirectory im Intranet	B 5.9	(9.4)	(A)	Planung	Novell eDirectory
M 2.240	Planung des Einsatzes von Novell eDirectory im Extranet	B 5.9	(9.4)	(A)	Planung	Novell eDirectory
M 2.241	Durchführung einer Anforderungsanalyse für den Telearbeitsplatz	B 5.9	(9.4)	(A)	Planung	Novell eDirectory
M 2.242	Zielsetzung der elektronischen Archivierung	B 5.8	(9.3)	(C)	Planung	Telearbeit

M 2.243	Entwicklung des Archivierungskonzepts	B 1.12	(9.5)	(A)	Planung	Archivierung
M 2.244	Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung	B 1.12	(9.5)	(A)	Planung	Archivierung
M 2.245	Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung	B 1.12	(9.5)	(A)	Planung	Archivierung
M 2.246	Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung	B 1.12	(9.5)	(A)	Planung	Archivierung
M 2.247	Planung des Einsatzes von Exchange/Outlook 2000	B 1.12	(9.5)	(A)	Planung	Archivierung
M 2.248	Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000	B 5.12	(7.10)	(A)	Planung	Exchange 2000 / Outlook 2000
M 2.249	Planung der Migration von "Exchange 5.5-Servern" nach "Exchange 2000"	B 5.12	(7.10)	(A)	Planung	Exchange 2000 / Outlook 2000
M 2.250	Festlegung einer Outsourcing-Strategie	B 5.12	(7.10)	(B)	Planung	Exchange 2000 / Outlook 2000
M 2.251	Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben	B 1.11	(3.10)	(A)	Planung	Outsourcing
M 2.252	Wahl eines geeigneten Outsourcing-Dienstleisters	B 1.11	(3.10)	(A)	Planung	Outsourcing
M 2.253	Vertragsgestaltung mit dem Outsourcing-Dienstleister	B 1.11	(3.10)	(A)	Beschaff.	Outsourcing
M 2.254	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben	B 1.11	(3.10)	(A)	Umsetzg.	Outsourcing
M 2.255	Sichere Migration bei Outsourcing-Vorhaben	B 1.11	(3.10)	(A)	Planung	Outsourcing
M 2.256	Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb	B 1.11	(3.10)	(A)	Umsetzg.	Outsourcing
M 2.257	Überwachung der Speicherressourcen von Archivmedien	B 1.11	(3.10)	(A)	Betrieb	Outsourcing
M 2.258	Konsistente Indizierung von Dokumenten bei der Archivierung	B 1.12	(9.5)	(C)	Betrieb	Archivierung
M 2.259	Einführung eines übergeordneten Dokumentenmanagements	B 1.12	(9.5)	(A)	Betrieb	Archivierung
M 2.260	Regelmäßige Revision des Archivierungsprozesses	B 1.12	(9.5)	(Z)	Planung	Archivierung
M 2.261	Regelmäßige Marktbeobachtung von Archivsystemen	B 1.12	(9.5)	(B)	Betrieb	Archivierung
		B 1.12	(9.5)	(B)	Betrieb	Archivierung

M 2.262	Regelung der Nutzung von Archivsystemen					
		B 1.12	(9.5)	(A)	Planung	Archivierung
M 2.263	Regelmäßige Aufbereitung von archivierten Datenbeständen					
		B 1.12	(9.5)	(A)	Betrieb	Archivierung
M 2.264	Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung					
		B 1.12	(9.5)	(B)	Betrieb	Archivierung
M 2.265	Geeigneter Einsatz digitaler Signaturen bei der Archivierung					
		B 1.12	(9.5)	(Z)	Planung	Archivierung
M 2.266	Regelmäßige Erneuerung technischer Archivsystem-Komponenten					
		B 1.12	(9.5)	(C)	Umsetzg.	Archivierung
M 2.267	Planen des IIS-Einsatzes					
		B 5.10	(7.8)	(A)	Planung	Internet Information Server
M 2.268	Festlegung einer IIS-Sicherheitsrichtlinie					
		B 5.10	(7.8)	(A)	Planung	Internet Information Server
M 2.269	Planung des Einsatzes eines Apache Webservers					
		B 5.11	(7.9)	(A)	Planung	Apache Webserver
M 2.270	Planung des SSL-Einsatzes beim Apache Webserver (zusätzlich)					
		B 5.11	(7.9)	(Z)	Planung	Apache Webserver
M 2.271	Festlegung einer Sicherheitsstrategie für den WWW-Zugang					
		B 5.4	(7.5)	(A)	Planung	Webserver
M 2.272	Einrichtung eines WWW-Redaktionsteams					
		B 5.4	(7.5)	(A)	Planung	Webserver
M 2.273	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates					
		B 3.101	(6.1)	(A)	Betrieb	Allgemeiner Server
		B 3.201	(5.99)	(A)	Betrieb	Allgemeiner Client
		B 5.4	(7.5)	(A)	Betrieb	Webserver
M 2.274	Vertretungsregelungen bei E-Mail-Nutzung					
		B 5.3	(7.4)	(A)	Planung	E-Mail
M 2.275	Einrichtung funktionsbezogener E-Mailadressen					
		B 5.3	(7.4)	(Z)	Umsetzg.	E-Mail
M 2.276	Funktionsweise eines Routers					
		B 3.302	(7.11)	(Z)	Planung	Router und Switches
M 2.277	Funktionsweise eines Switches					
		B 3.302	(7.11)	(Z)	Planung	Router und Switches
M 2.278	Typische Einsatzszenarien von Routern und Switches					
		B 3.302	(7.11)	(Z)	Planung	Router und Switches
M 2.279	Erstellung einer Sicherheitsrichtlinie für Router und Switches					
		B 3.302	(7.11)	(A)	Planung	Router und Switches
M 2.280	Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches					
		B 3.302	(7.11)	(C)	Beschaff.	Router und Switches
M 2.281	Dokumentation der Systemkonfiguration von Routern und Switches					

		B 3.302	(7.11)	(A)	Betrieb	Router und Switches
M 2.282	Regelmäßige Kontrolle von Routern und Switches	B 3.302	(7.11)	(A)	Betrieb	Router und Switches
M 2.283	Software-Pflege auf Routern und Switches	B 3.302	(7.11)	(B)	Betrieb	Router und Switches
M 2.284	Sichere Außerbetriebnahme von Routern und Switches	B 3.302	(7.11)	(C)	Aussnd.	Router und Switches
M 2.285	Festlegung von Standards für z/OS-Systemdefinitionen	B 3.107	(6.10)	(Z)	Planung	S/390- und zSeries-Mainframe
M 2.286	Planung und Einsatz von zSeries-Systemen	B 3.107	(6.10)	(Z)	Planung	S/390- und zSeries-Mainframe
M 2.287	Batch-Job-Planung für z/OS-Systeme	B 3.107	(6.10)	(Z)	Planung	S/390- und zSeries-Mainframe
M 2.288	Erstellung von Sicherheitsrichtlinien für z/OS-Systeme	B 3.107	(6.10)	(B)	Planung	S/390- und zSeries-Mainframe
M 2.289	Einsatz restriktiver z/OS-Kennungen	B 3.107	(6.10)	(A)	Umsetzg.	S/390- und zSeries-Mainframe
M 2.290	Einsatz von RACF-Exits	B 3.107	(6.10)	(Z)	Umsetzg.	S/390- und zSeries-Mainframe
M 2.291	Sicherheits-Berichtswesen und -Audits unter z/OS	B 3.107	(6.10)	(C)	Betrieb	S/390- und zSeries-Mainframe
M 2.292	Überwachung von z/OS-Systemen	B 3.107	(6.10)	(B)	Betrieb	S/390- und zSeries-Mainframe
M 2.293	Wartung von zSeries-Systemen	B 3.107	(6.10)	(C)	Betrieb	S/390- und zSeries-Mainframe
M 2.294	Synchronisierung von z/OS-Passwörtern und RACF-Kommandos	B 3.107	(6.10)	(Z)	Betrieb	S/390- und zSeries-Mainframe
M 2.295	Systemverwaltung von z/OS-Systemen	B 3.107	(6.10)	(A)	Planung	S/390- und zSeries-Mainframe
M 2.296	Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren	B 3.107	(6.10)	(Z)	Planung	S/390- und zSeries-Mainframe
M 2.297	Deinstallation von z/OS-Systemen	B 3.107	(6.10)	(B)	Aussnd.	S/390- und zSeries-Mainframe
M 2.298	Verwaltung von Internet-Domainnamen	B 5.4	(7.5)	(Z)	Betrieb	Webserver
M 2.299	Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway	B 3.301	(7.3)	(A)	Beschaff.	Sicherheitsgateway (Firewall)
M 2.300	Sichere Außerbetriebnahme oder Ersatz von Komponenten eines Sicherheitsgateways	B 3.301	(7.3)	(C)	Aussnd.	Sicherheitsgateway (Firewall)
M 2.301	Outsourcing des Sicherheitsgateway					

M 2.302	Sicherheitsgateways und Hochverfügbarkeit	B 3.301	(7.3)	(Z)	Planung	Sicherheitsgateway (Firewall)
M 2.303	Festlegung einer Strategie für den Einsatz von PDAs	B 3.301	(7.3)	(Z)	Betrieb	Sicherheitsgateway (Firewall)
M 2.304	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung	B 3.405	(8.7)	(A)	Planung	PDA
M 2.305	Geeignete Auswahl von PDAs	B 3.405	(8.7)	(A)	Planung	PDA
M 2.306	Verlustmeldung	B 3.405	(8.7)	(B)	Beschaff.	PDA
M 2.307	Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses	B 3.203	(5.3)	(B)	Aussnd.	Laptop
		B 3.405	(8.7)	(A)	Aussnd.	PDA
M 2.308	Auszug aus Gebäuden	B 1.11	(3.10)	(A)	Aussnd.	Outsourcing
M 2.309	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung	B 2.1	(4.1)	(Z)	Aussnd.	Gebäude
M 2.310	Geeignete Auswahl von Laptops	B 2.10	(4.7)	(C)	Planung	Mobiler Arbeitsplatz
		B 3.203	(5.3)	(A)	Planung	Laptop
M 2.311	Planung von Schutzschranken	B 3.203	(5.3)	(A)	Beschaff.	Laptop
M 2.312	Konzeption eines Schulungs- und Sensibilisierungsprogramms zur IT-Sicherheit	B 2.7	(4.4)	(A)	Planung	Schutzschrank
M 2.313	Sichere Anmeldung bei Internet-Diensten	B 1.13	(3.11)	(A)	Planung	IT-Sicherheitssensibilisierung und -schulung
M 2.314	Verwendung von hochverfügbaren Architekturen für Server	B 3.208	(5.8)	(A)	Betrieb	Internet-PC
M 2.315	Planung des Servereinsatzes	B 3.101	(6.1)	(Z)	Planung	Allgemeiner Server
M 2.316	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server	B 3.101	(6.1)	(A)	Planung	Allgemeiner Server
M 2.317	Beschaffungskriterien für einen Server	B 3.101	(6.1)	(A)	Planung	Allgemeiner Server
M 2.318	Sichere Installation eines Servers	B 3.101	(6.1)	(C)	Beschaff.	Allgemeiner Server
M 2.319	Migration eines Servers	B 3.101	(6.1)	(A)	Umsetzg.	Allgemeiner Server
M 2.320	Geregelte Außerbetriebnahme eines Servers	B 3.101	(6.1)	(C)	Aussnd.	Allgemeiner Server
		B 3.101	(6.1)	(A)	Aussnd.	Allgemeiner Server

