Bausteine mit zugeordneten Gefährdungen und Maßnahmen

Baustein	Alt	Bausteinname	Gefährdung	Gefährdungstitel	Maßnahme	Zertifikat	Maßnahmentitel
B 1.0	(3.0)	IT-Sicherheitsmanagement	G 2.66	Unzureichendes IT-Sicherheitsmanagement	M 2.192	(A)	Erstellung einer IT-Sicherheitsleitlinie
					M 2.193	(A)	Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit
					M 2.195	(A)	Erstellung eines IT-Sicherheitskonzepts
					M 2.197	(A)	Integration der Mitarbeiter in den Sicherheitsprozess
					M 2.199	(A)	Aufrechterhaltung der IT-Sicherheit
					M 2.200	(C)	Managementreporte und -bewertungen der IT-Sicherheit
					M 2.201	(C)	Dokumentation des IT-Sicherheitsprozesses
					M 2.335	(A)	Festlegung der IT-Sicherheitsziele und -strategie
					M 2.336	(A)	Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene
					M 2.337	(A)	Integration der IT-Sicherheit in organisationsweite Abläufe und Prozesse
					M 2.338	(Z)	Erstellung von zielgruppengerechten IT-Sicherheitsrichtlinien
			G 2.105	Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen	M 2.192	(A)	Erstellung einer IT-Sicherheitsleitlinie
					M 2.336	(A)	Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene
					M 2.339	(Z)	Wirtschaftlicher Einsatz von Ressourcen für IT-Sicherheit
					M 2.340	(A)	Beachtung rechtlicher Rahmenbedingungen
			G 2.106	Störung der Geschäftsabläufe aufgrund von IT-Sicherheitsvorfällen	M 2.192	(A)	Erstellung einer IT-Sicherheitsleitlinie
					M 2.335	(A)	Festlegung der IT-Sicherheitsziele und -strategie
					M 2.336	(A)	Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene
			G 2.107	Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes IT-Sicherheitsmanagement	M 2.193	(A)	Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit
					M 2.199	(A)	Aufrechterhaltung der IT-Sicherheit
					M 2.335	(A)	Festlegung der IT-Sicherheitsziele und -strategie
					M 2.336	(A)	Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene
					M 2.339	(Z)	Wirtschaftlicher Einsatz von Ressourcen für IT-Sicherheit
B 1.1	(3.1)	Organisation	G 1.4	Feuer	M 2.18	(Z)	Kontrollgänge
			G 1.5	Wasser	M 2.18	(Z)	Kontrollgänge
			G 1.7	Unzulässige Temperatur und Luftfeuchte	M 2.18	(Z)	Kontrollgänge
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.1	(A)	Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz
					M 2.2	(C)	Betriebsmittelverwaltung
					M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
					M 2.5	(A)	Aufgabenverteilung und Funktionstrennung
					M 2.6	(A)	Vergabe von Zutrittsberechtigungen
					M 2.7	(A)	Vergabe von Zugangsberechtigungen
					M 2.8	(A)	Vergabe von Zugriffsrechten
					M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
					M 2.14	(A)	Schlüsselverwaltung

					M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
					M 2.18	(Z)	Kontrollgänge
					M 2.40	(A)	Rechtzeitige Beteiligung des Personal-/Betriebsrates
					M 2.177	(Z)	Sicherheit bei Umzügen
					M 2.225	(B)	Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten
			G 2.2	Unzureichende Kenntnis über Regelungen	M 2.1	(A)	Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz
					M 2.5	(A)	Aufgabenverteilung und Funktionstrennung
					M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
					M 2.225	(B)	Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten
			G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel	M 2.2	(C)	Betriebsmittelverwaltung
					M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
			G 2.5	Fehlende oder unzureichende Wartung	M 2.2	(C)	Betriebsmittelverwaltung
					M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	M 2.1	(A)	Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz
					M 2.5	(A)	Aufgabenverteilung und Funktionstrennung
					M 2.6	(A)	Vergabe von Zutrittsberechtigungen
					M 2.14	(A)	Schlüsselverwaltung
					M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
					M 2.18	(Z)	Kontrollgänge
					M 2.37	(Z)	"Der aufgeräumte Arbeitsplatz"
					M 2.39	(B)	Reaktion auf Verletzungen der Sicherheitspolitik
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.1	(A)	Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz
					M 2.6	(A)	Vergabe von Zutrittsberechtigungen
					M 2.7	(A)	Vergabe von Zugangsberechtigungen
					M 2.8	(A)	Vergabe von Zugriffsrechten
					M 2.39	(B)	Reaktion auf Verletzungen der Sicherheitspolitik
					M 2.225	(B)	Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten
			G 2.8	Unkontrollierter Einsatz von Betriebsmitteln	M 2.1	(A)	Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz
					M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
					M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
					M 2.18	(Z)	Kontrollgänge
			G 4.1	Ausfall der Stromversorgung	M 2.18	(Z)	Kontrollgänge
			G 4.2	Ausfall interner Versorgungsnetze	M 2.18	(Z)	Kontrollgänge
			G 4.3	Ausfall vorhandener Sicherungseinrichtungen	M 2.18	(Z)	Kontrollgänge
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
					M 2.18	(Z)	Kontrollgänge
			G 5.2	Manipulation an Daten oder Software	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
			G 5.3	Unbefugtes Eindringen in ein Gebäude	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen

					M 2.18	(Z)	Kontrollgänge
			G 5.4	Diebstahl	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
					M 2.18	(Z)	Kontrollgänge
			G 5.5	Vandalismus	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
					M 2.18	(Z)	Kontrollgänge
			G 5.6	Anschlag	M 2.18	(Z)	Kontrollgänge
			G 5.12	Abhören von Telefongesprächen und Datenübertragungen	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
			G 5.13	Abhören von Räumen	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
			G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal	M 2.18	(Z)	Kontrollgänge
			G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
					M 2.18	(Z)	Kontrollgänge
			G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
			G 5.102	Sabotage	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
					M 2.18	(Z)	Kontrollgänge
B 1.2	(3.2)	Personal	G 1.1	Personalausfall	M 3.3	(A)	Vertretungsregelungen
					M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
					M 3.50	(Z)	Auswahl von Personal
			G 1.2	Ausfall des IT-Systems	M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			G 2.2	Unzureichende Kenntnis über Regelungen	M 3.1	(A)	Geregelte Einarbeitung/Einweisung neuer Mitarbeiter
					M 3.4	(A)	Schulung vor Programmnutzung
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
					M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			G 2.7	Unerlaubte Ausübung von Rechten	M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
					M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
					M 3.33	(Z)	Sicherheitsüberprüfung von Mitarbeitern
					M 3.51	(Z)	Geeignetes Konzept für Personaleinsatz und -qualifizierung
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 3.1	(A)	Geregelte Einarbeitung/Einweisung neuer Mitarbeiter
					M 3.4	(A)	Schulung vor Programmnutzung
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
					M 3.50	(Z)	Auswahl von Personal
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	M 3.1	(A)	Geregelte Einarbeitung/Einweisung neuer Mitarbeiter
					M 3.2	(A)	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
					M 3.4	(A)	Schulung vor Programmnutzung
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
					M 3.7	(Z)	Anlaufstelle bei persönlichen Problemen
					M 3.8	(Z)	Vermeidung von Störungen des Betriebsklimas
					M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			G 3.3	Nichtbeachtung von IT-	M 3.1	(A)	Geregelte Einarbeitung/Einweisung neuer Mitarbeiter

				Sicherheitsmaßnahmen	M 3.2	(A)	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
					M 3.4	(A)	Schulung vor Programmnutzung
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
					M 3.7	(Z)	Anlaufstelle bei persönlichen Problemen
					M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
					M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
					M 3.51	(Z)	Geeignetes Konzept für Personaleinsatz und -qualifizierung
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 3.1	(A)	Geregelte Einarbeitung/Einweisung neuer Mitarbeiter
					M 3.4	(A)	Schulung vor Programmnutzung
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
					M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
					M 3.51	(Z)	Geeignetes Konzept für Personaleinsatz und -qualifizierung
			G 3.9	Fehlerhafte Administration des IT-Systems	M 3.4	(A)	Schulung vor Programmnutzung
					M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
					M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
					M 3.51	(Z)	Geeignetes Konzept für Personaleinsatz und -qualifizierung
			G 3.36	Fehlinterpretation von Ereignissen	M 3.4	(A)	Schulung vor Programmnutzung
					M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			G 3.37	Unproduktive Suchzeiten	M 3.4	(A)	Schulung vor Programmnutzung
			G 3.43	Ungeeigneter Umgang mit Passwörtern	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
			G 3.44	Sorglosigkeit im Umgang mit Informationen	M 3.4	(A)	Schulung vor Programmnutzung
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
					M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 3.2	(A)	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
					M 3.4	(A)	Schulung vor Programmnutzung
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
					M 3.6	(A)	Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern
					M 3.7	(Z)	Anlaufstelle bei persönlichen Problemen
					M 3.8	(Z)	Vermeidung von Störungen des Betriebsklimas
					M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
					M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			G 5.2	Manipulation an Daten oder Software	M 3.2	(A)	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
					M 3.4	(A)	Schulung vor Programmnutzung

					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
					M 3.6	(A)	Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern
					M 3.7	(Z)	Anlaufstelle bei persönlichen Problemen
					M 3.8	(Z)	Vermeidung von Störungen des Betriebsklimas
					M 3.10	(A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
					M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
			G 5.20	Missbrauch von Administratorrechten	M 3.33	(Z)	Sicherheitsüberprüfung von Mitarbeitern
			G 5.23	Computer-Viren	M 3.4	(A)	Schulung vor Programmnutzung
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			G 5.42	Social Engineering	M 3.1	(A)	Geregelte Einarbeitung/Einweisung neuer Mitarbeiter
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			G 5.43	Makro-Viren	M 3.4	(A)	Schulung vor Programmnutzung
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			G 5.80	Hoax	M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
			G 5.104	Ausspähen von Informationen	M 3.1	(A)	Geregelte Einarbeitung/Einweisung neuer Mitarbeiter
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
B 1.3	(3.3)	Notfallvorsorgekonzept	G 1.2	Ausfall des IT-Systems	M 6.1	(A)	Erstellung einer Übersicht über Verfügbarkeitsanforderungen
					M 6.2	(A)	Notfall-Definition, Notfall-Verantwortlicher
					M 6.3	(C)	Erstellung eines Notfall-Handbuches
					M 6.4	(B)	Dokumentation der Kapazitätsanforderungen der IT-Anwendungen
					M 6.5	(B)	Definition des eingeschränkten IT-Betriebs
					M 6.6	(B)	Untersuchung interner und externer Ausweichmöglichkeiten
					M 6.7	(A)	Regelung der Verantwortung im Notfall
					M 6.8	(A)	Alarmierungsplan
					M 6.9	(C)	Notfall-Pläne für ausgewählte Schadensereignisse
					M 6.10	(C)	Notfall-Plan für DFÜ-Ausfall
					M 6.11	(B)	Erstellung eines Wiederanlaufplans
					M 6.12	(C)	Durchführung von Notfallübungen
					M 6.13	(A)	Erstellung eines Datensicherungsplans
					M 6.14	(B)	Ersatzbeschaffungsplan
					M 6.15	(Z)	Lieferantenvereinbarungen
					M 6.16	(Z)	Abschließen von Versicherungen
					M 6.75	(Z)	Redundante Kommunikationsverbindungen
B 1.4	(3.4)	Datensicherungskonzept	G 4.13	Verlust gespeicherter Daten	M 2.41	(A)	Verpflichtung der Mitarbeiter zur Datensicherung
					M 2.137	(A)	Beschaffung eines geeigneten Datensicherungssystems
					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
					M 6.33	(B)	Entwicklung eines Datensicherungskonzepts
					M 6.34	(B)	Erhebung der Einflussfaktoren der Datensicherung

					M 6.35	(B)	Festlegung der Verfahrensweise für die Datensicherung
					M 6.36	(A)	Festlegung des Minimaldatensicherungskonzeptes
					M 6.37	(A)	Dokumentation der Datensicherung
					M 6.41	(A)	Übungen zur Datenrekonstruktion
B 1.6	(3.6)	Computer-Virenschutzkonzept	G 2.1	Fehlende oder unzureichende Regelungen	M 2.154	(A)	Erstellung eines Computer-Virenschutzkonzepts
					M 2.156	(A)	Auswahl einer geeigneten Computer-Virenschutz-Strategie
					M 2.160	(A)	Regelungen zum Computer-Virenschutz
					M 2.224	(A)	Vorbeugung gegen Trojanische Pferde
			G 2.2	Unzureichende Kenntnis über Regelungen	M 2.154	(A)	Erstellung eines Computer-Virenschutzkonzepts
					M 2.160	(A)	Regelungen zum Computer-Virenschutz
			G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel	M 2.157	(A)	Auswahl eines geeigneten Computer-Viren-Suchprogramms
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	M 2.154	(A)	Erstellung eines Computer-Virenschutzkonzepts
			G 2.8	Unkontrollierter Einsatz von Betriebsmitteln	M 2.154	(A)	Erstellung eines Computer-Virenschutzkonzepts
					M 2.155	(A)	Identifikation potentiell von Computer-Viren betroffener IT-Systeme
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	M 2.154	(A)	Erstellung eines Computer-Virenschutzkonzepts
					M 2.155	(A)	Identifikation potentiell von Computer-Viren betroffener IT-Systeme
					M 2.156	(A)	Auswahl einer geeigneten Computer-Virenschutz-Strategie
					M 2.159	(A)	Aktualisierung der eingesetzten Computer-Viren-Suchprogramme
					M 2.160	(A)	Regelungen zum Computer-Virenschutz
			G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren	M 2.154	(A)	Erstellung eines Computer-Virenschutzkonzepts
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 2.224	(A)	Vorbeugung gegen Trojanische Pferde
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.160	(A)	Regelungen zum Computer-Virenschutz
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 6.23	(A)	Verhaltensregeln bei Auftreten eines Computer-Virus
			G 3.44	Sorglosigkeit im Umgang mit Informationen	M 2.224	(A)	Vorbeugung gegen Trojanische Pferde
			G 4.22	Software-Schwachstellen oder -Fehler	M 2.224	(A)	Vorbeugung gegen Trojanische Pferde
			G 5.2	Manipulation an Daten oder Software	M 2.157	(A)	Auswahl eines geeigneten Computer-Viren-Suchprogramms
					M 2.158	(A)	Meldung von Computer-Virusinfektionen
					M 2.159	(A)	Aktualisierung der eingesetzten Computer-Viren-Suchprogramme
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 6.23	(A)	Verhaltensregeln bei Auftreten eines Computer-Virus
			G 5.21	Trojanische Pferde	M 2.157	(A)	Auswahl eines geeigneten Computer-Viren-Suchprogramms
					M 2.158	(A)	Meldung von Computer-Virusinfektionen
					M 2.159	(A)	Aktualisierung der eingesetzten Computer-Viren-Suchprogramme
					M 2.224	(A)	Vorbeugung gegen Trojanische Pferde
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms

					M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
			G 5.23	Computer-Viren	M 2.157	(A)	Auswahl eines geeigneten Computer-Viren-Suchprogramms
					M 2.158	(A)	Meldung von Computer-Virusinfektionen
					M 2.159	(A)	Aktualisierung der eingesetzten Computer-Viren-Suchprogramme
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
					M 4.84	(A)	Nutzung der BIOS-Sicherheitsmechanismen
					M 6.23	(A)	Verhaltensregeln bei Auftreten eines Computer-Virus
			G 5.43	Makro-Viren	M 2.157	(A)	Auswahl eines geeigneten Computer-Viren-Suchprogramms
					M 2.158	(A)	Meldung von Computer-Virusinfektionen
					M 2.159	(A)	Aktualisierung der eingesetzten Computer-Viren-Suchprogramme
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
					M 6.23	(A)	Verhaltensregeln bei Auftreten eines Computer-Virus
			G 5.80	Hoax	M 2.157	(A)	Auswahl eines geeigneten Computer-Viren-Suchprogramms
					M 2.158	(A)	Meldung von Computer-Virusinfektionen
					M 2.159	(A)	Aktualisierung der eingesetzten Computer-Viren-Suchprogramme
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
			G 5.127	Spyware	M 4.253	(A)	Schutz vor Spyware
B 1.7	(3.7)	Kryptokonzept	G 2.1	Fehlende oder unzureichende Regelungen	M 2.46	(A)	Geeignetes Schlüsselmanagement
					M 2.166	(A)	Regelung des Einsatzes von Kryptomodulen
					M 4.86	(A)	Sichere Rollenteilung und Konfiguration der Kryptomodule
			G 2.2	Unzureichende Kenntnis über Regelungen	M 3.23	(A)	Einführung in kryptographische Grundbegriffe
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	M 2.166	(A)	Regelung des Einsatzes von Kryptomodulen
			G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung	M 2.46	(A)	Geeignetes Schlüsselmanagement
					M 2.164	(A)	Auswahl eines geeigneten kryptographischen Verfahrens
					M 2.165	(A)	Auswahl eines geeigneten kryptographischen Produktes
					M 3.23	(A)	Einführung in kryptographische Grundbegriffe
					M 6.56	(A)	Datensicherung bei Einsatz kryptographischer Verfahren
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 2.46	(A)	Geeignetes Schlüsselmanagement
					M 2.164	(A)	Auswahl eines geeigneten kryptographischen Verfahrens
					M 2.165	(A)	Auswahl eines geeigneten kryptographischen Produktes
					M 2.166	(A)	Regelung des Einsatzes von Kryptomodulen
					M 3.23	(A)	Einführung in kryptographische Grundbegriffe
					M 4.86	(A)	Sichere Rollenteilung und Konfiguration der Kryptomodule
			G 3.32	Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von	M 2.163	(A)	Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte

				kryptographischen Verfahren	M 2.165	(A)	Auswahl eines geeigneten kryptographischen Produktes
			G 3.33	Fehlbedienung von Kryptomodulen	M 3.23	(A)	Einführung in kryptographische Grundbegriffe
					M 4.86	(A)	Sichere Rollenteilung und Konfiguration der Kryptomodule
					M 4.90	(A)	Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells
			G 4.22	Software-Schwachstellen oder -Fehler	M 2.165	(A)	Auswahl eines geeigneten kryptographischen Produktes
					M 2.166	(A)	Regelung des Einsatzes von Kryptomodulen
					M 3.23	(A)	Einführung in kryptographische Grundbegriffe
					M 4.88	(A)	Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen
					M 4.90	(A)	Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells
			G 4.33	Schlechte oder fehlende Authentikation	M 2.164	(A)	Auswahl eines geeigneten kryptographischen Verfahrens
					M 2.165	(A)	Auswahl eines geeigneten kryptographischen Produktes
			G 4.34	Ausfall eines Kryptomoduls	M 2.46	(A)	Geeignetes Schlüsselmanagement
					M 2.165	(A)	Auswahl eines geeigneten kryptographischen Produktes
					M 2.166	(A)	Regelung des Einsatzes von Kryptomodulen
					M 4.87	(Z)	Physikalische Sicherheit von Kryptomodulen
					M 6.56	(A)	Datensicherung bei Einsatz kryptographischer Verfahren
			G 4.35	Unsichere kryptographische Algorithmen	M 2.46	(A)	Geeignetes Schlüsselmanagement
					M 2.161	(A)	Entwicklung eines Kryptokonzepts
					M 2.164	(A)	Auswahl eines geeigneten kryptographischen Verfahrens
					M 2.166	(A)	Regelung des Einsatzes von Kryptomodulen
					M 3.23	(A)	Einführung in kryptographische Grundbegriffe
			G 4.36	Fehler in verschlüsselten Daten	M 2.166	(A)	Regelung des Einsatzes von Kryptomodulen
					M 3.23	(A)	Einführung in kryptographische Grundbegriffe
					M 6.56	(A)	Datensicherung bei Einsatz kryptographischer Verfahren
			G 5.27	Nichtanerkennung einer Nachricht	M 2.164	(A)	Auswahl eines geeigneten kryptographischen Verfahrens
					M 2.165	(A)	Auswahl eines geeigneten kryptographischen Produktes
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 2.164	(A)	Auswahl eines geeigneten kryptographischen Verfahrens
					M 2.165	(A)	Auswahl eines geeigneten kryptographischen Produktes
			G 5.81	Unautorisierte Benutzung eines Kryptomoduls	M 2.161	(A)	Entwicklung eines Kryptokonzepts
					M 2.165	(A)	Auswahl eines geeigneten kryptographischen Produktes
					M 2.166	(A)	Regelung des Einsatzes von Kryptomodulen
					M 4.86	(A)	Sichere Rollenteilung und Konfiguration der Kryptomodule
					M 4.87	(Z)	Physikalische Sicherheit von Kryptomodulen
					M 4.88	(A)	Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen
			G 5.82	Manipulation eines Kryptomoduls	M 2.161	(A)	Entwicklung eines Kryptokonzepts
					M 2.162	(A)	Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte
					M 2.163	(A)	Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte
					M 2.164	(A)	Auswahl eines geeigneten kryptographischen Verfahrens
					M 2.165	(A)	Auswahl eines geeigneten kryptographischen Produktes
					M 2.166	(A)	Regelung des Einsatzes von Kryptomodulen
					M 4.86	(A)	Sichere Rollenteilung und Konfiguration der Kryptomodule

					M 4.87	(Z)	Physikalische Sicherheit von Kryptomodulen
					M 4.88	(A)	Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen
					M 4.89	(Z)	Abstrahlsicherheit
			G 5.83	Kompromittierung kryptographischer Schlüssel	M 2.46	(A)	Geeignetes Schlüsselmanagement
					M 2.161	(A)	Entwicklung eines Kryptokonzepts
					M 2.162	(A)	Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte
					M 2.163	(A)	Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte
					M 2.164	(A)	Auswahl eines geeigneten kryptographischen Verfahrens
					M 2.165	(A)	Auswahl eines geeigneten kryptographischen Produktes
					M 2.166	(A)	Regelung des Einsatzes von Kryptomodulen
					M 3.23	(A)	Einführung in kryptographische Grundbegriffe
					M 4.85	(Z)	Geeignetes Schnittstellendesign bei Kryptomodulen
					M 4.87	(Z)	Physikalische Sicherheit von Kryptomodulen
					M 4.88	(A)	Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen
					M 4.89	(Z)	Abstrahlsicherheit
					M 6.56	(A)	Datensicherung bei Einsatz kryptographischer Verfahren
			G 5.84	Gefälschte Zertifikate	M 2.46	(A)	Geeignetes Schlüsselmanagement
					M 2.161	(A)	Entwicklung eines Kryptokonzepts
					M 2.162	(A)	Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte
					M 2.163	(A)	Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte
					M 2.164	(A)	Auswahl eines geeigneten kryptographischen Verfahrens
					M 2.165	(A)	Auswahl eines geeigneten kryptographischen Produktes
					M 2.166	(A)	Regelung des Einsatzes von Kryptomodulen
					M 3.23	(A)	Einführung in kryptographische Grundbegriffe
					M 4.85	(Z)	Geeignetes Schnittstellendesign bei Kryptomodulen
			G 5.85	Integritätsverlust schützenswerter Informationen	M 2.164	(A)	Auswahl eines geeigneten kryptographischen Verfahrens
					M 2.165	(A)	Auswahl eines geeigneten kryptographischen Produktes
B 1.8	(3.8)	Behandlung von Sicherheitsvorfällen	G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfällen	M 6.58	(A)	Etablierung eines Managementsystems zur Behandlung von Sicherheitsvorfällen
					M 6.59	(A)	Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen
					M 6.60	(A)	Verhaltensregeln und Meldewege bei Sicherheitsvorfällen
					M 6.61	(C)	Eskalationsstrategie für Sicherheitsvorfälle
					M 6.62	(B)	Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen
					M 6.63	(A)	Untersuchung und Bewertung eines Sicherheitsvorfalls
					M 6.64	(A)	Behebung von Sicherheitsvorfällen
					M 6.65	(A)	Benachrichtigung betroffener Stellen
					M 6.66	(B)	Nachbereitung von Sicherheitsvorfällen
					M 6.67	(Z)	Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle

					M 6.68	(C)	Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen
B 1.9	(3.9)	Hard- und Software-Management	G 1.1	Personalausfall	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 2.34	(A)	Dokumentation der Veränderungen an einem bestehenden System
					M 2.38	(B)	Aufteilung der Administrationstätigkeiten
			G 1.2	Ausfall des IT-Systems	M 2.25	(A)	Dokumentation der Systemkonfiguration
					M 2.34	(A)	Dokumentation der Veränderungen an einem bestehenden System
					M 6.21	(C)	Sicherungskopie der eingesetzten Software
					M 6.27	(C)	Sicheres Update des BIOS
			G 1.4	Feuer	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
					M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 1.5	Wasser	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
					M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 1.8	Staub, Verschmutzung	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
					M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.3	(B)	Datenträgerverwaltung
					M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
					M 2.11	(A)	Regelung des Passwortgebrauchs
					M 2.26	(A)	Ernennung eines Administrators und eines Vertreters
					M 2.62	(B)	Software-Abnahme- und Freigabe-Verfahren
					M 2.64	(A)	Kontrolle der Protokolldateien
					M 2.167	(B)	Sicheres Löschen von Datenträgern
					M 2.182	(A)	Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen
					M 2.214	(A)	Konzeption des IT-Betriebs
					M 2.216	(C)	Genehmigungsverfahren für IT-Komponenten
					M 2.217	(B)	Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
					M 2.218	(C)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.219	(A)	Kontinuierliche Dokumentation der Informationsverarbeitung
					M 2.220	(A)	Richtlinien für die Zugriffs- bzw. Zugangskontrolle
					M 2.221	(B)	Änderungsmanagement
					M 2.226	(A)	Regelungen für den Einsatz von Fremdpersonal
					M 5.87	(C)	Vereinbarung über die Anbindung an Netze Dritter
					M 5.88	(C)	Vereinbarung über Datenaustausch mit Dritten
			G 2.2	Unzureichende Kenntnis über Regelungen	M 2.111	(A)	Bereithalten von Handbüchern
					M 2.182	(A)	Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen
					M 2.214	(A)	Konzeption des IT-Betriebs
					M 2.226	(A)	Regelungen für den Einsatz von Fremdpersonal
					M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
					M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes

					M 2.64	(A)	Kontrolle der Protokolldateien
					M 2.182	(A)	Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.38	(B)	Aufteilung der Administrationstätigkeiten
					M 4.7	(A)	Änderung voreingestellter Passwörter
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
					M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
					M 2.12	(C)	Betreuung und Beratung von IT-Benutzern
					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	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 2.62	(B)	Software-Abnahme- und Freigabe-Verfahren
					M 2.64	(A)	Kontrolle der Protokolldateien
					M 2.69	(B)	Einrichtung von Standardarbeitsplätzen
					M 2.110	(A)	Datenschutzaspekte bei der Protokollierung
					M 2.182	(A)	Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen
					M 2.221	(B)	Änderungsmanagement
					M 4.65	(C)	Test neuer Hard- und Software
					M 4.78	(A)	Sorgfältige Durchführung von Konfigurationsänderungen
					M 5.77	(Z)	Bildung von Teilnetzen
			G 2.10	Nicht fristgerecht verfügbare Datenträger	M 2.3	(B)	Datenträgerverwaltung
					M 2.218	(C)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
			G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System	M 4.107	(B)	Nutzung von Hersteller-Ressourcen
			G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzern	M 2.65	(C)	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
			G 2.22	Fehlende Auswertung von Protokolldaten	M 2.64	(A)	Kontrolle der Protokolldateien
					M 2.182	(A)	Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen
			G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz	M 4.107	(B)	Nutzung von Hersteller-Ressourcen
			G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten	M 2.11	(A)	Regelung des Passwortgebrauchs
					M 2.30	(A)	Regelung für die Einrichtung von Benutzern / Benutzergruppen
					M 2.110	(A)	Datenschutzaspekte bei der Protokollierung
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 2.214	(A)	Konzeption des IT-Betriebs
					M 2.220	(A)	Richtlinien für die Zugriffs- bzw. Zugangskontrolle
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.135	(A)	Restriktive Vergabe von Zugriffsrechten auf Systemdateien
					M 5.77	(Z)	Bildung von Teilnetzen

					M 5.87	(C)	Vereinbarung über die Anbindung an Netze Dritter
					M 5.88	(C)	Vereinbarung über Datenaustausch mit Dritten
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
					M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
					M 2.11	(A)	Regelung des Passwortgebrauchs
					M 2.62	(B)	Software-Abnahme- und Freigabe-Verfahren
					M 2.167	(B)	Sicheres Löschen von Datenträgern
					M 2.182	(A)	Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen
					M 2.217	(B)	Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
					M 2.219	(A)	Kontinuierliche Dokumentation der Informationsverarbeitung
					M 2.223	(B)	Sicherheitsvorgaben für die Nutzung von Standardsoftware
					M 2.226	(A)	Regelungen für den Einsatz von Fremdpersonal
					M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
					M 4.109	(Z)	Software-Reinstallation bei Arbeitsplatzrechnern
					M 4.134	(C)	Wahl geeigneter Datenformate
					M 4.254	(Z)	Sicherer Einsatz von drahtlosen Tastaturen und Mäusen
					M 5.68	(Z)	Einsatz von Verschlüsselungsverfahren zur Netzkommunikation
					M 5.88	(C)	Vereinbarung über Datenaustausch mit Dritten
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
					M 2.25	(A)	Dokumentation der Systemkonfiguration
					M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.22	(Z)	Hinterlegen des Passwortes
					M 2.25	(A)	Dokumentation der Systemkonfiguration
					M 2.34	(A)	Dokumentation der Veränderungen an einem bestehenden System
					M 2.38	(B)	Aufteilung der Administrationstätigkeiten
					M 4.84	(A)	Nutzung der BIOS-Sicherheitsmechanismen
					M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 3.5	Unbeabsichtigte Leitungsbeschädigung	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
					M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 2.38	(B)	Aufteilung der Administrationstätigkeiten
					M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.25	(A)	Dokumentation der Systemkonfiguration
					M 2.34	(A)	Dokumentation der Veränderungen an einem bestehenden System
					M 2.38	(B)	Aufteilung der Administrationstätigkeiten
					M 4.7	(A)	Änderung voreingestellter Passwörter
			G 3.11	Fehlerhafte Konfiguration von sendmail	M 4.107	(B)	Nutzung von Hersteller-Ressourcen
			G 3.17	Kein ordnungsgemäßer PC-Benutzerwechsel	M 2.65	(C)	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
			G 3.35	Server im laufenden Betrieb ausschalten	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
			G 3.44	Sorglosigkeit im Umgang mit Informationen	M 2.111	(A)	Bereithalten von Handbüchern
					M 2.138	(B)	Strukturierte Datenhaltung

					M 2.215	(B)	Fehlerbehandlung
					M 2.217	(B)	Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
					M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
					M 4.254	(Z)	Sicherer Einsatz von drahtlosen Tastaturen und Mäusen
					M 5.88	(C)	Vereinbarung über Datenaustausch mit Dritten
			G 4.1	Ausfall der Stromversorgung	M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 4.7	Defekte Datenträger	M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 4.8	Bekanntwerden von Softwareschwachstellen	M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
			G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen	M 2.34	(A)	Dokumentation der Veränderungen an einem bestehenden System
			G 4.13	Verlust gespeicherter Daten	M 4.234	(B)	Aussonderung von IT-Systemen
			G 4.22	Software-Schwachstellen oder -Fehler	M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
					M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 2.62	(B)	Software-Abnahme- und Freigabe-Verfahren
					M 2.69	(B)	Einrichtung von Standardarbeitsplätzen
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 2.223	(B)	Sicherheitsvorgaben für die Nutzung von Standardsoftware
					M 4.65	(C)	Test neuer Hard- und Software
					M 4.78	(A)	Sorgfältige Durchführung von Konfigurationsänderungen
					M 4.109	(Z)	Software-Reinstallation bei Arbeitsplatzrechnern
					M 4.134	(C)	Wahl geeigneter Datenformate
			G 4.31	Ausfall oder Störung von Netzkomponenten	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
			G 4.35	Unsichere kryptographische Algorithmen	M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
			G 4.38	Ausfall von Komponenten eines Netz- und Systemmanagementsystems	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
			G 4.39	Software-Konzeptionsfehler	M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
			G 4.43	Undokumentierte Funktionen	M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
					M 2.62	(B)	Software-Abnahme- und Freigabe-Verfahren
					M 2.223	(B)	Sicherheitsvorgaben für die Nutzung von Standardsoftware
					M 4.65	(C)	Test neuer Hard- und Software
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
					M 2.25	(A)	Dokumentation der Systemkonfiguration
					M 2.26	(A)	Ernennung eines Administrators und eines Vertreters
					M 2.64	(A)	Kontrolle der Protokolldateien
					M 2.182	(A)	Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen
					M 4.1	(A)	Passwortschutz für IT-Systeme
					M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 5.2	Manipulation an Daten oder Software	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
					M 2.3	(B)	Datenträgerverwaltung
					M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
					M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
					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	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 2.64	(A)	Kontrolle der Protokolldateien
					M 2.182	(A)	Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 4.1	(A)	Passwortschutz für IT-Systeme
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.84	(A)	Nutzung der BIOS-Sicherheitsmechanismen
					M 4.133	(Z)	Geeignete Auswahl von Authentikationsmechanismen
					M 4.134	(C)	Wahl geeigneter Datenformate
					M 4.135	(A)	Restriktive Vergabe von Zugriffsrechten auf Systemdateien
					M 4.254	(Z)	Sicherer Einsatz von drahtlosen Tastaturen und Mäusen
					M 5.77	(Z)	Bildung von Teilnetzen
					M 5.87	(C)	Vereinbarung über die Anbindung an Netze Dritter
					M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 5.4	Diebstahl	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
					M 1.46	(Z)	Einsatz von Diebstahl-Sicherungen
					M 2.25	(A)	Dokumentation der Systemkonfiguration
					M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 5.9	Unberechtigte IT-Nutzung	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems
					M 2.26	(A)	Ernennung eines Administrators und eines Vertreters
					M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 2.38	(B)	Aufteilung der Administrationstätigkeiten
					M 4.1	(A)	Passwortschutz für IT-Systeme
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.254	(Z)	Sicherer Einsatz von drahtlosen Tastaturen und Mäusen
					M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 5.21	Trojanische Pferde	M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
					M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
					M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.65	(C)	Test neuer Hard- und Software
					M 4.109	(Z)	Software-Reinstallation bei Arbeitsplatzrechnern
					M 4.134	(C)	Wahl geeigneter Datenformate
			G 5.23	Computer-Viren	M 4.84	(A)	Nutzung der BIOS-Sicherheitsmechanismen
					M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 5.26	Analyse des Nachrichtenflusses	M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
					M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
			G 5.43	Makro-Viren	M 4.84	(A)	Nutzung der BIOS-Sicherheitsmechanismen
					M 6.21	(C)	Sicherungskopie der eingesetzten Software
			G 5.68	Unberechtigter Zugang zu den aktiven	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems

