Gelöschte Maßnahmenzuordnungen

Baustein	Alt	Bausteinname	Maßnahme	Zertifikat	Maßnahmentitel
B 1.0	(3.0)	IT-Sicherheitsmanagement			
			M 2.191	(A)	Etablierung des IT-Sicherheitsprozesses
			M 2.194	(A)	Erstellung einer Übersicht über vorhandene IT-Systeme
			M 2.196	(C)	Umsetzung des IT-Sicherheitskonzepts nach einem Realisierungsplan
			M 2.198	(A)	Sensibilisierung der Mitarbeiter für IT-Sicherheit
			M 2.202	(Z)	Erstellung eines Handbuchs zur IT-Sicherheit
			M 2.203	(Z)	Aufbau einer Informationsbörse zur IT-Sicherheit
B 1.6	(3.6)	Computer-Virenschutzkonzept			
			M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
			M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
			M 2.34	(X)	Dokumentation der Veränderungen an einem bestehenden System
			M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
			M 6.24	(Z)	Erstellen eines Notfall-Bootmediums
			M 6.32	(A)	Regelmäßige Datensicherung
B 1.7	(3.7)	Kryptokonzept			
			M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
			M 2.39	(B)	Reaktion auf Verletzungen der Sicherheitspolitik
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
B 1.9	(3.9)	Hard- und Software-Management			
			M 2.222	(A)	Regelmäßige Kontrollen der technischen IT-Sicherheitsmaßnahmen
			M 2.224	(A)	Vorbeugung gegen Trojanische Pferde
			M 4.42	(Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
			M 6.75	(Z)	Redundante Kommunikationsverbindungen
B 1.10	(9.1)	Standardsoftware			
			M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
			M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
			M 2.35	(A)	Informationsbeschaffung über Sicherheitslücken des Systems
			M 2.40	(A)	Rechtzeitige Beteiligung des Personal-/Betriebsrates
			M 3.4	(A)	Schulung vor Programmnutzung
			M 4.78	(A)	Sorgfältige Durchführung von Konfigurationsänderungen
			M 6.21	(C)	Sicherungskopie der eingesetzten Software
B 1.11	(3.10)	Outsourcing			
			M 3.8	(Z)	Vermeidung von Störungen des Betriebsklimas
B 1.12	(9.5)	Archivierung			
			M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten

			M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
B 2.1	(4.1)	Gebäude			
			M 1.9	(A)	Brandabschottung von Trassen
			M 2.16	(Z)	Beaufsichtigung oder Begleitung von Fremdpersonen
			M 2.18	(Z)	Kontrollgänge
B 2.3	(4.3.1)	Büroraum			
			M 2.14	(A)	Schlüsselverwaltung
			M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
			M 2.18	(Z)	Kontrollgänge
B 2.4	(4.3.2)	Serverraum			
			M 1.8	(A)	Raumbelegung unter Berücksichtigung von Brandlasten
			M 2.14	(A)	Schlüsselverwaltung
			M 2.16	(A)	Beaufsichtigung oder Begleitung von Fremdpersonen
			M 2.18	(Z)	Kontrollgänge
B 2.5	(4.3.3)	Datenträgerarchiv			
			M 1.6	(A)	Einhaltung von Brandschutzvorschriften
			M 1.8	(A)	Raumbelegung unter Berücksichtigung von Brandlasten
			M 2.14	(A)	Schlüsselverwaltung
			M 2.16	(A)	Beaufsichtigung oder Begleitung von Fremdpersonen
			M 2.18	(Z)	Kontrollgänge
B 2.6	(4.3.4)	Raum für technische Infrastruktur			
			M 1.6	(A)	Einhaltung von Brandschutzvorschriften
			M 1.8	(A)	Raumbelegung unter Berücksichtigung von Brandlasten
			M 2.14	(A)	Schlüsselverwaltung
			M 2.16	(A)	Beaufsichtigung oder Begleitung von Fremdpersonen
			M 2.18	(Z)	Kontrollgänge
B 2.8	(4.5)	Häuslicher Arbeitsplatz			
			M 1.1	(A)	Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
			M 1.7	(Z)	Handfeuerlöscher
			M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
B 2.9	(4.6)	Rechenzentrum			
			M 1.1	(A)	Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
			M 1.2	(A)	Regelungen für Zutritt zu Verteilern
			M 1.4	(A)	Blitzschutzeinrichtungen
			M 1.5	(Z)	Galvanische Trennung von Außenleitungen
			M 1.6	(A)	Einhaltung von Brandschutzvorschriften
			M 1.8	(A)	Raumbelegung unter Berücksichtigung von Brandlasten
			M 1.9	(A)	Brandabschottung von Trassen
			M 1.11	(A)	Lagepläne der Versorgungsleitungen
			M 1.14	(Z)	Selbsttätige Entwässerung
			M 1.16	(Z)	Geeignete Standortauswahl