M 2.321	Planung des Einsatzes von Client-Server-Netzen						
		B 3.201	(5.99)	(A)	Planung	Allgemeiner Client	
M 2.322	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz						
		B 3.201	(5.99)	(A)	Planung	Allgemeiner Client	
M 2.323	Geregelte Außerbetriebnahme eines Clients						
		B 3.201	(5.99)	(A)	Aussnd.	Allgemeiner Client	
M 2.324	Einführung von Windows XP planen						
		B 3.209	(5.9)	(A)	Planung	Client unter Windows XP	
M 2.325	Planung der Windows XP Sicherheitsrichtlinie						
		B 3.209	(5.9)	(A)	Planung	Client unter Windows XP	
M 2.326	Planung der Windows XP Gruppenrichtlinien						
		B 3.209	(5.9)	(A)	Planung	Client unter Windows XP	
M 2.327	Sicherheit beim Fernzugriff unter Windows XP						
		B 3.209	(5.9)	(B)	Planung	Client unter Windows XP	
M 2.328	Einsatz von Windows XP auf mobilen Rechnern						
		B 3.209	(5.9)	(B)	Planung	Client unter Windows XP	
M 2.329	Einführung von Windows XP SP2						
		B 3.209	(5.9)	(A)	Betrieb	Client unter Windows XP	
M 2.330	Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung						
		B 3.209	(5.9)	(B)	Betrieb	Client unter Windows XP	
M 2.331	Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen						
		B 2.11	(4.8)	(A)	Planung	Besprechungs-, Veranstaltungs- und Schulungsräume	
M 2.332	Einrichtung von Besprechungs-, Vortrags- und Schulungsräumen						
		B 2.11	(4.8)	(B)	Planung	Besprechungs-, Veranstaltungs- und Schulungsräume	
M 2.333	Sichere Nutzung von Besprechungs-, Vortrags- und Schulungsräumen						
		B 2.11	(4.8)	(A)	Umsetzg.	Besprechungs-, Veranstaltungs- und Schulungsräume	
M 2.334	Auswahl eines geeigneten Gebäudes						
		B 2.1	(4.1)	(Z)	Planung	Gebäude	
M 2.335	Festlegung der IT-Sicherheitsziele und -strategie						
		B 1.0	(3.0)	(A)	Planung	IT-Sicherheitsmanagement	
M 2.336	Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene						
		B 1.0	(3.0)	(A)	Planung	IT-Sicherheitsmanagement	
M 2.337	Integration der IT-Sicherheit in organisationsweite Abläufe und Prozesse						
		B 1.0	(3.0)	(A)	Umsetzg.	IT-Sicherheitsmanagement	
M 2.338	Erstellung von zielgruppengerechten IT-Sicherheitsrichtlinien						
		B 1.0	(3.0)	(Z)	Umsetzg.	IT-Sicherheitsmanagement	
M 2.339	Wirtschaftlicher Einsatz von Ressourcen für IT-Sicherheit						
		B 1.0	(3.0)	(Z)	Umsetzg.	IT-Sicherheitsmanagement	

M 2.340	Beachtung rechtlicher Rahmenbedingungen					
		B 1.0	(3.0)	(A)	Betrieb	IT-Sicherheitsmanagement
M 3.1	Geregelte Einarbeitung/Einweisung neuer Mitarbeiter					
		B 1.2	(3.2)	(A)	Umsetzg.	Personal
M 3.2	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen					
		B 1.2	(3.2)	(A)	Umsetzg.	Personal
		B 1.12	(9.5)	(A)	Umsetzg.	Archivierung
M 3.3	Vertretungsregelungen					
		B 1.2	(3.2)	(A)	Betrieb	Personal
M 3.4	Schulung vor Programmnutzung					
		B 1.2	(3.2)	(A)	Betrieb	Personal
		B 1.13	(3.11)	(A)	Betrieb	IT-Sicherheitssensibilisierung und -schulung
M 3.5	Schulung zu IT-Sicherheitsmaßnahmen					
		B 1.2	(3.2)	(A)	Betrieb	Personal
		B 1.13	(3.11)	(A)	Umsetzg.	IT-Sicherheitssensibilisierung und -schulung
M 3.6	Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern					
		B 1.2	(3.2)	(A)	Aussnd.	Personal
M 3.7	Anlaufstelle bei persönlichen Problemen					
		B 1.2	(3.2)	(Z)	Betrieb	Personal
M 3.8	Vermeidung von Störungen des Betriebsklimas					
		B 1.2	(3.2)	(Z)	Betrieb	Personal
M 3.9	Ergonomischer Arbeitsplatz					
		B 2.3	(4.3.1)	(Z)	Planung	Bürraum
		B 2.8	(4.5)	(Z)	Planung	Häuslicher Arbeitsplatz
		B 2.11	(4.8)	(Z)	Planung	Besprechungs-, Veranstaltungs- und Schulungsräume
M 3.10	Auswahl eines vertrauenswürdigen Administrators und Vertreters					
		B 1.2	(3.2)	(A)	Umsetzg.	Personal
M 3.11	Schulung des Wartungs- und Administrationspersonals					
		B 1.2	(3.2)	(A)	Betrieb	Personal
		B 1.13	(3.11)	(A)	Betrieb	IT-Sicherheitssensibilisierung und -schulung
M 3.12	Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne					
		B 3.401	(8.1)	(B)	Betrieb	TK-Anlage
M 3.13	Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen					
		B 3.401	(8.1)	(B)	Betrieb	TK-Anlage
M 3.14	Einweisung des Personals in den geregelten Ablauf eines Datenträgeraustausches					
		B 5.2	(7.1)	(B)	Betrieb	Datenträgeraustausch
M 3.15	Informationen für alle Mitarbeiter über die Faxnutzung					
		B 3.402	(8.2)	(A)	Umsetzg.	Faxgerät



M 3.16	Einweisung in die Bedienung des Anrufbeantworters	B 5.6	(8.5)	(A)	Betrieb	Faxserver
M 3.17	Einweisung des Personals in die Modem-Benutzung	B 3.403	(8.3)	(A)	Umsetzg.	Anrufbeantworter
M 3.18	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung	B 4.3	(7.2)	(A)	Betrieb	Modem
		B 3.201	(5.99)	(A)	Betrieb	Allgemeiner Client
		B 3.202	(5.99)	(A)	Betrieb	Allgemeines nicht vernetztes IT-System
		B 3.206	(5.6)	(A)	Betrieb	Client unter Windows 95
		B 5.7	(9.2)	(A)	Betrieb	Datenbanken
M 3.19	Einweisung in den richtigen Einsatz der Sicherheitsfunktionen von Peer-to-Peer-Diensten					
		B 5.1	(6.3)	(A)	Umsetzg.	Peer-to-Peer-Dienste
M 3.20	Einweisung in die Bedienung von Schutzschranken					
		B 2.7	(4.4)	(A)	Umsetzg.	Schutzschrank
M 3.21	Sicherheitstechnische Einweisung und Fortbildung des Telearbeiters					
		B 5.8	(9.3)	(A)	Betrieb	Telearbeit
M 3.22	Vertretungsregelung für Telearbeit					
		B 5.8	(9.3)	(B)	Betrieb	Telearbeit
M 3.23	Einführung in kryptographische Grundbegriffe					
		B 1.7	(3.7)	(A)	Planung	Kryptokonzept
M 3.24	Schulung zur Lotus Notes Systemarchitektur für Administratoren					
		B 5.5	(7.7)	(A)	Umsetzg.	Lotus Notes
M 3.25	Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer					
		B 5.5	(7.7)	(A)	Umsetzg.	Lotus Notes
M 3.26	Einweisung des Personals in den sicheren Umgang mit IT					
		B 1.9	(3.9)	(A)	Betrieb	Hard- und Software-Management
		B 1.13	(3.11)	(A)	Betrieb	IT-Sicherheitssensibilisierung und -schulung
M 3.27	Schulung zur Active Directory-Verwaltung					
		B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
M 3.28	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer					
		B 3.207	(5.7)	(A)	Umsetzg.	Client unter Windows 2000
		B 3.209	(5.9)	(A)	Planung	Client unter Windows XP
M 3.29	Schulung zur Administration von Novell eDirectory					
		B 5.9	(9.4)	(A)	Umsetzg.	Novell eDirectory
M 3.30	Schulung zum Einsatz von Novell eDirectory Clientsoftware					
		B 5.9	(9.4)	(A)	Umsetzg.	Novell eDirectory
M 3.31	Schulung zur Systemarchitektur und Sicherheit von Exchange 2000 für Administratoren					
		B 5.12	(7.10)	(A)	Umsetzg.	Exchange 2000 / Outlook 2000
M 3.32	Schulung zu Sicherheitsmechanismen von Outlook 2000 für Benutzer					

M 3.33	Sicherheitsüberprüfung von Mitarbeitern	B 5.12	(7.10)	(A)	Umsetzg.	Exchange 2000 / Outlook 2000
		B 1.2	(3.2)	(Z)	Umsetzg.	Personal
		B 1.11	(3.10)	(Z)	Betrieb	Outsourcing
M 3.34	Einweisung in die Administration des Archivsystems	B 1.12	(9.5)	(A)	Umsetzg.	Archivierung
M 3.35	Einweisung der Benutzer in die Bedienung des Archivsystems	B 1.12	(9.5)	(A)	Umsetzg.	Archivierung
M 3.36	Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS	B 5.10	(7.8)	(A)	Umsetzg.	Internet Information Server
M 3.37	Schulung der Administratoren eines Apache-Webserver	B 5.11	(7.9)	(A)	Umsetzg.	Apache Webserver
M 3.38	Administratorenschulung für Router und Switches	B 3.302	(7.11)	(B)	Umsetzg.	Router und Switches
M 3.39	Einführung in die zSeries-Plattform	B 3.107	(6.10)	(A)	Planung	S/390- und zSeries-Mainframe
M 3.40	Einführung in das z/OS-Betriebssystem	B 3.107	(6.10)	(A)	Planung	S/390- und zSeries-Mainframe
M 3.41	Einführung in Linux und z/VM für zSeries-Systeme	B 3.107	(6.10)	(A)	Planung	S/390- und zSeries-Mainframe
M 3.42	Schulung des z/OS-Bedienungspersonals	B 3.107	(6.10)	(A)	Umsetzg.	S/390- und zSeries-Mainframe
M 3.43	Schulung der Administratoren des Sicherheitgateways	B 3.301	(7.3)	(C)	Umsetzg.	Sicherheitsgateway (Firewall)
M 3.44	Sensibilisierung des Managements für IT-Sicherheit	B 1.13	(3.11)	(A)	Planung	IT-Sicherheitssensibilisierung und -schulung
M 3.45	Planung von Schulungsinhalten zur IT-Sicherheit	B 1.13	(3.11)	(A)	Umsetzg.	IT-Sicherheitssensibilisierung und -schulung
M 3.46	Ansprechpartner zu Sicherheitsfragen	B 1.13	(3.11)	(A)	Umsetzg.	IT-Sicherheitssensibilisierung und -schulung
M 3.47	Durchführung von Planspielen zur IT-Sicherheit	B 1.13	(3.11)	(Z)	Betrieb	IT-Sicherheitssensibilisierung und -schulung
M 3.48	Auswahl von Trainern oder Schulungsanbietern	B 1.13	(3.11)	(A)	Beschaff.	IT-Sicherheitssensibilisierung und -schulung
M 3.49	Schulung zur Vorgehensweise nach IT-Grundschutz	B 1.13	(3.11)	(B)	Umsetzg.	IT-Sicherheitssensibilisierung und -schulung
M 3.50	Auswahl von Personal	B 1.2	(3.2)	(Z)	Beschaff.	Personal
M 3.51	Geeignetes Konzept für Personaleinsatz und -qualifizierung	B 1.2	(3.2)	(Z)	Planung	Personal
M 4.1	Passwortschutz für IT-Systeme					

M 4.2	Bildschirmsperre	B 1.9	(3.9)	(A)	Umsetzg.	Hard- und Software-Management
		B 3.201	(5.99)	(A)	Umsetzg.	Allgemeiner Client
M 4.3	Regelmäßiger Einsatz eines Anti-Viren-Programms	B 3.202	(5.99)	(A)	Umsetzg.	Allgemeines nicht vernetztes IT-System
		B 1.6	(3.6)	(A)	Betrieb	Computer-Virenschutzkonzept
M 4.4	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern	B 3.201	(5.99)	(A)	Betrieb	Allgemeiner Client
		B 3.203	(5.3)	(A)	Betrieb	Laptop
		B 3.208	(5.8)	(A)	Betrieb	Internet-PC
		B 3.405	(8.7)	(A)	Betrieb	PDA
		B 5.8	(9.3)	(A)	Betrieb	Telearbeit
		B 3.201	(5.99)	(C)	Betrieb	Allgemeiner Client
M 4.5	Protokollierung der TK-Administrationsarbeiten	B 3.202	(5.99)	(Z)	Betrieb	Allgemeines nicht vernetztes IT-System
		B 3.401	(8.1)	(B)	Betrieb	TK-Anlage
M 4.6	Revision der TK-Anlagenkonfiguration	B 3.401	(8.1)	(C)	Betrieb	TK-Anlage
M 4.7	Änderung voreingestellter Passwörter	B 1.9	(3.9)	(A)	Umsetzg.	Hard- und Software-Management
		B 3.101	(6.1)	(A)	Umsetzg.	Allgemeiner Server
		B 3.202	(5.99)	(A)	Umsetzg.	Allgemeines nicht vernetztes IT-System
		B 3.401	(8.1)	(A)	Umsetzg.	TK-Anlage
		B 4.1	(6.7)	(A)	Umsetzg.	Heterogene Netze
		B 4.3	(7.2)	(A)	Umsetzg.	Modem
		B 4.5	(8.4)	(A)	Umsetzg.	LAN-Anbindung eines IT-Systems über ISDN
		B 5.7	(9.2)	(A)	Umsetzg.	Datenbanken
M 4.8	Schutz des TK-Bedienplatzes	B 3.401	(8.1)	(A)	Planung	TK-Anlage
M 4.9	Einsatz der Sicherheitsmechanismen von X-Windows	B 3.102	(6.2)	(A)	Umsetzg.	Server unter Unix
		B 3.204	(5.2)	(A)	Umsetzg.	Client unter Unix
M 4.10	Passwortschutz für TK-Endgeräte	B 3.401	(8.1)	(Z)	Umsetzg.	TK-Anlage
M 4.11	Absicherung der TK-Anlagen-Schnittstellen	B 3.401	(8.1)	(B)	Umsetzg.	TK-Anlage
M 4.12	Sperren nicht benötigter TK-Leistungsmerkmale	B 3.401	(8.1)	(A)	Umsetzg.	TK-Anlage
M 4.13	Sorgfältige Vergabe von IDs	B 3.102	(6.2)	(A)	Planung	Server unter Unix