				Netzkomponenten	M 4.7	(A)	Änderung voreingestellter Passwörter
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.234	(B)	Aussonderung von IT-Systemen
					M 4.254	(Z)	Sicherer Einsatz von drahtlosen Tastaturen und Mäusen
			G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen	M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 4.7	(A)	Änderung voreingestellter Passwörter
			G 5.82	Manipulation eines Kryptomoduls	M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
			G 5.83	Kompromittierung kryptographischer Schlüssel	M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
			G 5.84	Gefälschte Zertifikate	M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
			G 5.87	Web-Spoofing	M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
B 1.10	(9.1)	Standardsoftware	G 1.2	Ausfall des IT-Systems	M 4.42	(Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.79	(A)	Festlegung der Verantwortlichkeiten im Bereich Standardsoftware
					M 2.85	(A)	Freigabe von Standardsoftware
					M 2.88	(A)	Lizenzverwaltung und Versionskontrolle von Standardsoftware
			G 2.2	Unzureichende Kenntnis über Regelungen	M 4.42	(Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
			G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel	M 2.66	(Z)	Beachtung des Beitrags der Zertifizierung für die Beschaffung
					M 2.80	(A)	Erstellung eines Anforderungskatalogs für Standardsoftware
					M 2.81	(A)	Vorauswahl eines geeigneten Standardsoftwareproduktes
					M 2.82	(B)	Entwicklung eines Testplans für Standardsoftware
					M 2.83	(B)	Testen von Standardsoftware
					M 2.84	(A)	Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware
					M 2.87	(A)	Installation und Konfiguration von Standardsoftware
					M 2.88	(A)	Lizenzverwaltung und Versionskontrolle von Standardsoftware
					M 2.90	(A)	Überprüfung der Lieferung
			G 2.7	Unerlaubte Ausübung von Rechten	M 4.42	(Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
			G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren	M 2.66	(Z)	Beachtung des Beitrags der Zertifizierung für die Beschaffung
					M 2.79	(A)	Festlegung der Verantwortlichkeiten im Bereich Standardsoftware
					M 2.80	(A)	Erstellung eines Anforderungskatalogs für Standardsoftware
					M 2.81	(A)	Vorauswahl eines geeigneten Standardsoftwareproduktes
					M 2.82	(B)	Entwicklung eines Testplans für Standardsoftware

					M 2.83	(B)	Testen von Standardsoftware
					M 2.84	(A)	Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware
					M 2.85	(A)	Freigabe von Standardsoftware
			G 2.27	Fehlende oder unzureichende Dokumentation	M 2.80	(A)	Erstellung eines Anforderungskatalogs für Standardsoftware
					M 2.81	(A)	Vorauswahl eines geeigneten Standardsoftwareproduktes
					M 2.82	(B)	Entwicklung eines Testplans für Standardsoftware
					M 2.83	(B)	Testen von Standardsoftware
					M 2.90	(A)	Überprüfung der Lieferung
			G 2.28	Verstöße gegen das Urheberrecht	M 2.85	(A)	Freigabe von Standardsoftware
					M 2.88	(A)	Lizenzverwaltung und Versionskontrolle von Standardsoftware
					M 2.89	(C)	Deinstallation von Standardsoftware
			G 2.29	Softwaretest mit Produktionsdaten	M 2.82	(B)	Entwicklung eines Testplans für Standardsoftware
					M 2.83	(B)	Testen von Standardsoftware
			G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten	M 4.42	(Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	M 4.42	(Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.66	(Z)	Beachtung des Beitrags der Zertifizierung für die Beschaffung
					M 2.79	(A)	Festlegung der Verantwortlichkeiten im Bereich Standardsoftware
					M 2.84	(A)	Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware
					M 2.85	(A)	Freigabe von Standardsoftware
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 4.42	(Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
			G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten	M 4.42	(Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
			G 3.17	Kein ordnungsgemäßer PC-Benutzerwechsel	M 4.42	(Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
			G 4.7	Defekte Datenträger	M 4.42	(Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
			G 4.8	Bekanntwerden von Softwareschwachstellen	M 2.66	(Z)	Beachtung des Beitrags der Zertifizierung für die Beschaffung
			G 4.22	Software-Schwachstellen oder -Fehler	M 2.66	(Z)	Beachtung des Beitrags der Zertifizierung für die Beschaffung
					M 2.80	(A)	Erstellung eines Anforderungskatalogs für Standardsoftware
					M 2.81	(A)	Vorauswahl eines geeigneten Standardsoftwareproduktes
					M 2.82	(B)	Entwicklung eines Testplans für Standardsoftware
					M 2.83	(B)	Testen von Standardsoftware
					M 2.84	(A)	Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware
					M 2.86	(B)	Sicherstellen der Integrität von Standardsoftware

					M 2.87	(A)	Installation und Konfiguration von Standardsoftware
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
			G 5.2	Manipulation an Daten oder Software	M 4.42	(Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
			G 5.9	Unberechtigte IT-Nutzung	M 4.42	(Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
			G 5.21	Trojanische Pferde	M 2.66	(Z)	Beachtung des Beitrags der Zertifizierung für die Beschaffung
					M 2.82	(B)	Entwicklung eines Testplans für Standardsoftware
					M 2.83	(B)	Testen von Standardsoftware
					M 2.86	(B)	Sicherstellen der Integrität von Standardsoftware
					M 2.87	(A)	Installation und Konfiguration von Standardsoftware
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 4.42	(Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
			G 5.23	Computer-Viren	M 2.82	(B)	Entwicklung eines Testplans für Standardsoftware
					M 2.83	(B)	Testen von Standardsoftware
					M 2.86	(B)	Sicherstellen der Integrität von Standardsoftware
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
			G 5.43	Makro-Viren	M 2.82	(B)	Entwicklung eines Testplans für Standardsoftware
					M 2.83	(B)	Testen von Standardsoftware
					M 2.86	(B)	Sicherstellen der Integrität von Standardsoftware
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
B 1.11	(3.10)	Outsourcing	G 1.10	Ausfall eines Weitverkehrsnetzes	M 2.253	(A)	Vertragsgestaltung mit dem Outsourcing-Dienstleister
					M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben
					M 6.70	(A)	Erstellen eines Notfallplans für den Ausfall des RAS-Systems
					M 6.83	(A)	Notfallvorsorge beim Outsourcing
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.42	(A)	Festlegung der möglichen Kommunikationspartner
					M 2.253	(A)	Vertragsgestaltung mit dem Outsourcing-Dienstleister
					M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben
					M 2.255	(A)	Sichere Migration bei Outsourcing-Vorhaben
					M 2.307	(A)	Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses
					M 5.87	(A)	Vereinbarung über die Anbindung an Netze Dritter
					M 5.88	(A)	Vereinbarung über Datenaustausch mit Dritten
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.221	(A)	Änderungsmanagement
					M 2.226	(A)	Regelungen für den Einsatz von Fremdpersonal
					M 2.253	(A)	Vertragsgestaltung mit dem Outsourcing-Dienstleister
					M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben

					M 2.255	(A)	Sichere Migration bei Outsourcing-Vorhaben
					M 2.256	(A)	Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb
					M 3.33	(Z)	Sicherheitsüberprüfung von Mitarbeitern
			G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren	M 2.221	(A)	Änderungsmanagement
					M 2.253	(A)	Vertragsgestaltung mit dem Outsourcing-Dienstleister
					M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben
					M 2.255	(A)	Sichere Migration bei Outsourcing-Vorhaben
					M 2.256	(A)	Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb
			G 2.47	Ungesicherter Akten- und Datenträgertransport	M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben
			G 2.66	Unzureichendes IT-Sicherheitsmanagement	M 2.250	(A)	Festlegung einer Outsourcing-Strategie
					M 2.253	(A)	Vertragsgestaltung mit dem Outsourcing-Dienstleister
					M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben
			G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten	M 2.221	(A)	Änderungsmanagement
					M 2.226	(A)	Regelungen für den Einsatz von Fremdpersonal
					M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben
					M 2.255	(A)	Sichere Migration bei Outsourcing-Vorhaben
			G 2.83	Fehlerhafte Outsourcing-Strategie	M 2.250	(A)	Festlegung einer Outsourcing-Strategie
			G 2.84	Unzulängliche vertragliche Regelungen mit einem externen Dienstleister	M 2.251	(A)	Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben
					M 2.253	(A)	Vertragsgestaltung mit dem Outsourcing-Dienstleister
					M 2.307	(A)	Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses
			G 2.85	Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens	M 2.253	(A)	Vertragsgestaltung mit dem Outsourcing-Dienstleister
					M 2.307	(A)	Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses
			G 2.86	Abhängigkeit von einem Outsourcing-Dienstleister	M 2.250	(A)	Festlegung einer Outsourcing-Strategie
					M 2.251	(A)	Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben
					M 2.252	(A)	Wahl eines geeigneten Outsourcing-Dienstleisters
					M 2.253	(A)	Vertragsgestaltung mit dem Outsourcing-Dienstleister
					M 2.307	(A)	Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses
			G 2.88	Störung des Betriebsklimas durch ein Outsourcing-Vorhaben	M 2.40	(Z)	Rechtzeitige Beteiligung des Personal-/Betriebsrates
					M 2.252	(A)	Wahl eines geeigneten Outsourcing-Dienstleisters
					M 2.253	(A)	Vertragsgestaltung mit dem Outsourcing-Dienstleister
			G 2.89	Mangelhafte IT-Sicherheit in der Outsourcing-Einführungsphase	M 2.221	(A)	Änderungsmanagement
					M 2.255	(A)	Sichere Migration bei Outsourcing-Vorhaben
			G 2.90	Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister	M 2.253	(A)	Vertragsgestaltung mit dem Outsourcing-Dienstleister
					M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben

					M 6.70	(A)	Erstellen eines Notfallplans für den Ausfall des RAS-Systems
			G 2.93	Unzureichendes Notfallvorsorgekonzept beim Outsourcing	M 6.83	(A)	Notfallvorsorge beim Outsourcing
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 2.221	(A)	Änderungsmanagement
					M 2.252	(A)	Wahl eines geeigneten Outsourcing-Dienstleisters
					M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben
					M 2.255	(A)	Sichere Migration bei Outsourcing-Vorhaben
					M 5.87	(A)	Vereinbarung über die Anbindung an Netze Dritter
					M 5.88	(A)	Vereinbarung über Datenaustausch mit Dritten
			G 4.33	Schlechte oder fehlende Authentikation	M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben
			G 4.34	Ausfall eines Kryptomoduls	M 6.83	(A)	Notfallvorsorge beim Outsourcing
			G 4.48	Ausfall der Systeme eines Outsourcing-Dienstleisters	M 2.252	(A)	Wahl eines geeigneten Outsourcing-Dienstleisters
					M 6.83	(A)	Notfallvorsorge beim Outsourcing
			G 5.10	Missbrauch von Fernwartungszugängen	M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben
					M 2.255	(A)	Sichere Migration bei Outsourcing-Vorhaben
					M 2.256	(A)	Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb
					M 5.87	(A)	Vereinbarung über die Anbindung an Netze Dritter
			G 5.20	Missbrauch von Administratorrechten	M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben
					M 2.256	(A)	Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb
					M 3.33	(Z)	Sicherheitsüberprüfung von Mitarbeitern
			G 5.42	Social Engineering	M 2.42	(A)	Festlegung der möglichen Kommunikationspartner
					M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben
					M 2.255	(A)	Sichere Migration bei Outsourcing-Vorhaben
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 2.42	(A)	Festlegung der möglichen Kommunikationspartner
					M 2.221	(A)	Änderungsmanagement
					M 2.253	(A)	Vertragsgestaltung mit dem Outsourcing-Dienstleister
					M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben
					M 2.255	(A)	Sichere Migration bei Outsourcing-Vorhaben
					M 2.256	(A)	Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb
					M 3.33	(Z)	Sicherheitsüberprüfung von Mitarbeitern
					M 5.87	(A)	Vereinbarung über die Anbindung an Netze Dritter
					M 5.88	(A)	Vereinbarung über Datenaustausch mit Dritten
			G 5.85	Integritätsverlust schützenswerter Informationen	M 2.221	(A)	Änderungsmanagement
					M 2.253	(A)	Vertragsgestaltung mit dem Outsourcing-Dienstleister
					M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben
					M 2.255	(A)	Sichere Migration bei Outsourcing-Vorhaben

					M 2.256	(A)	Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb
					M 3.33	(Z)	Sicherheitsüberprüfung von Mitarbeitern
					M 5.87	(A)	Vereinbarung über die Anbindung an Netze Dritter
					M 5.88	(A)	Vereinbarung über Datenaustausch mit Dritten
			G 5.107	Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister	M 2.221	(A)	Änderungsmanagement
					M 2.252	(A)	Wahl eines geeigneten Outsourcing-Dienstleisters
					M 2.254	(A)	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben
					M 3.33	(Z)	Sicherheitsüberprüfung von Mitarbeitern
B 1.12	(9.5)	Archivierung	G 1.2	Ausfall des IT-Systems	M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 1.7	Unzulässige Temperatur und Luftfeuchte	M 1.59	(B)	Geeignete Aufstellung von Archivsystemen
					M 1.60	(A)	Geeignete Lagerung von Archivmedien
			G 1.9	Datenverlust durch starke Magnetfelder	M 1.59	(B)	Geeignete Aufstellung von Archivsystemen
					M 1.60	(A)	Geeignete Lagerung von Archivmedien
					M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 1.14	Datenverlust durch starkes Licht	M 1.59	(B)	Geeignete Aufstellung von Archivsystemen
					M 1.60	(A)	Geeignete Lagerung von Archivmedien
					M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.260	(B)	Regelmäßige Revision des Archivierungsprozesses
					M 2.262	(A)	Regelung der Nutzung von Archivsystemen
					M 3.2	(A)	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
					M 4.172	(C)	Protokollierung der Archivzugriffe
			G 2.72	Unzureichende Migration von Archivsystemen	M 2.261	(B)	Regelmäßige Marktbeobachtung von Archivsystemen
					M 2.263	(A)	Regelmäßige Aufbereitung von archivierten Datenbeständen
					M 2.266	(C)	Regelmäßige Erneuerung technischer Archivsystem-Komponenten
			G 2.73	Fehlende Revisionsmöglichkeit von Archivsystemen	M 2.242	(A)	Zielsetzung der elektronischen Archivierung
					M 2.244	(A)	Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung
					M 4.168	(A)	Auswahl eines geeigneten Archivsystems
			G 2.74	Unzureichende Ordnungskriterien für Archive	M 2.244	(A)	Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung
					M 2.258	(A)	Konsistente Indizierung von Dokumenten bei der Archivierung
					M 2.260	(B)	Regelmäßige Revision des Archivierungsprozesses
					M 4.171	(A)	Schutz der Integrität der Index-Datenbank von Archivsystemen
			G 2.75	Mangelnde Kapazität von Archivdatenträgern	M 2.244	(A)	Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung
					M 2.257	(C)	Überwachung der Speicherressourcen von Archivmedien
					M 2.261	(B)	Regelmäßige Marktbeobachtung von Archivsystemen

					M 4.168	(A)	Auswahl eines geeigneten Archivsystems
					M 4.172	(C)	Protokollierung der Archivzugriffe
			G 2.76	Unzureichende Dokumentation von Archivzugriffen	M 2.243	(A)	Entwicklung des Archivierungskonzepts
					M 2.244	(A)	Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung
					M 2.245	(A)	Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung
					M 2.246	(A)	Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung
					M 4.172	(C)	Protokollierung der Archivzugriffe
			G 2.77	Unzulängliche Übertragung von Papierdaten in elektronische Archive	M 2.243	(A)	Entwicklung des Archivierungskonzepts
					M 2.244	(A)	Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung
					M 2.245	(A)	Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung
					M 2.246	(A)	Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung
					M 2.260	(B)	Regelmäßige Revision des Archivierungsprozesses
					M 3.2	(A)	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
					M 3.35	(A)	Einweisung der Benutzer in die Bedienung des Archivsystems
			G 2.78	Unzulängliche Auffrischung von Datenbeständen bei der Archivierung	M 2.243	(A)	Entwicklung des Archivierungskonzepts
					M 2.244	(A)	Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung
					M 2.245	(A)	Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung
					M 2.246	(A)	Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung
					M 3.34	(A)	Einweisung in die Administration des Archivsystems
					M 3.35	(A)	Einweisung der Benutzer in die Bedienung des Archivsystems
			G 2.79	Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung	M 2.243	(A)	Entwicklung des Archivierungskonzepts
					M 2.244	(A)	Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung
					M 2.246	(A)	Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung
					M 2.263	(A)	Regelmäßige Aufbereitung von archivierten Datenbeständen
					M 2.265	(Z)	Geeigneter Einsatz digitaler Signaturen bei der Archivierung
					M 3.35	(A)	Einweisung der Benutzer in die Bedienung des Archivsystems
			G 2.80	Unzureichende Durchführung von Revisionen bei der Archivierung	M 2.243	(A)	Entwicklung des Archivierungskonzepts
					M 2.246	(A)	Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung
					M 2.260	(B)	Regelmäßige Revision des Archivierungsprozesses

			G 2.81	Unzureichende Vernichtung von Datenträgern bei der Archivierung	M 2.243	(A)	Entwicklung des Archivierungskonzepts
					M 2.244	(A)	Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung
					M 2.245	(A)	Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung
					M 2.246	(A)	Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung
					M 3.34	(A)	Einweisung in die Administration des Archivsystems
					M 3.35	(A)	Einweisung der Benutzer in die Bedienung des Archivsystems
			G 2.82	Fehlerhafte Planung des Aufstellungsortes von Archivsystemen	M 1.59	(B)	Geeignete Aufstellung von Archivsystemen
					M 2.242	(A)	Zielsetzung der elektronischen Archivierung
					M 2.244	(A)	Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 3.2	(A)	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
					M 3.34	(A)	Einweisung in die Administration des Archivsystems
					M 3.35	(A)	Einweisung der Benutzer in die Bedienung des Archivsystems
					M 4.172	(C)	Protokollierung der Archivzugriffe
					M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten	M 3.2	(A)	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
					M 3.34	(A)	Einweisung in die Administration des Archivsystems
					M 4.172	(C)	Protokollierung der Archivzugriffe
					M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 3.35	Server im laufenden Betrieb ausschalten	M 1.59	(B)	Geeignete Aufstellung von Archivsystemen
					M 4.171	(A)	Schutz der Integrität der Index-Datenbank von Archivsystemen
					M 4.172	(C)	Protokollierung der Archivzugriffe
					M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 3.54	Verwendung ungeeigneter Datenträger bei der Archivierung	M 2.261	(B)	Regelmäßige Marktbeobachtung von Archivsystemen
					M 4.168	(A)	Auswahl eines geeigneten Archivsystems
					M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 3.55	Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen	M 2.260	(B)	Regelmäßige Revision des Archivierungsprozesses
					M 3.2	(A)	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
					M 3.34	(A)	Einweisung in die Administration des Archivsystems
					M 3.35	(A)	Einweisung der Benutzer in die Bedienung des Archivsystems
					M 4.172	(C)	Protokollierung der Archivzugriffe
			G 4.7	Defekte Datenträger	M 1.60	(A)	Geeignete Lagerung von Archivmedien

				M 2.266	(C)	Regelmäßige Erneuerung technischer Archivsystem-Komponenten
				M 4.172	(C)	Protokollierung der Archivzugriffe
				M 4.173	(B)	Regelmäßige Funktions- und Recoverytests bei der Archivierung
				M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 4.13	Verlust gespeicherter Daten	M 1.60	(A)	Geeignete Lagerung von Archivmedien
					M 2.263	(A)	Regelmäßige Aufbereitung von archivierten Datenbeständen
					M 2.266	(C)	Regelmäßige Erneuerung technischer Archivsystem-Komponenten
					M 4.172	(C)	Protokollierung der Archivzugriffe
					M 4.173	(B)	Regelmäßige Funktions- und Recoverytests bei der Archivierung
					M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 4.20	Datenverlust bei erschöpftem Speichermedium	M 2.257	(C)	Überwachung der Speicherressourcen von Archivmedien
					M 2.266	(C)	Regelmäßige Erneuerung technischer Archivsystem-Komponenten
					M 4.172	(C)	Protokollierung der Archivzugriffe
			G 4.26	Ausfall einer Datenbank	M 4.168	(A)	Auswahl eines geeigneten Archivsystems
					M 4.171	(A)	Schutz der Integrität der Index-Datenbank von Archivsystemen
					M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 4.30	Verlust der Datenbankintegrität/-konsistenz	M 4.171	(A)	Schutz der Integrität der Index-Datenbank von Archivsystemen
					M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 4.31	Ausfall oder Störung von Netzkomponenten	M 1.59	(B)	Geeignete Aufstellung von Archivsystemen
					M 4.168	(A)	Auswahl eines geeigneten Archivsystems
					M 4.171	(A)	Schutz der Integrität der Index-Datenbank von Archivsystemen
					M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 4.45	Verzögerte Archivauskunft	M 2.258	(A)	Konsistente Indizierung von Dokumenten bei der Archivierung
					M 2.259	(Z)	Einführung eines übergeordneten Dokumentenmanagements
					M 2.266	(C)	Regelmäßige Erneuerung technischer Archivsystem-Komponenten
					M 4.168	(A)	Auswahl eines geeigneten Archivsystems
					M 4.171	(A)	Schutz der Integrität der Index-Datenbank von Archivsystemen
					M 4.172	(C)	Protokollierung der Archivzugriffe

			G 4.46	Fehlerhafte Synchronisierung von Indexdaten bei der Archivierung	M 4.171	(A)	Schutz der Integrität der Index-Datenbank von Archivsystemen
			G 4.47	Veralten von Kryptoverfahren	M 2.261	(B)	Regelmäßige Marktbeobachtung von Archivsystemen
					M 2.264	(B)	Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung
					M 2.265	(Z)	Geeigneter Einsatz digitaler Signaturen bei der Archivierung
			G 5.2	Manipulation an Daten oder Software	M 1.59	(B)	Geeignete Aufstellung von Archivsystemen
					M 1.60	(A)	Geeignete Lagerung von Archivmedien
					M 3.2	(A)	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
					M 4.172	(C)	Protokollierung der Archivzugriffe
					M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 5.6	Anschlag	M 1.59	(B)	Geeignete Aufstellung von Archivsystemen
					M 1.60	(A)	Geeignete Lagerung von Archivmedien
					M 3.34	(A)	Einweisung in die Administration des Archivsystems
					M 3.35	(A)	Einweisung der Benutzer in die Bedienung des Archivsystems
					M 4.172	(C)	Protokollierung der Archivzugriffe
					M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 5.29	Unberechtigtes Kopieren der Datenträger	M 1.60	(A)	Geeignete Lagerung von Archivmedien
					M 4.172	(C)	Protokollierung der Archivzugriffe
			G 5.82	Manipulation eines Kryptomoduls	M 1.59	(B)	Geeignete Aufstellung von Archivsystemen
					M 1.60	(A)	Geeignete Lagerung von Archivmedien
					M 4.172	(C)	Protokollierung der Archivzugriffe
			G 5.83	Kompromittierung kryptographischer Schlüssel	M 1.59	(B)	Geeignete Aufstellung von Archivsystemen
					M 1.60	(A)	Geeignete Lagerung von Archivmedien
					M 4.172	(C)	Protokollierung der Archivzugriffe
			G 5.85	Integritätsverlust schützenswerter Informationen	M 2.263	(A)	Regelmäßige Aufbereitung von archivierten Datenbeständen
					M 2.265	(Z)	Geeigneter Einsatz digitaler Signaturen bei der Archivierung
					M 4.168	(A)	Auswahl eines geeigneten Archivsystems
					M 4.169	(A)	Verwendung geeigneter Archivmedien
					M 4.170	(A)	Auswahl geeigneter Datenformate für die Archivierung von Dokumenten
					M 4.171	(A)	Schutz der Integrität der Index-Datenbank von Archivsystemen
			G 5.102	Sabotage	M 1.59	(B)	Geeignete Aufstellung von Archivsystemen
					M 1.60	(A)	Geeignete Lagerung von Archivmedien
					M 4.172	(C)	Protokollierung der Archivzugriffe
					M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
			G 5.105	Verhinderung der Dienste von Archivsystemen	M 1.59	(B)	Geeignete Aufstellung von Archivsystemen
					M 1.60	(A)	Geeignete Lagerung von Archivmedien

					M 4.172	(C)	Protokollierung der Archivzugriffe
			G 5.106	Unberechtigtes Überschreiben oder Löschen von Archivmedien	M 3.34	(A)	Einweisung in die Administration des Archivsystems
					M 4.172	(C)	Protokollierung der Archivzugriffe
					M 6.84	(A)	Regelmäßige Datensicherung der System- und Archivdaten
B 1.13	(neu)	IT-Sicherheitssensibilisierung und -schulung	G 2.2	Unzureichende Kenntnis über Regelungen	M 2.198	(A)	Sensibilisierung der Mitarbeiter für IT-Sicherheit
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
					M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
					M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
			G 2.7	Unerlaubte Ausübung von Rechten	M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
			G 2.102	Unzureichende Sensibilisierung für IT-Sicherheit	M 2.198	(A)	Sensibilisierung der Mitarbeiter für IT-Sicherheit
					M 2.312	(A)	Konzeption eines Schulungs- und Sensibilisierungsprogramms zur IT-Sicherheit
					M 3.44	(A)	Sensibilisierung des Managements für IT-Sicherheit
					M 3.47	(Z)	Durchführung von Planspielen zur IT-Sicherheit
					M 3.48	(A)	Auswahl von Trainern oder Schulungsanbietern
					M 3.49	(B)	Schulung zur Vorgehensweise nach IT-Grundschutz
			G 2.103	Unzureichende Schulung der Mitarbeiter	M 2.312	(A)	Konzeption eines Schulungs- und Sensibilisierungsprogramms zur IT-Sicherheit
					M 3.44	(A)	Sensibilisierung des Managements für IT-Sicherheit
					M 3.48	(A)	Auswahl von Trainern oder Schulungsanbietern
					M 3.49	(B)	Schulung zur Vorgehensweise nach IT-Grundschutz
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 2.198	(A)	Sensibilisierung der Mitarbeiter für IT-Sicherheit
					M 3.4	(A)	Schulung vor Programmnutzung
					M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
					M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
					M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
					M 3.46	(A)	Ansprechpartner zu Sicherheitsfragen
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.198	(A)	Sensibilisierung der Mitarbeiter für IT-Sicherheit
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
					M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
					M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
					M 3.47	(Z)	Durchführung von Planspielen zur IT-Sicherheit
					M 3.48	(A)	Auswahl von Trainern oder Schulungsanbietern
					M 3.49	(B)	Schulung zur Vorgehensweise nach IT-Grundschutz
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 3.4	(A)	Schulung vor Programmnutzung
					M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
					M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
					M 3.46	(A)	Ansprechpartner zu Sicherheitsfragen
			G 3.9	Fehlerhafte Administration des IT-Systems	M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
					M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
					M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
			G 3.44	Sorglosigkeit im Umgang mit Informationen	M 2.198	(A)	Sensibilisierung der Mitarbeiter für IT-Sicherheit
					M 2.312	(A)	Konzeption eines Schulungs- und Sensibilisierungsprogramms zur IT-Sicherheit
					M 3.4	(A)	Schulung vor Programmnutzung
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen

					M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
					M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
					M 3.46	(A)	Ansprechpartner zu Sicherheitsfragen
					M 3.47	(Z)	Durchführung von Planspielen zur IT-Sicherheit
					M 3.49	(B)	Schulung zur Vorgehensweise nach IT-Grundschutz
			G 3.77	Mangelhafte Akzeptanz von IT-Sicherheitsmaßnahmen	M 2.198	(A)	Sensibilisierung der Mitarbeiter für IT-Sicherheit
					M 2.312	(A)	Konzeption eines Schulungs- und Sensibilisierungsprogramms zur IT-Sicherheit
					M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
					M 3.44	(A)	Sensibilisierung des Managements für IT-Sicherheit
					M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
					M 3.47	(Z)	Durchführung von Planspielen zur IT-Sicherheit
					M 3.48	(A)	Auswahl von Trainern oder Schulungsanbietern
			G 5.2	Manipulation an Daten oder Software	M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
					M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
					M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
			G 5.9	Unberechtigte IT-Nutzung	M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
					M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
					M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
			G 5.19	Missbrauch von Benutzerrechten	M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
					M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
			G 5.20	Missbrauch von Administratorrechten	M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
					M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
			G 5.42	Social Engineering	M 2.198	(A)	Sensibilisierung der Mitarbeiter für IT-Sicherheit
					M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
					M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
					M 3.47	(Z)	Durchführung von Planspielen zur IT-Sicherheit
					M 3.49	(B)	Schulung zur Vorgehensweise nach IT-Grundschutz
			G 5.104	Ausspähen von Informationen	M 2.198	(A)	Sensibilisierung der Mitarbeiter für IT-Sicherheit
					M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
					M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
					M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
B 2.1	(4.1)	Gebäude	G 1.3	Blitz	M 1.1	(A)	Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
					M 1.4	(B)	Blitzschutzeinrichtungen
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.16	(Z)	Geeignete Standortauswahl
			G 1.4	Feuer	M 1.1	(A)	Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
					M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.4	(B)	Blitzschutzeinrichtungen
					M 1.6	(A)	Einhaltung von Brandschutzvorschriften
					M 1.7	(A)	Handfeuerlöscher
					M 1.8	(A)	Raumbelegung unter Berücksichtigung von Brandlasten
					M 1.10	(Z)	Verwendung von Sicherheitstüren und -fenstern
					M 1.11	(A)	Lagepläne der Versorgungsleitungen
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 2.15	(B)	Brandschutzbegehungen

					M 6.17	(A)	Alarmierungsplan und Brandschutzübungen
			G 1.5	Wasser	M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.14	(Z)	Selbsttätige Entwässerung
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.16	(Z)	Geeignete Standortauswahl
					M 1.18	(Z)	Gefahrenmeldeanlage
			G 2.1	Fehlende oder unzureichende Regelungen	M 1.2	(A)	Regelungen für Zutritt zu Verteilern
					M 1.17	(Z)	Pförtnerdienst
					M 2.14	(A)	Schlüsselverwaltung
					M 2.17	(A)	Zutrittsregelung und -kontrolle
					M 2.308	(Z)	Auszug aus Gebäuden
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	M 1.2	(A)	Regelungen für Zutritt zu Verteilern
					M 1.10	(Z)	Verwendung von Sicherheitstüren und -fenstern
					M 1.12	(A)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.17	(Z)	Pförtnerdienst
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.19	(Z)	Einbruchsschutz
					M 2.14	(A)	Schlüsselverwaltung
					M 2.17	(A)	Zutrittsregelung und -kontrolle
					M 2.308	(Z)	Auszug aus Gebäuden
					M 2.334	(Z)	Auswahl eines geeigneten Gebäudes
			G 4.1	Ausfall der Stromversorgung	M 1.1	(A)	Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
					M 1.2	(A)	Regelungen für Zutritt zu Verteilern
					M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.11	(A)	Lagepläne der Versorgungsleitungen
					M 1.14	(Z)	Selbsttätige Entwässerung
					M 2.334	(Z)	Auswahl eines geeigneten Gebäudes
			G 4.2	Ausfall interner Versorgungsnetze	M 1.1	(A)	Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
					M 1.2	(A)	Regelungen für Zutritt zu Verteilern
					M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.5	(Z)	Galvanische Trennung von Außenleitungen
					M 1.6	(A)	Einhaltung von Brandschutzvorschriften
					M 1.7	(A)	Handfeuerlöscher
					M 1.11	(A)	Lagepläne der Versorgungsleitungen
					M 1.14	(Z)	Selbsttätige Entwässerung
					M 1.18	(Z)	Gefahrenmeldeanlage
			G 4.3	Ausfall vorhandener Sicherungseinrichtungen	M 1.1	(A)	Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
					M 1.2	(A)	Regelungen für Zutritt zu Verteilern
					M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.5	(Z)	Galvanische Trennung von Außenleitungen
					M 1.6	(A)	Einhaltung von Brandschutzvorschriften
					M 1.7	(A)	Handfeuerlöscher
					M 1.11	(A)	Lagepläne der Versorgungsleitungen
					M 1.14	(Z)	Selbsttätige Entwässerung