			M 1.17	(Z)	Pförtnerdienst
			M 1.19	(B)	Einbruchsschutz
			M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
			M 2.14	(A)	Schlüsselverwaltung
			M 2.15	(B)	Brandschutzbegehungen
			M 2.16	(A)	Beaufsichtigung oder Begleitung von Fremdpersonen
			M 2.18	(Z)	Kontrollgänge
			M 2.52	(C)	Versorgung und Kontrolle der Verbrauchsgüter
B 3.101	(6.1)	Allgemeiner Server			
			M 1.29	(C)	Geeignete Aufstellung eines IT-Systems
			M 1.32	(A)	Geeignete Aufstellung von Druckern und Kopierern
			M 2.3	(B)	Datenträgerverwaltung
			M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
			M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
			M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
			M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
			M 2.25	(A)	Dokumentation der Systemkonfiguration
			M 2.26	(A)	Ernennung eines Administrators und eines Vertreters
			M 2.30	(A)	Regelung für die Einrichtung von Benutzern / Benutzergruppen
			M 2.34	(A)	Dokumentation der Veränderungen an einem bestehenden System
			M 2.38	(B)	Aufteilung der Administrationstätigkeiten
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
			M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			M 4.1	(A)	Passwortschutz für IT-Systeme
			M 4.2	(A)	Bildschirmsperre
			M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
			M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
			M 4.65	(B)	Test neuer Hard- und Software
			M 5.6	(A)	Obligatorischer Einsatz eines Netzpasswortes
			M 5.7	(A)	Netzverwaltung
			M 5.13	(A)	Geeigneter Einsatz von Elementen zur Netzkopplung
			M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
			M 6.21	(C)	Sicherungskopie der eingesetzten Software
			M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			M 6.25	(X)	Regelmäßige Datensicherung der Server-Festplatte
			M 6.31	(A)	Verhaltensregeln nach Verlust der Systemintegrität
			M 6.32	(A)	Regelmäßige Datensicherung
B 3.102	(6.2)	Server unter Unix			
			M 1.28	(X)	Lokale unterbrechungsfreie Stromversorgung

			M 4.40	(C)	Verhinderung der unautorisierten Nutzung des Rechnermikrofons
			M 4.107	(B)	Nutzung von Hersteller-Ressourcen
B 3.103	(6.4)	Server unter Windows NT			
			M 4.40	(C)	Verhinderung der unautorisierten Nutzung des Rechnermikrofons
			M 5.37	(X)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
			M 6.32	(A)	Regelmäßige Datensicherung
B 3.104	(6.5)	Server unter Novell Netware 3.x			
			M 1.28	(X)	Lokale unterbrechungsfreie Stromversorgung
B 3.105	(6.6)	Server unter Novell Netware 4.x			
			M 1.28	(X)	Lokale unterbrechungsfreie Stromversorgung
B 3.106	(6.9)	Server unter Windows 2000			
			M 2.25	(A)	Dokumentation der Systemkonfiguration
			M 2.40	(A)	Rechtzeitige Beteiligung des Personal-/Betriebsrates
			M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
			M 5.68	(Z)	Einsatz von Verschlüsselungsverfahren zur Netzkommunikation
			M 6.32	(A)	Regelmäßige Datensicherung
B 3.107	(6.10)	S/390- und zSeries-Mainframe			
			M 2.26	(A)	Ernennung eines Administrators und eines Vertreters
			M 2.30	(A)	Regelung für die Einrichtung von Benutzern / Benutzergruppen
			M 4.15	(B)	Gesichertes Login
B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System			
			M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
			M 2.3	(B)	Datenträgerverwaltung
			M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
			M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
			M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
			M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
			M 2.24	(Z)	Einführung eines PC-Checkheftes
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 4.1	(A)	Passwortschutz für IT-Systeme
			M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
			M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
			M 4.84	(A)	Nutzung der BIOS-Sicherheitsmechanismen
			M 6.21	(C)	Sicherungskopie der eingesetzten Software
			M 6.23	(A)	Verhaltensregeln bei Auftreten eines Computer-Virus
			M 6.24	(A)	Erstellen eines Notfall-Bootmediums
			M 6.27	(C)	Sicheres Update des BIOS
B 3.203	(5.3)	Laptop			
			M 2.3	(B)	Datenträgerverwaltung
			M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten

			M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
			M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
			M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
			M 2.22	(Z)	Hinterlegen des Passwortes
			M 2.23	(Z)	Herausgabe einer PC-Richtlinie
			M 2.24	(Z)	Einführung eines PC-Checkheftes
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 4.2	(A)	Bildschirmsperre
			M 4.4	(X)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
			M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
			M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
			M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
			M 6.21	(C)	Sicherungskopie der eingesetzten Software
			M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			M 6.23	(A)	Verhaltensregeln bei Auftreten eines Computer-Virus
			M 6.24	(X)	Erstellen eines Notfall-Bootmediums
			M 6.27	(X)	Sicheres Update des BIOS
			M 6.32	(A)	Regelmäßige Datensicherung
B 3.204	(5.2)	Client unter Unix			
			M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
			M 2.3	(B)	Datenträgerverwaltung
			M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
			M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
			M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
			M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
			M 2.22	(Z)	Hinterlegen des Passwortes
			M 2.25	(A)	Dokumentation der Systemkonfiguration
			M 2.26	(A)	Ernennung eines Administrators und eines Vertreters
			M 2.30	(A)	Regelung für die Einrichtung von Benutzern / Benutzergruppen
			M 2.34	(A)	Dokumentation der Veränderungen an einem bestehenden System
			M 2.35	(A)	Informationsbeschaffung über Sicherheitslücken des Systems
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
			M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			M 4.2	(A)	Bildschirmsperre
			M 4.7	(A)	Änderung voreingestellter Passwörter
			M 4.15	(A)	Gesichertes Login
			M 4.40	(C)	Verhinderung der unautorisierten Nutzung des Rechnermikrofons
			M 4.93	(B)	Regelmäßige Integritätsprüfung

			M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
			M 6.21	(C)	Sicherungskopie der eingesetzten Software
			M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			M 6.32	(A)	Regelmäßige Datensicherung
B 3.205	(5.5)	Client unter Windows NT			
			M 1.29	(A)	Geeignete Aufstellung eines IT-Systems
			M 2.3	(C)	Datenträgerverwaltung
			M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
			M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
			M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
			M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
			M 2.22	(Z)	Hinterlegen des Passwortes
			M 2.23	(Z)	Herausgabe einer PC-Richtlinie
			M 2.24	(Z)	Einführung eines PC-Checkheftes
			M 2.25	(A)	Dokumentation der Systemkonfiguration
			M 2.26	(A)	Ernennung eines Administrators und eines Vertreters
			M 2.30	(X)	Regelung für die Einrichtung von Benutzern / Benutzergruppen
			M 2.34	(A)	Dokumentation der Veränderungen an einem bestehenden System
			M 2.35	(X)	Informationsbeschaffung über Sicherheitslücken des Systems
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
			M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			M 4.1	(A)	Passwortschutz für IT-Systeme
			M 4.2	(A)	Bildschirmsperre
			M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
			M 4.4	(Z)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
			M 4.15	(X)	Gesichertes Login
			M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
			M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
			M 4.84	(A)	Nutzung der BIOS-Sicherheitsmechanismen
			M 4.93	(Z)	Regelmäßige Integritätsprüfung
			M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
			M 6.21	(C)	Sicherungskopie der eingesetzten Software
			M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			M 6.23	(A)	Verhaltensregeln bei Auftreten eines Computer-Virus
			M 6.27	(X)	Sicheres Update des BIOS
			M 6.32	(A)	Regelmäßige Datensicherung
B 3.206	(5.6)	Client unter Windows 95			
			M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
			M 2.3	(B)	Datenträgerverwaltung

			M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
			M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
			M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
			M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
			M 2.22	(Z)	Hinterlegen des Passwortes
			M 2.23	(Z)	Herausgabe einer PC-Richtlinie
			M 2.24	(Z)	Einführung eines PC-Checkheftes
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 4.1	(A)	Passwortschutz für IT-Systeme
			M 4.2	(A)	Bildschirmsperre
			M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
			M 4.4	(Z)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
			M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
			M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
			M 4.84	(A)	Nutzung der BIOS-Sicherheitsmechanismen
			M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
			M 6.21	(C)	Sicherungskopie der eingesetzten Software
			M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			M 6.23	(A)	Verhaltensregeln bei Auftreten eines Computer-Virus
			M 6.27	(C)	Sicheres Update des BIOS
			M 6.32	(A)	Regelmäßige Datensicherung
B 3.207	(5.7)	Client unter Windows 2000			
			M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
			M 2.3	(B)	Datenträgerverwaltung
			M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
			M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
			M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
			M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
			M 2.22	(C)	Hinterlegen des Passwortes
			M 2.25	(A)	Dokumentation der Systemkonfiguration
			M 2.26	(A)	Ernennung eines Administrators und eines Vertreters
			M 2.30	(A)	Regelung für die Einrichtung von Benutzern / Benutzergruppen
			M 2.34	(A)	Dokumentation der Veränderungen an einem bestehenden System
			M 2.35	(A)	Informationsbeschaffung über Sicherheitslücken des Systems
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
			M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			M 4.2	(A)	Bildschirmsperre
			M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms

			M 4.4	(A)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
			M 4.15	(A)	Gesichertes Login
			M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
			M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
			M 4.84	(A)	Nutzung der BIOS-Sicherheitsmechanismen
			M 4.93	(B)	Regelmäßige Integritätsprüfung
			M 4.200	(Z)	Umgang mit USB-Speichermedien
			M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
			M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			M 6.27	(C)	Sicheres Update des BIOS
			M 6.32	(A)	Regelmäßige Datensicherung
B 3.208	(5.8)	Internet-PC			
			M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
B 3.301	(7.3)	Sicherheitsgateway (Firewall)			
			M 2.72	(A)	Anforderungen an eine Firewall
			M 5.45	(B)	Sicherheit von WWW-Browsern
B 3.401	(8.1)	TK-Anlage			
			M 1.2	(A)	Regelungen für Zutritt zu Verteilern
			M 1.9	(A)	Brandabschottung von Trassen
			M 1.22	(Z)	Materielle Sicherung von Leitungen und Verteilern
			M 1.23	(A)	Abgeschlossene Türen
			M 1.27	(B)	Klimatisierung
			M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
			M 2.16	(A)	Beaufsichtigung oder Begleitung von Fremdpersonen
			M 2.17	(A)	Zutrittsregelung und -kontrolle
			M 2.26	(A)	Ernennung eines Administrators und eines Vertreters
			M 2.40	(A)	Rechtzeitige Beteiligung des Personal-/Betriebsrates
			M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
			M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
B 3.403	(8.3)	Anrufbeantworter			
			M 1.23	(Z)	Abgeschlossene Türen
			M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
			M 2.4	(Z)	Regelungen für Wartungs- und Reparaturarbeiten
B 3.404	(8.6)	Mobiltelefon			
			M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
			M 2.22	(A)	Hinterlegen des Passwortes
B 4.1	(6.7)	Heterogene Netze			
			M 1.25	(A)	Überspannungsschutz
			M 1.27	(B)	Klimatisierung

			M 1.28	(A)	Lokale unterbrechungsfreie Stromversorgung
			M 1.29	(X)	Geeignete Aufstellung eines IT-Systems
			M 1.32	(A)	Geeignete Aufstellung von Druckern und Kopierern
			M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
			M 2.22	(A)	Hinterlegen des Passwortes
			M 2.25	(A)	Dokumentation der Systemkonfiguration
			M 2.26	(A)	Ernennung eines Administrators und eines Vertreters
			M 2.34	(A)	Dokumentation der Veränderungen an einem bestehenden System
			M 2.35	(A)	Informationsbeschaffung über Sicherheitslücken des Systems
			M 2.38	(B)	Aufteilung der Administrationstätigkeiten
			M 2.64	(A)	Kontrolle der Protokolldateien
			M 2.143	(B)	Entwicklung eines Netzmanagementkonzeptes
			M 2.144	(A)	Geeignete Auswahl eines Netzmanagement-Protokolls
			M 2.145	(B)	Anforderungen an ein Netzmanagement-Tool
			M 2.146	(A)	Sicherer Betrieb eines Netzmanagementsystems
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
			M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			M 4.15	(A)	Gesichertes Login
			M 4.24	(A)	Sicherstellung einer konsistenten Systemverwaltung
			M 5.12	(X)	Einrichtung eines zusätzlichen Netzadministrators
			M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
B 4.2	(6.8)	Netz- und Systemmanagement			
			M 1.29	(X)	Geeignete Aufstellung eines IT-Systems
			M 2.2	(X)	Betriebsmittelverwaltung
			M 2.25	(A)	Dokumentation der Systemkonfiguration
			M 2.40	(A)	Rechtzeitige Beteiligung des Personal-/Betriebsrates
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
			M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			M 5.68	(Z)	Einsatz von Verschlüsselungsverfahren zur Netzkommunikation
B 4.3	(7.2)	Modem			
			M 2.25	(A)	Dokumentation der Systemkonfiguration
			M 4.30	(B)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
			M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
B 4.4	(7.6)	Remote Access			
			M 1.29	(A)	Geeignete Aufstellung eines IT-Systems
			M 2.2	(B)	Betriebsmittelverwaltung
			M 2.25	(A)	Dokumentation der Systemkonfiguration