M 4.14	Obligatorischer Passwortschutz unter Unix	B 3.204	(5.2)	(A)	Planung	Client unter Unix
		B 3.102	(6.2)	(A)	Umsetzg.	Server unter Unix
M 4.15	Gesichertes Login	B 3.204	(5.2)	(A)	Umsetzg.	Client unter Unix
		B 3.101	(6.1)	(A)	Umsetzg.	Allgemeiner Server
M 4.16	Zugangsbeschränkungen für Accounts und / oder Terminals	B 3.202	(5.99)	(A)	Umsetzg.	Allgemeines nicht vernetztes IT-System
		B 3.101	(6.1)	(A)	Umsetzg.	Allgemeiner Server
M 4.17	Sperrern und Löschen nicht benötigter Accounts und Terminals	B 3.204	(5.2)	(C)	Umsetzg.	Client unter Unix
		B 3.101	(6.1)	(A)	Umsetzg.	Allgemeiner Server
M 4.18	Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus	B 3.204	(5.2)	(A)	Umsetzg.	Client unter Unix
		B 3.205	(5.5)	(B)	Umsetzg.	Client unter Windows NT
		B 3.207	(5.7)	(A)	Umsetzg.	Client unter Windows 2000
		B 3.102	(6.2)	(A)	Planung	Server unter Unix
M 4.19	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen	B 3.204	(5.2)	(A)	Planung	Client unter Unix
		B 3.102	(6.2)	(A)	Umsetzg.	Server unter Unix
M 4.20	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen	B 3.204	(5.2)	(A)	Umsetzg.	Client unter Unix
		B 3.102	(6.2)	(B)	Umsetzg.	Server unter Unix
M 4.21	Verhinderung des unautorisierten Erlangens von Administratorrechten	B 3.204	(5.2)	(B)	Umsetzg.	Client unter Unix
		B 3.102	(6.2)	(A)	Umsetzg.	Server unter Unix
M 4.22	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System	B 3.204	(5.2)	(A)	Umsetzg.	Client unter Unix
		B 3.102	(6.2)	(C)	Umsetzg.	Server unter Unix
M 4.23	Sicherer Aufruf ausführbarer Dateien	B 3.204	(5.2)	(Z)	Umsetzg.	Client unter Unix
		B 3.102	(6.2)	(A)	Umsetzg.	Server unter Unix
M 4.24	Sicherstellung einer konsistenten Systemverwaltung	B 3.204	(5.2)	(B)	Umsetzg.	Client unter Unix
		B 3.101	(6.1)	(A)	Betrieb	Allgemeiner Server
M 4.25	Einsatz der Protokollierung im Unix-System	B 3.102	(6.2)	(A)	Betrieb	Server unter Unix
		B 3.204	(5.2)	(A)	Betrieb	Client unter Unix
M 4.26	Regelmäßiger Sicherheitscheck des Unix-Systems					

M 4.27	Zugriffsschutz am Laptop	B 3.102	(6.2)	(B)	Betrieb	Server unter Unix
		B 3.204	(5.2)	(C)	Betrieb	Client unter Unix
M 4.28	Software-Reinstallation bei Benutzerwechsel eines Laptops	B 3.203	(5.3)	(A)	Betrieb	Laptop
M 4.29	Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme	B 3.203	(5.3)	(Z)	Betrieb	Laptop
M 4.30	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen	B 3.203	(5.3)	(Z)	Planung	Laptop
M 4.31	Sicherstellung der Energieversorgung im mobilen Einsatz	B 3.202	(5.99)	(A)	Betrieb	Allgemeines nicht vernetztes IT-System
M 4.32	Physikalisches Löschen der Datenträger vor und nach Verwendung	B 3.203	(5.3)	(A)	Betrieb	Laptop
		B 3.405	(8.7)	(A)	Betrieb	PDA
M 4.33	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung	B 5.2	(7.1)	(B)	Aussnd.	Datenträgeraustausch
M 4.34	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen	B 1.6	(3.6)	(A)	Betrieb	Computer-Virenschutzkonzept
		B 4.3	(7.2)	(A)	Betrieb	Modem
		B 5.2	(7.1)	(A)	Betrieb	Datenträgeraustausch
		B 5.3	(7.4)	(A)	Betrieb	E-Mail
		B 5.4	(7.5)	(A)	Betrieb	Webserver
		B 5.8	(9.3)	(A)	Betrieb	Telearbeit
		B 1.10	(9.1)	(Z)	Planung	Standardsoftware
		B 4.3	(7.2)	(Z)	Planung	Modem
M 4.35	Verifizieren der zu übertragenden Daten vor Versand	B 4.5	(8.4)	(Z)	Planung	LAN-Anbindung eines IT-Systems über ISDN
		B 5.2	(7.1)	(Z)	Planung	Datenträgeraustausch
		B 5.3	(7.4)	(Z)	Betrieb	E-Mail
		B 5.4	(7.5)	(Z)	Betrieb	Webserver
		B 5.2	(7.1)	(Z)	Betrieb	Datenträgeraustausch
M 4.36	Sperren bestimmter Faxempfänger-Rufnummern	B 3.402	(8.2)	(Z)	Umsetzg.	Faxgerät
M 4.37	Sperren bestimmter Absender-Faxnummern	B 5.6	(8.5)	(Z)	Umsetzg.	Faxserver
		B 3.402	(8.2)	(Z)	Umsetzg.	Faxgerät
		B 5.6	(8.5)	(Z)	Umsetzg.	Faxserver
M 4.38	Abschalten nicht benötigter Leistungsmerkmale	B 3.403	(8.3)	(A)	Umsetzg.	Anrufbeantworter
M 4.39	Abschalten des Anrufbeantworters bei Anwesenheit					

M 4.40	Verhinderung der unautorisierten Nutzung des Rechtermikrofons	B 3.403	(8.3)	(Z)	Betrieb	Anrufbeantworter
		B 3.101	(6.1)	(C)	Umsetzg.	Allgemeiner Server
		B 3.201	(5.99)	(A)	Umsetzg.	Allgemeiner Client
		B 3.202	(5.99)	(C)	Betrieb	Allgemeines nicht vernetztes IT-System
M 4.41	Einsatz angemessener Sicherheitsprodukte für IT-Systeme	B 3.203	(5.3)	(A)	Umsetzg.	Laptop
		B 3.201	(5.99)	(C)	Betrieb	Allgemeiner Client
		B 3.202	(5.99)	(Z)	Planung	Allgemeines nicht vernetztes IT-System
		B 3.206	(5.6)	(Z)	Planung	Client unter Windows 95
M 4.42	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung	B 3.208	(5.8)	(Z)	Planung	Internet-PC
		B 1.10	(9.1)	(Z)	Umsetzg.	Standardsoftware
		B 4.43				
		B 4.44				
M 4.43	Faxgerät mit automatischer Eingangskuvertierung	B 3.402	(8.2)	(Z)	Betrieb	Faxgerät
M 4.44	Prüfung eingehender Dateien auf Makro-Viren	B 3.208	(5.8)	(A)	Betrieb	Internet-PC
		B 5.3	(7.4)	(A)	Betrieb	E-Mail
		B 5.1	(6.3)	(A)	Umsetzg.	Peer-to-Peer-Dienste
		B 5.1	(6.3)	(A)	Betrieb	Peer-to-Peer-Dienste
M 4.45	Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW	B 3.301	(7.3)	(A)	Betrieb	Sicherheitsgateway (Firewall)
M 4.46	Nutzung des Anmeldepasswortes unter WfW und Windows 95	B 3.103	(6.4)	(A)	Umsetzg.	Server unter Windows NT
		B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
		B 3.205	(5.5)	(A)	Planung	Client unter Windows NT
		B 3.207	(5.7)	(A)	Umsetzg.	Client unter Windows 2000
M 4.47	Protokollierung der Sicherheitsgateway-Aktivitäten	B 3.209	(5.9)	(A)	Planung	Client unter Windows XP
		B 3.103	(6.4)	(A)	Umsetzg.	Server unter Windows NT
		B 3.205	(5.5)	(A)	Planung	Client unter Windows NT
		B 3.207	(5.7)	(A)	Umsetzg.	Client unter Windows 2000
M 4.48	Passwortschutz unter Windows NT/2000/XP	B 3.209	(5.9)	(A)	Betrieb	Client unter Windows XP
		B 3.103	(6.4)	(A)	Umsetzg.	Server unter Windows NT
		B 3.205	(5.5)	(A)	Planung	Client unter Windows NT
		B 3.207	(5.7)	(A)	Umsetzg.	Client unter Windows 2000
M 4.49	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System	B 3.209	(5.9)	(A)	Betrieb	Client unter Windows XP
		B 3.103	(6.4)	(Z)	Planung	Server unter Windows NT
		B 3.205	(5.5)	(Z)	Planung	Client unter Windows NT
		B 3.207	(5.7)	(Z)	Planung	Client unter Windows NT
M 4.50	Strukturierte Systemverwaltung unter Windows NT	B 3.103	(6.4)	(Z)	Planung	Server unter Windows NT
		B 3.205	(5.5)	(Z)	Planung	Client unter Windows NT
		B 3.103	(6.4)	(Z)	Planung	Server unter Windows NT
		B 3.205	(5.5)	(Z)	Planung	Client unter Windows NT
M 4.51	Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT	B 3.103	(6.4)	(Z)	Planung	Server unter Windows NT
		B 3.205	(5.5)	(Z)	Planung	Client unter Windows NT
		B 3.103	(6.4)	(Z)	Planung	Server unter Windows NT
		B 3.205	(5.5)	(Z)	Planung	Client unter Windows NT

M 4.52	Geräteschutz unter Windows NT/2000/XP	B 3.103	(6.4)	(A)	Umsetzg.	Server unter Windows NT
		B 3.205	(5.5)	(B)	Umsetzg.	Client unter Windows NT
		B 3.207	(5.7)	(A)	Umsetzg.	Client unter Windows 2000
		B 3.209	(5.9)	(A)	Betrieb	Client unter Windows XP
M 4.53	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT	B 3.103	(6.4)	(A)	Umsetzg.	Server unter Windows NT
		B 3.205	(5.5)	(A)	Planung	Client unter Windows NT
M 4.54	Protokollierung unter Windows NT	B 3.103	(6.4)	(A)	Betrieb	Server unter Windows NT
		B 3.205	(5.5)	(Z)	Umsetzg.	Client unter Windows NT
M 4.55	Sichere Installation von Windows NT	B 3.103	(6.4)	(A)	Umsetzg.	Server unter Windows NT
		B 3.205	(5.5)	(B)	Umsetzg.	Client unter Windows NT
M 4.56	Sicheres Löschen unter Windows-Betriebssystemen	B 3.103	(6.4)	(B)	Betrieb	Server unter Windows NT
		B 3.106	(6.9)	(C)	Betrieb	Server unter Windows 2000
		B 3.205	(5.5)	(B)	Betrieb	Client unter Windows NT
		B 3.206	(5.6)	(B)	Betrieb	Client unter Windows 95
		B 3.209	(5.9)	(C)	Betrieb	Client unter Windows XP
M 4.57	Deaktivieren der automatischen CD-ROM-Erkennung	B 3.103	(6.4)	(A)	Umsetzg.	Server unter Windows NT
		B 3.205	(5.5)	(A)	Umsetzg.	Client unter Windows NT
		B 3.206	(5.6)	(A)	Umsetzg.	Client unter Windows 95
		B 3.207	(5.7)	(A)	Umsetzg.	Client unter Windows 2000
		B 3.209	(5.9)	(A)	Planung	Client unter Windows XP
M 4.58	Freigabe von Verzeichnissen unter Windows 95	B 5.1	(6.3)	(B)	Betrieb	Peer-to-Peer-Dienste
M 4.59	Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten	B 4.5	(8.4)	(A)	Umsetzg.	LAN-Anbindung eines IT-Systems über ISDN
M 4.60	Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten	B 4.5	(8.4)	(A)	Umsetzg.	LAN-Anbindung eines IT-Systems über ISDN
M 4.61	Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten	B 4.5	(8.4)	(A)	Umsetzg.	LAN-Anbindung eines IT-Systems über ISDN
M 4.62	Einsatz eines D-Kanal-Filters	B 3.401	(8.1)	(Z)	Planung	TK-Anlage
		B 4.5	(8.4)	(Z)	Planung	LAN-Anbindung eines IT-Systems über ISDN
M 4.63	Sicherheitstechnische Anforderungen an den Telearbeitsrechner	B 5.8	(9.3)	(A)	Umsetzg.	Telearbeit