					M 1.18	(Z)	Gefahrenmeldeanlage
					M 2.15	(B)	Brandschutzbegehungen
			G 5.3	Unbefugtes Eindringen in ein Gebäude	M 1.10	(Z)	Verwendung von Sicherheitstüren und -fenstern
					M 1.12	(A)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.19	(Z)	Einbruchsschutz
					M 2.14	(A)	Schlüsselverwaltung
					M 2.334	(Z)	Auswahl eines geeigneten Gebäudes
			G 5.4	Diebstahl	M 1.10	(Z)	Verwendung von Sicherheitstüren und -fenstern
					M 1.12	(A)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.17	(Z)	Pförtnerdienst
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.19	(Z)	Einbruchsschutz
					M 2.14	(A)	Schlüsselverwaltung
					M 2.17	(A)	Zutrittsregelung und -kontrolle
					M 2.308	(Z)	Auszug aus Gebäuden
			G 5.5	Vandalismus	M 1.10	(Z)	Verwendung von Sicherheitstüren und -fenstern
					M 1.12	(A)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.16	(Z)	Geeignete Standortauswahl
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 2.14	(A)	Schlüsselverwaltung
					M 6.17	(A)	Alarmierungsplan und Brandschutzübungen
			G 5.6	Anschlag	M 1.10	(Z)	Verwendung von Sicherheitstüren und -fenstern
					M 1.12	(A)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.16	(Z)	Geeignete Standortauswahl
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 2.334	(Z)	Auswahl eines geeigneten Gebäudes
					M 6.17	(A)	Alarmierungsplan und Brandschutzübungen
B 2.2	(4.2)	Verkabelung	G 1.6	Kabelbrand	M 1.9	(A)	Brandabschottung von Trassen
					M 1.20	(A)	Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht
			G 2.11	Unzureichende Trassendimensionierung	M 1.21	(A)	Ausreichende Trassendimensionierung
					M 5.2	(A)	Auswahl einer geeigneten Netz-Topographie
					M 5.3	(A)	Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht
					M 6.18	(Z)	Redundante Leitungsführung

			G 2.12	Unzureichende Dokumentation der Verkabelung	M 2.19	(B)	Neutrale Dokumentation in den Verteilern
					M 5.4	(A)	Dokumentation und Kennzeichnung der Verkabelung
			G 2.13	Unzureichend geschützte Verteiler	M 1.22	(Z)	Materielle Sicherung von Leitungen und Verteilern
					M 2.19	(B)	Neutrale Dokumentation in den Verteilern
					M 2.20	(Z)	Kontrolle bestehender Verbindungen
			G 2.32	Unzureichende Leitungskapazitäten	M 5.2	(A)	Auswahl einer geeigneten Netz-Topographie
					M 5.3	(A)	Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht
			G 3.4	Unzulässige Kabelverbindungen	M 2.19	(B)	Neutrale Dokumentation in den Verteilern
					M 2.20	(Z)	Kontrolle bestehender Verbindungen
					M 5.1	(B)	Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen
					M 5.4	(A)	Dokumentation und Kennzeichnung der Verkabelung
			G 3.5	Unbeabsichtigte Leitungsbeschädigung	M 1.20	(A)	Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht
					M 1.21	(A)	Ausreichende Trassendimensionierung
					M 1.22	(Z)	Materielle Sicherung von Leitungen und Verteilern
					M 5.4	(A)	Dokumentation und Kennzeichnung der Verkabelung
					M 5.5	(A)	Schadensmindernde Kabelführung
					M 6.18	(Z)	Redundante Leitungsführung
			G 4.4	Leitungsbeeinträchtigung durch Umfeldfaktoren	M 1.9	(A)	Brandabschottung von Trassen
					M 1.20	(A)	Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht
					M 1.21	(A)	Ausreichende Trassendimensionierung
					M 5.1	(B)	Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen
					M 5.5	(A)	Schadensmindernde Kabelführung
					M 6.18	(Z)	Redundante Leitungsführung
			G 4.5	Übersprechen	M 1.20	(A)	Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht
					M 1.21	(A)	Ausreichende Trassendimensionierung
					M 5.1	(B)	Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen
					M 5.5	(A)	Schadensmindernde Kabelführung
			G 4.21	Ausgleichsströme auf Schirmungen	M 1.39	(Z)	Verhinderung von Ausgleichsströmen auf Schirmungen
			G 5.7	Abhören von Leitungen	M 1.20	(A)	Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht
					M 1.22	(Z)	Materielle Sicherung von Leitungen und Verteilern
					M 2.19	(B)	Neutrale Dokumentation in den Verteilern
					M 2.20	(Z)	Kontrolle bestehender Verbindungen
					M 5.1	(B)	Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen
			G 5.8	Manipulation an Leitungen	M 1.20	(A)	Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht
					M 1.21	(A)	Ausreichende Trassendimensionierung
					M 1.22	(Z)	Materielle Sicherung von Leitungen und Verteilern
					M 2.19	(B)	Neutrale Dokumentation in den Verteilern

					M 2.20	(Z)	Kontrolle bestehender Verbindungen
					M 5.1	(B)	Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen
					M 5.2	(A)	Auswahl einer geeigneten Netz-Topographie
					M 5.3	(A)	Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht
					M 5.5	(A)	Schadensmindernde Kabelführung
B 2.3	(4.3.1)	Büroraum	G 2.1	Fehlende oder unzureichende Regelungen	M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 1.46	(Z)	Einsatz von Diebstahl-Sicherungen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen	M 3.9	(Z)	Ergonomischer Arbeitsplatz
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 1.23	(A)	Abgeschlossene Türen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.2	Manipulation an Daten oder Software	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.4	Diebstahl	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 1.46	(Z)	Einsatz von Diebstahl-Sicherungen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.5	Vandalismus	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
B 2.4	(4.3.2)	Serverraum	G 1.4	Feuer	M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.7	(A)	Handfeuerlöscher
					M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.25	(B)	Überspannungsschutz
					M 1.26	(Z)	Not-Aus-Schalter
					M 1.31	(Z)	Fernanzeige von Störungen
					M 1.52	(Z)	Redundanzen in der technischen Infrastruktur
					M 1.58	(A)	Technische und organisatorische Vorgaben für Serverräume
					M 1.62	(C)	Brandschutz von Patchfeldern
					M 2.21	(A)	Rauchverbot
			G 1.5	Wasser	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.24	(C)	Vermeidung von wasserführenden Leitungen
					M 1.26	(Z)	Not-Aus-Schalter
					M 1.31	(Z)	Fernanzeige von Störungen
					M 1.52	(Z)	Redundanzen in der technischen Infrastruktur

					M 1.58	(A)	Technische und organisatorische Vorgaben für Serverräume
			G 1.7	Unzulässige Temperatur und Luftfeuchte	M 1.27	(B)	Klimatisierung
					M 1.52	(Z)	Redundanzen in der technischen Infrastruktur
			G 1.16	Ausfall von Patchfeldern durch Brand	M 1.62	(C)	Brandschutz von Patchfeldern
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 1.58	(A)	Technische und organisatorische Vorgaben für Serverräume
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 4.1	Ausfall der Stromversorgung	M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.25	(B)	Überspannungsschutz
					M 1.28	(B)	Lokale unterbrechungsfreie Stromversorgung
					M 1.31	(Z)	Fernanzeige von Störungen
					M 1.52	(Z)	Redundanzen in der technischen Infrastruktur
			G 4.2	Ausfall interner Versorgungsnetze	M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.7	(A)	Handfeuerlöscher
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.31	(Z)	Fernanzeige von Störungen
					M 1.52	(Z)	Redundanzen in der technischen Infrastruktur
			G 4.6	Spannungsschwankungen/Überspannung/Unterspannung	M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.25	(B)	Überspannungsschutz
					M 1.28	(B)	Lokale unterbrechungsfreie Stromversorgung
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 1.28	(B)	Lokale unterbrechungsfreie Stromversorgung
					M 1.52	(Z)	Redundanzen in der technischen Infrastruktur
					M 1.58	(A)	Technische und organisatorische Vorgaben für Serverräume
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.2	Manipulation an Daten oder Software	M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 1.58	(A)	Technische und organisatorische Vorgaben für Serverräume
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.3	Unbefugtes Eindringen in ein Gebäude	M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 1.31	(Z)	Fernanzeige von Störungen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.4	Diebstahl	M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern

					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 1.31	(Z)	Fernanzeige von Störungen
					M 1.52	(Z)	Redundanzen in der technischen Infrastruktur
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.5	Vandalismus	M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 1.52	(Z)	Redundanzen in der technischen Infrastruktur
					M 2.17	(A)	Zutrittsregelung und -kontrolle
B 2.5	(4.3.3)	Datenträgerarchiv	G 1.4	Feuer	M 1.7	(A)	Handfeuerlöscher
					M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 2.21	(A)	Rauchverbot
			G 1.5	Wasser	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.24	(Z)	Vermeidung von wasserführenden Leitungen
			G 1.7	Unzulässige Temperatur und Luftfeuchte	M 1.27	(Z)	Klimatisierung
			G 1.8	Staub, Verschmutzung	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 2.21	(A)	Rauchverbot
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.3	Unbefugtes Eindringen in ein Gebäude	M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.4	Diebstahl	M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.5	Vandalismus	M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
B 2.6	(4.3.4)	Raum für technische Infrastruktur	G 1.4	Feuer	M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.7	(A)	Handfeuerlöscher
					M 1.10	(Z)	Verwendung von Sicherheitstüren und -fenstern

					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.25	(A)	Überspannungsschutz
					M 1.26	(Z)	Not-Aus-Schalter
					M 1.31	(Z)	Fernanzeige von Störungen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
					M 2.21	(A)	Rauchverbot
			G 1.5	Wasser	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.24	(Z)	Vermeidung von wasserführenden Leitungen
					M 1.26	(Z)	Not-Aus-Schalter
					M 1.31	(Z)	Fernanzeige von Störungen
			G 1.7	Unzulässige Temperatur und Luftfeuchte	M 1.27	(B)	Klimatisierung
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	M 1.10	(Z)	Verwendung von Sicherheitstüren und -fenstern
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 4.1	Ausfall der Stromversorgung	M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.25	(A)	Überspannungsschutz
			G 4.2	Ausfall interner Versorgungsnetze	M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.7	(A)	Handfeuerlöscher
					M 1.18	(Z)	Gefahrenmeldeanlage
			G 4.6	Spannungsschwankungen/Überspannung/Unterspannung	M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.25	(A)	Überspannungsschutz
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 1.10	(Z)	Verwendung von Sicherheitstüren und -fenstern
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.3	Unbefugtes Eindringen in ein Gebäude	M 1.10	(Z)	Verwendung von Sicherheitstüren und -fenstern
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 1.31	(Z)	Fernanzeige von Störungen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.4	Diebstahl	M 1.10	(Z)	Verwendung von Sicherheitstüren und -fenstern
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.5	Vandalismus	M 1.10	(Z)	Verwendung von Sicherheitstüren und -fenstern
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 2.17	(A)	Zutrittsregelung und -kontrolle
B 2.7	(4.4)	Schutzschrank	G 1.4	Feuer	M 1.7	(B)	Handfeuerlöscher

				M 1.15	(A)	Geschlossene Fenster und Türen
				M 1.18	(Z)	Gefahrenmeldeanlage
				M 1.25	(B)	Überspannungsschutz
				M 1.26	(A)	Not-Aus-Schalter
				M 1.31	(Z)	Fernanzeige von Störungen
				M 2.21	(A)	Rauchverbot
				M 2.95	(A)	Beschaffung geeigneter Schutzschränke
				M 2.96	(A)	Verschluss von Schutzschränken
				M 3.20	(A)	Einweisung in die Bedienung von Schutzschränken
			G 1.5	Wasser	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.24	(Z)	Vermeidung von wasserführenden Leitungen
					M 1.31	(Z)	Fernanzeige von Störungen
					M 2.95	(A)	Beschaffung geeigneter Schutzschränke
					M 2.96	(A)	Verschluss von Schutzschränken
					M 3.20	(A)	Einweisung in die Bedienung von Schutzschränken
			G 1.7	Unzulässige Temperatur und Luftfeuchte	M 1.27	(B)	Klimatisierung
					M 1.31	(Z)	Fernanzeige von Störungen
					M 1.40	(A)	Geeignete Aufstellung von Schutzschränken
					M 2.95	(A)	Beschaffung geeigneter Schutzschränke
					M 2.96	(A)	Verschluss von Schutzschränken
					M 3.20	(A)	Einweisung in die Bedienung von Schutzschränken
			G 1.8	Staub, Verschmutzung	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.27	(B)	Klimatisierung
					M 1.40	(A)	Geeignete Aufstellung von Schutzschränken
					M 2.21	(A)	Rauchverbot
					M 2.95	(A)	Beschaffung geeigneter Schutzschränke
					M 2.96	(A)	Verschluss von Schutzschränken
					M 3.20	(A)	Einweisung in die Bedienung von Schutzschränken
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	M 1.18	(Z)	Gefahrenmeldeanlage
					M 2.17	(C)	Zutrittsregelung und -kontrolle
			G 3.21	Fehlbedienung von Codeschlössern	M 2.95	(A)	Beschaffung geeigneter Schutzschränke
					M 2.97	(A)	Korrekter Umgang mit Codeschlössern
					M 3.20	(A)	Einweisung in die Bedienung von Schutzschränken
			G 4.1	Ausfall der Stromversorgung	M 1.24	(Z)	Vermeidung von wasserführenden Leitungen
					M 1.25	(B)	Überspannungsschutz
					M 1.28	(B)	Lokale unterbrechungsfreie Stromversorgung
					M 1.31	(Z)	Fernanzeige von Störungen
					M 1.40	(A)	Geeignete Aufstellung von Schutzschränken
					M 3.20	(A)	Einweisung in die Bedienung von Schutzschränken
			G 4.2	Ausfall interner Versorgungsnetze	M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.24	(Z)	Vermeidung von wasserführenden Leitungen
					M 1.25	(B)	Überspannungsschutz
					M 1.28	(B)	Lokale unterbrechungsfreie Stromversorgung
					M 1.31	(Z)	Fernanzeige von Störungen
					M 1.40	(A)	Geeignete Aufstellung von Schutzschränken
					M 3.20	(A)	Einweisung in die Bedienung von Schutzschränken

			G 4.3	Ausfall vorhandener Sicherungseinrichtungen	M 1.7	(B)	Handfeuerlöscher
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.24	(Z)	Vermeidung von wasserführenden Leitungen
					M 1.25	(B)	Überspannungsschutz
					M 1.26	(A)	Not-Aus-Schalter
					M 1.28	(B)	Lokale unterbrechungsfreie Stromversorgung
					M 1.31	(Z)	Fernanzeige von Störungen
					M 1.40	(A)	Geeignete Aufstellung von Schutzschränken
					M 2.311	(A)	Planung von Schutzschränken
					M 3.20	(A)	Einweisung in die Bedienung von Schutzschränken
			G 4.4	Leitungsbeeinträchtigung durch Umfeldfaktoren	M 1.41	(Z)	Schutz gegen elektromagnetische Einstrahlung
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 1.28	(B)	Lokale unterbrechungsfreie Stromversorgung
					M 1.31	(Z)	Fernanzeige von Störungen
					M 1.40	(A)	Geeignete Aufstellung von Schutzschränken
					M 2.17	(C)	Zutrittsregelung und -kontrolle
					M 2.95	(A)	Beschaffung geeigneter Schutzschränke
					M 2.96	(A)	Verschluss von Schutzschränken
					M 2.97	(A)	Korrekter Umgang mit Codeschlössern
					M 2.311	(A)	Planung von Schutzschränken
					M 3.20	(A)	Einweisung in die Bedienung von Schutzschränken
			G 5.4	Diebstahl	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 2.17	(C)	Zutrittsregelung und -kontrolle
					M 2.95	(A)	Beschaffung geeigneter Schutzschränke
					M 2.96	(A)	Verschluss von Schutzschränken
					M 2.97	(A)	Korrekter Umgang mit Codeschlössern
					M 3.20	(A)	Einweisung in die Bedienung von Schutzschränken
			G 5.5	Vandalismus	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(Z)	Gefahrenmeldeanlage
					M 2.17	(C)	Zutrittsregelung und -kontrolle
					M 2.95	(A)	Beschaffung geeigneter Schutzschränke
					M 2.96	(A)	Verschluss von Schutzschränken
					M 2.97	(A)	Korrekter Umgang mit Codeschlössern
					M 3.20	(A)	Einweisung in die Bedienung von Schutzschränken
			G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes	M 1.18	(Z)	Gefahrenmeldeanlage
					M 2.17	(C)	Zutrittsregelung und -kontrolle
			G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal	M 1.18	(Z)	Gefahrenmeldeanlage
					M 2.17	(C)	Zutrittsregelung und -kontrolle
			G 5.53	Bewusste Fehlbedienung von Schutzschränken aus Bequemlichkeit	M 2.95	(A)	Beschaffung geeigneter Schutzschränke
					M 2.97	(A)	Korrekter Umgang mit Codeschlössern
					M 3.20	(A)	Einweisung in die Bedienung von Schutzschränken
B 2.8	(4.5)	Häuslicher Arbeitsplatz	G 1.5	Wasser	M 1.15	(A)	Geschlossene Fenster und Türen

			G 2.1	Fehlende oder unzureichende Regelungen	M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
					M 2.112	(A)	Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution
					M 2.136	(A)	Einhaltung von Regelungen bzgl. Arbeitsplatz und Arbeitsumgebung
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.19	(Z)	Einbruchsschutz
					M 1.23	(A)	Abgeschlossene Türen
					M 1.44	(A)	Geeignete Einrichtung eines häuslichen Arbeitsplatzes
					M 2.37	(C)	"Der aufgeräumte Arbeitsplatz"
			G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen	M 1.44	(A)	Geeignete Einrichtung eines häuslichen Arbeitsplatzes
					M 2.136	(A)	Einhaltung von Regelungen bzgl. Arbeitsplatz und Arbeitsumgebung
					M 3.9	(Z)	Ergonomischer Arbeitsplatz
			G 2.47	Ungesicherter Akten- und Datenträgertransport	M 2.112	(A)	Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution
			G 2.48	Ungeeignete Entsorgung der Datenträger und Dokumente	M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 1.45	(A)	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
					M 2.37	(C)	"Der aufgeräumte Arbeitsplatz"
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.19	(Z)	Einbruchsschutz
					M 1.23	(A)	Abgeschlossene Türen
			G 5.2	Manipulation an Daten oder Software	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.19	(Z)	Einbruchsschutz
					M 1.23	(A)	Abgeschlossene Türen
					M 2.37	(C)	"Der aufgeräumte Arbeitsplatz"
			G 5.3	Unbefugtes Eindringen in ein Gebäude	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.19	(Z)	Einbruchsschutz
					M 1.23	(A)	Abgeschlossene Türen
			G 5.69	Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.19	(Z)	Einbruchsschutz
					M 1.23	(A)	Abgeschlossene Türen
					M 2.37	(C)	"Der aufgeräumte Arbeitsplatz"
			G 5.70	Manipulation durch Familienangehörige und Besucher	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 2.37	(C)	"Der aufgeräumte Arbeitsplatz"
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.19	(Z)	Einbruchsschutz
					M 1.23	(A)	Abgeschlossene Türen
					M 1.45	(A)	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger

					M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
					M 2.37	(C)	"Der aufgeräumte Arbeitsplatz"
					M 2.112	(A)	Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution
B 2.9	(4.6)	Rechenzentrum	G 1.2	Ausfall des IT-Systems	M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.25	(A)	Überspannungsschutz
					M 1.27	(B)	Klimatisierung
					M 1.52	(Z)	Redundanzen in der technischen Infrastruktur
			G 1.3	Blitz	M 1.25	(A)	Überspannungsschutz
					M 6.16	(Z)	Abschließen von Versicherungen
			G 1.4	Feuer	M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.7	(A)	Handfeuerlöscher
					M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern
					M 1.26	(B)	Not-Aus-Schalter
					M 1.31	(Z)	Fernanzeige von Störungen
					M 1.47	(B)	Eigener Brandabschnitt
					M 1.48	(B)	Brandmeldeanlage
					M 1.50	(C)	Rauchschutz
					M 1.51	(A)	Brandlastreduzierung
					M 1.54	(Z)	Brandfrühesterkennung / Löschtechnik
					M 1.62	(C)	Brandschutz von Patchfeldern
					M 2.21	(A)	Rauchverbot
					M 6.16	(Z)	Abschließen von Versicherungen
					M 6.17	(A)	Alarmierungsplan und Brandschutzübungen
			G 1.5	Wasser	M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(B)	Gefahrenmeldeanlage
					M 1.24	(C)	Vermeidung von wasserführenden Leitungen
					M 1.31	(Z)	Fernanzeige von Störungen
					M 6.16	(Z)	Abschließen von Versicherungen
			G 1.6	Kabelbrand	M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.48	(B)	Brandmeldeanlage
			G 1.7	Unzulässige Temperatur und Luftfeuchte	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.27	(B)	Klimatisierung
					M 1.52	(Z)	Redundanzen in der technischen Infrastruktur
			G 1.8	Staub, Verschmutzung	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.27	(B)	Klimatisierung
					M 2.21	(A)	Rauchverbot
			G 1.11	Technische Katastrophen im Umfeld	M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern
					M 1.47	(B)	Eigener Brandabschnitt
					M 1.49	(A)	Technische und organisatorische Vorgaben für das Rechenzentrum
			G 1.12	Beeinträchtigung durch Großveranstaltungen	M 1.12	(A)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.15	(A)	Geschlossene Fenster und Türen

					M 1.18	(B)	Gefahrenmeldeanlage
					M 1.53	(Z)	Videoüberwachung
					M 1.55	(Z)	Perimeterschutz
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 1.13	Sturm	M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 6.16	(Z)	Abschließen von Versicherungen
			G 1.16	Ausfall von Patchfeldern durch Brand	M 1.62	(C)	Brandschutz von Patchfeldern
			G 2.1	Fehlende oder unzureichende Regelungen	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 1.49	(A)	Technische und organisatorische Vorgaben für das Rechenzentrum
					M 2.17	(A)	Zutrittsregelung und -kontrolle
					M 2.21	(A)	Rauchverbot
					M 2.212	(B)	Organisatorische Vorgaben für die Gebäudereinigung
					M 6.17	(A)	Alarmierungsplan und Brandschutzübungen
			G 2.2	Unzureichende Kenntnis über Regelungen	M 1.7	(A)	Handfeuerlöscher
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(B)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 1.57	(A)	Aktuelle Infrastruktur- und Baupläne
					M 2.17	(A)	Zutrittsregelung und -kontrolle
					M 2.212	(B)	Organisatorische Vorgaben für die Gebäudereinigung
					M 2.213	(A)	Wartung der technischen Infrastruktur
					M 6.17	(A)	Alarmierungsplan und Brandschutzübungen
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.7	(A)	Handfeuerlöscher
					M 1.18	(B)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 1.25	(A)	Überspannungsschutz
					M 1.48	(B)	Brandmeldeanlage
					M 1.54	(Z)	Brandfrühesterkennung / Löschtechnik
					M 1.56	(A)	Sekundär-Energieversorgung
					M 2.17	(A)	Zutrittsregelung und -kontrolle
					M 2.213	(A)	Wartung der technischen Infrastruktur
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	M 1.12	(A)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.18	(B)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
					M 1.49	(A)	Technische und organisatorische Vorgaben für das Rechenzentrum
			G 2.11	Unzureichende Trassendimensionierung	M 1.49	(A)	Technische und organisatorische Vorgaben für das Rechenzentrum
					M 1.56	(A)	Sekundär-Energieversorgung

				M 6.74	(Z)	Notfallarchiv
			G 2.12	Unzureichende Dokumentation der Verkabelung	M 1.57	(A)	Aktuelle Infrastruktur- und Baupläne
			G 4.1	Ausfall der Stromversorgung	M 1.3	(A)	Angepasste Aufteilung der Stromkreise
					M 1.25	(A)	Überspannungsschutz
					M 1.31	(Z)	Fernanzeige von Störungen
					M 1.56	(A)	Sekundär-Energieversorgung
			G 4.2	Ausfall interner Versorgungsnetze	M 1.31	(Z)	Fernanzeige von Störungen
					M 1.48	(B)	Brandmeldeanlage
			G 4.3	Ausfall vorhandener Sicherungseinrichtungen	M 1.52	(Z)	Redundanzen in der technischen Infrastruktur
					M 2.213	(A)	Wartung der technischen Infrastruktur
			G 5.3	Unbefugtes Eindringen in ein Gebäude	M 1.12	(A)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 1.31	(Z)	Fernanzeige von Störungen
					M 1.53	(Z)	Videoüberwachung
					M 1.55	(Z)	Perimeterschutz
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.4	Diebstahl	M 1.12	(A)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 1.31	(Z)	Fernanzeige von Störungen
					M 1.53	(Z)	Videoüberwachung
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.5	Vandalismus	M 1.12	(A)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 1.53	(Z)	Videoüberwachung
					M 1.55	(Z)	Perimeterschutz
					M 2.17	(A)	Zutrittsregelung und -kontrolle
			G 5.6	Anschlag	M 1.12	(A)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 1.53	(Z)	Videoüberwachung
					M 1.55	(Z)	Perimeterschutz
			G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes	M 1.18	(B)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen
			G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal	M 1.18	(B)	Gefahrenmeldeanlage
					M 1.23	(A)	Abgeschlossene Türen

			G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten	M 1.15	(A)	Geschlossene Fenster und Türen
			G 5.102	Sabotage	M 1.23	(A)	Abgeschlossene Türen
					M 1.53	(Z)	Videoüberwachung
					M 1.55	(Z)	Perimeterschutz
					M 2.17	(A)	Zutrittsregelung und -kontrolle
B 2.10	(neu)	Mobiler Arbeitsplatz	G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebung	M 1.61	(A)	Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes
					M 2.309	(C)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
					M 2.136	(A)	Einhaltung von Regelungen bzgl. Arbeitsplatz und Arbeitsumgebung
					M 2.218	(A)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.309	(C)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
					M 4.251	(A)	Arbeiten mit fremden IT-Systemen
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	M 2.136	(A)	Einhaltung von Regelungen bzgl. Arbeitsplatz und Arbeitsumgebung
					M 2.218	(A)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.309	(C)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
			G 2.47	Ungesicherter Akten- und Datenträgertransport	M 1.45	(A)	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
					M 2.218	(A)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.309	(C)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
			G 2.48	Ungeeignete Entsorgung der Datenträger und Dokumente	M 1.45	(A)	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
					M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
					M 2.37	(C)	"Der aufgeräumte Arbeitsplatz"
					M 2.218	(A)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.309	(C)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 1.61	(A)	Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes
					M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
					M 2.218	(A)	Regelung der Mitnahme von Datenträgern und IT-Komponenten

					M 2.309	(C)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
			G 3.43	Ungeeigneter Umgang mit Passwörtern	M 2.309	(C)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
			G 3.44	Sorglosigkeit im Umgang mit Informationen	M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
					M 2.218	(A)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.309	(C)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
					M 4.251	(A)	Arbeiten mit fremden IT-Systemen
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 1.61	(A)	Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes
					M 2.309	(C)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
			G 5.2	Manipulation an Daten oder Software	M 1.45	(A)	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
					M 2.218	(A)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.309	(C)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
					M 4.251	(A)	Arbeiten mit fremden IT-Systemen
			G 5.4	Diebstahl	M 1.15	(A)	Geschlossene Fenster und Türen
					M 1.23	(A)	Abgeschlossene Türen
					M 1.45	(A)	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
					M 1.46	(Z)	Einsatz von Diebstahl-Sicherungen
					M 1.61	(A)	Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes
					M 2.309	(C)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 1.45	(A)	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
					M 1.61	(A)	Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes
					M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
					M 2.37	(C)	"Der aufgeräumte Arbeitsplatz"
					M 2.218	(A)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.309	(C)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
					M 4.251	(A)	Arbeiten mit fremden IT-Systemen
B 2.11	(neu)	Besprechungs-, Veranstaltungs- und Schulungsräume	G 2.1	Fehlende oder unzureichende Regelungen	M 2.331	(A)	Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen

					M 2.333	(A)	Sichere Nutzung von Besprechungs-, Vortrags- und Schulungsräumen
					M 4.252	(C)	Sichere Konfiguration von Schulungsrechnern
					M 5.124	(C)	Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen
			G 2.2	Unzureichende Kenntnis über Regelungen	M 2.331	(A)	Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen
					M 2.333	(A)	Sichere Nutzung von Besprechungs-, Vortrags- und Schulungsräumen
					M 5.124	(C)	Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen
			G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen	M 2.69	(B)	Einrichtung von Standardarbeitsplätzen
					M 2.331	(A)	Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen
					M 2.332	(B)	Einrichtung von Besprechungs-, Vortrags- und Schulungsräumen
					M 3.9	(Z)	Ergonomischer Arbeitsplatz
					M 4.252	(C)	Sichere Konfiguration von Schulungsrechnern
			G 2.104	Inkompatibilität zwischen fremder und eigener IT	M 2.331	(A)	Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen
					M 2.333	(A)	Sichere Nutzung von Besprechungs-, Vortrags- und Schulungsräumen
					M 5.77	(Z)	Bildung von Teilnetzen
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 2.331	(A)	Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen
					M 2.333	(A)	Sichere Nutzung von Besprechungs-, Vortrags- und Schulungsräumen
					M 4.109	(C)	Software-Reinstallation bei Arbeitsplatzrechnern
					M 4.252	(C)	Sichere Konfiguration von Schulungsrechnern
					M 5.77	(Z)	Bildung von Teilnetzen
					M 5.124	(C)	Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen
			G 3.78	Fliegende Verkabelung	M 2.331	(A)	Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen
					M 3.9	(Z)	Ergonomischer Arbeitsplatz
			G 4.1	Ausfall der Stromversorgung	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
					M 2.332	(B)	Einrichtung von Besprechungs-, Vortrags- und Schulungsräumen
			G 4.2	Ausfall interner Versorgungsnetze	M 1.6	(A)	Einhaltung von Brandschutzvorschriften
					M 2.332	(B)	Einrichtung von Besprechungs-, Vortrags- und Schulungsräumen
			G 5.4	Diebstahl	M 1.15	(A)	Geschlossene Fenster und Türen
					M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
					M 2.333	(A)	Sichere Nutzung von Besprechungs-, Vortrags- und Schulungsräumen

B 3.101	(6.1)	Allgemeiner Server	G 1.1	Personalausfall	M 2.22	(A)	Hinterlegen des Passwortes
					M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.316	(A)	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 6.96	(A)	Notfallvorsorge für einen Server
			G 1.2	Ausfall des IT-Systems	M 1.28	(B)	Lokale unterbrechungsfreie Stromversorgung
					M 2.314	(Z)	Verwendung von hochverfügbaren Architekturen für Server
					M 2.318	(A)	Sichere Installation eines Servers
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 4.240	(Z)	Einrichten einer Testumgebung für einen Server
					M 5.9	(A)	Protokollierung am Server
					M 6.96	(A)	Notfallvorsorge für einen Server
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.16	(A)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.24	(A)	Sicherstellung einer konsistenten Systemverwaltung
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 4.240	(Z)	Einrichten einer Testumgebung für einen Server
					M 5.8	(B)	Regelmäßiger Sicherheitscheck des Netzes
					M 5.9	(A)	Protokollierung am Server
					M 5.10	(A)	Restriktive Rechtevergabe
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	M 2.22	(A)	Hinterlegen des Passwortes
					M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 2.315	(A)	Planung des Servereinsatzes
					M 2.319	(C)	Migration eines Servers
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.24	(A)	Sicherstellung einer konsistenten Systemverwaltung
					M 5.8	(B)	Regelmäßiger Sicherheitscheck des Netzes
					M 5.10	(A)	Restriktive Rechtevergabe
			G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten	M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.318	(A)	Sichere Installation eines Servers

					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.24	(A)	Sicherstellung einer konsistenten Systemverwaltung
					M 4.240	(Z)	Einrichten einer Testumgebung für einen Server
					M 5.9	(A)	Protokollierung am Server
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.22	(A)	Hinterlegen des Passwortes
					M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.316	(A)	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.16	(A)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 4.240	(Z)	Einrichten einer Testumgebung für einen Server
					M 5.8	(B)	Regelmäßiger Sicherheitscheck des Netzes
					M 5.9	(A)	Protokollierung am Server
					M 5.10	(A)	Restriktive Rechtevergabe
			G 3.5	Unbeabsichtigte Leitungsbeschädigung	M 1.28	(B)	Lokale unterbrechungsfreie Stromversorgung
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 1.28	(B)	Lokale unterbrechungsfreie Stromversorgung
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.16	(A)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 5.8	(B)	Regelmäßiger Sicherheitscheck des Netzes
					M 5.10	(A)	Restriktive Rechtevergabe
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.24	(A)	Sicherstellung einer konsistenten Systemverwaltung
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 4.240	(Z)	Einrichten einer Testumgebung für einen Server
					M 5.8	(B)	Regelmäßiger Sicherheitscheck des Netzes
					M 5.10	(A)	Restriktive Rechtevergabe
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.315	(A)	Planung des Servereinsatzes
					M 2.316	(A)	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
					M 2.318	(A)	Sichere Installation eines Servers
					M 2.319	(C)	Migration eines Servers
					M 4.24	(A)	Sicherstellung einer konsistenten Systemverwaltung
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.240	(Z)	Einrichten einer Testumgebung für einen Server

					M 5.8	(B)	Regelmäßiger Sicherheitscheck des Netzes
					M 5.9	(A)	Protokollierung am Server
					M 5.10	(A)	Restriktive Rechtevergabe
					M 6.24	(A)	Erstellen eines Notfall-Bootmediums
			G 3.31	Unstrukturierte Datenhaltung	M 2.138	(B)	Strukturierte Datenhaltung
			G 4.1	Ausfall der Stromversorgung	M 1.28	(B)	Lokale unterbrechungsfreie Stromversorgung
			G 4.6	Spannungsschwankungen/Überspannung/Unterspannung	M 1.28	(B)	Lokale unterbrechungsfreie Stromversorgung
			G 4.7	Defekte Datenträger	M 5.9	(A)	Protokollierung am Server
					M 6.96	(A)	Notfallvorsorge für einen Server
			G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 2.315	(A)	Planung des Servereinsatzes
					M 2.316	(A)	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
					M 2.319	(C)	Migration eines Servers
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.24	(A)	Sicherstellung einer konsistenten Systemverwaltung
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
					M 4.238	(A)	Einsatz eines lokalen Paketfilters
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 4.240	(Z)	Einrichten einer Testumgebung für einen Server
			G 4.13	Verlust gespeicherter Daten	M 6.24	(A)	Erstellen eines Notfall-Bootmediums
					M 6.96	(A)	Notfallvorsorge für einen Server
			G 4.22	Software-Schwachstellen oder -Fehler	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 2.273	(A)	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
					M 2.315	(A)	Planung des Servereinsatzes
					M 2.316	(A)	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
					M 2.317	(C)	Beschaffungskriterien für einen Server
					M 2.319	(C)	Migration eines Servers
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
					M 4.238	(A)	Einsatz eines lokalen Paketfilters
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 4.240	(Z)	Einrichten einer Testumgebung für einen Server
					M 6.96	(A)	Notfallvorsorge für einen Server
			G 4.39	Software-Konzeptionsfehler	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 2.273	(A)	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
					M 2.315	(A)	Planung des Servereinsatzes
					M 2.317	(C)	Beschaffungskriterien für einen Server