			M 2.40	(A)	Rechtzeitige Beteiligung des Personal-/Betriebsrates
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
			M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			M 5.68	(Z)	Einsatz von Verschlüsselungsverfahren zur Netzkommunikation
B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN			
			M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
			M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
			M 2.35	(A)	Informationsbeschaffung über Sicherheitslücken des Systems
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
B 5.1	(6.3)	Peer-to-Peer-Dienste			
			M 4.1	(A)	Passwortschutz für IT-Systeme
			M 4.2	(A)	Bildschirmsperre
			M 4.7	(A)	Änderung voreingestellter Passwörter
			M 6.32	(A)	Regelmäßige Datensicherung
B 5.2	(7.1)	Datenträgeraustausch			
			M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
B 5.3	(7.4)	E-Mail			
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
			M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			M 4.65	(C)	Test neuer Hard- und Software
			M 6.23	(A)	Verhaltensregeln bei Auftreten eines Computer-Virus
B 5.4	(7.5)	Webserver			
			M 2.35	(A)	Informationsbeschaffung über Sicherheitslücken des Systems
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
			M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
			M 4.65	(C)	Test neuer Hard- und Software
			M 5.45	(B)	Sicherheit von WWW-Browsern
B 5.5	(7.7)	Lotus Notes			
			M 1.29	(A)	Geeignete Aufstellung eines IT-Systems
			M 2.2	(B)	Betriebsmittelverwaltung
			M 2.25	(A)	Dokumentation der Systemkonfiguration
			M 2.40	(A)	Rechtzeitige Beteiligung des Personal-/Betriebsrates

			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
			M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			M 5.68	(Z)	Einsatz von Verschlüsselungsverfahren zur Netzkommunikation
			M 6.71	(B)	Datensicherung bei mobiler Nutzung des IT-Systems
B 5.6	(8.5)	Faxserver			
			M 2.30	(A)	Regelung für die Einrichtung von Benutzern / Benutzergruppen
			M 2.64	(A)	Kontrolle der Protokolldateien
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
			M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
B 5.7	(9.2)	Datenbanken			
			M 2.22	(A)	Hinterlegen des Passwortes
			M 2.25	(A)	Dokumentation der Systemkonfiguration
			M 2.111	(A)	Bereithalten von Handbüchern
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
			M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			M 4.1	(A)	Passwortschutz für IT-Systeme
			M 6.32	(A)	Regelmäßige Datensicherung
B 5.8	(9.3)	Telearbeit			
			M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
			M 2.22	(A)	Hinterlegen des Passwortes
			M 2.23	(Z)	Herausgabe einer PC-Richtlinie
			M 2.64	(B)	Kontrolle der Protokolldateien
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
			M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
			M 5.68	(Z)	Einsatz von Verschlüsselungsverfahren zur Netzkommunikation
			M 6.13	(A)	Erstellung eines Datensicherungsplans
			M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			M 6.23	(A)	Verhaltensregeln bei Auftreten eines Computer-Virus
			M 6.32	(A)	Regelmäßige Datensicherung
B 5.9	(9.4)	Novell eDirectory			
			M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
			M 2.22	(A)	Hinterlegen des Passwortes
			M 2.25	(A)	Dokumentation der Systemkonfiguration

			M 2.26	(A)	Ernennung eines Administrators und eines Vertreters
			M 2.30	(A)	Regelung für die Einrichtung von Benutzern / Benutzergruppen
			M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
			M 2.35	(A)	Informationsbeschaffung über Sicherheitslücken des Systems
			M 2.46	(Z)	Geeignetes Schlüsselmanagement
			M 3.4	(A)	Schulung vor Programmnutzung
			M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
			M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			M 4.1	(A)	Passwortschutz für IT-Systeme
			M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
			M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
			M 5.68	(Z)	Einsatz von Verschlüsselungsverfahren zur Netzkommunikation
			M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
			M 6.21	(Z)	Sicherungskopie der eingesetzten Software
B 5.10	(7.8)	Internet Information Server			
			M 5.66	(Z)	Verwendung von SSL