M 4.64	Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen	B 5.3	(7.4)	(C)	Betrieb	E-Mail
		B 5.4	(7.5)	(C)	Betrieb	Webserver
M 4.65	Test neuer Hard- und Software	B 1.9	(3.9)	(C)	Umsetzg.	Hard- und Software-Management
M 4.67	Sperren und Löschen nicht benötigter Datenbank-Accounts	B 5.7	(9.2)	(A)	Umsetzg.	Datenbanken
M 4.68	Sicherstellung einer konsistenten Datenbankverwaltung	B 5.7	(9.2)	(A)	Betrieb	Datenbanken
M 4.69	Regelmäßiger Sicherheitscheck der Datenbank	B 5.7	(9.2)	(B)	Betrieb	Datenbanken
M 4.70	Durchführung einer Datenbanküberwachung	B 5.7	(9.2)	(C)	Betrieb	Datenbanken
M 4.71	Restriktive Handhabung von Datenbank-Links	B 5.7	(9.2)	(C)	Umsetzg.	Datenbanken
M 4.72	Datenbank-Verschlüsselung	B 5.7	(9.2)	(Z)	Planung	Datenbanken
M 4.73	Festlegung von Obergrenzen für selektierbare Datensätze	B 5.7	(9.2)	(C)	Planung	Datenbanken
M 4.74	Vernetzte Windows 95 Rechner	B 3.206	(5.6)	(A)	Planung	Client unter Windows 95
M 4.75	Schutz der Registrierung unter Windows NT/2000/XP	B 3.103	(6.4)	(A)	Umsetzg.	Server unter Windows NT
		B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
		B 3.205	(5.5)	(A)	Umsetzg.	Client unter Windows NT
		B 3.207	(5.7)	(A)	Umsetzg.	Client unter Windows 2000
		B 3.209	(5.9)	(A)	Planung	Client unter Windows XP
M 4.76	Sichere Systemversion von Windows NT	B 3.103	(6.4)	(B)	Planung	Server unter Windows NT
		B 3.205	(5.5)	(C)	Planung	Client unter Windows NT
M 4.77	Schutz der Administratorkonten unter Windows NT	B 3.103	(6.4)	(A)	Umsetzg.	Server unter Windows NT
		B 3.205	(5.5)	(A)	Umsetzg.	Client unter Windows NT
M 4.78	Sorgfältige Durchführung von Konfigurationsänderungen	B 1.9	(3.9)	(A)	Betrieb	Hard- und Software-Management
		B 5.4	(7.5)	(A)	Betrieb	Webserver
M 4.79	Sichere Zugriffsmechanismen bei lokaler Administration	B 4.1	(6.7)	(A)	Planung	Heterogene Netze
M 4.80	Sichere Zugriffsmechanismen bei Fernadministration	B 4.1	(6.7)	(B)	Planung	Heterogene Netze



M 4.81	Audit und Protokollierung der Aktivitäten im Netz						
		B 4.1	(6.7)	(B)	Betrieb	Heterogene Netze	
M 4.82	Sichere Konfiguration der aktiven Netzkomponenten						
		B 4.1	(6.7)	(A)	Umsetzg.	Heterogene Netze	
M 4.83	Update/Upgrade von Soft- und Hardware im Netzbereich						
		B 4.1	(6.7)	(C)	Betrieb	Heterogene Netze	
M 4.84	Nutzung der BIOS-Sicherheitsmechanismen						
		B 1.6	(3.6)	(A)	Umsetzg.	Computer-Virenschutzkonzept	
		B 1.9	(3.9)	(A)	Umsetzg.	Hard- und Software-Management	
M 4.85	Geeignetes Schnittstellendesign bei Kryptomodulen						
		B 1.7	(3.7)	(Z)	Beschaff.	Kryptokonzept	
M 4.86	Sichere Rollenteilung und Konfiguration der Kryptomodule						
		B 1.7	(3.7)	(A)	Umsetzg.	Kryptokonzept	
M 4.87	Physikalische Sicherheit von Kryptomodulen						
		B 1.7	(3.7)	(Z)	Umsetzg.	Kryptokonzept	
M 4.88	Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen						
		B 1.7	(3.7)	(A)	Beschaff.	Kryptokonzept	
M 4.89	Abstrahlsicherheit						
		B 1.7	(3.7)	(Z)	Umsetzg.	Kryptokonzept	
M 4.90	Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells						
		B 1.7	(3.7)	(A)	Planung	Kryptokonzept	
M 4.91	Sichere Installation eines Systemmanagementsystems						
		B 4.2	(6.8)	(A)	Umsetzg.	Netz- und Systemmanagement	
M 4.92	Sicherer Betrieb eines Systemmanagementsystems						
		B 4.2	(6.8)	(A)	Betrieb	Netz- und Systemmanagement	
M 4.93	Regelmäßige Integritätsprüfung						
		B 3.101	(6.1)	(B)	Betrieb	Allgemeiner Server	
		B 3.201	(5.99)	(B)	Betrieb	Allgemeiner Client	
		B 3.301	(7.3)	(B)	Betrieb	Sicherheitsgateway (Firewall)	
		B 5.4	(7.5)	(B)	Betrieb	Webserver	
M 4.94	Schutz der WWW-Dateien						
		B 5.4	(7.5)	(A)	Umsetzg.	Webserver	
M 4.95	Minimales Betriebssystem						
		B 5.4	(7.5)	(A)	Umsetzg.	Webserver	
M 4.96	Abschaltung von DNS						
		B 5.4	(7.5)	(Z)	Umsetzg.	Webserver	
M 4.97	Ein Dienst pro Server						
		B 5.4	(7.5)	(Z)	Umsetzg.	Webserver	
M 4.98	Kommunikation durch Paketfilter auf Minimum beschränken						

M 4.99	Schutz gegen nachträgliche Veränderungen von Informationen	B 5.4	(7.5)	(A)	Umsetzg.	Webserver
M 4.100	Sicherheitsgateways und aktive Inhalte	B 5.4	(7.5)	(C)	Umsetzg.	Webserver
M 4.101	Sicherheitsgateways und Verschlüsselung	B 3.301	(7.3)	(C)	Betrieb	Sicherheitsgateway (Firewall)
M 4.102	C2-Sicherheit unter Novell 4.11	B 3.301	(7.3)	(C)	Betrieb	Sicherheitsgateway (Firewall)
M 4.103	DHCP-Server unter Novell Netware 4.x	B 3.105	(6.6)	(Z)	Umsetzg.	Server unter Novell Netware 4.x
M 4.104	LDAP Services for NDS	B 3.105	(6.6)	(Z)	Umsetzg.	Server unter Novell Netware 4.x
M 4.105	Erste Maßnahmen nach einer Unix-Standardinstallation	B 3.105	(6.6)	(Z)	Umsetzg.	Server unter Novell Netware 4.x
M 4.106	Aktivieren der Systemprotokollierung	B 3.102	(6.2)	(A)	Umsetzg.	Server unter Unix
		B 3.204	(5.2)	(A)	Umsetzg.	Client unter Unix
M 4.107	Nutzung von Hersteller-Ressourcen	B 3.102	(6.2)	(A)	Umsetzg.	Server unter Unix
		B 3.204	(5.2)	(B)	Umsetzg.	Client unter Unix
M 4.108	Vereinfachtes und sicheres Netzmanagement mit DNS Services unter Novell NetWare 4.11	B 1.9	(3.9)	(B)	Betrieb	Hard- und Software-Management
M 4.109	Software-Reinstallation bei Arbeitsplatzrechnern	B 3.105	(6.6)	(Z)	Betrieb	Server unter Novell Netware 4.x
		B 1.9	(3.9)	(Z)	Betrieb	Hard- und Software-Management
		B 2.11	(4.8)	(C)	Betrieb	Besprechungs-, Veranstaltungs- und Schulungsräume
M 4.110	Sichere Installation des RAS-Systems	B 4.4	(7.6)	(A)	Umsetzg.	Remote Access
M 4.111	Sichere Konfiguration des RAS-Systems	B 4.4	(7.6)	(A)	Umsetzg.	Remote Access
M 4.112	Sicherer Betrieb des RAS-Systems	B 4.4	(7.6)	(A)	Betrieb	Remote Access
M 4.113	Nutzung eines Authentisierungservers beim RAS-Einsatz	B 4.4	(7.6)	(Z)	Planung	Remote Access
M 4.114	Nutzung der Sicherheitsmechanismen von Mobiltelefonen	B 3.404	(8.6)	(A)	Umsetzg.	Mobiltelefon
M 4.115	Sicherstellung der Energieversorgung von Mobiltelefonen	B 3.404	(8.6)	(B)	Betrieb	Mobiltelefon
M 4.116	Sichere Installation von Lotus Notes					

M 4.117	Sichere Konfiguration eines Lotus Notes Servers	B 5.5	(7.7)	(A)	Umsetzg.	Lotus Notes
M 4.118	Konfiguration als Lotus Notes Server	B 5.5	(7.7)	(A)	Umsetzg.	Lotus Notes
M 4.119	Einrichten von Zugangsbeschränkungen auf Lotus Notes Server	B 5.5	(7.7)	(A)	Umsetzg.	Lotus Notes
M 4.120	Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken	B 5.5	(7.7)	(A)	Umsetzg.	Lotus Notes
M 4.121	Konfiguration der Zugriffsrechte auf das Namens- und Adressbuch von Lotus Notes	B 5.5	(7.7)	(A)	Umsetzg.	Lotus Notes
M 4.122	Konfiguration für den Browser-Zugriff auf Lotus Notes	B 5.5	(7.7)	(A)	Umsetzg.	Lotus Notes
M 4.123	Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes	B 5.5	(7.7)	(B)	Umsetzg.	Lotus Notes
M 4.124	Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes	B 5.5	(7.7)	(B)	Umsetzg.	Lotus Notes
M 4.125	Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken	B 5.5	(7.7)	(A)	Umsetzg.	Lotus Notes
M 4.126	Sichere Konfiguration eines Lotus Notes Clients	B 5.5	(7.7)	(A)	Umsetzg.	Lotus Notes
M 4.127	Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes	B 5.5	(7.7)	(A)	Umsetzg.	Lotus Notes
M 4.128	Sicherer Betrieb von Lotus Notes	B 5.5	(7.7)	(A)	Umsetzg.	Lotus Notes
M 4.129	Sicherer Umgang mit Notes-ID-Dateien	B 5.5	(7.7)	(A)	Betrieb	Lotus Notes
M 4.130	Sicherheitsmaßnahmen nach dem Anlegen neuer Lotus Notes Datenbanken	B 5.5	(7.7)	(A)	Betrieb	Lotus Notes
M 4.131	Verschlüsselung von Lotus Notes Datenbanken	B 5.5	(7.7)	(A)	Betrieb	Lotus Notes
M 4.132	Überwachen eines Lotus Notes-Systems	B 5.5	(7.7)	(Z)	Planung	Lotus Notes
M 4.133	Geeignete Auswahl von Authentikationsmechanismen	B 5.5	(7.7)	(C)	Betrieb	Lotus Notes
M 4.134	Wahl geeigneter Datenformate	B 1.9	(3.9)	(Z)	Planung	Hard- und Software-Management
M 4.135	Restriktive Vergabe von Zugriffsrechten auf Systemdateien	B 1.9	(3.9)	(C)	Planung	Hard- und Software-Management

M 4.136	Sichere Installation von Windows 2000	B 1.9	(3.9)	(A)	Umsetzg.	Hard- und Software-Management
		B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
M 4.137	Sichere Konfiguration von Windows 2000	B 3.207	(5.7)	(A)	Umsetzg.	Client unter Windows 2000
		B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
M 4.138	Konfiguration von Windows 2000 als Domänen-Controller	B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
M 4.139	Konfiguration von Windows 2000 als Server	B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
M 4.140	Sichere Konfiguration wichtiger Windows 2000 Dienste	B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
M 4.141	Sichere Konfiguration des DDNS unter Windows 2000	B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
M 4.142	Sichere Konfiguration des WINS unter Windows 2000	B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
M 4.143	Sichere Konfiguration des DHCP unter Windows 2000	B 3.106	(6.9)	(B)	Umsetzg.	Server unter Windows 2000
M 4.144	Nutzung der Windows 2000 CA	B 3.106	(6.9)	(B)	Umsetzg.	Server unter Windows 2000
M 4.145	Sichere Konfiguration von RRAS unter Windows 2000	B 3.106	(6.9)	(B)	Umsetzg.	Server unter Windows 2000
M 4.146	Sicherer Betrieb von Windows 2000/XP	B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
		B 3.209	(5.9)	(A)	Betrieb	Client unter Windows XP
M 4.147	Sichere Nutzung von EFS unter Windows 2000/XP	B 3.106	(6.9)	(Z)	Planung	Server unter Windows 2000
		B 3.207	(5.7)	(Z)	Betrieb	Client unter Windows 2000
		B 3.209	(5.9)	(Z)	Planung	Client unter Windows XP
M 4.148	Überwachung eines Windows 2000/XP Systems	B 3.106	(6.9)	(B)	Betrieb	Server unter Windows 2000
		B 3.207	(5.7)	(B)	Betrieb	Client unter Windows 2000
		B 3.209	(5.9)	(B)	Betrieb	Client unter Windows XP
M 4.149	Datei- und Freigabeberechtigungen unter Windows 2000/XP	B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
		B 3.207	(5.7)	(A)	Umsetzg.	Client unter Windows 2000
		B 3.209	(5.9)	(A)	Planung	Client unter Windows XP
		B 5.1	(6.3)	(A)	Umsetzg.	Peer-to-Peer-Dienste
M 4.150	Konfiguration von Windows 2000 als Workstation	B 3.207	(5.7)	(A)	Umsetzg.	Client unter Windows 2000
M 4.151	Sichere Installation von Internet-PCs					