					M 2.318	(A)	Sichere Installation eines Servers
					M 2.319	(C)	Migration eines Servers
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
					M 4.238	(A)	Einsatz eines lokalen Paketfilters
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 4.240	(Z)	Einrichten einer Testumgebung für einen Server
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 5.9	(A)	Protokollierung am Server
			G 5.2	Manipulation an Daten oder Software	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 2.316	(A)	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
					M 4.238	(A)	Einsatz eines lokalen Paketfilters
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 4.240	(Z)	Einrichten einer Testumgebung für einen Server
					M 5.8	(B)	Regelmäßiger Sicherheitscheck des Netzes
					M 5.9	(A)	Protokollierung am Server
					M 5.10	(A)	Restriktive Rechtevergabe
					M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
			G 5.7	Abhören von Leitungen	M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 2.316	(A)	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
					M 2.318	(A)	Sichere Installation eines Servers
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.16	(A)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.24	(A)	Sicherstellung einer konsistenten Systemverwaltung
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 5.8	(B)	Regelmäßiger Sicherheitscheck des Netzes
					M 5.10	(A)	Restriktive Rechtevergabe
			G 5.9	Unberechtigte IT-Nutzung	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge

					M 2.273	(A)	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
					M 2.316	(A)	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
					M 2.320	(A)	Geregelte Außerbetriebnahme eines Servers
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.16	(A)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
					M 4.238	(A)	Einsatz eines lokalen Paketfilters
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 5.8	(B)	Regelmäßiger Sicherheitscheck des Netzes
					M 5.9	(A)	Protokollierung am Server
					M 5.10	(A)	Restriktive Rechtevergabe
					M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
			G 5.15	"Neugierige" Mitarbeiter	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.320	(A)	Geregelte Außerbetriebnahme eines Servers
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 5.10	(A)	Restriktive Rechtevergabe
					M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 2.316	(A)	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
					M 4.239	(A)	Sicherer Betrieb eines Servers
			G 5.19	Missbrauch von Benutzerrechten	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.316	(A)	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.16	(A)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.93	(B)	Regelmäßige Integritätsprüfung

					M 5.9	(A)	Protokollierung am Server
					M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
			G 5.20	Missbrauch von Administratorrechten	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.316	(A)	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.24	(A)	Sicherstellung einer konsistenten Systemverwaltung
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 5.9	(A)	Protokollierung am Server
					M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
			G 5.21	Trojanische Pferde	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 2.273	(A)	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.238	(A)	Einsatz eines lokalen Paketfilters
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 6.24	(A)	Erstellen eines Notfall-Bootmediums
			G 5.23	Computer-Viren	M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 6.24	(A)	Erstellen eines Notfall-Bootmediums
			G 5.26	Analyse des Nachrichtenflusses	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.318	(A)	Sichere Installation eines Servers
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 5.8	(B)	Regelmäßiger Sicherheitscheck des Netzes
			G 5.40	Abhören von Räumen mittels Rechner mit Mikrofon	M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.40	(C)	Verhinderung der unautorisierten Nutzung des Rechnermikrofons
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 2.138	(B)	Strukturierte Datenhaltung
					M 2.273	(A)	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
					M 2.315	(A)	Planung des Servereinsatzes
					M 2.316	(A)	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server

					M 2.320	(A)	Geregelte Außerbetriebnahme eines Servers
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.16	(A)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.24	(A)	Sicherstellung einer konsistenten Systemverwaltung
					M 4.40	(C)	Verhinderung der unautorisierten Nutzung des Rechnermikrofons
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 4.240	(Z)	Einrichten einer Testumgebung für einen Server
					M 5.8	(B)	Regelmäßiger Sicherheitscheck des Netzes
					M 5.9	(A)	Protokollierung am Server
					M 5.10	(A)	Restriktive Rechtevergabe
					M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
			G 5.85	Integritätsverlust schützenswerter Informationen	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
					M 2.138	(B)	Strukturierte Datenhaltung
					M 2.273	(A)	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
					M 2.315	(A)	Planung des Servereinsatzes
					M 2.316	(A)	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.16	(A)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.24	(A)	Sicherstellung einer konsistenten Systemverwaltung
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
					M 4.239	(A)	Sicherer Betrieb eines Servers
					M 4.240	(Z)	Einrichten einer Testumgebung für einen Server
					M 5.8	(B)	Regelmäßiger Sicherheitscheck des Netzes
					M 5.9	(A)	Protokollierung am Server
					M 5.10	(A)	Restriktive Rechtevergabe
					M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
B 3.102	(6.2)	Server unter Unix	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System	M 2.33	(C)	Aufteilung der Administrationstätigkeiten unter Unix
					M 4.9	(A)	Einsatz der Sicherheitsmechanismen von X-Windows
					M 4.13	(A)	Sorgfältige Vergabe von IDs

					M 4.14	(A)	Obligatorischer Passwortschutz unter Unix
					M 4.18	(A)	Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
					M 4.19	(A)	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
					M 4.20	(B)	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
					M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten
					M 4.22	(C)	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
					M 4.105	(A)	Erste Maßnahmen nach einer Unix-Standardinstallation
					M 5.16	(B)	Übersicht über Netzdienste
					M 5.17	(A)	Einsatz der Sicherheitsmechanismen von NFS
					M 5.18	(A)	Einsatz der Sicherheitsmechanismen von NIS
					M 5.19	(A)	Einsatz der Sicherheitsmechanismen von sendmail
					M 5.20	(A)	Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp
					M 5.21	(A)	Sicherer Einsatz von telnet, ftp, tftp und rexec
					M 5.34	(Z)	Einsatz von Einmalpasswörtern
					M 5.35	(A)	Einsatz der Sicherheitsmechanismen von UUCP
					M 5.36	(Z)	Verschlüsselung unter Unix und Windows NT
					M 5.72	(A)	Deaktivieren nicht benötigter Netzdienste
					M 5.82	(A)	Sicherer Einsatz von SAMBA
					M 5.83	(Z)	Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN
					M 6.31	(A)	Verhaltensregeln nach Verlust der Systemintegrität
			G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz	M 5.38	(B)	Sichere Einbindung von DOS-PCs in ein Unix-Netz
			G 2.65	Komplexität der SAMBA-Konfiguration	M 5.82	(A)	Sicherer Einsatz von SAMBA
			G 3.10	Falsches Exportieren von Dateisystemen unter Unix	M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten
					M 4.26	(B)	Regelmäßiger Sicherheitscheck des Unix-Systems
					M 5.17	(A)	Einsatz der Sicherheitsmechanismen von NFS
					M 5.20	(A)	Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp
					M 5.21	(A)	Sicherer Einsatz von telnet, ftp, tftp und rexec
			G 3.11	Fehlerhafte Konfiguration von sendmail	M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten
					M 4.26	(B)	Regelmäßiger Sicherheitscheck des Unix-Systems
					M 5.19	(A)	Einsatz der Sicherheitsmechanismen von sendmail
			G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client	M 4.14	(A)	Obligatorischer Passwortschutz unter Unix
					M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten
					M 4.22	(C)	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
					M 5.18	(A)	Einsatz der Sicherheitsmechanismen von NIS

			G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client	M 4.9	(A)	Einsatz der Sicherheitsmechanismen von X-Windows
					M 4.19	(A)	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
					M 4.20	(B)	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
					M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten
					M 4.22	(C)	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
					M 6.31	(A)	Verhaltensregeln nach Verlust der Systemintegrität
			G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp	M 2.33	(C)	Aufteilung der Administrationstätigkeiten unter Unix
					M 4.13	(A)	Sorgfältige Vergabe von IDs
					M 4.14	(A)	Obligatorischer Passwortschutz unter Unix
					M 4.19	(A)	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
					M 4.20	(B)	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
					M 4.22	(C)	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
					M 4.23	(A)	Sicherer Aufruf ausführbarer Dateien
					M 4.25	(A)	Einsatz der Protokollierung im Unix-System
					M 4.26	(B)	Regelmäßiger Sicherheitscheck des Unix-Systems
					M 4.106	(A)	Aktivieren der Systemprotokollierung
					M 5.19	(A)	Einsatz der Sicherheitsmechanismen von sendmail
					M 5.34	(Z)	Einsatz von Einmalpasswörtern
					M 5.35	(A)	Einsatz der Sicherheitsmechanismen von UUCP
			G 5.89	Hijacking von Netz-Verbindungen	M 4.9	(A)	Einsatz der Sicherheitsmechanismen von X-Windows
					M 5.36	(Z)	Verschlüsselung unter Unix und Windows NT
					M 5.64	(Z)	Secure Shell
					M 5.83	(Z)	Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN
B 3.103	(6.4)	Server unter Windows NT	G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz	M 2.91	(A)	Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz
					M 2.92	(B)	Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz
					M 2.93	(A)	Planung des Windows NT Netzes
					M 2.94	(B)	Freigabe von Verzeichnissen unter Windows NT
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.50	(Z)	Strukturierte Systemverwaltung unter Windows NT
					M 4.51	(Z)	Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT
					M 4.53	(A)	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
					M 4.54	(A)	Protokollierung unter Windows NT
					M 5.40	(B)	Sichere Einbindung von DOS-PCs in ein Windows NT Netz
					M 5.41	(C)	Sichere Konfiguration des Fernzugriffs unter Windows NT

			G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten	M 2.91	(A)	Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz
					M 2.92	(B)	Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz
					M 2.93	(A)	Planung des Windows NT Netzes
			G 2.30	Unzureichende Domänenplanung	M 2.91	(A)	Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz
					M 2.93	(A)	Planung des Windows NT Netzes
			G 2.31	Unzureichender Schutz des Windows NT Systems	M 2.91	(A)	Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz
					M 2.92	(B)	Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz
					M 2.93	(A)	Planung des Windows NT Netzes
					M 2.94	(B)	Freigabe von Verzeichnissen unter Windows NT
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.50	(Z)	Strukturierte Systemverwaltung unter Windows NT
					M 4.51	(Z)	Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.53	(A)	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
					M 4.54	(A)	Protokollierung unter Windows NT
					M 4.55	(A)	Sichere Installation von Windows NT
					M 4.56	(B)	Sicheres Löschen unter Windows-Betriebssystemen
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 5.36	(Z)	Verschlüsselung unter Unix und Windows NT
					M 5.41	(C)	Sichere Konfiguration des Fernzugriffs unter Windows NT
					M 5.42	(C)	Sichere Konfiguration der TCP/IP-Netzverwaltung unter Windows NT
					M 5.43	(B)	Sichere Konfiguration der TCP/IP-Netzdienste unter Windows NT
					M 6.42	(A)	Erstellung von Rettungsdisketten für Windows NT
					M 6.43	(Z)	Einsatz redundanter Windows NT/2000 Server
					M 6.44	(A)	Datensicherung unter Windows NT
			G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen	M 2.91	(A)	Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz
					M 2.92	(B)	Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz
					M 2.93	(A)	Planung des Windows NT Netzes
					M 4.76	(B)	Sichere Systemversion von Windows NT
					M 4.77	(A)	Schutz der Administratorkonten unter Windows NT
					M 5.41	(C)	Sichere Konfiguration des Fernzugriffs unter Windows NT
					M 5.42	(C)	Sichere Konfiguration der TCP/IP-Netzverwaltung unter Windows NT
					M 5.43	(B)	Sichere Konfiguration der TCP/IP-Netzdienste unter Windows NT

			G 4.23	Automatische CD-ROM-Erkennung	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
			G 5.23	Computer-Viren	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
					M 6.42	(A)	Erstellung von Rettungsdisketten für Windows NT
			G 5.43	Makro-Viren	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
					M 6.42	(A)	Erstellung von Rettungsdisketten für Windows NT
					M 6.44	(A)	Datensicherung unter Windows NT
			G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System	M 2.91	(A)	Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz
					M 2.92	(B)	Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz
					M 2.93	(A)	Planung des Windows NT Netzes
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.50	(Z)	Strukturierte Systemverwaltung unter Windows NT
					M 4.51	(Z)	Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.53	(A)	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
					M 4.54	(A)	Protokollierung unter Windows NT
					M 4.55	(A)	Sichere Installation von Windows NT
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 4.76	(B)	Sichere Systemversion von Windows NT
					M 4.77	(A)	Schutz der Administratorkonten unter Windows NT
					M 5.36	(Z)	Verschlüsselung unter Unix und Windows NT
			G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen	M 2.91	(A)	Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz
					M 2.93	(A)	Planung des Windows NT Netzes
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.50	(Z)	Strukturierte Systemverwaltung unter Windows NT
					M 4.51	(Z)	Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.53	(A)	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
					M 4.54	(A)	Protokollierung unter Windows NT
					M 4.55	(A)	Sichere Installation von Windows NT
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 4.76	(B)	Sichere Systemversion von Windows NT
					M 4.77	(A)	Schutz der Administratorkonten unter Windows NT
B 3.104	(6.5)	Server unter Novell Netware 3.x	G 1.2	Ausfall des IT-Systems	M 1.42	(A)	Gesicherte Aufstellung von Novell Netware Servern
					M 2.98	(A)	Sichere Installation von Novell Netware Servern
					M 2.99	(A)	Sichere Einrichtung von Novell Netware Servern
					M 2.100	(A)	Sicherer Betrieb von Novell Netware Servern

			G 2.33	Nicht gesicherter Aufstellungsort von Novell Netware Servern	M 1.42	(A)	Gesicherte Aufstellung von Novell Netware Servern
			G 2.34	Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen	M 2.98	(A)	Sichere Installation von Novell Netware Servern
					M 2.99	(A)	Sichere Einrichtung von Novell Netware Servern
					M 2.101	(B)	Revision von Novell Netware Servern
			G 4.1	Ausfall der Stromversorgung	M 2.98	(A)	Sichere Installation von Novell Netware Servern
					M 2.99	(A)	Sichere Einrichtung von Novell Netware Servern
			G 5.23	Computer-Viren	M 2.100	(A)	Sicherer Betrieb von Novell Netware Servern
			G 5.43	Makro-Viren	M 2.100	(A)	Sicherer Betrieb von Novell Netware Servern
			G 5.54	Vorsätzliches Herbeiführen eines Abnormal End	M 1.42	(A)	Gesicherte Aufstellung von Novell Netware Servern
					M 2.100	(A)	Sicherer Betrieb von Novell Netware Servern
			G 5.55	Login Bypass	M 2.100	(A)	Sicherer Betrieb von Novell Netware Servern
			G 5.56	Temporär frei zugängliche Accounts	M 2.100	(A)	Sicherer Betrieb von Novell Netware Servern
					M 2.101	(B)	Revision von Novell Netware Servern
			G 5.57	Netzanalyse-Tools	M 2.101	(B)	Revision von Novell Netware Servern
			G 5.58	"Hacking Novell Netware"	M 1.42	(A)	Gesicherte Aufstellung von Novell Netware Servern
					M 2.99	(A)	Sichere Einrichtung von Novell Netware Servern
					M 2.100	(A)	Sicherer Betrieb von Novell Netware Servern
					M 2.101	(B)	Revision von Novell Netware Servern
					M 2.102	(Z)	Verzicht auf die Aktivierung der Remote Console
			G 5.59	Missbrauch von Administratorrechten unter Novell Netware 3.x	M 2.100	(A)	Sicherer Betrieb von Novell Netware Servern
					M 2.101	(B)	Revision von Novell Netware Servern
B 3.105	(6.6)	Server unter Novell Netware 4.x	G 1.2	Ausfall des IT-Systems	M 2.153	(A)	Dokumentation von Novell Netware 4.x Netzen
					M 6.55	(C)	Reduzierung der Wiederanlaufzeit für Novell Netware Server
			G 2.33	Nicht gesicherter Aufstellungsort von Novell Netware Servern	M 1.42	(A)	Gesicherte Aufstellung von Novell Netware Servern
			G 2.34	Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen	M 2.148	(A)	Sichere Einrichtung von Novell Netware 4.x Netzen
					M 2.149	(A)	Sicherer Betrieb von Novell Netware 4.x Netzen
					M 2.150	(B)	Revision von Novell Netware 4.x Netzen
					M 4.102	(Z)	C2-Sicherheit unter Novell 4.11
			G 2.42	Komplexität der NDS	M 2.147	(A)	Sichere Migration von Novell Netware 3.x Servern in Novell Netware 4.x Netze
					M 2.151	(A)	Entwurf eines NDS-Konzeptes
			G 2.43	Migration von Novell Netware 3.x nach Novell Netware Version 4	M 2.147	(A)	Sichere Migration von Novell Netware 3.x Servern in Novell Netware 4.x Netze
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 4.103	(Z)	DHCP-Server unter Novell Netware 4.x
					M 4.104	(Z)	LDAP Services for NDS
			G 3.25	Fahrlässiges Löschen von Objekten	M 2.148	(A)	Sichere Einrichtung von Novell Netware 4.x Netzen
					M 2.149	(A)	Sicherer Betrieb von Novell Netware 4.x Netzen
			G 3.26	Ungewollte Freigabe des Dateisystems	M 2.148	(A)	Sichere Einrichtung von Novell Netware 4.x Netzen
					M 2.149	(A)	Sicherer Betrieb von Novell Netware 4.x Netzen
					M 2.150	(B)	Revision von Novell Netware 4.x Netzen
			G 3.27	Fehlerhafte Zeitsynchronisation	M 2.148	(A)	Sichere Einrichtung von Novell Netware 4.x Netzen
					M 2.149	(A)	Sicherer Betrieb von Novell Netware 4.x Netzen
					M 2.151	(A)	Entwurf eines NDS-Konzeptes
					M 2.152	(B)	Entwurf eines Zeitsynchronisations-Konzeptes

			G 3.38	Konfigurations- und Bedienungsfehler	M 4.108	(Z)	Vereinfachtes und sicheres Netzmanagement mit DNS Services unter Novell NetWare 4.11
			G 5.23	Computer-Viren	M 2.148	(A)	Sichere Einrichtung von Novell Netware 4.x Netzen
					M 2.149	(A)	Sicherer Betrieb von Novell Netware 4.x Netzen
			G 5.43	Makro-Viren	M 2.148	(A)	Sichere Einrichtung von Novell Netware 4.x Netzen
					M 2.149	(A)	Sicherer Betrieb von Novell Netware 4.x Netzen
			G 5.55	Login Bypass	M 2.148	(A)	Sichere Einrichtung von Novell Netware 4.x Netzen
			G 5.56	Temporär frei zugängliche Accounts	M 2.148	(A)	Sichere Einrichtung von Novell Netware 4.x Netzen
			G 5.57	Netzanalyse-Tools	M 2.102	(Z)	Verzicht auf die Aktivierung der Remote Console
			G 5.58	"Hacking Novell Netware"	M 1.42	(A)	Gesicherte Aufstellung von Novell Netware Servern
					M 2.102	(Z)	Verzicht auf die Aktivierung der Remote Console
					M 2.148	(A)	Sichere Einrichtung von Novell Netware 4.x Netzen
					M 2.149	(A)	Sicherer Betrieb von Novell Netware 4.x Netzen
					M 4.102	(Z)	C2-Sicherheit unter Novell 4.11
			G 5.59	Missbrauch von Administratorrechten unter Novell Netware 3.x	M 2.147	(A)	Sichere Migration von Novell Netware 3.x Servern in Novell Netware 4.x Netze
B 3.106	(6.9)	Server unter Windows 2000	G 1.2	Ausfall des IT-Systems	M 6.43	(Z)	Einsatz redundanter Windows NT/2000 Server
					M 6.76	(C)	Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes
					M 6.77	(A)	Erstellung von Rettungsdisketten für Windows 2000
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 2.1	Fehlende oder unzureichende Regelungen	M 3.27	(A)	Schulung zur Active Directory-Verwaltung
			G 2.2	Unzureichende Kenntnis über Regelungen	M 3.27	(A)	Schulung zur Active Directory-Verwaltung
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	M 2.229	(A)	Planung des Active Directory
					M 3.27	(A)	Schulung zur Active Directory-Verwaltung
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.228	(A)	Festlegen einer Windows 2000 Sicherheitsrichtlinie
					M 2.229	(A)	Planung des Active Directory
					M 2.230	(A)	Planung der Active Directory-Administration
					M 2.232	(B)	Planung der Windows 2000 CA-Struktur
					M 3.27	(A)	Schulung zur Active Directory-Verwaltung
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.137	(A)	Sichere Konfiguration von Windows 2000
					M 4.138	(A)	Konfiguration von Windows 2000 als Domänen-Controller
					M 4.139	(A)	Konfiguration von Windows 2000 als Server
					M 4.140	(A)	Sichere Konfiguration wichtiger Windows 2000 Dienste
					M 4.141	(A)	Sichere Konfiguration des DDNS unter Windows 2000
					M 4.142	(B)	Sichere Konfiguration des WINS unter Windows 2000
					M 4.143	(B)	Sichere Konfiguration des DHCP unter Windows 2000
					M 4.144	(B)	Nutzung der Windows 2000 CA
					M 4.145	(A)	Sichere Konfiguration von RRAS unter Windows 2000
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
			G 2.18	Ungeordnete Zustellung der Datenträger	M 4.56	(C)	Sicheres Löschen unter Windows-Betriebssystemen
			G 2.68	Fehlende oder unzureichende Planung des	M 2.227	(A)	Planung des Windows 2000 Einsatzes

				Active Directory	M 2.229	(A)	Planung des Active Directory
					M 2.231	(A)	Planung der Gruppenrichtlinien unter Windows 2000
					M 2.233	(B)	Planung der Migration von Windows NT auf Windows 2000
					M 3.27	(A)	Schulung zur Active Directory-Verwaltung
					M 4.144	(B)	Nutzung der Windows 2000 CA
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.227	(A)	Planung des Windows 2000 Einsatzes
					M 2.230	(A)	Planung der Active Directory-Administration
					M 2.233	(B)	Planung der Migration von Windows NT auf Windows 2000
					M 3.27	(A)	Schulung zur Active Directory-Verwaltung
					M 4.137	(A)	Sichere Konfiguration von Windows 2000
					M 4.139	(A)	Konfiguration von Windows 2000 als Server
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 6.43	(Z)	Einsatz redundanter Windows NT/2000 Server
					M 6.76	(C)	Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes
					M 6.77	(A)	Erstellung von Rettungsdisketten für Windows 2000
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 3.48	Fehlkonfiguration von Windows 2000/XP Rechnern	M 2.227	(A)	Planung des Windows 2000 Einsatzes
					M 2.233	(B)	Planung der Migration von Windows NT auf Windows 2000
					M 3.27	(A)	Schulung zur Active Directory-Verwaltung
					M 4.137	(A)	Sichere Konfiguration von Windows 2000
					M 4.139	(A)	Konfiguration von Windows 2000 als Server
					M 4.140	(A)	Sichere Konfiguration wichtiger Windows 2000 Dienste
					M 4.141	(A)	Sichere Konfiguration des DDNS unter Windows 2000
					M 4.142	(B)	Sichere Konfiguration des WINS unter Windows 2000
					M 4.143	(B)	Sichere Konfiguration des DHCP unter Windows 2000
					M 4.145	(A)	Sichere Konfiguration von RRAS unter Windows 2000
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
			G 3.49	Fehlkonfiguration des Active Directory	M 2.227	(A)	Planung des Windows 2000 Einsatzes
					M 2.230	(A)	Planung der Active Directory-Administration
					M 2.233	(B)	Planung der Migration von Windows NT auf Windows 2000
					M 3.27	(A)	Schulung zur Active Directory-Verwaltung
					M 4.137	(A)	Sichere Konfiguration von Windows 2000
					M 4.140	(A)	Sichere Konfiguration wichtiger Windows 2000 Dienste
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
			G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen	M 3.27	(A)	Schulung zur Active Directory-Verwaltung
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.137	(A)	Sichere Konfiguration von Windows 2000
					M 4.138	(A)	Konfiguration von Windows 2000 als Domänen-Controller
					M 4.139	(A)	Konfiguration von Windows 2000 als Server
					M 4.145	(A)	Sichere Konfiguration von RRAS unter Windows 2000
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
			G 4.23	Automatische CD-ROM-Erkennung	M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.137	(A)	Sichere Konfiguration von Windows 2000

					M 4.138	(A)	Konfiguration von Windows 2000 als Domänen-Controller
					M 4.139	(A)	Konfiguration von Windows 2000 als Server
					M 4.140	(A)	Sichere Konfiguration wichtiger Windows 2000 Dienste
					M 4.142	(B)	Sichere Konfiguration des WINS unter Windows 2000
					M 4.143	(B)	Sichere Konfiguration des DHCP unter Windows 2000
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
			G 4.35	Unsichere kryptographische Algorithmen	M 2.232	(B)	Planung der Windows 2000 CA-Struktur
					M 2.233	(B)	Planung der Migration von Windows NT auf Windows 2000
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.137	(A)	Sichere Konfiguration von Windows 2000
					M 4.139	(A)	Konfiguration von Windows 2000 als Server
					M 4.140	(A)	Sichere Konfiguration wichtiger Windows 2000 Dienste
					M 4.141	(A)	Sichere Konfiguration des DDNS unter Windows 2000
					M 4.142	(B)	Sichere Konfiguration des WINS unter Windows 2000
					M 4.143	(B)	Sichere Konfiguration des DHCP unter Windows 2000
					M 4.145	(A)	Sichere Konfiguration von RRAS unter Windows 2000
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
			G 5.7	Abhören von Leitungen	M 2.233	(B)	Planung der Migration von Windows NT auf Windows 2000
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.137	(A)	Sichere Konfiguration von Windows 2000
					M 4.138	(A)	Konfiguration von Windows 2000 als Domänen-Controller
					M 4.139	(A)	Konfiguration von Windows 2000 als Server
					M 4.141	(A)	Sichere Konfiguration des DDNS unter Windows 2000
					M 4.145	(A)	Sichere Konfiguration von RRAS unter Windows 2000
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 5.89	(A)	Konfiguration des sicheren Kanals unter Windows 2000/XP
					M 5.90	(Z)	Einsatz von IPSec unter Windows 2000/XP
			G 5.23	Computer-Viren	M 2.233	(B)	Planung der Migration von Windows NT auf Windows 2000
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.137	(A)	Sichere Konfiguration von Windows 2000
					M 4.138	(A)	Konfiguration von Windows 2000 als Domänen-Controller
					M 4.139	(A)	Konfiguration von Windows 2000 als Server
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 6.43	(Z)	Einsatz redundanter Windows NT/2000 Server
					M 6.76	(C)	Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes
					M 6.77	(A)	Erstellung von Rettungsdisketten für Windows 2000
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System	M 2.227	(A)	Planung des Windows 2000 Einsatzes
					M 2.228	(A)	Festlegen einer Windows 2000 Sicherheitsrichtlinie
					M 2.233	(B)	Planung der Migration von Windows NT auf Windows 2000
					M 3.27	(A)	Schulung zur Active Directory-Verwaltung
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.137	(A)	Sichere Konfiguration von Windows 2000
					M 4.138	(A)	Konfiguration von Windows 2000 als Domänen-Controller

					M 4.139	(A)	Konfiguration von Windows 2000 als Server
					M 4.140	(A)	Sichere Konfiguration wichtiger Windows 2000 Dienste
					M 4.141	(A)	Sichere Konfiguration des DDNS unter Windows 2000
					M 4.142	(B)	Sichere Konfiguration des WINS unter Windows 2000
					M 4.143	(B)	Sichere Konfiguration des DHCP unter Windows 2000
					M 4.144	(B)	Nutzung der Windows 2000 CA
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 4.147	(Z)	Sichere Nutzung von EFS unter Windows 2000/XP
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 2.232	(B)	Planung der Windows 2000 CA-Struktur
					M 2.233	(B)	Planung der Migration von Windows NT auf Windows 2000
					M 3.27	(A)	Schulung zur Active Directory-Verwaltung
					M 4.56	(C)	Sicheres Löschen unter Windows-Betriebssystemen
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.137	(A)	Sichere Konfiguration von Windows 2000
					M 4.138	(A)	Konfiguration von Windows 2000 als Domänen-Controller
					M 4.139	(A)	Konfiguration von Windows 2000 als Server
					M 4.140	(A)	Sichere Konfiguration wichtiger Windows 2000 Dienste
					M 4.144	(B)	Nutzung der Windows 2000 CA
					M 4.145	(A)	Sichere Konfiguration von RRAS unter Windows 2000
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 4.147	(Z)	Sichere Nutzung von EFS unter Windows 2000/XP
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
			G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows	M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
			G 5.83	Kompromittierung kryptographischer Schlüssel	M 2.227	(A)	Planung des Windows 2000 Einsatzes
					M 2.233	(B)	Planung der Migration von Windows NT auf Windows 2000
					M 3.27	(A)	Schulung zur Active Directory-Verwaltung
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.137	(A)	Sichere Konfiguration von Windows 2000
					M 4.138	(A)	Konfiguration von Windows 2000 als Domänen-Controller
					M 4.139	(A)	Konfiguration von Windows 2000 als Server
					M 4.144	(B)	Nutzung der Windows 2000 CA
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 5.89	(A)	Konfiguration des sicheren Kanals unter Windows 2000/XP
					M 5.90	(Z)	Einsatz von IPSec unter Windows 2000/XP
			G 5.84	Gefälschte Zertifikate	M 2.232	(B)	Planung der Windows 2000 CA-Struktur
					M 2.233	(B)	Planung der Migration von Windows NT auf Windows 2000
					M 3.27	(A)	Schulung zur Active Directory-Verwaltung
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.137	(A)	Sichere Konfiguration von Windows 2000
					M 4.144	(B)	Nutzung der Windows 2000 CA
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
			G 5.85	Integritätsverlust schützenswerter Informationen	M 2.227	(A)	Planung des Windows 2000 Einsatzes
					M 2.228	(A)	Festlegen einer Windows 2000 Sicherheitsrichtlinie

					M 2.232	(B)	Planung der Windows 2000 CA-Struktur
					M 2.233	(B)	Planung der Migration von Windows NT auf Windows 2000
					M 3.27	(A)	Schulung zur Active Directory-Verwaltung
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.137	(A)	Sichere Konfiguration von Windows 2000
					M 4.138	(A)	Konfiguration von Windows 2000 als Domänen-Controller
					M 4.139	(A)	Konfiguration von Windows 2000 als Server
					M 4.140	(A)	Sichere Konfiguration wichtiger Windows 2000 Dienste
					M 4.141	(A)	Sichere Konfiguration des DDNS unter Windows 2000
					M 4.142	(B)	Sichere Konfiguration des WINS unter Windows 2000
					M 4.143	(B)	Sichere Konfiguration des DHCP unter Windows 2000
					M 4.144	(B)	Nutzung der Windows 2000 CA
					M 4.145	(A)	Sichere Konfiguration von RRAS unter Windows 2000
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 4.147	(Z)	Sichere Nutzung von EFS unter Windows 2000/XP
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
					M 5.89	(A)	Konfiguration des sicheren Kanals unter Windows 2000/XP
					M 5.90	(Z)	Einsatz von IPSec unter Windows 2000/XP
B 3.107	(6.10)	S/390- und zSeries-Mainframe	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	M 2.291	(C)	Sicherheits-Berichtswesen und -Audits unter z/OS
					M 6.67	(A)	Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle
			G 2.27	Fehlende oder unzureichende Dokumentation	M 2.285	(Z)	Festlegung von Standards für z/OS-Systemdefinitionen
					M 2.288	(B)	Erstellung von Sicherheitsrichtlinien für z/OS-Systeme
					M 2.293	(C)	Wartung von zSeries-Systemen
					M 4.219	(C)	Lizenzschlüssel-Management für z/OS-Software
					M 6.93	(A)	Notfallvorsorge für z/OS-Systeme
			G 2.54	Vertraulichkeitsverlust durch Restinformationen	M 2.297	(B)	Deinstallation von z/OS-Systemen
					M 4.211	(A)	Einsatz des z/OS-Sicherheitssystems RACF
			G 2.99	Unzureichende oder fehlerhafte Konfiguration der zSeries-Systemumgebung	M 2.286	(Z)	Planung und Einsatz von zSeries-Systemen
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	M 3.39	(A)	Einführung in die zSeries-Plattform
					M 4.215	(B)	Absicherung sicherheitskritischer z/OS-Dienstprogramme
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.292	(B)	Überwachung von z/OS-Systemen
					M 3.39	(A)	Einführung in die zSeries-Plattform
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.295	(A)	Systemverwaltung von z/OS-Systemen
					M 3.39	(A)	Einführung in die zSeries-Plattform
					M 4.219	(C)	Lizenzschlüssel-Management für z/OS-Software
			G 3.38	Konfigurations- und Bedienungsfehler	M 4.211	(A)	Einsatz des z/OS-Sicherheitssystems RACF
			G 3.66	Fehlerhafte Zeichensatzkonvertierung beim Einsatz von z/OS	M 4.218	(Z)	Hinweise zur Zeichensatzkonvertierung bei z/OS-Systemen
			G 3.67	Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems	M 3.40	(A)	Einführung in das z/OS-Betriebssystem
					M 3.42	(A)	Schulung des z/OS-Bedienungspersonals
					M 4.209	(A)	Sichere Grundkonfiguration von z/OS-Systemen
			G 3.68	Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers	M 3.40	(A)	Einführung in das z/OS-Betriebssystem
					M 3.42	(A)	Schulung des z/OS-Bedienungspersonals
					M 4.209	(A)	Sichere Grundkonfiguration von z/OS-Systemen