M 4.152	Sicherer Betrieb von Internet-PCs	B 3.208	(5.8)	(B)	Umsetzg.	Internet-PC
M 4.153	Sichere Installation von Novell eDirectory	B 3.208	(5.8)	(B)	Betrieb	Internet-PC
M 4.154	Sichere Installation der Novell eDirectory Clientsoftware	B 5.9	(9.4)	(A)	Umsetzg.	Novell eDirectory
M 4.155	Sichere Konfiguration von Novell eDirectory	B 5.9	(9.4)	(A)	Umsetzg.	Novell eDirectory
M 4.156	Sichere Konfiguration der Novell eDirectory Clientsoftware	B 5.9	(9.4)	(A)	Umsetzg.	Novell eDirectory
M 4.157	Einrichten von Zugriffsberechtigungen auf Novell eDirectory	B 5.9	(9.4)	(A)	Umsetzg.	Novell eDirectory
M 4.158	Einrichten des LDAP-Zugriffs auf Novell eDirectory	B 5.9	(9.4)	(A)	Umsetzg.	Novell eDirectory
M 4.159	Sicherer Betrieb von Novell eDirectory	B 5.9	(9.4)	(B)	Umsetzg.	Novell eDirectory
M 4.160	Überwachen von Novell eDirectory	B 5.9	(9.4)	(A)	Betrieb	Novell eDirectory
M 4.161	Sichere Installation von Exchange/Outlook 2000	B 5.9	(9.4)	(B)	Betrieb	Novell eDirectory
M 4.162	Sichere Konfiguration von Exchange 2000 Servern	B 5.12	(7.10)	(A)	Umsetzg.	Exchange 2000 / Outlook 2000
M 4.163	Zugriffsrechte auf Exchange 2000 Objekte	B 5.12	(7.10)	(A)	Umsetzg.	Exchange 2000 / Outlook 2000
M 4.164	Browser-Zugriff auf Exchange 2000	B 5.12	(7.10)	(A)	Umsetzg.	Exchange 2000 / Outlook 2000
M 4.165	Sichere Konfiguration von Outlook 2000	B 5.12	(7.10)	(A)	Umsetzg.	Exchange 2000 / Outlook 2000
M 4.166	Sicherer Betrieb von Exchange/Outlook 2000	B 5.12	(7.10)	(A)	Umsetzg.	Exchange 2000 / Outlook 2000
M 4.167	Überwachung und Protokollierung von Exchange 2000 Systemen	B 5.12	(7.10)	(A)	Betrieb	Exchange 2000 / Outlook 2000
M 4.168	Auswahl eines geeigneten Archivsystems	B 5.12	(7.10)	(B)	Betrieb	Exchange 2000 / Outlook 2000
M 4.169	Verwendung geeigneter Archivmedien	B 1.12	(9.5)	(A)	Beschaff.	Archivierung
M 4.170	Auswahl geeigneter Datenformate für die Archivierung von Dokumenten	B 1.12	(9.5)	(A)	Beschaff.	Archivierung
M 4.171	Schutz der Integrität der Index-Datenbank von Archivsystemen	B 1.12	(9.5)	(A)	Beschaff.	Archivierung
		B 1.12	(9.5)	(A)	Betrieb	Archivierung

M 4.172	Protokollierung der Archivzugriffe	B 1.12	(9.5)	(C)	Betrieb	Archivierung
M 4.173	Regelmäßige Funktions- und Recoverytests bei der Archivierung	B 1.12	(9.5)	(B)	Betrieb	Archivierung
M 4.174	Vorbereitung der Installation von Windows NT/2000 für den IIS	B 5.10	(7.8)	(A)	Umsetzg.	Internet Information Server
M 4.175	Sichere Konfiguration von Windows NT/2000 für den IIS	B 5.10	(7.8)	(A)	Umsetzg.	Internet Information Server
M 4.176	Auswahl einer Authentisierungsmethode für Webangebote	B 5.4	(7.5)	(B)	Planung	Webserver
M 4.177	Sicherstellung der Integrität und Authentizität von Softwarepaketen	B 5.4	(7.5)	(B)	Betrieb	Webserver
M 4.178	Absicherung der Administrator- und Benutzerkonten beim IIS-Einsatz	B 5.10	(7.8)	(A)	Umsetzg.	Internet Information Server
M 4.179	Schutz von sicherheitskritischen Dateien beim IIS-Einsatz	B 5.10	(7.8)	(A)	Umsetzg.	Internet Information Server
M 4.180	Konfiguration der Authentisierungsmechanismen für den Zugriff auf den IIS	B 5.10	(7.8)	(A)	Umsetzg.	Internet Information Server
M 4.181	Ausführen des IIS in einem separaten Prozess	B 5.10	(7.8)	(A)	Umsetzg.	Internet Information Server
M 4.182	Überwachen des IIS-Systems	B 5.10	(7.8)	(A)	Umsetzg.	Internet Information Server
M 4.183	Sicherstellen der Verfügbarkeit und Performance des IIS	B 5.10	(7.8)	(B)	Betrieb	Internet Information Server
M 4.184	Deaktivieren nicht benötigter Dienste beim IIS-Einsatz	B 5.10	(7.8)	(A)	Betrieb	Internet Information Server
M 4.185	Absichern von virtuellen Verzeichnissen und Web-Anwendungen beim IIS-Einsatz	B 5.10	(7.8)	(A)	Umsetzg.	Internet Information Server
M 4.186	Entfernen von Beispieldateien und Administrations-Scripts des IIS	B 5.10	(7.8)	(A)	Umsetzg.	Internet Information Server
M 4.187	Entfernen der FrontPage Server-Erweiterung des IIS	B 5.10	(7.8)	(A)	Umsetzg.	Internet Information Server
M 4.188	Prüfen der Benutzereingaben beim IIS-Einsatz	B 5.10	(7.8)	(A)	Umsetzg.	Internet Information Server
M 4.189	Schutz vor unzulässigen Programmaufrufen beim IIS-Einsatz	B 5.10	(7.8)	(B)	Umsetzg.	Internet Information Server
M 4.190	Entfernen der RDS-Unterstützung des IIS	B 5.10	(7.8)	(B)	Umsetzg.	Internet Information Server
M 4.191	Überprüfung der Integrität und Authentizität der Apache-Pakete	B 5.11	(7.9)	(A)	Beschaff.	Apache Webserver

M 4.192	Konfiguration des Betriebssystems für einen Apache-Webserver	B 5.11	(7.9)	(A)	Umsetzg.	Apache Webserver
M 4.193	Sichere Installation eines Apache-Webservers	B 5.11	(7.9)	(A)	Umsetzg.	Apache Webserver
M 4.194	Sichere Grundkonfiguration eines Apache-Webservers	B 5.11	(7.9)	(A)	Umsetzg.	Apache Webserver
M 4.195	Konfiguration der Zugriffssteuerung beim Apache-Webserver	B 5.11	(7.9)	(A)	Umsetzg.	Apache Webserver
M 4.196	Sicherer Betrieb eines Apache-Webservers	B 5.11	(7.9)	(A)	Betrieb	Apache Webserver
M 4.197	Servererweiterungen für dynamische Webseiten beim Apache-Webserver	B 5.11	(7.9)	(B)	Umsetzg.	Apache Webserver
M 4.198	Installation eines Apache-Webservers in einem chroot-Käfig	B 5.11	(7.9)	(Z)	Umsetzg.	Apache Webserver
M 4.199	Vermeidung gefährlicher Dateiformate	B 5.3	(7.4)	(B)	Betrieb	E-Mail
M 4.200	Umgang mit USB-Speichermedien	B 3.201	(5.99)	(Z)	Betrieb	Allgemeiner Client
M 4.201	Sichere lokale Grundkonfiguration von Routern und Switches	B 3.302	(7.11)	(A)	Umsetzg.	Router und Switches
M 4.202	Sichere Netz-Grundkonfiguration von Routern und Switches	B 3.302	(7.11)	(A)	Umsetzg.	Router und Switches
M 4.203	Konfigurations-Checkliste für Router und Switches	B 3.302	(7.11)	(A)	Umsetzg.	Router und Switches
M 4.204	Sichere Administration von Routern und Switches	B 3.302	(7.11)	(C)	Betrieb	Router und Switches
M 4.205	Protokollierung bei Routern und Switches	B 3.302	(7.11)	(C)	Betrieb	Router und Switches
M 4.206	Sicherung von Switch-Ports	B 3.302	(7.11)	(C)	Betrieb	Router und Switches
M 4.207	Einsatz und Sicherung systemnaher z/OS-Terminals	B 3.107	(6.10)	(A)	Umsetzg.	S/390- und zSeries-Mainframe
M 4.208	Absichern des Start-Vorgangs von z/OS-Systemen	B 3.107	(6.10)	(B)	Umsetzg.	S/390- und zSeries-Mainframe
M 4.209	Sichere Grundkonfiguration von z/OS-Systemen	B 3.107	(6.10)	(A)	Umsetzg.	S/390- und zSeries-Mainframe
M 4.210	Sicherer Betrieb des z/OS-Betriebssystems	B 3.107	(6.10)	(B)	Betrieb	S/390- und zSeries-Mainframe
M 4.211	Einsatz des z/OS-Sicherheitssystems RACF	B 3.107	(6.10)	(A)	Umsetzg.	S/390- und zSeries-Mainframe
M 4.212	Absicherung von Linux für zSeries					

M 4.213	Absichern des Login-Vorgangs unter z/OS	B 3.107	(6.10)	(Z)	Umsetzg.	S/390- und zSeries-Mainframe
M 4.214	Datenträgerverwaltung unter z/OS-Systemen	B 3.107	(6.10)	(A)	Umsetzg.	S/390- und zSeries-Mainframe
M 4.215	Absicherung sicherheitskritischer z/OS-Dienstprogramme	B 3.107	(6.10)	(B)	Betrieb	S/390- und zSeries-Mainframe
M 4.216	Festlegung der Systemgrenzen von z/OS	B 3.107	(6.10)	(B)	Betrieb	S/390- und zSeries-Mainframe
M 4.217	Workload Management für z/OS-Systeme	B 3.107	(6.10)	(C)	Umsetzg.	S/390- und zSeries-Mainframe
M 4.218	Hinweise zur Zeichensatzkonvertierung bei z/OS-Systemen	B 3.107	(6.10)	(C)	Umsetzg.	S/390- und zSeries-Mainframe
M 4.219	Lizenzschlüssel-Management für z/OS-Software	B 3.107	(6.10)	(Z)	Betrieb	S/390- und zSeries-Mainframe
M 4.220	Absicherung von Unix System Services bei z/OS-Systemen	B 3.107	(6.10)	(C)	Umsetzg.	S/390- und zSeries-Mainframe
M 4.221	Parallel-Sysplex unter z/OS	B 3.107	(6.10)	(B)	Umsetzg.	S/390- und zSeries-Mainframe
M 4.222	Festlegung geeigneter Einstellungen von Sicherheitsproxies	B 3.107	(6.10)	(C)	Planung	S/390- und zSeries-Mainframe
M 4.223	Integration von Proxy-Servern in das Sicherheitsgateway	B 3.301	(7.3)	(B)	Betrieb	Sicherheitsgateway (Firewall)
M 4.224	Integration von Virtual Private Networks in ein Sicherheitsgateway	B 3.301	(7.3)	(B)	Betrieb	Sicherheitsgateway (Firewall)
M 4.225	Einsatz eines Protokollierungsservers in einem Sicherheitsgateway	B 3.301	(7.3)	(Z)	Betrieb	Sicherheitsgateway (Firewall)
M 4.226	Integration von Virenscannern in ein Sicherheitsgateway	B 3.301	(7.3)	(Z)	Betrieb	Sicherheitsgateway (Firewall)
M 4.227	Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation	B 3.301	(7.3)	(Z)	Betrieb	Sicherheitsgateway (Firewall)
M 4.228	Nutzung der Sicherheitsmechanismen von PDAs	B 3.301	(7.3)	(C)	Betrieb	Sicherheitsgateway (Firewall)
M 4.229	Sicherer Betrieb von PDAs	B 3.405	(8.7)	(A)	Betrieb	PDA
M 4.230	Zentrale Administration von PDAs	B 3.405	(8.7)	(C)	Betrieb	PDA
M 4.231	Einsatz zusätzlicher Sicherheitswerkzeuge für PDAs	B 3.405	(8.7)	(Z)	Betrieb	PDA
M 4.232	Sichere Nutzung von Zusatzspeicherkarten	B 3.405	(8.7)	(Z)	Beschaff.	PDA
		B 3.405	(8.7)	(Z)	Betrieb	PDA