			G 3.69	Fehlerhafte Konfiguration der Unix System Services unter z/OS	M 3.40	(A)	Einführung in das z/OS-Betriebssystem
					M 3.42	(A)	Schulung des z/OS-Bedienungspersonals
					M 4.209	(A)	Sichere Grundkonfiguration von z/OS-Systemen
					M 4.220	(B)	Absicherung von Unix System Services bei z/OS-Systemen
			G 3.70	Unzureichender Dateischutz des z/OS-Systems	M 2.295	(A)	Systemverwaltung von z/OS-Systemen
					M 2.296	(Z)	Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren
					M 3.40	(A)	Einführung in das z/OS-Betriebssystem
					M 3.42	(A)	Schulung des z/OS-Bedienungspersonals
					M 4.211	(A)	Einsatz des z/OS-Sicherheitssystems RACF
					M 4.212	(Z)	Absicherung von Linux für zSeries
					M 4.214	(B)	Datenträgerverwaltung unter z/OS-Systemen
					M 4.215	(B)	Absicherung sicherheitskritischer z/OS-Dienstprogramme
			G 3.71	Fehlerhafte Systemzeit bei z/OS-Systemen	M 3.42	(A)	Schulung des z/OS-Bedienungspersonals
					M 4.221	(C)	Parallel-Sysplex unter z/OS
			G 3.72	Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF	M 2.288	(B)	Erstellung von Sicherheitsrichtlinien für z/OS-Systeme
					M 3.40	(A)	Einführung in das z/OS-Betriebssystem
					M 3.42	(A)	Schulung des z/OS-Bedienungspersonals
					M 4.211	(A)	Einsatz des z/OS-Sicherheitssystems RACF
			G 3.73	Fehlbedienung der z/OS-Systemfunktionen	M 2.294	(Z)	Synchronisierung von z/OS-Passwörtern und RACF-Kommandos
					M 3.40	(A)	Einführung in das z/OS-Betriebssystem
					M 3.42	(A)	Schulung des z/OS-Bedienungspersonals
					M 4.207	(A)	Einsatz und Sicherung systemnaher z/OS-Terminals
					M 4.208	(B)	Absichern des Start-Vorgangs von z/OS-Systemen
					M 4.210	(B)	Sicherer Betrieb des z/OS-Betriebssystems
					M 4.212	(Z)	Absicherung von Linux für zSeries
					M 6.93	(A)	Notfallvorsorge für z/OS-Systeme
			G 3.74	Unzureichender Schutz der z/OS-Systemeinstellungen vor dynamischen Änderungen	M 2.292	(B)	Überwachung von z/OS-Systemen
					M 4.207	(A)	Einsatz und Sicherung systemnaher z/OS-Terminals
					M 4.212	(Z)	Absicherung von Linux für zSeries
			G 3.75	Mangelhafte Kontrolle der Batch-Jobs bei z/OS	M 2.287	(Z)	Batch-Job-Planung für z/OS-Systeme
					M 2.292	(B)	Überwachung von z/OS-Systemen
					M 4.210	(B)	Sicherer Betrieb des z/OS-Betriebssystems
			G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen	M 4.209	(A)	Sichere Grundkonfiguration von z/OS-Systemen
					M 4.210	(B)	Sicherer Betrieb des z/OS-Betriebssystems
					M 4.211	(A)	Einsatz des z/OS-Sicherheitssystems RACF
					M 4.213	(A)	Absichern des Login-Vorgangs unter z/OS
					M 5.113	(Z)	Einsatz des VTAM Session Management Exit unter z/OS
			G 4.22	Software-Schwachstellen oder -Fehler	M 2.293	(C)	Wartung von zSeries-Systemen
					M 6.93	(A)	Notfallvorsorge für z/OS-Systeme
			G 4.50	Überlastung des z/OS-Betriebssystems	M 4.210	(B)	Sicherer Betrieb des z/OS-Betriebssystems
					M 4.216	(C)	Festlegung der Systemgrenzen von z/OS
					M 4.217	(C)	Workload Management für z/OS-Systeme
			G 5.2	Manipulation an Daten oder Software	M 2.288	(B)	Erstellung von Sicherheitsrichtlinien für z/OS-Systeme
					M 4.210	(B)	Sicherer Betrieb des z/OS-Betriebssystems

					M 4.215	(B)	Absicherung sicherheitskritischer z/OS-Dienstprogramme
			G 5.10	Missbrauch von Fernwartungszugängen	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 4.207	(A)	Einsatz und Sicherung systemnaher z/OS-Terminals
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 2.291	(C)	Sicherheits-Berichtswesen und -Audits unter z/OS
					M 2.292	(B)	Überwachung von z/OS-Systemen
					M 4.211	(A)	Einsatz des z/OS-Sicherheitssystems RACF
					M 6.67	(A)	Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle
			G 5.19	Missbrauch von Benutzerrechten	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.288	(B)	Erstellung von Sicherheitsrichtlinien für z/OS-Systeme
					M 2.289	(A)	Einsatz restriktiver z/OS-Kennungen
					M 2.292	(B)	Überwachung von z/OS-Systemen
					M 4.211	(A)	Einsatz des z/OS-Sicherheitssystems RACF
					M 4.213	(A)	Absichern des Login-Vorgangs unter z/OS
			G 5.21	Trojanische Pferde	M 4.209	(A)	Sichere Grundkonfiguration von z/OS-Systemen
					M 4.210	(B)	Sicherer Betrieb des z/OS-Betriebssystems
					M 4.211	(A)	Einsatz des z/OS-Sicherheitssystems RACF
					M 4.213	(A)	Absichern des Login-Vorgangs unter z/OS
			G 5.28	Verhinderung von Diensten	M 4.219	(C)	Lizenzschlüssel-Management für z/OS-Software
			G 5.57	Netzanalyse-Tools	M 5.114	(B)	Absicherung der z/OS-Tracefunktionen
			G 5.116	Manipulation der z/OS-Systemsteuerung	M 2.291	(C)	Sicherheits-Berichtswesen und -Audits unter z/OS
					M 4.207	(A)	Einsatz und Sicherung systemnaher z/OS-Terminals
					M 4.208	(B)	Absichern des Start-Vorgangs von z/OS-Systemen
					M 4.210	(B)	Sicherer Betrieb des z/OS-Betriebssystems
					M 4.212	(Z)	Absicherung von Linux für zSeries
					M 6.67	(A)	Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle
			G 5.117	Verschleiern von Manipulationen unter z/OS	M 2.291	(C)	Sicherheits-Berichtswesen und -Audits unter z/OS
					M 6.67	(A)	Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle
			G 5.118	Unbefugtes Erlangen höherer Rechte im RACF	M 2.290	(Z)	Einsatz von RACF-Exits
					M 4.211	(A)	Einsatz des z/OS-Sicherheitssystems RACF
					M 4.215	(B)	Absicherung sicherheitskritischer z/OS-Dienstprogramme
			G 5.119	Benutzung fremder Kennungen unter z/OS-Systemen	M 2.288	(B)	Erstellung von Sicherheitsrichtlinien für z/OS-Systeme
					M 2.290	(Z)	Einsatz von RACF-Exits
					M 2.291	(C)	Sicherheits-Berichtswesen und -Audits unter z/OS
					M 2.292	(B)	Überwachung von z/OS-Systemen
					M 2.296	(Z)	Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren
					M 6.67	(A)	Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle
			G 5.120	Manipulation der Linux/zSeries Systemsteuerung	M 3.41	(A)	Einführung in Linux und z/VM für zSeries-Systeme
					M 4.207	(A)	Einsatz und Sicherung systemnaher z/OS-Terminals
					M 4.210	(B)	Sicherer Betrieb des z/OS-Betriebssystems
					M 4.212	(Z)	Absicherung von Linux für zSeries
			G 5.121	Angriffe über TCP/IP auf z/OS-Systeme	M 4.213	(A)	Absichern des Login-Vorgangs unter z/OS
					M 4.215	(B)	Absicherung sicherheitskritischer z/OS-Dienstprogramme
			G 5.122	Missbrauch von RACF-Attributen unter z/OS	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile

					M 2.288	(B)	Erstellung von Sicherheitsrichtlinien für z/OS-Systeme
					M 2.289	(A)	Einsatz restriktiver z/OS-Kennungen
					M 2.290	(Z)	Einsatz von RACF-Exits
					M 2.292	(B)	Überwachung von z/OS-Systemen
					M 2.295	(A)	Systemverwaltung von z/OS-Systemen
B 3.201	(neu)	Allgemeiner Client	G 1.1	Personalausfall	M 2.22	(A)	Hinterlegen des Passwortes
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 2.321	(A)	Planung des Einsatzes von Client-Server-Netzen
					M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
					M 4.2	(A)	Bildschirmsperre
					M 4.41	(C)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 4.200	(Z)	Umgang mit USB-Speichermedien
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
					M 4.241	(A)	Sicherer Betrieb von Clients
					M 4.242	(Z)	Einrichten einer Referenzinstallation für Clients
			G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzern	M 2.25	(A)	Dokumentation der Systemkonfiguration
					M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
					M 3.18	(A)	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
					M 4.2	(A)	Bildschirmsperre
			G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes	M 2.273	(A)	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
					M 2.321	(A)	Planung des Einsatzes von Client-Server-Netzen
					M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
					M 2.323	(A)	Geregelte Außerbetriebnahme eines Clients
					M 4.2	(A)	Bildschirmsperre
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.4	(C)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.41	(C)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.200	(Z)	Umgang mit USB-Speichermedien
					M 4.236	(Z)	Zentrale Administration von Laptops
					M 4.241	(A)	Sicherer Betrieb von Clients
					M 4.242	(Z)	Einrichten einer Referenzinstallation für Clients
					M 5.45	(B)	Sicherheit von WWW-Browsern
			G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten	M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz

			G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen	M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.236	(Z)	Zentrale Administration von Laptops
					M 4.241	(A)	Sicherer Betrieb von Clients
					M 4.242	(Z)	Einrichten einer Referenzinstallation für Clients
					M 5.45	(B)	Sicherheit von WWW-Browsern
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
					M 4.2	(A)	Bildschirmsperre
					M 4.200	(Z)	Umgang mit USB-Speichermedien
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
					M 4.2	(A)	Bildschirmsperre
					M 4.4	(C)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.41	(C)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 4.200	(Z)	Umgang mit USB-Speichermedien
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
					M 4.4	(C)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.200	(Z)	Umgang mit USB-Speichermedien
			G 3.9	Fehlerhafte Administration des IT-Systems	M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
			G 3.17	Kein ordnungsgemäßer PC-Benutzerwechsel	M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
					M 3.18	(A)	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
					M 4.2	(A)	Bildschirmsperre
			G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen	M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
			G 4.13	Verlust gespeicherter Daten	M 2.323	(A)	Geregelte Außerbetriebnahme eines Clients
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 4.4	(C)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.200	(Z)	Umgang mit USB-Speichermedien
			G 5.2	Manipulation an Daten oder Software	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 2.273	(A)	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
					M 2.321	(A)	Planung des Einsatzes von Client-Server-Netzen
					M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz

					M 3.18	(A)	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
					M 4.2	(A)	Bildschirmsperre
					M 4.4	(C)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.200	(Z)	Umgang mit USB-Speichermedien
					M 4.236	(Z)	Zentrale Administration von Laptops
					M 4.238	(A)	Einsatz eines lokalen Paketfilters
					M 4.241	(A)	Sicherer Betrieb von Clients
					M 4.242	(Z)	Einrichten einer Referenzinstallation für Clients
					M 5.45	(B)	Sicherheit von WWW-Browsern
					M 6.32	(A)	Regelmäßige Datensicherung
			G 5.4	Diebstahl	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 4.200	(Z)	Umgang mit USB-Speichermedien
					M 6.32	(A)	Regelmäßige Datensicherung
			G 5.7	Abhören von Leitungen	M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
			G 5.9	Unberechtigte IT-Nutzung	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 2.321	(A)	Planung des Einsatzes von Client-Server-Netzen
					M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
					M 2.323	(A)	Geregelte Außerbetriebnahme eines Clients
					M 4.2	(A)	Bildschirmsperre
					M 4.4	(C)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.200	(Z)	Umgang mit USB-Speichermedien
					M 4.234	(A)	Aussonderung von IT-Systemen
					M 4.238	(A)	Einsatz eines lokalen Paketfilters
					M 4.241	(A)	Sicherer Betrieb von Clients
					M 4.242	(Z)	Einrichten einer Referenzinstallation für Clients
			G 5.20	Missbrauch von Administratorrechten	M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
			G 5.21	Trojanische Pferde	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 2.273	(A)	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
					M 2.321	(A)	Planung des Einsatzes von Client-Server-Netzen
					M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.200	(Z)	Umgang mit USB-Speichermedien
					M 4.236	(Z)	Zentrale Administration von Laptops
					M 4.238	(A)	Einsatz eines lokalen Paketfilters
					M 4.241	(A)	Sicherer Betrieb von Clients
					M 4.242	(Z)	Einrichten einer Referenzinstallation für Clients
					M 5.45	(B)	Sicherheit von WWW-Browsern

					M 6.24	(A)	Erstellen eines Notfall-Bootmediums
					M 6.32	(A)	Regelmäßige Datensicherung
			G 5.23	Computer-Viren	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 2.273	(A)	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
					M 2.321	(A)	Planung des Einsatzes von Client-Server-Netzen
					M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.4	(C)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.200	(Z)	Umgang mit USB-Speichermedien
					M 4.236	(Z)	Zentrale Administration von Laptops
					M 4.241	(A)	Sicherer Betrieb von Clients
					M 4.242	(Z)	Einrichten einer Referenzinstallation für Clients
					M 5.45	(B)	Sicherheit von WWW-Browsern
					M 6.24	(A)	Erstellen eines Notfall-Bootmediums
					M 6.32	(A)	Regelmäßige Datensicherung
			G 5.40	Abhören von Räumen mittels Rechner mit Mikrofon	M 2.321	(A)	Planung des Einsatzes von Client-Server-Netzen
					M 4.40	(A)	Verhinderung der unautorisierten Nutzung des Rechnermikrofons
					M 4.241	(A)	Sicherer Betrieb von Clients
					M 4.242	(Z)	Einrichten einer Referenzinstallation für Clients
			G 5.43	Makro-Viren	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 2.273	(A)	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
					M 2.321	(A)	Planung des Einsatzes von Client-Server-Netzen
					M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.4	(C)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.200	(Z)	Umgang mit USB-Speichermedien
					M 4.236	(Z)	Zentrale Administration von Laptops
					M 4.241	(A)	Sicherer Betrieb von Clients
					M 4.242	(Z)	Einrichten einer Referenzinstallation für Clients
					M 5.45	(B)	Sicherheit von WWW-Browsern
					M 6.24	(A)	Erstellen eines Notfall-Bootmediums
					M 6.32	(A)	Regelmäßige Datensicherung
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
			G 5.85	Integritätsverlust schützenswerter Informationen	M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems
B 3.202	(5.99)	Allgemeines nicht vernetztes IT-	G 1.1	Personalausfall	M 2.22	(Z)	Hinterlegen des Passwortes

		System			M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
			G 1.2	Ausfall des IT-Systems	M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
					M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
					M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			G 1.4	Feuer	M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
					M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			G 1.5	Wasser	M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
					M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			G 1.8	Staub, Verschmutzung	M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
					M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
			G 2.7	Unerlaubte Ausübung von Rechten	M 4.2	(A)	Bildschirmsperre
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
			G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzern	M 2.63	(A)	Einrichten der Zugriffsrechte
					M 3.18	(A)	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
					M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.22	(Z)	Hinterlegen des Passwortes
					M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 4.2	(A)	Bildschirmsperre
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
					M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
					M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 4.2	(A)	Bildschirmsperre
					M 4.4	(Z)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen

					M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 4.4	(Z)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
					M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
			G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
			G 3.17	Kein ordnungsgemäßer PC-Benutzerwechsel	M 3.18	(A)	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
			G 4.1	Ausfall der Stromversorgung	M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
					M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
			G 4.7	Defekte Datenträger	M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
					M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
					M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 4.4	(Z)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
					M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
					M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
			G 5.2	Manipulation an Daten oder Software	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 4.2	(A)	Bildschirmsperre
					M 4.4	(Z)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
					M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
					M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
					M 6.32	(A)	Regelmäßige Datensicherung
			G 5.4	Diebstahl	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
					M 6.32	(A)	Regelmäßige Datensicherung
			G 5.9	Unberechtigte IT-Nutzung	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 4.2	(A)	Bildschirmsperre
					M 4.4	(Z)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login

					M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
					M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
			G 5.19	Missbrauch von Benutzerrechten	M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
			G 5.20	Missbrauch von Administratorrechten	M 2.63	(A)	Einrichten der Zugriffsrechte
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.15	(A)	Gesichertes Login
			G 5.21	Trojanische Pferde	M 2.63	(A)	Einrichten der Zugriffsrechte
					M 6.32	(A)	Regelmäßige Datensicherung
			G 5.23	Computer-Viren	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 4.2	(A)	Bildschirmsperre
					M 4.4	(Z)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
					M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
					M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
					M 6.32	(A)	Regelmäßige Datensicherung
			G 5.40	Abhören von Räumen mittels Rechner mit Mikrofon	M 4.40	(C)	Verhinderung der unautorisierten Nutzung des Rechnermikrofons
			G 5.43	Makro-Viren	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
					M 4.2	(A)	Bildschirmsperre
					M 4.4	(Z)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
					M 4.30	(A)	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
					M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
					M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
					M 6.32	(A)	Regelmäßige Datensicherung
B 3.203	(5.3)	Laptop	G 1.2	Ausfall des IT-Systems	M 2.218	(B)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 4.31	(A)	Sicherstellung der Energieversorgung im mobilen Einsatz
			G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebung	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 2.218	(B)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 4.31	(A)	Sicherstellung der Energieversorgung im mobilen Einsatz

			G 2.7	Unerlaubte Ausübung von Rechten	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 1.34	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz
					M 1.35	(Z)	Sammelaufbewahrung tragbarer IT-Systeme
					M 2.309	(A)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
					M 2.310	(A)	Geeignete Auswahl von Laptops
					M 4.27	(A)	Zugriffsschutz am Laptop
					M 4.29	(Z)	Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme
			G 2.8	Unkontrollierter Einsatz von Betriebsmitteln	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 1.34	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz
					M 1.35	(Z)	Sammelaufbewahrung tragbarer IT-Systeme
					M 2.36	(B)	Geregelte Übergabe und Rücknahme eines tragbaren PC
					M 2.218	(B)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.309	(A)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
					M 4.28	(Z)	Software-Reinstallation bei Benutzerwechsel eines Laptops
					M 4.29	(Z)	Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme
					M 4.236	(Z)	Zentrale Administration von Laptops
			G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PCs	M 1.35	(Z)	Sammelaufbewahrung tragbarer IT-Systeme
					M 2.36	(B)	Geregelte Übergabe und Rücknahme eines tragbaren PC
					M 2.309	(A)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
					M 4.28	(Z)	Software-Reinstallation bei Benutzerwechsel eines Laptops
					M 4.29	(Z)	Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme
					M 4.236	(Z)	Zentrale Administration von Laptops
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 1.34	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz
					M 1.35	(Z)	Sammelaufbewahrung tragbarer IT-Systeme
					M 4.235	(B)	Abgleich der Datenbestände von Laptops
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 1.34	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz
					M 1.35	(Z)	Sammelaufbewahrung tragbarer IT-Systeme
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms

					M 4.27	(A)	Zugriffsschutz am Laptop
					M 6.71	(A)	Datensicherung bei mobiler Nutzung des IT-Systems
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 1.34	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz
					M 1.35	(Z)	Sammelaufbewahrung tragbarer IT-Systeme
					M 4.27	(A)	Zugriffsschutz am Laptop
					M 4.29	(Z)	Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 2.309	(A)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
					M 4.29	(Z)	Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme
					M 4.236	(Z)	Zentrale Administration von Laptops
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
			G 3.38	Konfigurations- und Bedienungsfehler	M 4.236	(Z)	Zentrale Administration von Laptops
					M 5.91	(A)	Einsatz von Personal Firewalls für Internet-PCs
			G 3.76	Fehler bei der Synchronisation mobiler Endgeräte	M 4.235	(B)	Abgleich der Datenbestände von Laptops
			G 4.9	Ausfall der internen Stromversorgung	M 4.31	(A)	Sicherstellung der Energieversorgung im mobilen Einsatz
			G 4.13	Verlust gespeicherter Daten	M 4.235	(B)	Abgleich der Datenbestände von Laptops
					M 6.71	(A)	Datensicherung bei mobiler Nutzung des IT-Systems
			G 4.19	Informationsverlust bei erschöpftem Speichermedium	M 4.235	(B)	Abgleich der Datenbestände von Laptops
			G 4.22	Software-Schwachstellen oder -Fehler	M 5.91	(A)	Einsatz von Personal Firewalls für Internet-PCs
			G 4.52	Datenverlust bei mobilem Einsatz	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 2.218	(B)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 4.31	(A)	Sicherstellung der Energieversorgung im mobilen Einsatz
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 1.34	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz
					M 1.35	(Z)	Sammelaufbewahrung tragbarer IT-Systeme
					M 4.27	(A)	Zugriffsschutz am Laptop
					M 5.121	(A)	Sichere Kommunikation von unterwegs
					M 5.122	(A)	Sicherer Anschluss von Laptops an lokale Netze
			G 5.2	Manipulation an Daten oder Software	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 1.34	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz
					M 1.35	(Z)	Sammelaufbewahrung tragbarer IT-Systeme
					M 2.309	(A)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms

					M 4.27	(A)	Zugriffsschutz am Laptop
					M 4.28	(Z)	Software-Reinstallation bei Benutzerwechsel eines Laptops
					M 4.29	(Z)	Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
					M 5.121	(A)	Sichere Kommunikation von unterwegs
					M 5.122	(A)	Sicherer Anschluss von Laptops an lokale Netze
					M 6.71	(A)	Datensicherung bei mobiler Nutzung des IT-Systems
			G 5.4	Diebstahl	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 1.34	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz
					M 1.35	(Z)	Sammelaufbewahrung tragbarer IT-Systeme
					M 1.46	(Z)	Einsatz von Diebstahl-Sicherungen
					M 4.27	(A)	Zugriffsschutz am Laptop
					M 4.29	(Z)	Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme
			G 5.9	Unberechtigte IT-Nutzung	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 1.34	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz
					M 1.35	(Z)	Sammelaufbewahrung tragbarer IT-Systeme
					M 2.36	(B)	Geregelte Übergabe und Rücknahme eines tragbaren PC
					M 2.309	(A)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
					M 2.310	(A)	Geeignete Auswahl von Laptops
					M 4.27	(A)	Zugriffsschutz am Laptop
					M 4.28	(Z)	Software-Reinstallation bei Benutzerwechsel eines Laptops
					M 4.29	(Z)	Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 4.27	(A)	Zugriffsschutz am Laptop
					M 5.91	(A)	Einsatz von Personal Firewalls für Internet-PCs
			G 5.21	Trojanische Pferde	M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 5.121	(A)	Sichere Kommunikation von unterwegs
					M 5.122	(A)	Sicherer Anschluss von Laptops an lokale Netze
					M 6.71	(A)	Datensicherung bei mobiler Nutzung des IT-Systems
			G 5.22	Diebstahl bei mobiler Nutzung des IT-Systems	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 4.29	(Z)	Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme
			G 5.23	Computer-Viren	M 2.36	(B)	Geregelte Übergabe und Rücknahme eines tragbaren PC
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.28	(Z)	Software-Reinstallation bei Benutzerwechsel eines Laptops

					M 5.121	(A)	Sichere Kommunikation von unterwegs
					M 5.122	(A)	Sicherer Anschluss von Laptops an lokale Netze
					M 6.71	(A)	Datensicherung bei mobiler Nutzung des IT-Systems
			G 5.43	Makro-Viren	M 2.36	(B)	Geregelte Übergabe und Rücknahme eines tragbaren PC
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.28	(Z)	Software-Reinstallation bei Benutzerwechsel eines Laptops
					M 5.121	(A)	Sichere Kommunikation von unterwegs
					M 5.122	(A)	Sicherer Anschluss von Laptops an lokale Netze
					M 6.71	(A)	Datensicherung bei mobiler Nutzung des IT-Systems
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 2.218	(B)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.306	(B)	Verlustmeldung
					M 4.29	(Z)	Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
			G 5.123	Abhören von Raumgesprächen über mobile Endgeräte	M 4.40	(A)	Verhinderung der unautorisierten Nutzung des Rechnermikrofons
			G 5.124	Missbrauch der Informationen von mobilen Endgeräten	M 2.218	(B)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.309	(A)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
					M 5.121	(A)	Sichere Kommunikation von unterwegs
			G 5.125	Unberechtigte Datenweitergabe über mobile Endgeräte	M 2.218	(B)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.309	(A)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
					M 5.121	(A)	Sichere Kommunikation von unterwegs
			G 5.126	Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten	M 2.309	(A)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
					M 2.310	(A)	Geeignete Auswahl von Laptops
B 3.204	(5.2)	Client unter Unix	G 1.1	Personalausfall	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.33	(Z)	Aufteilung der Administrationstätigkeiten unter Unix
			G 1.2	Ausfall des IT-Systems	M 6.31	(A)	Verhaltensregeln nach Verlust der Systemintegrität
			G 1.8	Staub, Verschmutzung	M 5.72	(A)	Deaktivieren nicht benötigter Netzdienste
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.33	(Z)	Aufteilung der Administrationstätigkeiten unter Unix
					M 4.9	(A)	Einsatz der Sicherheitsmechanismen von X-Windows
					M 4.13	(A)	Sorgfältige Vergabe von IDs
					M 4.14	(A)	Obligatorischer Passwortschutz unter Unix
					M 4.16	(C)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals

					M 4.18	(A)	Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
					M 4.19	(A)	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
					M 4.20	(B)	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
					M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten
					M 4.22	(Z)	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
					M 4.23	(B)	Sicherer Aufruf ausführbarer Dateien
					M 4.25	(A)	Einsatz der Protokollierung im Unix-System
					M 4.105	(A)	Erste Maßnahmen nach einer Unix-Standardinstallation
					M 4.106	(B)	Aktivieren der Systemprotokollierung
					M 5.17	(A)	Einsatz der Sicherheitsmechanismen von NFS
					M 5.18	(A)	Einsatz der Sicherheitsmechanismen von NIS
					M 5.19	(A)	Einsatz der Sicherheitsmechanismen von sendmail
					M 5.20	(A)	Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp
					M 5.21	(A)	Sicherer Einsatz von telnet, ftp, tftp und rexec
					M 5.34	(Z)	Einsatz von Einmalpasswörtern
					M 5.35	(A)	Einsatz der Sicherheitsmechanismen von UUCP
					M 5.36	(Z)	Verschlüsselung unter Unix und Windows NT
					M 5.72	(A)	Deaktivieren nicht benötigter Netzdienste
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.26	(C)	Regelmäßiger Sicherheitscheck des Unix-Systems
					M 4.105	(A)	Erste Maßnahmen nach einer Unix-Standardinstallation
			G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.33	(Z)	Aufteilung der Administrationstätigkeiten unter Unix
					M 4.9	(A)	Einsatz der Sicherheitsmechanismen von X-Windows
					M 4.13	(A)	Sorgfältige Vergabe von IDs
					M 4.14	(A)	Obligatorischer Passwortschutz unter Unix
					M 4.16	(C)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.18	(A)	Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
					M 4.19	(A)	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
					M 4.20	(B)	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
					M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten

					M 4.22	(Z)	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
					M 4.105	(A)	Erste Maßnahmen nach einer Unix-Standardinstallation
					M 6.31	(A)	Verhaltensregeln nach Verlust der Systemintegrität
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.18	(A)	Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
					M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten
					M 4.25	(A)	Einsatz der Protokollierung im Unix-System
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.33	(Z)	Aufteilung der Administrationstätigkeiten unter Unix
					M 4.9	(A)	Einsatz der Sicherheitsmechanismen von X-Windows
					M 4.13	(A)	Sorgfältige Vergabe von IDs
					M 4.14	(A)	Obligatorischer Passwortschutz unter Unix
					M 4.16	(C)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.25	(A)	Einsatz der Protokollierung im Unix-System
					M 4.26	(C)	Regelmäßiger Sicherheitscheck des Unix-Systems
					M 4.105	(A)	Erste Maßnahmen nach einer Unix-Standardinstallation
					M 6.31	(A)	Verhaltensregeln nach Verlust der Systemintegrität
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.14	(A)	Obligatorischer Passwortschutz unter Unix
					M 4.16	(C)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.18	(A)	Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.33	(Z)	Aufteilung der Administrationstätigkeiten unter Unix
					M 4.18	(A)	Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
					M 4.19	(A)	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
					M 4.20	(B)	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
					M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten
					M 4.25	(A)	Einsatz der Protokollierung im Unix-System
					M 4.26	(C)	Regelmäßiger Sicherheitscheck des Unix-Systems

					M 4.105	(A)	Erste Maßnahmen nach einer Unix-Standardinstallation
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.33	(Z)	Aufteilung der Administrationstätigkeiten unter Unix
					M 4.13	(A)	Sorgfältige Vergabe von IDs
					M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten
					M 4.25	(A)	Einsatz der Protokollierung im Unix-System
					M 4.26	(C)	Regelmäßiger Sicherheitscheck des Unix-Systems
					M 4.105	(A)	Erste Maßnahmen nach einer Unix-Standardinstallation
			G 4.8	Bekanntwerden von Softwareschwachstellen	M 4.16	(C)	Zugangsbeschränkungen für Accounts und / oder Terminals
			G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.14	(A)	Obligatorischer Passwortschutz unter Unix
					M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten
					M 4.22	(Z)	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
					M 5.18	(A)	Einsatz der Sicherheitsmechanismen von NIS
			G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.9	(A)	Einsatz der Sicherheitsmechanismen von X-Windows
					M 4.13	(A)	Sorgfältige Vergabe von IDs
					M 4.16	(C)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.19	(A)	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
					M 4.20	(B)	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
					M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten
					M 4.22	(Z)	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
					M 6.31	(A)	Verhaltensregeln nach Verlust der Systemintegrität
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 4.16	(C)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.18	(A)	Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
			G 5.2	Manipulation an Daten oder Software	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.13	(A)	Sorgfältige Vergabe von IDs
					M 4.14	(A)	Obligatorischer Passwortschutz unter Unix
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.18	(A)	Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus

					M 4.19	(A)	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
					M 4.20	(B)	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
					M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten
					M 4.22	(Z)	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
					M 4.25	(A)	Einsatz der Protokollierung im Unix-System
					M 4.26	(C)	Regelmäßiger Sicherheitscheck des Unix-Systems
					M 4.105	(A)	Erste Maßnahmen nach einer Unix-Standardinstallation
					M 6.31	(A)	Verhaltensregeln nach Verlust der Systemintegrität
			G 5.4	Diebstahl	M 4.18	(A)	Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
			G 5.7	Abhören von Leitungen	M 6.31	(A)	Verhaltensregeln nach Verlust der Systemintegrität
			G 5.8	Manipulation an Leitungen	M 6.31	(A)	Verhaltensregeln nach Verlust der Systemintegrität
			G 5.9	Unberechtigte IT-Nutzung	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.33	(Z)	Aufteilung der Administrationstätigkeiten unter Unix
					M 4.13	(A)	Sorgfältige Vergabe von IDs
					M 4.14	(A)	Obligatorischer Passwortschutz unter Unix
					M 4.16	(C)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.18	(A)	Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
					M 4.19	(A)	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
					M 4.20	(B)	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
					M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten
					M 4.25	(A)	Einsatz der Protokollierung im Unix-System
					M 4.26	(C)	Regelmäßiger Sicherheitscheck des Unix-Systems
					M 4.105	(A)	Erste Maßnahmen nach einer Unix-Standardinstallation
					M 5.72	(A)	Deaktivieren nicht benötigter Netzdienste
					M 6.31	(A)	Verhaltensregeln nach Verlust der Systemintegrität
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.14	(A)	Obligatorischer Passwortschutz unter Unix
					M 4.25	(A)	Einsatz der Protokollierung im Unix-System
					M 4.26	(C)	Regelmäßiger Sicherheitscheck des Unix-Systems
					M 4.105	(A)	Erste Maßnahmen nach einer Unix-Standardinstallation
					M 4.106	(B)	Aktivieren der Systemprotokollierung
			G 5.19	Missbrauch von Benutzerrechten	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile

					M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.9	(A)	Einsatz der Sicherheitsmechanismen von X-Windows
					M 4.13	(A)	Sorgfältige Vergabe von IDs
					M 4.14	(A)	Obligatorischer Passwortschutz unter Unix
					M 4.16	(C)	Zugangsbeschränkungen für Accounts und / oder Terminals
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.19	(A)	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
					M 4.20	(B)	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
					M 4.22	(Z)	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
					M 4.25	(A)	Einsatz der Protokollierung im Unix-System
					M 4.26	(C)	Regelmäßiger Sicherheitscheck des Unix-Systems
					M 4.105	(A)	Erste Maßnahmen nach einer Unix-Standardinstallation
			G 5.20	Missbrauch von Administratorrechten	M 2.33	(Z)	Aufteilung der Administrationstätigkeiten unter Unix
					M 4.9	(A)	Einsatz der Sicherheitsmechanismen von X-Windows
					M 4.13	(A)	Sorgfältige Vergabe von IDs
					M 4.14	(A)	Obligatorischer Passwortschutz unter Unix
					M 4.18	(A)	Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
					M 4.19	(A)	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
					M 4.21	(A)	Verhinderung des unautorisierten Erlangens von Administratorrechten
					M 4.25	(A)	Einsatz der Protokollierung im Unix-System
					M 4.26	(C)	Regelmäßiger Sicherheitscheck des Unix-Systems
			G 5.21	Trojanische Pferde	M 4.13	(A)	Sorgfältige Vergabe von IDs
					M 4.14	(A)	Obligatorischer Passwortschutz unter Unix
					M 4.19	(A)	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
					M 4.20	(B)	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
					M 4.23	(B)	Sicherer Aufruf ausführbarer Dateien
					M 4.25	(A)	Einsatz der Protokollierung im Unix-System
					M 4.26	(C)	Regelmäßiger Sicherheitscheck des Unix-Systems
					M 6.31	(A)	Verhaltensregeln nach Verlust der Systemintegrität
			G 5.23	Computer-Viren	M 4.13	(A)	Sorgfältige Vergabe von IDs
					M 4.19	(A)	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
					M 4.20	(B)	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
					M 4.23	(B)	Sicherer Aufruf ausführbarer Dateien
					M 4.26	(C)	Regelmäßiger Sicherheitscheck des Unix-Systems
					M 6.31	(A)	Verhaltensregeln nach Verlust der Systemintegrität

			G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp	M 5.19	(A)	Einsatz der Sicherheitsmechanismen von sendmail
					M 5.34	(Z)	Einsatz von Einmalpasswörtern
					M 5.35	(A)	Einsatz der Sicherheitsmechanismen von UUCP
			G 5.89	Hijacking von Netz-Verbindungen	M 5.36	(Z)	Verschlüsselung unter Unix und Windows NT
					M 5.64	(Z)	Secure Shell
B 3.205	(5.5)	Client unter Windows NT	G 1.1	Personalausfall	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile
			G 1.2	Ausfall des IT-Systems	M 6.42	(A)	Erstellung von Rettungsdisketten für Windows NT
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.17	(B)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.50	(Z)	Strukturierte Systemverwaltung unter Windows NT
					M 4.52	(B)	Geräteschutz unter Windows NT/2000/XP
					M 4.53	(A)	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
					M 4.54	(Z)	Protokollierung unter Windows NT
					M 4.55	(B)	Sichere Installation von Windows NT
					M 4.56	(B)	Sicheres Löschen unter Windows-Betriebssystemen
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 4.17	(B)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
			G 2.31	Unzureichender Schutz des Windows NT Systems	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.17	(B)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.50	(Z)	Strukturierte Systemverwaltung unter Windows NT
					M 4.51	(Z)	Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT
					M 4.52	(B)	Geräteschutz unter Windows NT/2000/XP
					M 4.53	(A)	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
					M 4.54	(Z)	Protokollierung unter Windows NT
					M 4.55	(B)	Sichere Installation von Windows NT
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 6.42	(A)	Erstellung von Rettungsdisketten für Windows NT
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.17	(B)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.50	(Z)	Strukturierte Systemverwaltung unter Windows NT
					M 4.52	(B)	Geräteschutz unter Windows NT/2000/XP
					M 4.53	(A)	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
					M 6.42	(A)	Erstellung von Rettungsdisketten für Windows NT

					M 6.44	(A)	Datensicherung unter Windows NT
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.17	(B)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.50	(Z)	Strukturierte Systemverwaltung unter Windows NT
					M 4.52	(B)	Geräteschutz unter Windows NT/2000/XP
					M 4.53	(A)	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
					M 4.56	(B)	Sicheres Löschen unter Windows-Betriebssystemen
					M 6.42	(A)	Erstellung von Rettungsdisketten für Windows NT
					M 6.44	(A)	Datensicherung unter Windows NT
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.50	(Z)	Strukturierte Systemverwaltung unter Windows NT
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 6.42	(A)	Erstellung von Rettungsdisketten für Windows NT
					M 6.44	(A)	Datensicherung unter Windows NT
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 6.42	(A)	Erstellung von Rettungsdisketten für Windows NT
					M 6.44	(A)	Datensicherung unter Windows NT
			G 4.1	Ausfall der Stromversorgung	M 6.44	(A)	Datensicherung unter Windows NT
			G 4.7	Defekte Datenträger	M 6.44	(A)	Datensicherung unter Windows NT
			G 4.23	Automatische CD-ROM-Erkennung	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.50	(Z)	Strukturierte Systemverwaltung unter Windows NT
					M 4.76	(C)	Sichere Systemversion von Windows NT
					M 6.44	(A)	Datensicherung unter Windows NT
			G 5.2	Manipulation an Daten oder Software	M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.50	(Z)	Strukturierte Systemverwaltung unter Windows NT
					M 4.52	(B)	Geräteschutz unter Windows NT/2000/XP
					M 4.53	(A)	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
					M 4.54	(Z)	Protokollierung unter Windows NT
					M 6.44	(A)	Datensicherung unter Windows NT
			G 5.4	Diebstahl	M 6.44	(A)	Datensicherung unter Windows NT
			G 5.9	Unberechtigte IT-Nutzung	M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System

					M 4.50	(Z)	Strukturierte Systemverwaltung unter Windows NT
					M 4.54	(Z)	Protokollierung unter Windows NT
					M 4.77	(A)	Schutz der Administratorkonten unter Windows NT
					M 6.44	(A)	Datensicherung unter Windows NT
			G 5.21	Trojanische Pferde	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
			G 5.23	Computer-Viren	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
					M 6.42	(A)	Erstellung von Rettungsdisketten für Windows NT
					M 6.44	(A)	Datensicherung unter Windows NT
			G 5.43	Makro-Viren	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
					M 6.42	(A)	Erstellung von Rettungsdisketten für Windows NT
					M 6.44	(A)	Datensicherung unter Windows NT
			G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System	M 4.50	(Z)	Strukturierte Systemverwaltung unter Windows NT
					M 4.51	(Z)	Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT
					M 4.52	(B)	Geräteschutz unter Windows NT/2000/XP
					M 4.53	(A)	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
					M 4.54	(Z)	Protokollierung unter Windows NT
					M 4.55	(B)	Sichere Installation von Windows NT
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 4.76	(C)	Sichere Systemversion von Windows NT
					M 4.77	(A)	Schutz der Administratorkonten unter Windows NT
			G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.50	(Z)	Strukturierte Systemverwaltung unter Windows NT
					M 4.51	(Z)	Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT
					M 4.52	(B)	Geräteschutz unter Windows NT/2000/XP
					M 4.53	(A)	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
					M 4.54	(Z)	Protokollierung unter Windows NT
					M 4.55	(B)	Sichere Installation von Windows NT
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 4.76	(C)	Sichere Systemversion von Windows NT
					M 4.77	(A)	Schutz der Administratorkonten unter Windows NT
B 3.206	(5.6)	Client unter Windows 95	G 1.2	Ausfall des IT-Systems	M 6.45	(A)	Datensicherung unter Windows 95
					M 6.46	(A)	Erstellung von Rettungsdisketten für Windows 95
			G 1.4	Feuer	M 6.45	(A)	Datensicherung unter Windows 95
			G 1.5	Wasser	M 6.45	(A)	Datensicherung unter Windows 95
			G 1.8	Staub, Verschmutzung	M 6.45	(A)	Datensicherung unter Windows 95
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.63	(A)	Einrichten der Zugriffsrechte
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.63	(A)	Einrichten der Zugriffsrechte
					M 2.65	(Z)	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System

					M 2.104	(Z)	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 4.56	(B)	Sicheres Löschen unter Windows-Betriebssystemen
					M 4.74	(A)	Vernetzte Windows 95 Rechner
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	M 2.63	(A)	Einrichten der Zugriffsrechte
					M 2.65	(Z)	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
			G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzern	M 2.63	(A)	Einrichten der Zugriffsrechte
					M 2.65	(Z)	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
					M 2.103	(A)	Einrichten von Benutzerprofilen unter Windows 95
					M 2.104	(Z)	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
					M 3.18	(A)	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
					M 4.56	(B)	Sicheres Löschen unter Windows-Betriebssystemen
					M 6.46	(A)	Erstellung von Rettungsdisketten für Windows 95
			G 2.22	Fehlende Auswertung von Protokolldaten	M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
			G 2.35	Fehlende Protokollierung unter Windows 95	M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
			G 2.36	Ungeeignete Einschränkung der Benutzerumgebung	M 2.65	(Z)	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
					M 2.104	(Z)	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	M 4.74	(A)	Vernetzte Windows 95 Rechner
					M 6.45	(A)	Datensicherung unter Windows 95
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.104	(Z)	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 6.45	(A)	Datensicherung unter Windows 95
					M 6.46	(A)	Erstellung von Rettungsdisketten für Windows 95
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 2.63	(A)	Einrichten der Zugriffsrechte
					M 2.104	(Z)	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 6.45	(A)	Datensicherung unter Windows 95
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 6.45	(A)	Datensicherung unter Windows 95
					M 6.46	(A)	Erstellung von Rettungsdisketten für Windows 95
			G 3.16	Fehlerhafte Administration von Zugangs- und	M 2.63	(A)	Einrichten der Zugriffsrechte

				Zugriffsrechten	M 2.65	(Z)	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
					M 2.104	(Z)	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 4.56	(B)	Sicheres Löschen unter Windows-Betriebssystemen
			G 3.17	Kein ordnungsgemäßer PC-Benutzerwechsel	M 2.65	(Z)	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
					M 2.103	(A)	Einrichten von Benutzerprofilen unter Windows 95
					M 2.104	(Z)	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
					M 3.18	(A)	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 4.56	(B)	Sicheres Löschen unter Windows-Betriebssystemen
			G 3.22	Fehlerhafte Änderung der Registrierung	M 2.104	(Z)	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
					M 6.45	(A)	Datensicherung unter Windows 95
					M 6.46	(A)	Erstellung von Rettungsdisketten für Windows 95
			G 4.23	Automatische CD-ROM-Erkennung	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
			G 4.24	Dateinamenkonvertierung bei Datensicherungen unter Windows 95	M 6.45	(A)	Datensicherung unter Windows 95
			G 5.2	Manipulation an Daten oder Software	M 2.63	(A)	Einrichten der Zugriffsrechte
					M 2.104	(Z)	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 4.56	(B)	Sicheres Löschen unter Windows-Betriebssystemen
					M 4.74	(A)	Vernetzte Windows 95 Rechner
			G 5.4	Diebstahl	M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
			G 5.9	Unberechtigte IT-Nutzung	M 2.63	(A)	Einrichten der Zugriffsrechte
					M 2.104	(Z)	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
			G 5.21	Trojanische Pferde	M 2.63	(A)	Einrichten der Zugriffsrechte
					M 2.104	(Z)	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
					M 6.45	(A)	Datensicherung unter Windows 95
					M 6.46	(A)	Erstellung von Rettungsdisketten für Windows 95
			G 5.23	Computer-Viren	M 2.63	(A)	Einrichten der Zugriffsrechte

					M 2.104	(Z)	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
					M 6.46	(A)	Erstellung von Rettungsdisketten für Windows 95
			G 5.43	Makro-Viren	M 2.63	(A)	Einrichten der Zugriffsrechte
					M 2.104	(Z)	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
					M 6.46	(A)	Erstellung von Rettungsdisketten für Windows 95
			G 5.60	Umgehen der Systemrichtlinien	M 2.63	(A)	Einrichten der Zugriffsrechte
					M 2.65	(Z)	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
					M 2.103	(A)	Einrichten von Benutzerprofilen unter Windows 95
					M 2.104	(Z)	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
					M 3.18	(A)	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
B 3.207	(5.7)	Client unter Windows 2000	G 1.1	Personalausfall	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile
			G 1.2	Ausfall des IT-Systems	M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 6.77	(A)	Erstellung von Rettungsdisketten für Windows 2000
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 1.4	Feuer	M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 1.5	Wasser	M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 1.8	Staub, Verschmutzung	M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.227	(A)	Planung des Windows 2000 Einsatzes
					M 2.228	(A)	Festlegen einer Windows 2000 Sicherheitsrichtlinie
					M 2.231	(A)	Planung der Gruppenrichtlinien unter Windows 2000
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP

					M 4.150	(A)	Konfiguration von Windows 2000 als Workstation
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.231	(A)	Planung der Gruppenrichtlinien unter Windows 2000
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
					M 4.150	(A)	Konfiguration von Windows 2000 als Workstation
					M 6.77	(A)	Erstellung von Rettungsdisketten für Windows 2000
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.227	(A)	Planung des Windows 2000 Einsatzes
					M 2.228	(A)	Festlegen einer Windows 2000 Sicherheitsrichtlinie
					M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 4.150	(A)	Konfiguration von Windows 2000 als Workstation
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 6.77	(A)	Erstellung von Rettungsdisketten für Windows 2000
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.227	(A)	Planung des Windows 2000 Einsatzes
					M 2.228	(A)	Festlegen einer Windows 2000 Sicherheitsrichtlinie
					M 2.231	(A)	Planung der Gruppenrichtlinien unter Windows 2000

					M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
					M 4.150	(A)	Konfiguration von Windows 2000 als Workstation
					M 6.77	(A)	Erstellung von Rettungsdisketten für Windows 2000
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.227	(A)	Planung des Windows 2000 Einsatzes
					M 2.228	(A)	Festlegen einer Windows 2000 Sicherheitsrichtlinie
					M 2.231	(A)	Planung der Gruppenrichtlinien unter Windows 2000
					M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 6.77	(A)	Erstellung von Rettungsdisketten für Windows 2000
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 4.1	Ausfall der Stromversorgung	M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 4.7	Defekte Datenträger	M 6.77	(A)	Erstellung von Rettungsdisketten für Windows 2000
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 4.8	Bekanntwerden von Softwareschwachstellen	M 4.136	(A)	Sichere Installation von Windows 2000
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 4.23	Automatische CD-ROM-Erkennung	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 5.2	Manipulation an Daten oder Software	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.231	(A)	Planung der Gruppenrichtlinien unter Windows 2000
					M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
					M 4.150	(A)	Konfiguration von Windows 2000 als Workstation
					M 6.77	(A)	Erstellung von Rettungsdisketten für Windows 2000
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 5.4	Diebstahl	M 6.78	(A)	Datensicherung unter Windows 2000/XP

			G 5.9	Unberechtigte IT-Nutzung	M 2.31	(B)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.227	(A)	Planung des Windows 2000 Einsatzes
					M 2.228	(A)	Festlegen einer Windows 2000 Sicherheitsrichtlinie
					M 2.231	(A)	Planung der Gruppenrichtlinien unter Windows 2000
					M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.17	(A)	Sperren und Löschen nicht benötigter Accounts und Terminals
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
					M 4.150	(A)	Konfiguration von Windows 2000 als Workstation
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.231	(A)	Planung der Gruppenrichtlinien unter Windows 2000
					M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
			G 5.21	Trojanische Pferde	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
			G 5.23	Computer-Viren	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 5.43	Makro-Viren	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System	M 2.227	(A)	Planung des Windows 2000 Einsatzes
					M 2.228	(A)	Festlegen einer Windows 2000 Sicherheitsrichtlinie
					M 2.231	(A)	Planung der Gruppenrichtlinien unter Windows 2000
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 4.147	(Z)	Sichere Nutzung von EFS unter Windows 2000/XP
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 4.147	(Z)	Sichere Nutzung von EFS unter Windows 2000/XP
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
			G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP

					M 4.136	(A)	Sichere Installation von Windows 2000
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
			G 5.85	Integritätsverlust schützenswerter Informationen	M 4.147	(Z)	Sichere Nutzung von EFS unter Windows 2000/XP
B 3.208	(5.8)	Internet-PC	G 1.2	Ausfall des IT-Systems	M 2.234	(A)	Konzeption von Internet-PCs
					M 4.151	(B)	Sichere Installation von Internet-PCs
					M 4.152	(B)	Sicherer Betrieb von Internet-PCs
					M 5.95	(B)	Sicherer E-Commerce bei der Nutzung von Internet-PCs
					M 6.79	(A)	Datensicherung beim Einsatz von Internet-PCs
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.234	(A)	Konzeption von Internet-PCs
					M 2.235	(A)	Richtlinien für die Nutzung von Internet-PCs
					M 2.313	(A)	Sichere Anmeldung bei Internet-Diensten
					M 5.95	(B)	Sicherer E-Commerce bei der Nutzung von Internet-PCs
			G 2.2	Unzureichende Kenntnis über Regelungen	M 2.235	(A)	Richtlinien für die Nutzung von Internet-PCs
			G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzern	M 2.313	(A)	Sichere Anmeldung bei Internet-Diensten
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 5.95	(B)	Sicherer E-Commerce bei der Nutzung von Internet-PCs
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 2.235	(A)	Richtlinien für die Nutzung von Internet-PCs
					M 2.313	(A)	Sichere Anmeldung bei Internet-Diensten
					M 4.151	(B)	Sichere Installation von Internet-PCs
					M 4.152	(B)	Sicherer Betrieb von Internet-PCs
					M 5.66	(B)	Verwendung von SSL
					M 5.93	(A)	Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs
					M 5.94	(A)	Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.234	(A)	Konzeption von Internet-PCs
					M 2.235	(A)	Richtlinien für die Nutzung von Internet-PCs
					M 4.151	(B)	Sichere Installation von Internet-PCs
					M 4.152	(B)	Sicherer Betrieb von Internet-PCs
			G 3.38	Konfigurations- und Bedienungsfehler	M 2.234	(A)	Konzeption von Internet-PCs
					M 2.235	(A)	Richtlinien für die Nutzung von Internet-PCs
					M 4.151	(B)	Sichere Installation von Internet-PCs
					M 4.152	(B)	Sicherer Betrieb von Internet-PCs
					M 5.91	(Z)	Einsatz von Personal Firewalls für Internet-PCs
					M 5.92	(B)	Sichere Internet-Anbindung von Internet-PCs
					M 6.79	(A)	Datensicherung beim Einsatz von Internet-PCs
			G 4.22	Software-Schwachstellen oder -Fehler	M 4.151	(B)	Sichere Installation von Internet-PCs
					M 4.152	(B)	Sicherer Betrieb von Internet-PCs
					M 5.91	(Z)	Einsatz von Personal Firewalls für Internet-PCs
					M 5.92	(B)	Sichere Internet-Anbindung von Internet-PCs
					M 5.93	(A)	Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs

					M 5.94	(A)	Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs
					M 5.95	(B)	Sicherer E-Commerce bei der Nutzung von Internet-PCs
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 6.79	(A)	Datensicherung beim Einsatz von Internet-PCs
			G 5.2	Manipulation an Daten oder Software	M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
			G 5.21	Trojanische Pferde	M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 5.98	(C)	Schutz vor Missbrauch kostenpflichtiger Einwahlnummern
			G 5.23	Computer-Viren	M 2.235	(A)	Richtlinien für die Nutzung von Internet-PCs
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 4.151	(B)	Sichere Installation von Internet-PCs
					M 4.152	(B)	Sicherer Betrieb von Internet-PCs
					M 5.93	(A)	Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs
					M 5.94	(A)	Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs
					M 6.79	(A)	Datensicherung beim Einsatz von Internet-PCs
			G 5.43	Makro-Viren	M 2.235	(A)	Richtlinien für die Nutzung von Internet-PCs
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.41	(Z)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
					M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
					M 4.151	(B)	Sichere Installation von Internet-PCs
					M 4.152	(B)	Sicherer Betrieb von Internet-PCs
					M 5.93	(A)	Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs
					M 5.94	(A)	Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs
					M 6.79	(A)	Datensicherung beim Einsatz von Internet-PCs
			G 5.48	IP-Spoofing	M 5.66	(B)	Verwendung von SSL
					M 5.96	(A)	Sichere Nutzung von Webmail
			G 5.78	DNS-Spoofing	M 5.59	(C)	Schutz vor DNS-Spoofing
					M 5.92	(B)	Sichere Internet-Anbindung von Internet-PCs
			G 5.87	Web-Spoofing	M 5.66	(B)	Verwendung von SSL
					M 5.95	(B)	Sicherer E-Commerce bei der Nutzung von Internet-PCs
			G 5.88	Missbrauch aktiver Inhalte	M 2.235	(A)	Richtlinien für die Nutzung von Internet-PCs
					M 5.66	(B)	Verwendung von SSL
					M 5.93	(A)	Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs
					M 5.96	(A)	Sichere Nutzung von Webmail
					M 5.98	(C)	Schutz vor Missbrauch kostenpflichtiger Einwahlnummern
			G 5.91	Abschalten von Sicherheitsmechanismen für den RAS-Zugang	M 5.91	(Z)	Einsatz von Personal Firewalls für Internet-PCs
			G 5.103	Missbrauch von Webmail	M 5.96	(A)	Sichere Nutzung von Webmail

B 3.209	(neu)	Client unter Windows XP	G 1.2	Ausfall des IT-Systems	M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 6.76	(C)	Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 1.4	Feuer	M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 1.5	Wasser	M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 1.8	Staub, Verschmutzung	M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.324	(A)	Einführung von Windows XP planen
					M 2.325	(A)	Planung der Windows XP Sicherheitsrichtlinie
					M 2.326	(A)	Planung der Windows XP Gruppenrichtlinien
					M 2.329	(A)	Einführung von Windows XP SP2
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
					M 4.244	(A)	Sichere Windows XP Systemkonfiguration
					M 4.245	(A)	Basiseinstellungen für Windows XP GPOs
					M 4.246	(A)	Konfiguration der Systemdienste unter Windows XP
					M 4.247	(A)	Restriktive Berechtigungsvergabe unter Windows XP
					M 4.249	(A)	Windows XP Systeme aktuell halten
					M 5.123	(B)	Absicherung der Netzwerkkommunikation unter Windows XP
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	M 2.326	(A)	Planung der Windows XP Gruppenrichtlinien
					M 2.329	(A)	Einführung von Windows XP SP2
					M 2.330	(B)	Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
					M 4.247	(A)	Restriktive Berechtigungsvergabe unter Windows XP
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
					M 4.244	(A)	Sichere Windows XP Systemkonfiguration
					M 4.245	(A)	Basiseinstellungen für Windows XP GPOs
					M 4.246	(A)	Konfiguration der Systemdienste unter Windows XP
					M 4.247	(A)	Restriktive Berechtigungsvergabe unter Windows XP

					M 5.123	(B)	Absicherung der Netzwerkkommunikation unter Windows XP
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.324	(A)	Einführung von Windows XP planen
					M 2.325	(A)	Planung der Windows XP Sicherheitsrichtlinie
					M 2.326	(A)	Planung der Windows XP Gruppenrichtlinien
					M 2.329	(A)	Einführung von Windows XP SP2
					M 2.330	(B)	Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung
					M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 4.244	(A)	Sichere Windows XP Systemkonfiguration
					M 4.245	(A)	Basiseinstellungen für Windows XP GPOs
					M 4.246	(A)	Konfiguration der Systemdienste unter Windows XP
					M 5.123	(B)	Absicherung der Netzwerkkommunikation unter Windows XP
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.324	(A)	Einführung von Windows XP planen
					M 2.325	(A)	Planung der Windows XP Sicherheitsrichtlinie
					M 2.326	(A)	Planung der Windows XP Gruppenrichtlinien
					M 2.327	(B)	Sicherheit beim Fernzugriff unter Windows XP
					M 2.329	(A)	Einführung von Windows XP SP2
					M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
					M 4.244	(A)	Sichere Windows XP Systemkonfiguration
					M 4.245	(A)	Basiseinstellungen für Windows XP GPOs
					M 4.246	(A)	Konfiguration der Systemdienste unter Windows XP
					M 4.247	(A)	Restriktive Berechtigungsvergabe unter Windows XP
					M 4.248	(A)	Sichere Installation von Windows XP
					M 5.123	(B)	Absicherung der Netzwerkkommunikation unter Windows XP
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.324	(A)	Einführung von Windows XP planen

					M 2.325	(A)	Planung der Windows XP Sicherheitsrichtlinie
					M 2.326	(A)	Planung der Windows XP Gruppenrichtlinien
					M 2.329	(A)	Einführung von Windows XP SP2
					M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 4.243	(Z)	Windows XP Verwaltungswerkzeuge
					M 4.248	(A)	Sichere Installation von Windows XP
					M 6.76	(C)	Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 3.22	Fehlerhafte Änderung der Registrierung	M 4.247	(A)	Restriktive Berechtigungsvergabe unter Windows XP
			G 3.48	Fehlkonfiguration von Windows 2000/XP Rechnern	M 2.325	(A)	Planung der Windows XP Sicherheitsrichtlinie
					M 2.326	(A)	Planung der Windows XP Gruppenrichtlinien
					M 2.327	(B)	Sicherheit beim Fernzugriff unter Windows XP
					M 2.330	(B)	Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 4.244	(A)	Sichere Windows XP Systemkonfiguration
					M 4.245	(A)	Basiseinstellungen für Windows XP GPOs
					M 4.246	(A)	Konfiguration der Systemdienste unter Windows XP
					M 4.247	(A)	Restriktive Berechtigungsvergabe unter Windows XP
					M 4.248	(A)	Sichere Installation von Windows XP
					M 5.123	(B)	Absicherung der Netzwerkkommunikation unter Windows XP
			G 4.1	Ausfall der Stromversorgung	M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 4.7	Defekte Datenträger	M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 4.8	Bekanntwerden von Softwareschwachstellen	M 2.329	(A)	Einführung von Windows XP SP2
					M 4.248	(A)	Sichere Installation von Windows XP
					M 4.249	(A)	Windows XP Systeme aktuell halten
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 4.23	Automatische CD-ROM-Erkennung	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 4.244	(A)	Sichere Windows XP Systemkonfiguration
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 5.2	Manipulation an Daten oder Software	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.326	(A)	Planung der Windows XP Gruppenrichtlinien
					M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
					M 4.244	(A)	Sichere Windows XP Systemkonfiguration

					M 4.245	(A)	Basiseinstellungen für Windows XP GPOs
					M 4.246	(A)	Konfiguration der Systemdienste unter Windows XP
					M 4.247	(A)	Restriktive Berechtigungsvergabe unter Windows XP
					M 4.248	(A)	Sichere Installation von Windows XP
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 5.4	Diebstahl	M 2.328	(B)	Einsatz von Windows XP auf mobilen Rechnern
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 5.7	Abhören von Leitungen	M 2.327	(B)	Sicherheit beim Fernzugriff unter Windows XP
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
					M 5.89	(A)	Konfiguration des sicheren Kanals unter Windows 2000/XP
					M 5.90	(Z)	Einsatz von IPSec unter Windows 2000/XP
					M 5.123	(B)	Absicherung der Netzwerkkommunikation unter Windows XP
			G 5.9	Unberechtigte IT-Nutzung	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.324	(A)	Einführung von Windows XP planen
					M 2.325	(A)	Planung der Windows XP Sicherheitsrichtlinie
					M 2.326	(A)	Planung der Windows XP Gruppenrichtlinien
					M 2.327	(B)	Sicherheit beim Fernzugriff unter Windows XP
					M 2.328	(B)	Einsatz von Windows XP auf mobilen Rechnern
					M 2.329	(A)	Einführung von Windows XP SP2
					M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
					M 4.247	(A)	Restriktive Berechtigungsvergabe unter Windows XP
					M 4.248	(A)	Sichere Installation von Windows XP
					M 5.123	(B)	Absicherung der Netzwerkkommunikation unter Windows XP
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 2.326	(A)	Planung der Windows XP Gruppenrichtlinien
					M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
			G 5.21	Trojanische Pferde	M 2.329	(A)	Einführung von Windows XP SP2
					M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
					M 4.247	(A)	Restriktive Berechtigungsvergabe unter Windows XP
					M 4.249	(A)	Windows XP Systeme aktuell halten
			G 5.23	Computer-Viren	M 2.329	(A)	Einführung von Windows XP SP2
					M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung

					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 4.249	(A)	Windows XP Systeme aktuell halten
					M 6.76	(C)	Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 5.43	Makro-Viren	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
					M 4.249	(A)	Windows XP Systeme aktuell halten
					M 6.78	(A)	Datensicherung unter Windows 2000/XP
			G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System	M 2.324	(A)	Einführung von Windows XP planen
					M 2.325	(A)	Planung der Windows XP Sicherheitsrichtlinie
					M 2.326	(A)	Planung der Windows XP Gruppenrichtlinien
					M 2.329	(A)	Einführung von Windows XP SP2
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 4.147	(Z)	Sichere Nutzung von EFS unter Windows 2000/XP
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 2.328	(B)	Einsatz von Windows XP auf mobilen Rechnern
					M 4.56	(C)	Sicheres Löschen unter Windows-Betriebssystemen
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 4.147	(Z)	Sichere Nutzung von EFS unter Windows 2000/XP
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
					M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
			G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
					M 4.48	(A)	Passwortschutz unter Windows NT/2000/XP
					M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
					M 4.52	(A)	Geräteschutz unter Windows NT/2000/XP
					M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
					M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
					M 4.248	(A)	Sichere Installation von Windows XP
			G 5.83	Kompromittierung kryptographischer Schlüssel	M 2.328	(B)	Einsatz von Windows XP auf mobilen Rechnern
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
					M 5.89	(A)	Konfiguration des sicheren Kanals unter Windows 2000/XP
					M 5.90	(Z)	Einsatz von IPSec unter Windows 2000/XP
			G 5.85	Integritätsverlust schützenswerter Informationen	M 2.328	(B)	Einsatz von Windows XP auf mobilen Rechnern
					M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
					M 4.147	(Z)	Sichere Nutzung von EFS unter Windows 2000/XP

					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
					M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
					M 5.89	(A)	Konfiguration des sicheren Kanals unter Windows 2000/XP
					M 5.90	(Z)	Einsatz von IPSec unter Windows 2000/XP
B 3.301	(7.3)	Sicherheitsgateway (Firewall)	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes	M 2.70	(A)	Entwicklung eines Konzepts für Sicherheitsgateways
					M 2.71	(A)	Festlegung einer Policy für ein Sicherheitsgateway
					M 2.73	(A)	Auswahl geeigneter Grundstrukturen für Sicherheitsgateways
					M 2.74	(A)	Geeignete Auswahl eines Paketfilters
					M 2.75	(A)	Geeignete Auswahl eines Application-Level-Gateways
					M 2.76	(A)	Auswahl und Einrichtung geeigneter Filterregeln
					M 2.77	(A)	Integration von Servern in das Sicherheitsgateway
					M 2.78	(A)	Sicherer Betrieb eines Sicherheitsgateways
					M 2.299	(A)	Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway
					M 2.300	(C)	Sichere Außerbetriebnahme oder Ersatz von Komponenten eines Sicherheitsgateways
					M 2.301	(Z)	Outsourcing des Sicherheitsgateway
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.100	(C)	Sicherheitsgateways und aktive Inhalte
					M 4.101	(C)	Sicherheitsgateways und Verschlüsselung
					M 4.222	(B)	Festlegung geeigneter Einstellungen von Sicherheitsproxies
					M 4.223	(B)	Integration von Proxy-Servern in das Sicherheitsgateway
					M 4.224	(Z)	Integration von Virtual Private Networks in ein Sicherheitsgateway
					M 4.225	(Z)	Einsatz eines Protokollierungsservers in einem Sicherheitsgateway
					M 4.226	(Z)	Integration von Virenscannern in ein Sicherheitsgateway
					M 4.227	(C)	Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation
					M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste
					M 5.46	(A)	Einsatz von Stand-alone-Systemen zur Nutzung des Internets
					M 5.70	(A)	Adreßumsetzung - NAT (Network Address Translation)
					M 5.71	(Z)	Intrusion Detection und Intrusion Response Systeme
					M 5.115	(Z)	Integration eines Webservers in ein Sicherheitsgateway
					M 5.116	(Z)	Integration eines E-Mailservers in ein Sicherheitsgateway
					M 5.117	(Z)	Integration eines Datenbank-Servers in ein Sicherheitsgateway
					M 5.118	(Z)	Integration eines DNS-Servers in ein Sicherheitsgateway
					M 5.119	(Z)	Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway
					M 5.120	(A)	Behandlung von ICMP am Sicherheitsgateway

			G 2.101	Unzureichende Notfallvorsorge bei einem Sicherheitsgateway	M 6.94	(C)	Notfallvorsorge bei Sicherheitsgateways
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.78	(A)	Sicherer Betrieb eines Sicherheitsgateways
					M 4.47	(A)	Protokollierung der Sicherheitsgateway-Aktivitäten
					M 5.46	(A)	Einsatz von Stand-alone-Systemen zur Nutzung des Internets
					M 5.71	(Z)	Intrusion Detection und Intrusion Response Systeme
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.78	(A)	Sicherer Betrieb eines Sicherheitsgateways
					M 2.299	(A)	Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway
					M 2.301	(Z)	Outsourcing des Sicherheitsgateway
					M 3.43	(C)	Schulung der Administratoren des Sicherheitsgateways
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 5.46	(A)	Einsatz von Stand-alone-Systemen zur Nutzung des Internets
					M 5.71	(Z)	Intrusion Detection und Intrusion Response Systeme
			G 3.38	Konfigurations- und Bedienungsfehler	M 2.71	(A)	Festlegung einer Policy für ein Sicherheitsgateway
					M 2.78	(A)	Sicherer Betrieb eines Sicherheitsgateways
					M 2.299	(A)	Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway
					M 2.301	(Z)	Outsourcing des Sicherheitsgateway
					M 3.43	(C)	Schulung der Administratoren des Sicherheitsgateways
					M 4.47	(A)	Protokollierung der Sicherheitsgateway-Aktivitäten
					M 5.46	(A)	Einsatz von Stand-alone-Systemen zur Nutzung des Internets
					M 5.71	(Z)	Intrusion Detection und Intrusion Response Systeme
			G 4.8	Bekanntwerden von Softwareschwachstellen	M 2.71	(A)	Festlegung einer Policy für ein Sicherheitsgateway
					M 2.78	(A)	Sicherer Betrieb eines Sicherheitsgateways
			G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen	M 2.70	(A)	Entwicklung eines Konzepts für Sicherheitsgateways
					M 2.71	(A)	Festlegung einer Policy für ein Sicherheitsgateway
					M 2.73	(A)	Auswahl geeigneter Grundstrukturen für Sicherheitsgateways
					M 2.76	(A)	Auswahl und Einrichtung geeigneter Filterregeln
					M 2.77	(A)	Integration von Servern in das Sicherheitsgateway
					M 2.78	(A)	Sicherer Betrieb eines Sicherheitsgateways
					M 4.47	(A)	Protokollierung der Sicherheitsgateway-Aktivitäten
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.100	(C)	Sicherheitsgateways und aktive Inhalte
					M 4.101	(C)	Sicherheitsgateways und Verschlüsselung
					M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste
					M 5.46	(A)	Einsatz von Stand-alone-Systemen zur Nutzung des Internets
					M 5.70	(A)	Adreßumsetzung - NAT (Network Address Translation)
					M 5.71	(Z)	Intrusion Detection und Intrusion Response Systeme
			G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client	M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste

			G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client	M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste
			G 4.20	Datenverlust bei erschöpftem Speichermedium	M 2.78	(A)	Sicherer Betrieb eines Sicherheitsgateways
					M 4.47	(A)	Protokollierung der Sicherheitsgateway-Aktivitäten
					M 5.46	(A)	Einsatz von Stand-alone-Systemen zur Nutzung des Internets
			G 4.22	Software-Schwachstellen oder -Fehler	M 2.71	(A)	Festlegung einer Policy für ein Sicherheitsgateway
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste
					M 5.46	(A)	Einsatz von Stand-alone-Systemen zur Nutzung des Internets
					M 5.71	(Z)	Intrusion Detection und Intrusion Response Systeme
			G 4.39	Software-Konzeptionsfehler	M 2.71	(A)	Festlegung einer Policy für ein Sicherheitsgateway
					M 4.100	(C)	Sicherheitsgateways und aktive Inhalte
					M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste
					M 5.46	(A)	Einsatz von Stand-alone-Systemen zur Nutzung des Internets
					M 5.71	(Z)	Intrusion Detection und Intrusion Response Systeme
			G 5.2	Manipulation an Daten oder Software	M 2.70	(A)	Entwicklung eines Konzepts für Sicherheitsgateways
					M 2.71	(A)	Festlegung einer Policy für ein Sicherheitsgateway
					M 2.73	(A)	Auswahl geeigneter Grundstrukturen für Sicherheitsgateways
					M 2.74	(A)	Geeignete Auswahl eines Paketfilters
					M 2.75	(A)	Geeignete Auswahl eines Application-Level-Gateways
					M 2.76	(A)	Auswahl und Einrichtung geeigneter Filterregeln
					M 2.77	(A)	Integration von Servern in das Sicherheitsgateway
					M 2.78	(A)	Sicherer Betrieb eines Sicherheitsgateways
					M 4.47	(A)	Protokollierung der Sicherheitsgateway-Aktivitäten
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.100	(C)	Sicherheitsgateways und aktive Inhalte
					M 4.101	(C)	Sicherheitsgateways und Verschlüsselung
					M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste
					M 5.46	(A)	Einsatz von Stand-alone-Systemen zur Nutzung des Internets
					M 5.71	(Z)	Intrusion Detection und Intrusion Response Systeme
			G 5.9	Unberechtigte IT-Nutzung	M 2.70	(A)	Entwicklung eines Konzepts für Sicherheitsgateways
					M 2.71	(A)	Festlegung einer Policy für ein Sicherheitsgateway
					M 2.73	(A)	Auswahl geeigneter Grundstrukturen für Sicherheitsgateways
					M 2.74	(A)	Geeignete Auswahl eines Paketfilters
					M 2.75	(A)	Geeignete Auswahl eines Application-Level-Gateways
					M 2.76	(A)	Auswahl und Einrichtung geeigneter Filterregeln
					M 2.77	(A)	Integration von Servern in das Sicherheitsgateway
					M 2.78	(A)	Sicherer Betrieb eines Sicherheitsgateways
					M 4.47	(A)	Protokollierung der Sicherheitsgateway-Aktivitäten
					M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste

					M 5.46	(A)	Einsatz von Stand-alone-Systemen zur Nutzung des Internets
					M 5.71	(Z)	Intrusion Detection und Intrusion Response Systeme
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 2.78	(A)	Sicherer Betrieb eines Sicherheitsgateways
					M 4.47	(A)	Protokollierung der Sicherheitsgateway-Aktivitäten
					M 5.46	(A)	Einsatz von Stand-alone-Systemen zur Nutzung des Internets
			G 5.24	Wiedereinspielen von Nachrichten	M 4.47	(A)	Protokollierung der Sicherheitsgateway-Aktivitäten
					M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste
			G 5.25	Maskerade	M 2.70	(A)	Entwicklung eines Konzepts für Sicherheitsgateways
					M 2.71	(A)	Festlegung einer Policy für ein Sicherheitsgateway
					M 2.78	(A)	Sicherer Betrieb eines Sicherheitsgateways
					M 4.47	(A)	Protokollierung der Sicherheitsgateway-Aktivitäten
					M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste
			G 5.28	Verhinderung von Diensten	M 2.70	(A)	Entwicklung eines Konzepts für Sicherheitsgateways
					M 2.71	(A)	Festlegung einer Policy für ein Sicherheitsgateway
					M 2.78	(A)	Sicherer Betrieb eines Sicherheitsgateways
					M 2.302	(Z)	Sicherheitsgateways und Hochverfügbarkeit
					M 4.47	(A)	Protokollierung der Sicherheitsgateway-Aktivitäten
					M 5.46	(A)	Einsatz von Stand-alone-Systemen zur Nutzung des Internets
					M 5.70	(A)	Adreßumsetzung - NAT (Network Address Translation)
					M 5.71	(Z)	Intrusion Detection und Intrusion Response Systeme
			G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten	M 2.70	(A)	Entwicklung eines Konzepts für Sicherheitsgateways
					M 2.71	(A)	Festlegung einer Policy für ein Sicherheitsgateway
					M 2.77	(A)	Integration von Servern in das Sicherheitsgateway
					M 5.46	(A)	Einsatz von Stand-alone-Systemen zur Nutzung des Internets
			G 5.48	IP-Spoofing	M 2.74	(A)	Geeignete Auswahl eines Paketfilters
					M 2.75	(A)	Geeignete Auswahl eines Application-Level-Gateways
					M 2.76	(A)	Auswahl und Einrichtung geeigneter Filterregeln
					M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste
			G 5.49	Missbrauch des Source-Routing	M 2.74	(A)	Geeignete Auswahl eines Paketfilters
					M 2.75	(A)	Geeignete Auswahl eines Application-Level-Gateways
					M 2.76	(A)	Auswahl und Einrichtung geeigneter Filterregeln
					M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste
					M 5.71	(Z)	Intrusion Detection und Intrusion Response Systeme
			G 5.50	Missbrauch des ICMP-Protokolls	M 2.74	(A)	Geeignete Auswahl eines Paketfilters
					M 2.75	(A)	Geeignete Auswahl eines Application-Level-Gateways
					M 2.76	(A)	Auswahl und Einrichtung geeigneter Filterregeln
					M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste
					M 5.71	(Z)	Intrusion Detection und Intrusion Response Systeme
					M 5.120	(A)	Behandlung von ICMP am Sicherheitsgateway
			G 5.51	Missbrauch der Routing-Protokolle	M 2.74	(A)	Geeignete Auswahl eines Paketfilters
					M 2.75	(A)	Geeignete Auswahl eines Application-Level-Gateways
					M 2.76	(A)	Auswahl und Einrichtung geeigneter Filterregeln
					M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste

					M 5.71	(Z)	Intrusion Detection und Intrusion Response Systeme
			G 5.78	DNS-Spoofing	M 2.78	(A)	Sicherer Betrieb eines Sicherheitsgateways
					M 5.39	(A)	Sicherer Einsatz der Protokolle und Dienste
					M 5.59	(A)	Schutz vor DNS-Spoofing
					M 5.118	(Z)	Integration eines DNS-Servers in ein Sicherheitsgateway
B 3.302	(7.11)	Router und Switches	G 2.1	Fehlende oder unzureichende Regelungen	M 2.279	(A)	Erstellung einer Sicherheitsrichtlinie für Router und Switches
			G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel	M 2.280	(C)	Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	M 2.282	(A)	Regelmäßige Kontrolle von Routern und Switches
			G 2.22	Fehlende Auswertung von Protokolldaten	M 4.205	(C)	Protokollierung bei Routern und Switches
			G 2.27	Fehlende oder unzureichende Dokumentation	M 2.281	(A)	Dokumentation der Systemkonfiguration von Routern und Switches
			G 2.44	Inkompatible aktive und passive Netzkomponenten	M 2.280	(C)	Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches
			G 2.54	Vertraulichkeitsverlust durch Restinformationen	M 2.284	(C)	Sichere Außerbetriebnahme von Routern und Switches
			G 2.98	Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switches	M 2.276	(Z)	Funktionsweise eines Routers
					M 2.277	(Z)	Funktionsweise eines Switches
					M 2.278	(Z)	Typische Einsatzszenarien von Routern und Switches
					M 2.280	(C)	Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches
			G 3.64	Fehlerhafte Konfiguration von Routern und Switches	M 3.38	(B)	Administratorenschulung für Router und Switches
					M 4.201	(A)	Sichere lokale Grundkonfiguration von Routern und Switches
					M 4.202	(A)	Sichere Netz-Grundkonfiguration von Routern und Switches
					M 4.203	(A)	Konfigurations-Checkliste für Router und Switches
			G 3.65	Fehlerhafte Administration von Routern und Switches	M 3.38	(B)	Administratorenschulung für Router und Switches
					M 4.204	(C)	Sichere Administration von Routern und Switches
					M 5.111	(C)	Einrichtung von Access Control Lists auf Routern
					M 6.91	(C)	Datensicherung und Recovery bei Routern und Switches
					M 6.92	(C)	Notfallvorsorge bei Routern und Switches
			G 4.8	Bekanntwerden von Softwareschwachstellen	M 2.283	(B)	Software-Pflege auf Routern und Switches
			G 4.49	Unsichere Default-Einstellungen auf Routern und Switches	M 4.201	(A)	Sichere lokale Grundkonfiguration von Routern und Switches
					M 4.202	(A)	Sichere Netz-Grundkonfiguration von Routern und Switches
					M 4.203	(A)	Konfigurations-Checkliste für Router und Switches
			G 5.4	Diebstahl	M 1.43	(A)	Gesicherte Aufstellung aktiver Netzkomponenten
			G 5.51	Missbrauch der Routing-Protokolle	M 5.112	(C)	Sicherheitsaspekte von Routing-Protokollen
			G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz	M 4.206	(C)	Sicherung von Switch-Ports
			G 5.112	Manipulation von ARP-Tabellen	M 4.202	(A)	Sichere Netz-Grundkonfiguration von Routern und Switches
					M 4.204	(C)	Sichere Administration von Routern und Switches

			G 5.113	MAC-Spoofing	M 4.202	(A)	Sichere Netz-Grundkonfiguration von Routern und Switches
			G 5.114	Missbrauch von Spanning Tree	M 4.204	(C)	Sichere Administration von Routern und Switches
			G 5.115	Überwindung der Grenzen zwischen VLANs	M 4.202	(A)	Sichere Netz-Grundkonfiguration von Routern und Switches
					M 4.204	(C)	Sichere Administration von Routern und Switches
B 3.401	(8.1)	TK-Anlage	G 1.4	Feuer	M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 6.26	(B)	Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten
					M 6.28	(Z)	Vereinbarung über Lieferzeiten "lebensnotwendiger" TK-Baugruppen
					M 6.29	(Z)	TK-Basisanschluss für Notrufe
					M 6.30	(Z)	Katastrophenschaltung
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	M 1.12	(B)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.30	(A)	Absicherung der Datenträger mit TK-Gebührendaten
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 1.12	(B)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
			G 3.7	Ausfall der TK-Anlage durch Fehlbedienung	M 2.28	(Z)	Bereitstellung externer TK-Beratungskapazität
					M 2.29	(B)	Bedienungsanleitung der TK-Anlage für die Benutzer
					M 4.5	(B)	Protokollierung der TK-Administrationsarbeiten
					M 4.6	(C)	Revision der TK-Anlagenkonfiguration
					M 4.11	(B)	Absicherung der TK-Anlagen-Schnittstellen
					M 4.12	(A)	Sperren nicht benötigter TK-Leistungsmerkmale
					M 5.14	(A)	Absicherung interner Remote-Zugänge
					M 5.15	(A)	Absicherung externer Remote-Zugänge
					M 6.10	(B)	Notfall-Plan für DFÜ-Ausfall
					M 6.26	(B)	Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten
					M 6.28	(Z)	Vereinbarung über Lieferzeiten "lebensnotwendiger" TK-Baugruppen
					M 6.29	(Z)	TK-Basisanschluss für Notrufe
					M 6.30	(Z)	Katastrophenschaltung
			G 4.6	Spannungsschwankungen/Überspannung/Unterspannung	M 1.25	(B)	Überspannungsschutz
					M 1.28	(B)	Lokale unterbrechungsfreie Stromversorgung
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 1.12	(B)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 1.30	(A)	Absicherung der Datenträger mit TK-Gebührendaten
					M 4.5	(B)	Protokollierung der TK-Administrationsarbeiten
					M 4.6	(C)	Revision der TK-Anlagenkonfiguration
					M 4.11	(B)	Absicherung der TK-Anlagen-Schnittstellen
					M 6.10	(B)	Notfall-Plan für DFÜ-Ausfall
					M 6.28	(Z)	Vereinbarung über Lieferzeiten "lebensnotwendiger" TK-Baugruppen
					M 6.29	(Z)	TK-Basisanschluss für Notrufe

					M 6.30	(Z)	Katastrophenschaltung
			G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten	M 1.12	(B)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.30	(A)	Absicherung der Datenträger mit TK-Gebührendaten
					M 2.29	(B)	Bedienungsanleitung der TK-Anlage für die Benutzer
					M 2.105	(A)	Beschaffung von TK-Anlagen
					M 3.12	(B)	Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne
					M 3.13	(B)	Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen
					M 4.5	(B)	Protokollierung der TK-Administrationsarbeiten
					M 4.6	(C)	Revision der TK-Anlagenkonfiguration
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.8	(A)	Schutz des TK-Bedienplatzes
					M 4.10	(Z)	Passwortschutz für TK-Endgeräte
					M 4.11	(B)	Absicherung der TK-Anlagen-Schnittstellen
					M 4.12	(A)	Sperren nicht benötigter TK-Leistungsmerkmale
					M 5.14	(A)	Absicherung interner Remote-Zugänge
					M 5.15	(A)	Absicherung externer Remote-Zugänge
			G 5.12	Abhören von Telefongesprächen und Datenübertragungen	M 2.27	(Z)	Verzicht auf Fernwartung der TK-Anlage
					M 3.12	(B)	Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne
					M 3.13	(B)	Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen
					M 4.5	(B)	Protokollierung der TK-Administrationsarbeiten
					M 4.6	(C)	Revision der TK-Anlagenkonfiguration
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.8	(A)	Schutz des TK-Bedienplatzes
					M 4.10	(Z)	Passwortschutz für TK-Endgeräte
					M 4.11	(B)	Absicherung der TK-Anlagen-Schnittstellen
					M 4.12	(A)	Sperren nicht benötigter TK-Leistungsmerkmale
					M 5.14	(A)	Absicherung interner Remote-Zugänge
					M 5.15	(A)	Absicherung externer Remote-Zugänge
			G 5.13	Abhören von Räumen	M 1.12	(B)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
					M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
					M 2.27	(Z)	Verzicht auf Fernwartung der TK-Anlage
					M 2.29	(B)	Bedienungsanleitung der TK-Anlage für die Benutzer
					M 3.12	(B)	Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne
					M 3.13	(B)	Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen
					M 4.5	(B)	Protokollierung der TK-Administrationsarbeiten
					M 4.6	(C)	Revision der TK-Anlagenkonfiguration
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.8	(A)	Schutz des TK-Bedienplatzes
					M 4.10	(Z)	Passwortschutz für TK-Endgeräte

					M 4.11	(B)	Absicherung der TK-Anlagen-Schnittstellen
					M 4.12	(A)	Sperren nicht benötigter TK-Leistungsmerkmale
					M 5.14	(A)	Absicherung interner Remote-Zugänge
					M 5.15	(A)	Absicherung externer Remote-Zugänge
			G 5.14	Gebührenbetrug	M 1.30	(A)	Absicherung der Datenträger mit TK-Gebührendaten
					M 2.29	(B)	Bedienungsanleitung der TK-Anlage für die Benutzer
					M 3.12	(B)	Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne
					M 3.13	(B)	Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen
					M 4.5	(B)	Protokollierung der TK-Administrationsarbeiten
					M 4.6	(C)	Revision der TK-Anlagenkonfiguration
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.8	(A)	Schutz des TK-Bedienplatzes
					M 4.10	(Z)	Passwortschutz für TK-Endgeräte
					M 4.11	(B)	Absicherung der TK-Anlagen-Schnittstellen
					M 4.12	(A)	Sperren nicht benötigter TK-Leistungsmerkmale
					M 4.62	(Z)	Einsatz eines D-Kanal-Filters
			G 5.15	"Neugierige" Mitarbeiter	M 2.29	(B)	Bedienungsanleitung der TK-Anlage für die Benutzer
					M 3.12	(B)	Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne
					M 3.13	(B)	Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen
					M 4.5	(B)	Protokollierung der TK-Administrationsarbeiten
					M 4.6	(C)	Revision der TK-Anlagenkonfiguration
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.8	(A)	Schutz des TK-Bedienplatzes
					M 4.10	(Z)	Passwortschutz für TK-Endgeräte
					M 4.11	(B)	Absicherung der TK-Anlagen-Schnittstellen
					M 4.12	(A)	Sperren nicht benötigter TK-Leistungsmerkmale
					M 5.14	(A)	Absicherung interner Remote-Zugänge
			G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal	M 2.28	(Z)	Bereitstellung externer TK-Beratungskapazität
					M 2.105	(A)	Beschaffung von TK-Anlagen
					M 4.5	(B)	Protokollierung der TK-Administrationsarbeiten
					M 4.6	(C)	Revision der TK-Anlagenkonfiguration
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.8	(A)	Schutz des TK-Bedienplatzes
					M 5.14	(A)	Absicherung interner Remote-Zugänge
					M 6.26	(B)	Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten
					M 6.29	(Z)	TK-Basisanschluss für Notrufe
					M 6.30	(Z)	Katastrophenschaltung
			G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal	M 2.28	(Z)	Bereitstellung externer TK-Beratungskapazität
					M 2.105	(A)	Beschaffung von TK-Anlagen
					M 4.5	(B)	Protokollierung der TK-Administrationsarbeiten
					M 4.6	(C)	Revision der TK-Anlagenkonfiguration
					M 4.7	(A)	Änderung voreingestellter Passwörter

					M 5.15	(A)	Absicherung externer Remote-Zugänge
					M 6.29	(Z)	TK-Basisanschluss für Notrufe
					M 6.30	(Z)	Katastrophenschaltung
			G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlagen	M 2.27	(Z)	Verzicht auf Fernwartung der TK-Anlage
					M 2.28	(Z)	Bereitstellung externer TK-Beratungskapazität
					M 2.105	(A)	Beschaffung von TK-Anlagen
					M 4.5	(B)	Protokollierung der TK-Administrationsarbeiten
					M 4.6	(C)	Revision der TK-Anlagenkonfiguration
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.8	(A)	Schutz des TK-Bedienplatzes
					M 4.10	(Z)	Passwortschutz für TK-Endgeräte
					M 4.11	(B)	Absicherung der TK-Anlagen-Schnittstellen
					M 4.12	(A)	Sperren nicht benötigter TK-Leistungsmerkmale
					M 4.62	(Z)	Einsatz eines D-Kanal-Filters
					M 5.14	(A)	Absicherung interner Remote-Zugänge
					M 5.15	(A)	Absicherung externer Remote-Zugänge
					M 6.10	(B)	Notfall-Plan für DFÜ-Ausfall
					M 6.26	(B)	Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten
					M 6.29	(Z)	TK-Basisanschluss für Notrufe
					M 6.30	(Z)	Katastrophenschaltung
B 3.402	(8.2)	Faxgerät	G 2.20	Unzureichende oder falsche Versorgung mit Verbrauchsgütern	M 2.47	(B)	Ernennung eines Fax-Verantwortlichen
					M 2.52	(C)	Versorgung und Kontrolle der Verbrauchsgüter
					M 2.53	(Z)	Abschalten des Faxgerätes außerhalb der Bürozeiten
					M 4.37	(Z)	Sperren bestimmter Absender-Faxnummern
					M 6.39	(C)	Auflistung von Händleradressen zur Fax-Wiederbeschaffung
			G 3.14	Fehleinschätzung der Rechtsverbindlichkeit eines Fax	M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung
			G 4.14	Verblassen spezieller Faxpapiere	M 2.49	(A)	Beschaffung geeigneter Faxgeräte
					M 2.51	(Z)	Fertigung von Kopien eingehender Faxsendungen
			G 4.15	Fehlerhafte Faxübertragung	M 2.49	(A)	Beschaffung geeigneter Faxgeräte
					M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung
					M 4.36	(Z)	Sperren bestimmter Faxempfänger-Rufnummern
					M 5.24	(Z)	Nutzung eines geeigneten Faxvorblattes
					M 5.25	(A)	Nutzung von Sende- und Empfangsprotokollen
					M 5.27	(Z)	Telefonische Rückversicherung über korrekten Faxempfang
					M 5.28	(Z)	Telefonische Rückversicherung über korrekten Faxabsender
					M 5.29	(C)	Gelegentliche Kontrolle programmierter Zieladressen und Protokolle
			G 5.7	Abhören von Leitungen	M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung
			G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers	M 1.37	(A)	Geeignete Aufstellung eines Faxgerätes
					M 2.48	(Z)	Festlegung berechtigter Faxbediener
					M 2.53	(Z)	Abschalten des Faxgerätes außerhalb der Bürozeiten
					M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung

					M 5.25	(A)	Nutzung von Sende- und Empfangsprotokollen
					M 5.29	(C)	Gelegentliche Kontrolle programmierter Zieladressen und Protokolle
			G 5.31	Unbefugtes Lesen von Faxsendungen	M 1.37	(A)	Geeignete Aufstellung eines Faxgerätes
					M 2.47	(B)	Ernennung eines Fax-Verantwortlichen
					M 2.48	(Z)	Festlegung berechtigter Faxbediener
					M 2.53	(Z)	Abschalten des Faxgerätes außerhalb der Bürozeiten
					M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung
					M 4.43	(Z)	Faxgerät mit automatischer Eingangskuvertierung
					M 5.26	(Z)	Telefonische Ankündigung einer Faxsendung
					M 5.29	(C)	Gelegentliche Kontrolle programmierter Zieladressen und Protokolle
			G 5.32	Auswertung von Restinformationen in Faxgeräten und Faxservern	M 1.37	(A)	Geeignete Aufstellung eines Faxgerätes
					M 2.47	(B)	Ernennung eines Fax-Verantwortlichen
					M 2.50	(B)	Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen
					M 2.53	(Z)	Abschalten des Faxgerätes außerhalb der Bürozeiten
					M 4.43	(Z)	Faxgerät mit automatischer Eingangskuvertierung
			G 5.33	Vortäuschen eines falschen Absenders bei Faxsendungen	M 1.37	(A)	Geeignete Aufstellung eines Faxgerätes
					M 2.48	(Z)	Festlegung berechtigter Faxbediener
					M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung
					M 4.37	(Z)	Sperren bestimmter Absender-Faxnummern
					M 5.24	(Z)	Nutzung eines geeigneten Faxvorblattes
					M 5.25	(A)	Nutzung von Sende- und Empfangsprotokollen
					M 5.26	(Z)	Telefonische Ankündigung einer Faxsendung
					M 5.28	(Z)	Telefonische Rückversicherung über korrekten Faxabsender
			G 5.34	Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes	M 1.37	(A)	Geeignete Aufstellung eines Faxgerätes
					M 2.47	(B)	Ernennung eines Fax-Verantwortlichen
					M 2.48	(Z)	Festlegung berechtigter Faxbediener
					M 2.53	(Z)	Abschalten des Faxgerätes außerhalb der Bürozeiten
					M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung
					M 4.36	(Z)	Sperren bestimmter Faxempfänger-Rufnummern
					M 5.25	(A)	Nutzung von Sende- und Empfangsprotokollen
					M 5.27	(Z)	Telefonische Rückversicherung über korrekten Faxempfang
					M 5.29	(C)	Gelegentliche Kontrolle programmierter Zieladressen und Protokolle
			G 5.35	Überlastung durch Faxsendungen	M 2.49	(A)	Beschaffung geeigneter Faxgeräte
					M 2.53	(Z)	Abschalten des Faxgerätes außerhalb der Bürozeiten
					M 4.37	(Z)	Sperren bestimmter Absender-Faxnummern
B 3.403	(8.3)	Anrufbeantworter	G 2.1	Fehlende oder unzureichende Regelungen	M 3.16	(A)	Einweisung in die Bedienung des Anrufbeantworters
			G 2.5	Fehlende oder unzureichende Wartung	M 6.40	(A)	Regelmäßige Batterieprüfung/-wechsel
			G 3.15	Fehlbedienung eines Anrufbeantworters	M 2.54	(A)	Beschaffung geeigneter Anrufbeantworter
					M 3.16	(A)	Einweisung in die Bedienung des Anrufbeantworters
					M 4.38	(A)	Abschalten nicht benötigter Leistungsmerkmale
					M 4.39	(Z)	Abschalten des Anrufbeantworters bei Anwesenheit

			G 4.1	Ausfall der Stromversorgung	M 2.54	(A)	Beschaffung geeigneter Anrufbeantworter
			G 4.18	Entladene oder überalterte Notstromversorgung im Anrufbeantworter	M 6.40	(A)	Regelmäßige Batterieprüfung/-wechsel
			G 4.19	Informationsverlust bei erschöpftem Speichermedium	M 2.54	(A)	Beschaffung geeigneter Anrufbeantworter
					M 2.57	(A)	Regelmäßiges Abhören und Löschen aufgezeichneter Gespräche
			G 5.36	Absichtliche Überlastung des Anrufbeantworters	M 2.54	(A)	Beschaffung geeigneter Anrufbeantworter
					M 2.58	(Z)	Begrenzung der Sprechdauer
					M 4.39	(Z)	Abschalten des Anrufbeantworters bei Anwesenheit
			G 5.37	Ermitteln des Sicherungscodes	M 2.11	(A)	Regelung des Passwortgebrauchs
			G 5.38	Missbrauch der Fernabfrage	M 2.11	(A)	Regelung des Passwortgebrauchs
					M 2.54	(A)	Beschaffung geeigneter Anrufbeantworter
					M 2.55	(Z)	Einsatz eines Sicherungscodes
					M 2.56	(A)	Vermeidung schutzbedürftiger Informationen auf dem Anrufbeantworter
					M 2.57	(A)	Regelmäßiges Abhören und Löschen aufgezeichneter Gespräche
					M 4.38	(A)	Abschalten nicht benötigter Leistungsmerkmale
					M 4.39	(Z)	Abschalten des Anrufbeantworters bei Anwesenheit
B 3.404	(8.6)	Mobiltelefon	G 2.2	Unzureichende Kenntnis über Regelungen	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
					M 2.190	(Z)	Einrichtung eines Mobiltelefon-Pools
					M 5.81	(B)	Sichere Datenübertragung über Mobiltelefone
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
					M 2.190	(Z)	Einrichtung eines Mobiltelefon-Pools
			G 2.7	Unerlaubte Ausübung von Rechten	M 4.114	(A)	Nutzung der Sicherheitsmechanismen von Mobiltelefonen
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
					M 2.190	(Z)	Einrichtung eines Mobiltelefon-Pools
			G 3.43	Ungeeigneter Umgang mit Passwörtern	M 2.190	(Z)	Einrichtung eines Mobiltelefon-Pools
					M 4.114	(A)	Nutzung der Sicherheitsmechanismen von Mobiltelefonen
			G 3.44	Sorglosigkeit im Umgang mit Informationen	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
			G 3.45	Unzureichende Identifikationsprüfung von Kommunikationspartnern	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
			G 4.41	Nicht-Verfügbarkeit des Mobilfunknetzes	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
			G 4.42	Ausfall des Mobiltelefons oder des PDAs	M 2.190	(Z)	Einrichtung eines Mobiltelefon-Pools
					M 4.115	(B)	Sicherstellung der Energieversorgung von Mobiltelefonen
			G 5.2	Manipulation an Daten oder Software	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
					M 4.114	(A)	Nutzung der Sicherheitsmechanismen von Mobiltelefonen
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
					M 6.72	(C)	Ausfallvorsorge bei Mobiltelefonen
			G 5.4	Diebstahl	M 2.189	(A)	Sperrung des Mobiltelefons bei Verlust

					M 4.114	(A)	Nutzung der Sicherheitsmechanismen von Mobiltelefonen
					M 5.81	(B)	Sichere Datenübertragung über Mobiltelefone
					M 6.72	(C)	Ausfallvorsorge bei Mobiltelefonen
			G 5.80	Hoax	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
			G 5.94	Kartenmissbrauch	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
					M 2.189	(A)	Sperrung des Mobiltelefons bei Verlust
					M 2.190	(Z)	Einrichtung eines Mobiltelefon-Pools
					M 4.114	(A)	Nutzung der Sicherheitsmechanismen von Mobiltelefonen
			G 5.95	Abhören von Raumgesprächen über Mobiltelefone	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
					M 5.80	(Z)	Schutz vor Abhören der Raumgespräche über Mobiltelefone
			G 5.96	Manipulation von Mobiltelefonen	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
					M 4.114	(A)	Nutzung der Sicherheitsmechanismen von Mobiltelefonen
					M 6.72	(C)	Ausfallvorsorge bei Mobiltelefonen
			G 5.97	Unberechtigte Datenweitergabe über Mobiltelefone	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
			G 5.98	Abhören von Mobiltelefonaten	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
			G 5.99	Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
					M 5.78	(Z)	Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung
					M 5.79	(Z)	Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung
			G 5.126	Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten	M 2.188	(A)	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
B 3.405	(8.7)	PDA	G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebung	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 2.305	(B)	Geeignete Auswahl von PDAs
					M 4.31	(A)	Sicherstellung der Energieversorgung im mobilen Einsatz
					M 4.228	(A)	Nutzung der Sicherheitsmechanismen von PDAs
					M 4.229	(C)	Sicherer Betrieb von PDAs
					M 4.231	(Z)	Einsatz zusätzlicher Sicherheitswerkzeuge für PDAs
					M 6.95	(C)	Ausfallvorsorge und Datensicherung bei PDAs
			G 2.2	Unzureichende Kenntnis über Regelungen	M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung
					M 4.230	(Z)	Zentrale Administration von PDAs
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung
					M 4.230	(Z)	Zentrale Administration von PDAs
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung

					M 2.306	(A)	Verlustmeldung
					M 4.230	(Z)	Zentrale Administration von PDAs
					M 4.231	(Z)	Einsatz zusätzlicher Sicherheitswerkzeuge für PDAs
					M 4.232	(Z)	Sichere Nutzung von Zusatzspeicherkarten
					M 5.121	(B)	Sichere Kommunikation von unterwegs
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung
					M 4.230	(Z)	Zentrale Administration von PDAs
			G 3.43	Ungeeigneter Umgang mit Passwörtern	M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung
					M 4.230	(Z)	Zentrale Administration von PDAs
					M 4.231	(Z)	Einsatz zusätzlicher Sicherheitswerkzeuge für PDAs
			G 3.44	Sorglosigkeit im Umgang mit Informationen	M 2.303	(A)	Festlegung einer Strategie für den Einsatz von PDAs
					M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung
					M 4.230	(Z)	Zentrale Administration von PDAs
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
			G 3.45	Unzureichende Identifikationsprüfung von Kommunikationspartnern	M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung
			G 3.76	Fehler bei der Synchronisation mobiler Endgeräte	M 2.303	(A)	Festlegung einer Strategie für den Einsatz von PDAs
					M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung
					M 2.305	(B)	Geeignete Auswahl von PDAs
					M 4.229	(C)	Sicherer Betrieb von PDAs
					M 4.230	(Z)	Zentrale Administration von PDAs
					M 6.95	(C)	Ausfallvorsorge und Datensicherung bei PDAs
			G 4.42	Ausfall des Mobiltelefons oder des PDAs	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 2.218	(C)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 4.31	(A)	Sicherstellung der Energieversorgung im mobilen Einsatz
					M 4.230	(Z)	Zentrale Administration von PDAs
			G 4.51	Unzureichende Sicherheitsmechanismen bei PDAs	M 2.303	(A)	Festlegung einer Strategie für den Einsatz von PDAs
					M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung
					M 2.305	(B)	Geeignete Auswahl von PDAs
					M 4.229	(C)	Sicherer Betrieb von PDAs
					M 4.230	(Z)	Zentrale Administration von PDAs
					M 4.231	(Z)	Einsatz zusätzlicher Sicherheitswerkzeuge für PDAs
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
					M 5.121	(B)	Sichere Kommunikation von unterwegs
			G 4.52	Datenverlust bei mobilem Einsatz	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 2.218	(C)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.305	(B)	Geeignete Auswahl von PDAs
					M 4.31	(A)	Sicherstellung der Energieversorgung im mobilen Einsatz