M 4.233	Sperrung nicht mehr benötigter RAS-Zugänge						
		B 4.4	(7.6)	(B)	Aussnd.	Remote Access	
M 4.234	Aussonderung von IT-Systemen						
		B 1.9	(3.9)	(B)	Aussnd.	Hard- und Software-Management	
		B 3.201	(5.99)	(A)	Aussnd.	Allgemeiner Client	
M 4.235	Abgleich der Datenbestände von Laptops						
		B 3.203	(5.3)	(B)	Betrieb	Laptop	
M 4.236	Zentrale Administration von Laptops						
		B 3.201	(5.99)	(Z)	Betrieb	Allgemeiner Client	
		B 3.203	(5.3)	(Z)	Betrieb	Laptop	
M 4.237	Sichere Grundkonfiguration eines IT-Systems						
		B 3.101	(6.1)	(A)	Umsetzg.	Allgemeiner Server	
		B 3.201	(5.99)	(A)	Umsetzg.	Allgemeiner Client	
M 4.238	Einsatz eines lokalen Paketfilters						
		B 3.101	(6.1)	(A)	Betrieb	Allgemeiner Server	
		B 3.201	(5.99)	(A)	Betrieb	Allgemeiner Client	
M 4.239	Sicherer Betrieb eines Servers						
		B 3.101	(6.1)	(A)	Betrieb	Allgemeiner Server	
M 4.240	Einrichten einer Testumgebung für einen Server						
		B 3.101	(6.1)	(Z)	Betrieb	Allgemeiner Server	
M 4.241	Sicherer Betrieb von Clients						
		B 3.201	(5.99)	(A)	Betrieb	Allgemeiner Client	
M 4.242	Einrichten einer Referenzinstallation für Clients						
		B 3.201	(5.99)	(Z)	Umsetzg.	Allgemeiner Client	
M 4.243	Windows XP Verwaltungswerkzeuge						
		B 3.209	(5.9)	(Z)	Planung	Client unter Windows XP	
M 4.244	Sichere Windows XP Systemkonfiguration						
		B 3.209	(5.9)	(A)	Planung	Client unter Windows XP	
M 4.245	Basiseinstellungen für Windows XP GPOs						
		B 3.209	(5.9)	(A)	Planung	Client unter Windows XP	
M 4.246	Konfiguration der Systemdienste unter Windows XP						
		B 3.209	(5.9)	(A)	Planung	Client unter Windows XP	
M 4.247	Restriktive Berechtigungsvergabe unter Windows XP						
		B 3.209	(5.9)	(A)	Planung	Client unter Windows XP	
M 4.248	Sichere Installation von Windows XP						
		B 3.209	(5.9)	(A)	Umsetzg.	Client unter Windows XP	
M 4.249	Windows XP Systeme aktuell halten						
		B 3.209	(5.9)	(A)	Betrieb	Client unter Windows XP	
M 4.251	Arbeiten mit fremden IT-Systemen						
		B 2.10	(4.7)	(A)	Betrieb	Mobiler Arbeitsplatz	
M 4.252	Sichere Konfiguration von Schulungsrechnern						

		B 2.11	(4.8)	(C)	Umsetzg.	Besprechungs-, Veranstaltungs- und Schulungsräume
M 4.253	Schutz vor Spyware					
M 4.254	Sicherer Einsatz von drahtlosen Tastaturen und Mäusen	B 1.6	(3.6)	(A)	Planung	Computer-Virenschutzkonzept
M 4.255	Nutzung von IrDA-Schnittstellen	B 1.9	(3.9)	(Z)	Betrieb	Hard- und Software-Management
		B 3.203	(5.3)	(A)	Betrieb	Laptop
		B 3.404	(8.6)	(A)	Betrieb	Mobiltelefon
		B 3.405	(8.7)	(A)	Betrieb	PDA
M 5.1	Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen					
M 5.2	Auswahl einer geeigneten Netz-Topographie	B 2.2	(4.2)	(B)	Betrieb	Verkabelung
		B 2.2	(4.2)	(A)	Planung	Verkabelung
		B 4.1	(6.7)	(A)	Planung	Heterogene Netze
M 5.3	Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht					
M 5.4	Dokumentation und Kennzeichnung der Verkabelung	B 2.2	(4.2)	(A)	Planung	Verkabelung
M 5.5	Schadensmindernde Kabelführung	B 2.2	(4.2)	(A)	Umsetzg.	Verkabelung
M 5.7	Netzverwaltung	B 2.2	(4.2)	(A)	Umsetzg.	Verkabelung
M 5.8	Regelmäßiger Sicherheitscheck des Netzes	B 4.1	(6.7)	(A)	Umsetzg.	Heterogene Netze
M 5.9	Protokollierung am Server	B 3.101	(6.1)	(B)	Betrieb	Allgemeiner Server
M 5.10	Restriktive Rechtevergabe	B 3.101	(6.1)	(A)	Betrieb	Allgemeiner Server
M 5.13	Geeigneter Einsatz von Elementen zur Netzkopplung	B 3.101	(6.1)	(A)	Planung	Allgemeiner Server
M 5.14	Absicherung interner Remote-Zugänge	B 4.1	(6.7)	(A)	Planung	Heterogene Netze
M 5.15	Absicherung externer Remote-Zugänge	B 3.401	(8.1)	(A)	Umsetzg.	TK-Anlage
M 5.16	Übersicht über Netzdienste	B 3.401	(8.1)	(A)	Umsetzg.	TK-Anlage
M 5.17	Einsatz der Sicherheitsmechanismen von NFS	B 3.102	(6.2)	(B)	Planung	Server unter Unix
		B 3.102	(6.2)	(A)	Umsetzg.	Server unter Unix
		B 3.204	(5.2)	(A)	Umsetzg.	Client unter Unix
M 5.18	Einsatz der Sicherheitsmechanismen von NIS					

M 5.19	Einsatz der Sicherheitsmechanismen von sendmail	B 3.102	(6.2)	(A)	Umsetzg.	Server unter Unix
		B 3.204	(5.2)	(A)	Umsetzg.	Client unter Unix
M 5.20	Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp	B 3.102	(6.2)	(A)	Umsetzg.	Server unter Unix
		B 3.204	(5.2)	(A)	Umsetzg.	Client unter Unix
M 5.21	Sicherer Einsatz von telnet, ftp, tftp und rexec	B 3.102	(6.2)	(A)	Umsetzg.	Server unter Unix
		B 3.204	(5.2)	(A)	Umsetzg.	Client unter Unix
M 5.22	Kompatibilitätsprüfung des Sender- und Empfängersystems	B 3.102	(6.2)	(A)	Umsetzg.	Server unter Unix
		B 3.204	(5.2)	(A)	Umsetzg.	Client unter Unix
M 5.23	Auswahl einer geeigneten Versandart für den Datenträger	B 5.2	(7.1)	(B)	Umsetzg.	Datenträgeraustausch
		B 5.3	(7.4)	(B)	Umsetzg.	E-Mail
M 5.24	Nutzung eines geeigneten Faxvorblattes	B 5.2	(7.1)	(A)	Umsetzg.	Datenträgeraustausch
M 5.25	Nutzung von Sende- und Empfangsprotokollen	B 3.402	(8.2)	(Z)	Betrieb	Faxgerät
		B 5.6	(8.5)	(Z)	Betrieb	Faxserver
M 5.26	Telefonische Ankündigung einer Faxesendung	B 3.402	(8.2)	(A)	Betrieb	Faxgerät
		B 5.6	(8.5)	(A)	Betrieb	Faxserver
M 5.27	Telefonische Rückversicherung über korrekten Faxempfang	B 3.402	(8.2)	(Z)	Betrieb	Faxgerät
		B 5.6	(8.5)	(Z)	Betrieb	Faxserver
M 5.28	Telefonische Rückversicherung über korrekten Faxabsender	B 3.402	(8.2)	(Z)	Betrieb	Faxgerät
		B 5.6	(8.5)	(Z)	Betrieb	Faxserver
M 5.29	Gelegentliche Kontrolle programmierter Zieladressen und Protokolle	B 3.402	(8.2)	(Z)	Betrieb	Faxgerät
		B 4.5	(8.4)	(C)	Betrieb	LAN-Anbindung eines IT-Systems über ISDN
M 5.30	Aktivierung einer vorhandenen Callback-Option	B 4.3	(7.2)	(Z)	Umsetzg.	Modem
M 5.31	Geeignete Modem-Konfiguration	B 4.3	(7.2)	(A)	Umsetzg.	Modem
M 5.32	Sicherer Einsatz von Kommunikationssoftware	B 4.3	(7.2)	(A)	Planung	Modem
		B 4.5	(8.4)	(A)	Planung	LAN-Anbindung eines IT-Systems über ISDN

M 5.33	Absicherung der per Modem durchgeführten Fernwartung	B 5.3	(7.4)	(A)	Umsetzg.	E-Mail
M 5.34	Einsatz von Einmalpasswörtern	B 4.3	(7.2)	(A)	Betrieb	Modem
M 5.35	Einsatz der Sicherheitsmechanismen von UUCP	B 3.102	(6.2)	(Z)	Planung	Server unter Unix
		B 3.204	(5.2)	(Z)	Planung	Client unter Unix
M 5.36	Verschlüsselung unter Unix und Windows NT	B 3.102	(6.2)	(A)	Umsetzg.	Server unter Unix
		B 3.204	(5.2)	(A)	Umsetzg.	Client unter Unix
M 5.37	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz	B 3.102	(6.2)	(Z)	Planung	Server unter Unix
		B 3.103	(6.4)	(Z)	Planung	Server unter Windows NT
		B 3.204	(5.2)	(Z)	Planung	Client unter Unix
		B 3.101	(6.1)	(B)	Planung	Allgemeiner Server
M 5.38	Sichere Einbindung von DOS-PCs in ein Unix-Netz	B 3.201	(5.99)	(B)	Planung	Allgemeiner Client
		B 3.209	(5.9)	(B)	Planung	Client unter Windows XP
		B 5.1	(6.3)	(B)	Planung	Peer-to-Peer-Dienste
		B 3.102	(6.2)	(B)	Planung	Server unter Unix
M 5.39	Sicherer Einsatz der Protokolle und Dienste	B 3.301	(7.3)	(A)	Betrieb	Sicherheitsgateway (Firewall)
M 5.40	Sichere Einbindung von DOS-PCs in ein Windows NT Netz	B 3.103	(6.4)	(B)	Planung	Server unter Windows NT
M 5.41	Sichere Konfiguration des Fernzugriffs unter Windows NT	B 3.103	(6.4)	(C)	Planung	Server unter Windows NT
M 5.42	Sichere Konfiguration der TCP/IP-Netzverwaltung unter Windows NT	B 3.103	(6.4)	(C)	Planung	Server unter Windows NT
M 5.43	Sichere Konfiguration der TCP/IP-Netzdienste unter Windows NT	B 3.103	(6.4)	(B)	Planung	Server unter Windows NT
M 5.44	Einseitiger Verbindungsaufbau	B 4.3	(7.2)	(Z)	Betrieb	Modem
M 5.45	Sicherheit von WWW-Browsern	B 3.201	(5.99)	(B)	Betrieb	Allgemeiner Client
M 5.46	Einsatz von Stand-alone-Systemen zur Nutzung des Internets	B 3.301	(7.3)	(A)	Betrieb	Sicherheitsgateway (Firewall)
M 5.47	Einrichten einer Closed User Group	B 4.5	(8.4)	(Z)	Planung	LAN-Anbindung eines IT-Systems über ISDN
M 5.48	Authentisierung mittels CLIP/COLP	B 4.5	(8.4)	(A)	Umsetzg.	LAN-Anbindung eines IT-Systems über ISDN
M 5.49	Callback basierend auf CLIP/COLP					

M 5.50	Authentisierung mittels PAP/CHAP	B 4.5	(8.4)	(A)	Umsetzg.	LAN-Anbindung eines IT-Systems über ISDN
M 5.51	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution	B 4.5	(8.4)	(A)	Umsetzg.	LAN-Anbindung eines IT-Systems über ISDN
M 5.52	Sicherheitstechnische Anforderungen an den Kommunikationsrechner	B 5.8	(9.3)	(A)	Umsetzg.	Telearbeit
M 5.53	Schutz vor Mailbomben	B 5.8	(9.3)	(A)	Umsetzg.	Telearbeit
M 5.54	Schutz vor Mailüberlastung und Spam	B 5.3	(7.4)	(B)	Betrieb	E-Mail
M 5.55	Kontrolle von Alias-Dateien und Verteilerlisten	B 5.3	(7.4)	(B)	Betrieb	E-Mail
M 5.56	Sicherer Betrieb eines Mailservers	B 5.3	(7.4)	(B)	Betrieb	E-Mail
M 5.57	Sichere Konfiguration der Mail-Clients	B 5.3	(7.4)	(A)	Betrieb	E-Mail
M 5.58	Installation von ODBC-Treibern	B 5.3	(7.4)	(A)	Umsetzg.	E-Mail
M 5.59	Schutz vor DNS-Spoofing	B 5.7	(9.2)	(B)	Umsetzg.	Datenbanken
M 5.60	Auswahl einer geeigneten Backbone-Technologie	B 3.208	(5.8)	(C)	Umsetzg.	Internet-PC
		B 3.301	(7.3)	(A)	Betrieb	Sicherheitsgateway (Firewall)
		B 5.4	(7.5)	(A)	Betrieb	Webserver
M 5.61	Geeignete physikalische Segmentierung	B 4.1	(6.7)	(A)	Planung	Heterogene Netze
M 5.62	Geeignete logische Segmentierung	B 4.1	(6.7)	(A)	Planung	Heterogene Netze
M 5.63	Einsatz von GnuPG oder PGP	B 4.1	(6.7)	(Z)	Planung	Heterogene Netze
M 5.64	Secure Shell	B 5.3	(7.4)	(Z)	Planung	E-Mail
M 5.66	Verwendung von SSL	B 3.102	(6.2)	(Z)	Planung	Server unter Unix
		B 3.204	(5.2)	(Z)	Planung	Client unter Unix
		B 5.4	(7.5)	(Z)	Planung	Webserver
M 5.67	Verwendung eines Zeitstempel-Dienstes	B 3.208	(5.8)	(B)	Planung	Internet-PC
		B 5.4	(7.5)	(Z)	Planung	Webserver
		B 5.3	(7.4)	(Z)	Planung	E-Mail

M 5.68	Einsatz von Verschlüsselungsverfahren zur Netzkommunikation	B 1.9	(3.9)	(Z)	Planung	Hard- und Software-Management
M 5.69	Schutz vor aktiven Inhalten	B 5.4	(7.5)	(A)	Planung	Webserver
M 5.70	Adreßumsetzung - NAT (Network Address Translation)	B 3.301	(7.3)	(A)	Betrieb	Sicherheitsgateway (Firewall)
M 5.71	Intrusion Detection und Intrusion Response Systeme	B 3.301	(7.3)	(Z)	Betrieb	Sicherheitsgateway (Firewall)
M 5.72	Deaktivieren nicht benötigter Netzdienste	B 3.102	(6.2)	(A)	Umsetzg.	Server unter Unix
		B 3.204	(5.2)	(A)	Umsetzg.	Client unter Unix
M 5.73	Sicherer Betrieb eines Faxservers	B 5.6	(8.5)	(A)	Betrieb	Faxserver
M 5.74	Pflege der Faxserver-Adressbücher und der Verteillisten	B 5.6	(8.5)	(A)	Betrieb	Faxserver
M 5.75	Schutz vor Überlastung des Faxservers	B 5.6	(8.5)	(Z)	Betrieb	Faxserver
M 5.76	Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikation	B 4.4	(7.6)	(Z)	Planung	Remote Access
M 5.77	Bildung von Teilnetzen	B 1.9	(3.9)	(Z)	Planung	Hard- und Software-Management
		B 2.11	(4.8)	(Z)	Planung	Besprechungs-, Veranstaltungs- und Schulungsräume
M 5.78	Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung	B 4.1	(6.7)	(Z)	Planung	Heterogene Netze
M 5.79	Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung	B 3.404	(8.6)	(Z)	Betrieb	Mobiltelefon
M 5.80	Schutz vor Abhören der Raumgespräche über Mobiltelefone	B 3.404	(8.6)	(Z)	Betrieb	Mobiltelefon
M 5.81	Sichere Datenübertragung über Mobiltelefone	B 3.404	(8.6)	(Z)	Betrieb	Mobiltelefon
M 5.82	Sicherer Einsatz von SAMBA	B 3.404	(8.6)	(B)	Betrieb	Mobiltelefon
		B 3.102	(6.2)	(A)	Planung	Server unter Unix
		B 5.1	(6.3)	(A)	Betrieb	Peer-to-Peer-Dienste
M 5.83	Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN	B 3.102	(6.2)	(Z)	Planung	Server unter Unix
M 5.84	Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation	B 5.5	(7.7)	(Z)	Betrieb	Lotus Notes
M 5.85	Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail	B 5.5	(7.7)	(Z)	Betrieb	Lotus Notes

M 5.86	Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes	B 5.5	(7.7)	(C)	Betrieb	Lotus Notes
M 5.87	Vereinbarung über die Anbindung an Netze Dritter	B 1.9	(3.9)	(C)	Planung	Hard- und Software-Management
		B 1.11	(3.10)	(A)	Umsetzg.	Outsourcing
M 5.88	Vereinbarung über Datenaustausch mit Dritten	B 1.9	(3.9)	(C)	Planung	Hard- und Software-Management
		B 1.11	(3.10)	(A)	Umsetzg.	Outsourcing
M 5.89	Konfiguration des sicheren Kanals unter Windows 2000/XP	B 3.106	(6.9)	(A)	Umsetzg.	Server unter Windows 2000
		B 3.209	(5.9)	(A)	Umsetzg.	Client unter Windows XP
M 5.90	Einsatz von IPSec unter Windows 2000/XP	B 3.106	(6.9)	(Z)	Umsetzg.	Server unter Windows 2000
		B 3.209	(5.9)	(Z)	Umsetzg.	Client unter Windows XP
M 5.91	Einsatz von Personal Firewalls für Internet-PCs	B 3.203	(5.3)	(A)	Betrieb	Laptop
		B 3.208	(5.8)	(Z)	Planung	Internet-PC
M 5.92	Sichere Internet-Anbindung von Internet-PCs	B 3.208	(5.8)	(B)	Planung	Internet-PC
M 5.93	Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs	B 3.208	(5.8)	(A)	Betrieb	Internet-PC
M 5.94	Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs	B 3.208	(5.8)	(A)	Betrieb	Internet-PC
M 5.95	Sicherer E-Commerce bei der Nutzung von Internet-PCs	B 3.208	(5.8)	(B)	Betrieb	Internet-PC
M 5.96	Sichere Nutzung von Webmail	B 3.208	(5.8)	(A)	Betrieb	Internet-PC
M 5.97	Absicherung der Kommunikation mit Novell eDirectory	B 5.9	(9.4)	(B)	Betrieb	Novell eDirectory
M 5.98	Schutz vor Missbrauch kostenpflichtiger Einwahlnummern	B 3.208	(5.8)	(C)	Umsetzg.	Internet-PC
M 5.99	SSL/TLS-Absicherung für Exchange 2000	B 5.12	(7.10)	(C)	Umsetzg.	Exchange 2000 / Outlook 2000
M 5.100	Einsatz von Verschlüsselungs- und Signaturverfahren für die Exchange 2000 Kommunikation	B 5.12	(7.10)	(Z)	Betrieb	Exchange 2000 / Outlook 2000
M 5.101	Entfernen nicht benötigter ODBC-Treiber beim IIS-Einsatz	B 5.10	(7.8)	(B)	Umsetzg.	Internet Information Server
M 5.102	Installation von URL-Filtern beim IIS-Einsatz	B 5.10	(7.8)	(B)	Umsetzg.	Internet Information Server
M 5.103	Entfernen sämtlicher Netzwerkfreigaben beim IIS-Einsatz					

M 5.104	Konfiguration des TCP/IP-Filters beim IIS-Einsatz	B 5.10	(7.8)	(B)	Umsetzg.	Internet Information Server
M 5.105	Vorbeugen vor SYN-Attacken auf den IIS	B 5.10	(7.8)	(C)	Umsetzg.	Internet Information Server
M 5.106	Entfernen nicht vertrauenswürdiger Root-Zertifikate beim IIS-Einsatz	B 5.10	(7.8)	(C)	Umsetzg.	Internet Information Server
M 5.107	Verwendung von SSL im Apache-Webserver	B 5.10	(7.8)	(A)	Umsetzg.	Internet Information Server
M 5.108	Kryptographische Absicherung von E-Mail	B 5.11	(7.9)	(Z)	Umsetzg.	Apache Webserver
M 5.109	Einsatz eines E-Mail-Scanners auf dem Mailserver	B 5.3	(7.4)	(Z)	Planung	E-Mail
M 5.110	Absicherung von E-Mail mit SPHINX (S/MIME)	B 5.3	(7.4)	(Z)	Betrieb	E-Mail
M 5.111	Einrichtung von Access Control Lists auf Routern	B 5.3	(7.4)	(Z)	Planung	E-Mail
M 5.112	Sicherheitsaspekte von Routing-Protokollen	B 3.302	(7.11)	(C)	Umsetzg.	Router und Switches
M 5.113	Einsatz des VTAM Session Management Exit unter z/OS	B 3.302	(7.11)	(C)	Betrieb	Router und Switches
M 5.114	Absicherung der z/OS-Tracefunktionen	B 3.107	(6.10)	(Z)	Umsetzg.	S/390- und zSeries-Mainframe
M 5.115	Integration eines Webserver in ein Sicherheitgateway	B 3.107	(6.10)	(B)	Umsetzg.	S/390- und zSeries-Mainframe
M 5.116	Integration eines E-Mailserver in ein Sicherheitgateway	B 3.301	(7.3)	(Z)	Betrieb	Sicherheitgateway (Firewall)
M 5.117	Integration eines Datenbank-Servers in ein Sicherheitgateway	B 3.301	(7.3)	(Z)	Betrieb	Sicherheitgateway (Firewall)
M 5.118	Integration eines DNS-Servers in ein Sicherheitgateway	B 3.301	(7.3)	(Z)	Betrieb	Sicherheitgateway (Firewall)
M 5.119	Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitgateway	B 3.301	(7.3)	(Z)	Betrieb	Sicherheitgateway (Firewall)
M 5.120	Behandlung von ICMP am Sicherheitgateway	B 3.301	(7.3)	(Z)	Betrieb	Sicherheitgateway (Firewall)
M 5.121	Sichere Kommunikation von unterwegs	B 3.301	(7.3)	(A)	Betrieb	Sicherheitgateway (Firewall)
M 5.122	Sicherer Anschluss von Laptops an lokale Netze	B 3.203	(5.3)	(A)	Betrieb	Laptop
		B 3.405	(8.7)	(B)	Umsetzg.	PDA
		B 3.203	(5.3)	(A)	Betrieb	Laptop



M 5.123	Absicherung der Netzwerkkommunikation unter Windows XP	B 3.209	(5.9)	(B)	Planung	Client unter Windows XP
M 5.124	Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen	B 2.11	(4.8)	(C)	Planung	Besprechungs-, Veranstaltungs- und Schulungsräume
M 6.1	Erstellung einer Übersicht über Verfügbarkeitsanforderungen	B 1.3	(3.3)	(A)	Planung	Notfallvorsorgekonzept
M 6.2	Notfall-Definition, Notfall-Verantwortlicher	B 1.3	(3.3)	(A)	Planung	Notfallvorsorgekonzept
M 6.3	Erstellung eines Notfall-Handbuches	B 1.3	(3.3)	(C)	Planung	Notfallvorsorgekonzept
M 6.4	Dokumentation der Kapazitätsanforderungen der IT-Anwendungen	B 1.3	(3.3)	(B)	Umsetzg.	Notfallvorsorgekonzept
M 6.5	Definition des eingeschränkten IT-Betriebs	B 1.3	(3.3)	(B)	Umsetzg.	Notfallvorsorgekonzept
M 6.6	Untersuchung interner und externer Ausweichmöglichkeiten	B 1.3	(3.3)	(B)	Umsetzg.	Notfallvorsorgekonzept
M 6.7	Regelung der Verantwortung im Notfall	B 1.3	(3.3)	(A)	Umsetzg.	Notfallvorsorgekonzept
M 6.8	Alarmierungsplan	B 1.3	(3.3)	(A)	Umsetzg.	Notfallvorsorgekonzept
M 6.9	Notfall-Pläne für ausgewählte Schadensereignisse	B 1.3	(3.3)	(C)	Umsetzg.	Notfallvorsorgekonzept
M 6.10	Notfall-Plan für DFÜ-Ausfall	B 1.3 B 3.401	(3.3) (8.1)	(C) (B)	Umsetzg. Notfallv.	Notfallvorsorgekonzept TK-Anlage
M 6.11	Erstellung eines Wiederanlaufplans	B 1.3	(3.3)	(B)	Umsetzg.	Notfallvorsorgekonzept
M 6.12	Durchführung von Notfallübungen	B 1.3	(3.3)	(C)	Betrieb	Notfallvorsorgekonzept
M 6.13	Erstellung eines Datensicherungsplans	B 1.3	(3.3)	(A)	Umsetzg.	Notfallvorsorgekonzept
M 6.14	Ersatzbeschaffungsplan	B 1.3	(3.3)	(B)	Beschaff.	Notfallvorsorgekonzept
M 6.15	Lieferantenvereinbarungen	B 1.3	(3.3)	(Z)	Beschaff.	Notfallvorsorgekonzept
M 6.16	Abschließen von Versicherungen	B 1.3 B 2.9	(3.3) (4.6)	(Z) (Z)	Umsetzg. Notfallv.	Notfallvorsorgekonzept Rechenzentrum
M 6.17	Alarmierungsplan und Brandschutzübungen	B 2.1	(4.1)	(A)	Notfallv.	Gebäude

M 6.18	Redundante Leitungsführung	B 2.9	(4.6)	(A)	Notfallv.	Rechenzentrum
M 6.20	Geeignete Aufbewahrung der Backup-Datenträger	B 2.2	(4.2)	(Z)	Notfallv.	Verkabelung
M 6.21	Sicherungskopie der eingesetzten Software	B 1.4 B 3.202	(3.4) (5.99)	(A) (A)	Betrieb Notfallv.	Datensicherungskonzept Allgemeines nicht vernetztes IT-System
M 6.22	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen	B 1.4 B 1.9	(3.4) (3.9)	(C) (C)	Umsetzg. Notfallv.	Datensicherungskonzept Hard- und Software-Management
M 6.23	Verhaltensregeln bei Auftreten eines Computer-Virus	B 1.4 B 3.202	(3.4) (5.99)	(A) (A)	Betrieb Notfallv.	Datensicherungskonzept Allgemeines nicht vernetztes IT-System
M 6.24	Erstellen eines Notfall-Bootmediums	B 1.6	(3.6)	(A)	Notfallv.	Computer-Virenschutzkonzept
M 6.26	Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten	B 3.101 B 3.201	(6.1) (5.99)	(A) (A)	Notfallv. Notfallv.	Allgemeiner Server Allgemeiner Client
M 6.27	Sicheres Update des BIOS	B 3.401	(8.1)	(B)	Notfallv.	TK-Anlage
M 6.28	Vereinbarung über Lieferzeiten "lebensnotwendiger" TK-Baugruppen	B 1.9	(3.9)	(C)	Notfallv.	Hard- und Software-Management
M 6.29	TK-Basisanschluss für Notrufe	B 3.401	(8.1)	(Z)	Notfallv.	TK-Anlage
M 6.30	Katastrophenschaltung	B 3.401	(8.1)	(Z)	Notfallv.	TK-Anlage
M 6.31	Verhaltensregeln nach Verlust der Systemintegrität	B 3.401	(8.1)	(Z)	Notfallv.	TK-Anlage
M 6.32	Regelmäßige Datensicherung	B 3.102 B 3.204	(6.2) (5.2)	(A) (A)	Notfallv. Notfallv.	Server unter Unix Client unter Unix
M 6.33	Entwicklung eines Datensicherungskonzepts	B 1.4 B 3.201 B 3.202	(3.4) (5.99) (5.99)	(A) (A) (A)	Betrieb Notfallv. Notfallv.	Datensicherungskonzept Allgemeiner Client Allgemeines nicht vernetztes IT-System
M 6.34	Erhebung der Einflussfaktoren der Datensicherung	B 1.4	(3.4)	(B)	Planung	Datensicherungskonzept
M 6.35	Festlegung der Verfahrensweise für die Datensicherung	B 1.4	(3.4)	(B)	Planung	Datensicherungskonzept
M 6.36	Festlegung des Minimaldatensicherungskonzeptes	B 1.4	(3.4)	(B)	Planung	Datensicherungskonzept

		B 1.4	(3.4)	(A)	Planung	Datensicherungskonzept
M 6.37	Dokumentation der Datensicherung					
		B 1.4	(3.4)	(A)	Umsetzg.	Datensicherungskonzept
M 6.38	Sicherungskopie der übermittelten Daten					
		B 5.2	(7.1)	(A)	Notfallv.	Datenträgeraustausch
		B 5.3	(7.4)	(A)	Notfallv.	E-Mail
		B 5.8	(9.3)	(B)	Notfallv.	Telearbeit
M 6.39	Auflistung von Händleradressen zur Fax-Wiederbeschaffung					
		B 3.402	(8.2)	(C)	Notfallv.	Faxgerät
M 6.40	Regelmäßige Batterieprüfung/-wechsel					
		B 3.403	(8.3)	(A)	Notfallv.	Anrufbeantworter
M 6.41	Übungen zur Datenrekonstruktion					
		B 1.4	(3.4)	(A)	Notfallv.	Datensicherungskonzept
M 6.42	Erstellung von Rettungsdisketten für Windows NT					
		B 3.103	(6.4)	(A)	Notfallv.	Server unter Windows NT
		B 3.205	(5.5)	(A)	Notfallv.	Client unter Windows NT
M 6.43	Einsatz redundanter Windows NT/2000 Server					
		B 3.103	(6.4)	(Z)	Notfallv.	Server unter Windows NT
		B 3.106	(6.9)	(Z)	Notfallv.	Server unter Windows 2000
M 6.44	Datensicherung unter Windows NT					
		B 3.103	(6.4)	(A)	Notfallv.	Server unter Windows NT
		B 3.205	(5.5)	(A)	Notfallv.	Client unter Windows NT
M 6.45	Datensicherung unter Windows 95					
		B 3.206	(5.6)	(A)	Notfallv.	Client unter Windows 95
M 6.46	Erstellung von Rettungsdisketten für Windows 95					
		B 3.206	(5.6)	(A)	Notfallv.	Client unter Windows 95
M 6.47	Datensicherung bei der Telearbeit					
		B 5.8	(9.3)	(B)	Notfallv.	Telearbeit
M 6.48	Verhaltensregeln nach Verlust der Datenbankintegrität					
		B 5.7	(9.2)	(A)	Notfallv.	Datenbanken
M 6.49	Datensicherung einer Datenbank					
		B 5.5	(7.7)	(A)	Notfallv.	Lotus Notes
		B 5.7	(9.2)	(A)	Notfallv.	Datenbanken
M 6.50	Archivierung von Datenbeständen					
		B 5.7	(9.2)	(A)	Notfallv.	Datenbanken
M 6.51	Wiederherstellung einer Datenbank					
		B 5.7	(9.2)	(B)	Notfallv.	Datenbanken
M 6.52	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten					
		B 4.1	(6.7)	(A)	Notfallv.	Heterogene Netze
M 6.53	Redundante Auslegung der Netzkomponenten					
		B 4.1	(6.7)	(Z)	Notfallv.	Heterogene Netze

M 6.54	Verhaltensregeln nach Verlust der Netzintegrität	B 4.1	(6.7)	(B)	Notfallv.	Heterogene Netze
M 6.55	Reduzierung der Wiederanlaufzeit für Novell Netware Server	B 3.105	(6.6)	(C)	Notfallv.	Server unter Novell Netware 4.x
M 6.56	Datensicherung bei Einsatz kryptographischer Verfahren	B 1.7	(3.7)	(A)	Notfallv.	Kryptokonzept
M 6.57	Erstellen eines Notfallplans für den Ausfall des Managementsystems	B 4.2	(6.8)	(C)	Notfallv.	Netz- und Systemmanagement
M 6.58	Etablierung eines Managementsystems zur Behandlung von Sicherheitsvorfällen	B 1.8	(3.8)	(A)	Planung	Behandlung von Sicherheitsvorfällen
M 6.59	Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen	B 1.8	(3.8)	(A)	Planung	Behandlung von Sicherheitsvorfällen
M 6.60	Verhaltensregeln und Meldewege bei Sicherheitsvorfällen	B 1.8	(3.8)	(A)	Planung	Behandlung von Sicherheitsvorfällen
M 6.61	Eskalationsstrategie für Sicherheitsvorfälle	B 1.8	(3.8)	(C)	Planung	Behandlung von Sicherheitsvorfällen
M 6.62	Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen	B 1.8	(3.8)	(B)	Planung	Behandlung von Sicherheitsvorfällen
M 6.63	Untersuchung und Bewertung eines Sicherheitsvorfalls	B 1.8	(3.8)	(A)	Betrieb	Behandlung von Sicherheitsvorfällen
M 6.64	Behebung von Sicherheitsvorfällen	B 1.8	(3.8)	(A)	Betrieb	Behandlung von Sicherheitsvorfällen
M 6.65	Benachrichtigung betroffener Stellen	B 1.8	(3.8)	(A)	Betrieb	Behandlung von Sicherheitsvorfällen
M 6.66	Nachbereitung von Sicherheitsvorfällen	B 1.8	(3.8)	(B)	Betrieb	Behandlung von Sicherheitsvorfällen
M 6.67	Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle	B 1.8	(3.8)	(Z)	Planung	Behandlung von Sicherheitsvorfällen
M 6.68	Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen	B 3.107	(6.10)	(A)	Notfallv.	S/390- und zSeries-Mainframe
M 6.69	Notfallvorsorge und Ausfallsicherheit bei Faxservern	B 1.8	(3.8)	(C)	Betrieb	Behandlung von Sicherheitsvorfällen
M 6.70	Erstellen eines Notfallplans für den Ausfall des RAS-Systems	B 5.6	(8.5)	(B)	Notfallv.	Faxserver
M 6.71	Datensicherung bei mobiler Nutzung des IT-Systems	B 1.11	(3.10)	(A)	Notfallv.	Outsourcing
		B 4.4	(7.6)	(B)	Notfallv.	Remote Access
M 6.72	Ausfallvorsorge bei Mobiltelefonen	B 3.203	(5.3)	(A)	Notfallv.	Laptop
		B 4.4	(7.6)	(B)	Notfallv.	Remote Access

M 6.73	Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems	B 3.404	(8.6)	(C)	Notfallv.	Mobiltelefon
M 6.74	Notfallarchiv	B 5.5	(7.7)	(B)	Notfallv.	Lotus Notes
M 6.75	Redundante Kommunikationsverbindungen	B 2.9	(4.6)	(Z)	Notfallv.	Rechenzentrum
M 6.76	Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes	B 1.3	(3.3)	(Z)	Planung	Notfallvorsorgekonzept
M 6.77	Erstellung von Rettungsdisketten für Windows 2000	B 3.106	(6.9)	(C)	Notfallv.	Server unter Windows 2000
		B 3.209	(5.9)	(C)	Notfallv.	Client unter Windows XP
M 6.78	Datensicherung unter Windows 2000/XP	B 3.106	(6.9)	(A)	Notfallv.	Server unter Windows 2000
		B 3.207	(5.7)	(A)	Notfallv.	Client unter Windows 2000
M 6.79	Datensicherung beim Einsatz von Internet-PCs	B 3.106	(6.9)	(A)	Notfallv.	Server unter Windows 2000
		B 3.207	(5.7)	(A)	Notfallv.	Client unter Windows 2000
		B 3.209	(5.9)	(A)	Notfallv.	Client unter Windows XP
M 6.80	Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes	B 3.208	(5.8)	(A)	Notfallv.	Internet-PC
M 6.81	Erstellen von Datensicherungen für Novell eDirectory	B 5.9	(9.4)	(A)	Notfallv.	Novell eDirectory
M 6.82	Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen	B 5.9	(9.4)	(A)	Notfallv.	Novell eDirectory
M 6.83	Notfallvorsorge beim Outsourcing	B 5.12	(7.10)	(C)	Notfallv.	Exchange 2000 / Outlook 2000
M 6.84	Regelmäßige Datensicherung der System- und Archivdaten	B 1.11	(3.10)	(A)	Notfallv.	Outsourcing
M 6.85	Erstellung eines Notfallplans für den Ausfall des IIS	B 1.12	(9.5)	(A)	Notfallv.	Archivierung
M 6.86	Schutz vor schädlichem Code auf dem IIS	B 5.10	(7.8)	(C)	Notfallv.	Internet Information Server
M 6.87	Datensicherung auf dem IIS	B 5.10	(7.8)	(B)	Umsetzg.	Internet Information Server
M 6.88	Erstellen eines Notfallplans für den Webserver	B 5.10	(7.8)	(A)	Notfallv.	Internet Information Server
M 6.89	Notfallvorsorge für einen Apache-Webserver	B 5.4	(7.5)	(B)	Notfallv.	Webserver
M 6.90	Datensicherung und Archivierung von E-Mails	B 5.11	(7.9)	(A)	Notfallv.	Apache Webserver

M 6.91	Datensicherung und Recovery bei Routern und Switches	B 5.3	(7.4)	(C)	Notfallv.	E-Mail
M 6.92	Notfallvorsorge bei Routern und Switches	B 3.302	(7.11)	(C)	Notfallv.	Router und Switches
M 6.93	Notfallvorsorge für z/OS-Systeme	B 3.302	(7.11)	(C)	Notfallv.	Router und Switches
M 6.94	Notfallvorsorge bei Sicherheit Gateways	B 3.107	(6.10)	(A)	Notfallv.	S/390- und zSeries-Mainframe
M 6.95	Ausfallvorsorge und Datensicherung bei PDAs	B 3.301	(7.3)	(C)	Notfallv.	Sicherheit Gateway (Firewall)
M 6.96	Notfallvorsorge für einen Server	B 3.405	(8.7)	(C)	Notfallv.	PDA
		B 3.101	(6.1)	(A)	Notfallv.	Allgemeiner Server