					M 4.228	(A)	Nutzung der Sicherheitsmechanismen von PDAs
					M 4.229	(C)	Sicherer Betrieb von PDAs
					M 4.230	(Z)	Zentrale Administration von PDAs
					M 4.231	(Z)	Einsatz zusätzlicher Sicherheitswerkzeuge für PDAs
					M 4.232	(Z)	Sichere Nutzung von Zusatzspeicherkarten
					M 6.95	(C)	Ausfallvorsorge und Datensicherung bei PDAs
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
			G 5.2	Manipulation an Daten oder Software	M 2.218	(C)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.305	(B)	Geeignete Auswahl von PDAs
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.228	(A)	Nutzung der Sicherheitsmechanismen von PDAs
					M 4.229	(C)	Sicherer Betrieb von PDAs
					M 4.230	(Z)	Zentrale Administration von PDAs
					M 4.231	(Z)	Einsatz zusätzlicher Sicherheitswerkzeuge für PDAs
					M 4.232	(Z)	Sichere Nutzung von Zusatzspeicherkarten
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
					M 5.121	(B)	Sichere Kommunikation von unterwegs
			G 5.9	Unberechtigte IT-Nutzung	M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung
					M 2.305	(B)	Geeignete Auswahl von PDAs
					M 2.306	(A)	Verlustmeldung
					M 4.228	(A)	Nutzung der Sicherheitsmechanismen von PDAs
					M 4.229	(C)	Sicherer Betrieb von PDAs
					M 4.230	(Z)	Zentrale Administration von PDAs
					M 4.231	(Z)	Einsatz zusätzlicher Sicherheitswerkzeuge für PDAs
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
					M 5.121	(B)	Sichere Kommunikation von unterwegs
			G 5.22	Diebstahl bei mobiler Nutzung des IT-Systems	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
					M 2.218	(C)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
			G 5.23	Computer-Viren	M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
			G 5.123	Abhören von Raumgesprächen über mobile Endgeräte	M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung
			G 5.124	Missbrauch der Informationen von mobilen Endgeräten	M 2.218	(C)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.303	(A)	Festlegung einer Strategie für den Einsatz von PDAs
					M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung
					M 2.305	(B)	Geeignete Auswahl von PDAs
					M 4.228	(A)	Nutzung der Sicherheitsmechanismen von PDAs
					M 4.229	(C)	Sicherer Betrieb von PDAs
					M 4.230	(Z)	Zentrale Administration von PDAs

					M 4.231	(Z)	Einsatz zusätzlicher Sicherheitswerkzeuge für PDAs
					M 4.232	(Z)	Sichere Nutzung von Zusatzspeicherkarten
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
					M 5.121	(B)	Sichere Kommunikation von unterwegs
			G 5.125	Unberechtigte Datenweitergabe über mobile Endgeräte	M 2.218	(C)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
					M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung
					M 4.228	(A)	Nutzung der Sicherheitsmechanismen von PDAs
					M 4.229	(C)	Sicherer Betrieb von PDAs
					M 4.230	(Z)	Zentrale Administration von PDAs
					M 4.231	(Z)	Einsatz zusätzlicher Sicherheitswerkzeuge für PDAs
					M 4.255	(A)	Nutzung von IrDA-Schnittstellen
					M 5.121	(B)	Sichere Kommunikation von unterwegs
			G 5.126	Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten	M 2.304	(A)	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung
B 4.1	(6.7)	Heterogene Netze	G 1.2	Ausfall des IT-Systems	M 5.13	(A)	Geeigneter Einsatz von Elementen zur Netzkopplung
					M 6.52	(A)	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
					M 6.53	(Z)	Redundante Auslegung der Netzkomponenten
			G 1.3	Blitz	M 6.52	(A)	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
					M 6.53	(Z)	Redundante Auslegung der Netzkomponenten
			G 1.4	Feuer	M 6.52	(A)	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
					M 6.53	(Z)	Redundante Auslegung der Netzkomponenten
			G 1.5	Wasser	M 6.52	(A)	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
					M 6.53	(Z)	Redundante Auslegung der Netzkomponenten
			G 1.7	Unzulässige Temperatur und Luftfeuchte	M 6.52	(A)	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
					M 6.53	(Z)	Redundante Auslegung der Netzkomponenten
			G 1.8	Staub, Verschmutzung	M 6.52	(A)	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
					M 6.53	(Z)	Redundante Auslegung der Netzkomponenten
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.79	(A)	Sichere Zugriffsmechanismen bei lokaler Administration
					M 4.81	(B)	Audit und Protokollierung der Aktivitäten im Netz
					M 5.61	(A)	Geeignete physikalische Segmentierung
					M 5.62	(Z)	Geeignete logische Segmentierung
					M 5.77	(Z)	Bildung von Teilnetzen
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	M 2.139	(A)	Ist-Aufnahme der aktuellen Netzsituation
					M 4.83	(C)	Update/Upgrade von Soft- und Hardware im Netzbereich
			G 2.22	Fehlende Auswertung von Protokolldaten	M 4.80	(B)	Sichere Zugriffsmechanismen bei Fernadministration
			G 2.27	Fehlende oder unzureichende Dokumentation	M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 5.61	(A)	Geeignete physikalische Segmentierung

			G 2.32	Unzureichende Leitungskapazitäten	M 2.140	(Z)	Analyse der aktuellen Netzsituation
					M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 2.142	(B)	Entwicklung eines Netz-Realisierungsplans
					M 4.82	(A)	Sichere Konfiguration der aktiven Netzkomponenten
					M 4.83	(C)	Update/Upgrade von Soft- und Hardware im Netzbereich
					M 5.7	(A)	Netzverwaltung
					M 5.60	(A)	Auswahl einer geeigneten Backbone-Technologie
					M 5.61	(A)	Geeignete physikalische Segmentierung
					M 5.62	(Z)	Geeignete logische Segmentierung
					M 5.77	(Z)	Bildung von Teilnetzen
					M 6.53	(Z)	Redundante Auslegung der Netzkomponenten
			G 2.44	Inkompatible aktive und passive Netzkomponenten	M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 4.80	(B)	Sichere Zugriffsmechanismen bei Fernadministration
					M 4.82	(A)	Sichere Konfiguration der aktiven Netzkomponenten
					M 4.83	(C)	Update/Upgrade von Soft- und Hardware im Netzbereich
					M 5.61	(A)	Geeignete physikalische Segmentierung
					M 5.62	(Z)	Geeignete logische Segmentierung
			G 2.45	Konzeptionelle Schwächen des Netzes	M 2.139	(A)	Ist-Aufnahme der aktuellen Netzsituation
					M 2.140	(Z)	Analyse der aktuellen Netzsituation
					M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 4.83	(C)	Update/Upgrade von Soft- und Hardware im Netzbereich
					M 5.60	(A)	Auswahl einer geeigneten Backbone-Technologie
					M 5.61	(A)	Geeignete physikalische Segmentierung
					M 5.62	(Z)	Geeignete logische Segmentierung
					M 5.77	(Z)	Bildung von Teilnetzen
					M 6.53	(Z)	Redundante Auslegung der Netzkomponenten
			G 2.46	Überschreiten der zulässigen Kabel- bzw. Buslänge oder der Ringgröße	M 2.139	(A)	Ist-Aufnahme der aktuellen Netzsituation
					M 2.140	(Z)	Analyse der aktuellen Netzsituation
					M 2.142	(B)	Entwicklung eines Netz-Realisierungsplans
					M 4.83	(C)	Update/Upgrade von Soft- und Hardware im Netzbereich
					M 5.60	(A)	Auswahl einer geeigneten Backbone-Technologie
					M 5.62	(Z)	Geeignete logische Segmentierung
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	M 6.54	(B)	Verhaltensregeln nach Verlust der Netzintegrität
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.79	(A)	Sichere Zugriffsmechanismen bei lokaler Administration
					M 4.80	(B)	Sichere Zugriffsmechanismen bei Fernadministration
					M 6.54	(B)	Verhaltensregeln nach Verlust der Netzintegrität
			G 3.5	Unbeabsichtigte Leitungsbeschädigung	M 2.142	(B)	Entwicklung eines Netz-Realisierungsplans
					M 4.83	(C)	Update/Upgrade von Soft- und Hardware im Netzbereich
					M 5.60	(A)	Auswahl einer geeigneten Backbone-Technologie
					M 5.61	(A)	Geeignete physikalische Segmentierung
					M 5.62	(Z)	Geeignete logische Segmentierung
					M 5.77	(Z)	Bildung von Teilnetzen
					M 6.53	(Z)	Redundante Auslegung der Netzkomponenten
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 2.142	(B)	Entwicklung eines Netz-Realisierungsplans
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.79	(A)	Sichere Zugriffsmechanismen bei lokaler Administration

					M 4.81	(B)	Audit und Protokollierung der Aktivitäten im Netz
					M 5.61	(A)	Geeignete physikalische Segmentierung
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 4.80	(B)	Sichere Zugriffsmechanismen bei Fernadministration
					M 6.52	(A)	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
					M 6.54	(B)	Verhaltensregeln nach Verlust der Netzintegrität
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.140	(Z)	Analyse der aktuellen Netzsituation
					M 4.80	(B)	Sichere Zugriffsmechanismen bei Fernadministration
					M 5.2	(A)	Auswahl einer geeigneten Netz-Topographie
					M 6.52	(A)	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
					M 6.53	(Z)	Redundante Auslegung der Netzkomponenten
					M 6.54	(B)	Verhaltensregeln nach Verlust der Netzintegrität
			G 3.28	Ungeeignete Konfiguration der aktiven Netzkomponenten	M 2.140	(Z)	Analyse der aktuellen Netzsituation
					M 4.80	(B)	Sichere Zugriffsmechanismen bei Fernadministration
					M 4.81	(B)	Audit und Protokollierung der Aktivitäten im Netz
					M 4.82	(A)	Sichere Konfiguration der aktiven Netzkomponenten
					M 6.52	(A)	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
			G 3.29	Fehlende oder ungeeignete Segmentierung	M 2.139	(A)	Ist-Aufnahme der aktuellen Netzsituation
					M 2.140	(Z)	Analyse der aktuellen Netzsituation
					M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 5.62	(Z)	Geeignete logische Segmentierung
			G 4.1	Ausfall der Stromversorgung	M 6.52	(A)	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
					M 6.53	(Z)	Redundante Auslegung der Netzkomponenten
			G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen	M 5.7	(A)	Netzverwaltung
					M 5.13	(A)	Geeigneter Einsatz von Elementen zur Netzkopplung
			G 4.31	Ausfall oder Störung von Netzkomponenten	M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 6.52	(A)	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
					M 6.53	(Z)	Redundante Auslegung der Netzkomponenten
					M 6.54	(B)	Verhaltensregeln nach Verlust der Netzintegrität
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 4.79	(A)	Sichere Zugriffsmechanismen bei lokaler Administration
					M 4.80	(B)	Sichere Zugriffsmechanismen bei Fernadministration
					M 4.82	(A)	Sichere Konfiguration der aktiven Netzkomponenten
					M 4.83	(C)	Update/Upgrade von Soft- und Hardware im Netzbereich
					M 6.52	(A)	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
			G 5.2	Manipulation an Daten oder Software	M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.79	(A)	Sichere Zugriffsmechanismen bei lokaler Administration
					M 4.80	(B)	Sichere Zugriffsmechanismen bei Fernadministration
					M 4.82	(A)	Sichere Konfiguration der aktiven Netzkomponenten
			G 5.4	Diebstahl	M 2.139	(A)	Ist-Aufnahme der aktuellen Netzsituation
					M 2.140	(Z)	Analyse der aktuellen Netzsituation

			G 5.5	Vandalismus	M 5.2	(A)	Auswahl einer geeigneten Netz-Topographie
			G 5.6	Anschlag	M 5.2	(A)	Auswahl einer geeigneten Netz-Topographie
			G 5.7	Abhören von Leitungen	M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 5.2	(A)	Auswahl einer geeigneten Netz-Topographie
					M 5.61	(A)	Geeignete physikalische Segmentierung
					M 5.62	(Z)	Geeignete logische Segmentierung
					M 5.77	(Z)	Bildung von Teilnetzen
			G 5.8	Manipulation an Leitungen	M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 4.81	(B)	Audit und Protokollierung der Aktivitäten im Netz
					M 5.2	(A)	Auswahl einer geeigneten Netz-Topographie
					M 5.61	(A)	Geeignete physikalische Segmentierung
					M 5.62	(Z)	Geeignete logische Segmentierung
					M 5.77	(Z)	Bildung von Teilnetzen
			G 5.9	Unberechtigte IT-Nutzung	M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.79	(A)	Sichere Zugriffsmechanismen bei lokaler Administration
					M 4.80	(B)	Sichere Zugriffsmechanismen bei Fernadministration
					M 5.7	(A)	Netzverwaltung
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.79	(A)	Sichere Zugriffsmechanismen bei lokaler Administration
					M 4.80	(B)	Sichere Zugriffsmechanismen bei Fernadministration
					M 4.81	(B)	Audit und Protokollierung der Aktivitäten im Netz
			G 5.20	Missbrauch von Administratorrechten	M 5.7	(A)	Netzverwaltung
			G 5.28	Verhinderung von Diensten	M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 4.81	(B)	Audit und Protokollierung der Aktivitäten im Netz
					M 4.82	(A)	Sichere Konfiguration der aktiven Netzkomponenten
					M 5.61	(A)	Geeignete physikalische Segmentierung
					M 5.62	(Z)	Geeignete logische Segmentierung
					M 5.77	(Z)	Bildung von Teilnetzen
					M 6.53	(Z)	Redundante Auslegung der Netzkomponenten
			G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz	M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.79	(A)	Sichere Zugriffsmechanismen bei lokaler Administration
					M 4.80	(B)	Sichere Zugriffsmechanismen bei Fernadministration
					M 4.81	(B)	Audit und Protokollierung der Aktivitäten im Netz
					M 4.82	(A)	Sichere Konfiguration der aktiven Netzkomponenten
					M 5.2	(A)	Auswahl einer geeigneten Netz-Topographie
					M 5.60	(A)	Auswahl einer geeigneten Backbone-Technologie
					M 5.61	(A)	Geeignete physikalische Segmentierung
					M 5.62	(Z)	Geeignete logische Segmentierung
					M 5.77	(Z)	Bildung von Teilnetzen
			G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktionen	M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 2.142	(B)	Entwicklung eines Netz-Realisierungsplans
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.79	(A)	Sichere Zugriffsmechanismen bei lokaler Administration
					M 4.80	(B)	Sichere Zugriffsmechanismen bei Fernadministration
					M 4.81	(B)	Audit und Protokollierung der Aktivitäten im Netz
					M 4.82	(A)	Sichere Konfiguration der aktiven Netzkomponenten

					M 5.61	(A)	Geeignete physikalische Segmentierung
					M 5.62	(Z)	Geeignete logische Segmentierung
					M 5.77	(Z)	Bildung von Teilnetzen
			G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten	M 2.141	(B)	Entwicklung eines Netzkonzeptes
					M 4.79	(A)	Sichere Zugriffsmechanismen bei lokaler Administration
					M 4.81	(B)	Audit und Protokollierung der Aktivitäten im Netz
					M 4.82	(A)	Sichere Konfiguration der aktiven Netzkomponenten
					M 5.2	(A)	Auswahl einer geeigneten Netz-Topographie
					M 5.61	(A)	Geeignete physikalische Segmentierung
					M 5.62	(Z)	Geeignete logische Segmentierung
B 4.2	(6.8)	Netz- und Systemmanagement	G 1.1	Personalausfall	M 4.92	(A)	Sicherer Betrieb eines Systemmanagementsystems
			G 1.2	Ausfall des IT-Systems	M 4.92	(A)	Sicherer Betrieb eines Systemmanagementsystems
					M 6.57	(C)	Erstellen eines Notfallplans für den Ausfall des Managementsystems
			G 1.7	Unzulässige Temperatur und Luftfeuchte	M 2.146	(A)	Sicherer Betrieb eines Netzmanagementsystems
			G 2.27	Fehlende oder unzureichende Dokumentation	M 2.146	(A)	Sicherer Betrieb eines Netzmanagementsystems
			G 2.32	Unzureichende Leitungskapazitäten	M 2.145	(B)	Anforderungen an ein Netzmanagement-Tool
			G 2.59	Betreiben von nicht angemeldeten Komponenten	M 2.169	(A)	Entwickeln einer Systemmanagementstrategie
					M 4.91	(A)	Sichere Installation eines Systemmanagementsystems
					M 4.92	(A)	Sicherer Betrieb eines Systemmanagementsystems
			G 2.60	Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement	M 2.143	(A)	Entwicklung eines Netzmanagementkonzeptes
					M 2.144	(A)	Geeignete Auswahl eines Netzmanagement-Protokolls
					M 2.168	(A)	IT-System-Analyse vor Einführung eines Systemmanagementsystems
					M 2.169	(A)	Entwickeln einer Systemmanagementstrategie
					M 2.170	(A)	Anforderungen an ein Systemmanagementsystem
					M 2.171	(A)	Geeignete Auswahl eines Systemmanagement-Produktes
			G 2.61	Unberechtigte Sammlung personenbezogener Daten	M 2.169	(A)	Entwickeln einer Systemmanagementstrategie
					M 2.171	(A)	Geeignete Auswahl eines Systemmanagement-Produktes
					M 4.91	(A)	Sichere Installation eines Systemmanagementsystems
					M 4.92	(A)	Sicherer Betrieb eines Systemmanagementsystems
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.145	(B)	Anforderungen an ein Netzmanagement-Tool
					M 2.146	(A)	Sicherer Betrieb eines Netzmanagementsystems
			G 3.28	Ungeeignete Konfiguration der aktiven Netzkomponenten	M 2.146	(A)	Sicherer Betrieb eines Netzmanagementsystems
			G 3.34	Ungeeignete Konfiguration des Managementsystems	M 2.143	(A)	Entwicklung eines Netzmanagementkonzeptes
					M 2.169	(A)	Entwickeln einer Systemmanagementstrategie
					M 2.171	(A)	Geeignete Auswahl eines Systemmanagement-Produktes
					M 4.91	(A)	Sichere Installation eines Systemmanagementsystems
					M 4.92	(A)	Sicherer Betrieb eines Systemmanagementsystems
			G 3.35	Server im laufenden Betrieb ausschalten	M 4.91	(A)	Sichere Installation eines Systemmanagementsystems
					M 4.92	(A)	Sicherer Betrieb eines Systemmanagementsystems
					M 6.57	(C)	Erstellen eines Notfallplans für den Ausfall des Managementsystems
			G 3.36	Fehlinterpretation von Ereignissen	M 2.146	(A)	Sicherer Betrieb eines Netzmanagementsystems
					M 4.92	(A)	Sicherer Betrieb eines Systemmanagementsystems
			G 4.31	Ausfall oder Störung von Netzkomponenten	M 2.145	(B)	Anforderungen an ein Netzmanagement-Tool

			G 4.38	Ausfall von Komponenten eines Netz- und Systemmanagementsystems	M 2.171	(A)	Geeignete Auswahl eines Systemmanagement-Produktes
					M 6.57	(C)	Erstellen eines Notfallplans für den Ausfall des Managementsystems
			G 5.2	Manipulation an Daten oder Software	M 2.146	(A)	Sicherer Betrieb eines Netzmanagementsystems
			G 5.8	Manipulation an Leitungen	M 2.145	(B)	Anforderungen an ein Netzmanagement-Tool
			G 5.9	Unberechtigte IT-Nutzung	M 2.145	(B)	Anforderungen an ein Netzmanagement-Tool
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 2.145	(B)	Anforderungen an ein Netzmanagement-Tool
			G 5.28	Verhinderung von Diensten	M 2.145	(B)	Anforderungen an ein Netzmanagement-Tool
			G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz	M 2.145	(B)	Anforderungen an ein Netzmanagement-Tool
			G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktionen	M 2.145	(B)	Anforderungen an ein Netzmanagement-Tool
			G 5.86	Manipulation von Managementparametern	M 4.91	(A)	Sichere Installation eines Systemmanagementsystems
					M 4.92	(A)	Sicherer Betrieb eines Systemmanagementsystems
					M 6.57	(C)	Erstellen eines Notfallplans für den Ausfall des Managementsystems
B 4.3	(7.2)	Modem	G 1.2	Ausfall des IT-Systems	M 1.25	(Z)	Überspannungsschutz
			G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	M 1.38	(A)	Geeignete Aufstellung eines Modems
					M 2.42	(B)	Festlegung der möglichen Kommunikationspartner
					M 2.60	(A)	Sichere Administration eines Modems
					M 2.61	(A)	Regelung des Modem-Einsatzes
					M 3.17	(A)	Einweisung des Personals in die Modem-Benutzung
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.60	(A)	Sichere Administration eines Modems
					M 2.61	(A)	Regelung des Modem-Einsatzes
					M 3.17	(A)	Einweisung des Personals in die Modem-Benutzung
			G 3.5	Unbeabsichtigte Leitungsbeschädigung	M 1.38	(A)	Geeignete Aufstellung eines Modems
					M 2.42	(B)	Festlegung der möglichen Kommunikationspartner
					M 3.17	(A)	Einweisung des Personals in die Modem-Benutzung
			G 4.6	Spannungsschwankungen/Überspannung/Unterspannung	M 1.25	(Z)	Überspannungsschutz
			G 5.2	Manipulation an Daten oder Software	M 1.38	(A)	Geeignete Aufstellung eines Modems
					M 2.42	(B)	Festlegung der möglichen Kommunikationspartner
					M 2.60	(A)	Sichere Administration eines Modems
					M 2.61	(A)	Regelung des Modem-Einsatzes
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 5.31	(A)	Geeignete Modem-Konfiguration
					M 5.32	(A)	Sicherer Einsatz von Kommunikationssoftware
					M 5.33	(A)	Absicherung der per Modem durchgeführten Fernwartung
					M 5.44	(Z)	Einseitiger Verbindungsaufbau
			G 5.7	Abhören von Leitungen	M 2.46	(Z)	Geeignetes Schlüsselmanagement
					M 2.59	(A)	Auswahl eines geeigneten Modems in der Beschaffung
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
			G 5.8	Manipulation an Leitungen	M 2.59	(A)	Auswahl eines geeigneten Modems in der Beschaffung

					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
			G 5.9	Unberechtigte IT-Nutzung	M 1.38	(A)	Geeignete Aufstellung eines Modems
					M 2.60	(A)	Sichere Administration eines Modems
					M 2.61	(A)	Regelung des Modem-Einsatzes
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 5.30	(Z)	Aktivierung einer vorhandenen Callback-Option
					M 5.31	(A)	Geeignete Modem-Konfiguration
					M 5.32	(A)	Sicherer Einsatz von Kommunikationssoftware
					M 5.33	(A)	Absicherung der per Modem durchgeführten Fernwartung
			G 5.10	Missbrauch von Fernwartungszugängen	M 2.59	(A)	Auswahl eines geeigneten Modems in der Beschaffung
					M 2.60	(A)	Sichere Administration eines Modems
					M 2.61	(A)	Regelung des Modem-Einsatzes
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 5.30	(Z)	Aktivierung einer vorhandenen Callback-Option
					M 5.33	(A)	Absicherung der per Modem durchgeführten Fernwartung
					M 5.44	(Z)	Einseitiger Verbindungsaufbau
			G 5.12	Abhören von Telefongesprächen und Datenübertragungen	M 2.46	(Z)	Geeignetes Schlüsselmanagement
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 4.7	(A)	Änderung voreingestellter Passwörter
					M 5.30	(Z)	Aktivierung einer vorhandenen Callback-Option
					M 5.31	(A)	Geeignete Modem-Konfiguration
					M 5.32	(A)	Sicherer Einsatz von Kommunikationssoftware
					M 5.44	(Z)	Einseitiger Verbindungsaufbau
			G 5.23	Computer-Viren	M 2.42	(B)	Festlegung der möglichen Kommunikationspartner
					M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
			G 5.25	Maskerade	M 4.7	(A)	Änderung voreingestellter Passwörter
					M 5.30	(Z)	Aktivierung einer vorhandenen Callback-Option
					M 5.33	(A)	Absicherung der per Modem durchgeführten Fernwartung
					M 5.44	(Z)	Einseitiger Verbindungsaufbau
			G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten	M 2.60	(A)	Sichere Administration eines Modems
					M 2.61	(A)	Regelung des Modem-Einsatzes
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 5.30	(Z)	Aktivierung einer vorhandenen Callback-Option
					M 5.31	(A)	Geeignete Modem-Konfiguration
					M 5.32	(A)	Sicherer Einsatz von Kommunikationssoftware
					M 5.33	(A)	Absicherung der per Modem durchgeführten Fernwartung
					M 5.44	(Z)	Einseitiger Verbindungsaufbau
B 4.4	(7.6)	Remote Access	G 1.2	Ausfall des IT-Systems	M 2.183	(A)	Durchführung einer RAS-Anforderungsanalyse
					M 2.185	(A)	Auswahl einer geeigneten RAS-Systemarchitektur
					M 2.186	(A)	Geeignete Auswahl eines RAS-Produktes
					M 4.111	(A)	Sichere Konfiguration des RAS-Systems
					M 4.112	(A)	Sicherer Betrieb des RAS-Systems

					M 6.70	(B)	Erstellen eines Notfallplans für den Ausfall des RAS-Systems
					M 6.71	(B)	Datensicherung bei mobiler Nutzung des IT-Systems
			G 2.2	Unzureichende Kenntnis über Regelungen	M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie
			G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PCs	M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie
			G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung	M 2.183	(A)	Durchführung einer RAS-Anforderungsanalyse
					M 2.184	(A)	Entwicklung eines RAS-Konzeptes
					M 2.186	(A)	Geeignete Auswahl eines RAS-Produktes
					M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie
					M 4.110	(A)	Sichere Installation des RAS-Systems
					M 4.111	(A)	Sichere Konfiguration des RAS-Systems
					M 4.112	(A)	Sicherer Betrieb des RAS-Systems
			G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen	M 2.183	(A)	Durchführung einer RAS-Anforderungsanalyse
					M 2.184	(A)	Entwicklung eines RAS-Konzeptes
					M 4.110	(A)	Sichere Installation des RAS-Systems
					M 4.111	(A)	Sichere Konfiguration des RAS-Systems
					M 4.112	(A)	Sicherer Betrieb des RAS-Systems
					M 4.113	(Z)	Nutzung eines Authentisierungsservers beim RAS-Einsatz
					M 4.233	(B)	Sperrung nicht mehr benötigter RAS-Zugänge
			G 2.44	Inkompatible aktive und passive Netzkomponenten	M 2.183	(A)	Durchführung einer RAS-Anforderungsanalyse
					M 2.185	(A)	Auswahl einer geeigneten RAS-Systemarchitektur
					M 2.186	(A)	Geeignete Auswahl eines RAS-Produktes
					M 4.110	(A)	Sichere Installation des RAS-Systems
			G 2.64	Fehlende Regelungen für das RAS-System	M 2.184	(A)	Entwicklung eines RAS-Konzeptes
					M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie
					M 2.205	(A)	Übertragung und Abruf personenbezogener Daten
			G 3.39	Fehlerhafte Administration des RAS-Systems	M 2.183	(A)	Durchführung einer RAS-Anforderungsanalyse
					M 2.184	(A)	Entwicklung eines RAS-Konzeptes
					M 2.185	(A)	Auswahl einer geeigneten RAS-Systemarchitektur
					M 2.186	(A)	Geeignete Auswahl eines RAS-Produktes
					M 4.111	(A)	Sichere Konfiguration des RAS-Systems
					M 4.112	(A)	Sicherer Betrieb des RAS-Systems
			G 3.40	Ungeeignete Nutzung von Authentisierungsdiensten bei Remote Access	M 2.184	(A)	Entwicklung eines RAS-Konzeptes
					M 2.185	(A)	Auswahl einer geeigneten RAS-Systemarchitektur
					M 4.112	(A)	Sicherer Betrieb des RAS-Systems
					M 4.113	(Z)	Nutzung eines Authentisierungsservers beim RAS-Einsatz
			G 3.41	Fehlverhalten bei der Nutzung von RAS-Diensten	M 2.184	(A)	Entwicklung eines RAS-Konzeptes
					M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie
					M 4.112	(A)	Sicherer Betrieb des RAS-Systems
			G 3.42	Unsichere Konfiguration der RAS-Clients	M 2.184	(A)	Entwicklung eines RAS-Konzeptes
					M 2.185	(A)	Auswahl einer geeigneten RAS-Systemarchitektur
					M 2.186	(A)	Geeignete Auswahl eines RAS-Produktes
					M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie
					M 4.111	(A)	Sichere Konfiguration des RAS-Systems
					M 4.112	(A)	Sicherer Betrieb des RAS-Systems
			G 3.43	Ungeeigneter Umgang mit Passwörtern	M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie

					M 4.112	(A)	Sicherer Betrieb des RAS-Systems
			G 3.44	Sorglosigkeit im Umgang mit Informationen	M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie
					M 4.112	(A)	Sicherer Betrieb des RAS-Systems
			G 4.35	Unsichere kryptographische Algorithmen	M 2.186	(A)	Geeignete Auswahl eines RAS-Produktes
					M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie
					M 4.112	(A)	Sicherer Betrieb des RAS-Systems
			G 4.40	Ungeeignete Ausrüstung der Betriebsumgebung des RAS-Clients	M 2.183	(A)	Durchführung einer RAS-Anforderungsanalyse
					M 2.184	(A)	Entwicklung eines RAS-Konzeptes
					M 2.185	(A)	Auswahl einer geeigneten RAS-Systemarchitektur
					M 4.110	(A)	Sichere Installation des RAS-Systems
					M 4.112	(A)	Sicherer Betrieb des RAS-Systems
			G 5.7	Abhören von Leitungen	M 2.185	(A)	Auswahl einer geeigneten RAS-Systemarchitektur
					M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie
					M 4.110	(A)	Sichere Installation des RAS-Systems
					M 5.76	(Z)	Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikation
			G 5.8	Manipulation an Leitungen	M 2.185	(A)	Auswahl einer geeigneten RAS-Systemarchitektur
					M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie
					M 4.110	(A)	Sichere Installation des RAS-Systems
			G 5.22	Diebstahl bei mobiler Nutzung des IT-Systems	M 4.112	(A)	Sicherer Betrieb des RAS-Systems
					M 6.70	(B)	Erstellen eines Notfallplans für den Ausfall des RAS-Systems
					M 6.71	(B)	Datensicherung bei mobiler Nutzung des IT-Systems
			G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten	M 2.185	(A)	Auswahl einer geeigneten RAS-Systemarchitektur
					M 4.110	(A)	Sichere Installation des RAS-Systems
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 2.183	(A)	Durchführung einer RAS-Anforderungsanalyse
					M 2.184	(A)	Entwicklung eines RAS-Konzeptes
					M 2.185	(A)	Auswahl einer geeigneten RAS-Systemarchitektur
					M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie
					M 4.111	(A)	Sichere Konfiguration des RAS-Systems
					M 5.76	(Z)	Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikation
					M 6.71	(B)	Datensicherung bei mobiler Nutzung des IT-Systems
			G 5.83	Kompromittierung kryptographischer Schlüssel	M 2.185	(A)	Auswahl einer geeigneten RAS-Systemarchitektur
					M 4.111	(A)	Sichere Konfiguration des RAS-Systems
					M 6.71	(B)	Datensicherung bei mobiler Nutzung des IT-Systems
			G 5.91	Abschalten von Sicherheitsmechanismen für den RAS-Zugang	M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie
					M 4.111	(A)	Sichere Konfiguration des RAS-Systems
					M 4.112	(A)	Sicherer Betrieb des RAS-Systems
			G 5.92	Nutzung des RAS-Clients als RAS-Server	M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie
					M 4.111	(A)	Sichere Konfiguration des RAS-Systems
					M 4.112	(A)	Sicherer Betrieb des RAS-Systems
			G 5.93	Erlauben von Fremdnutzung von RAS-Komponenten	M 2.187	(A)	Festlegen einer RAS-Sicherheitsrichtlinie
					M 4.112	(A)	Sicherer Betrieb des RAS-Systems
B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN	G 1.2	Ausfall des IT-Systems	M 1.25	(B)	Überspannungsschutz
					M 1.43	(A)	Gesicherte Aufstellung aktiver Netzkomponenten
					M 2.106	(A)	Auswahl geeigneter ISDN-Karten in der Beschaffung

					M 2.107	(A)	Dokumentation der ISDN-Karten-Konfiguration
			G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	M 1.43	(A)	Gesicherte Aufstellung aktiver Netzkomponenten
			G 2.7	Unerlaubte Ausübung von Rechten	M 1.43	(A)	Gesicherte Aufstellung aktiver Netzkomponenten
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 4.7	(A)	Änderung voreingestellter Passwörter
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	M 2.64	(A)	Kontrolle der Protokolldateien
					M 2.107	(A)	Dokumentation der ISDN-Karten-Konfiguration
					M 5.29	(C)	Gelegentliche Kontrolle programmierter Zieladressen und Protokolle
			G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung	M 2.46	(Z)	Geeignetes Schlüsselmanagement
			G 2.22	Fehlende Auswertung von Protokolldaten	M 2.64	(A)	Kontrolle der Protokolldateien
			G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes	M 1.43	(A)	Gesicherte Aufstellung aktiver Netzkomponenten
					M 2.106	(A)	Auswahl geeigneter ISDN-Karten in der Beschaffung
					M 2.108	(Z)	Verzicht auf Fernwartung der ISDN-Netzkoppelelemente
					M 2.109	(A)	Rechtevergabe für den Fernzugriff
					M 4.59	(A)	Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten
					M 4.60	(A)	Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten
					M 4.61	(A)	Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten
					M 4.62	(Z)	Einsatz eines D-Kanal-Filters
					M 5.47	(Z)	Einrichten einer Closed User Group
					M 5.49	(A)	Callback basierend auf CLIP/COLP
					M 5.50	(A)	Authentisierung mittels PAP/CHAP
			G 2.32	Unzureichende Leitungskapazitäten	M 4.59	(A)	Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten
			G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen	M 2.42	(A)	Festlegung der möglichen Kommunikationspartner
					M 2.64	(A)	Kontrolle der Protokolldateien
					M 2.106	(A)	Auswahl geeigneter ISDN-Karten in der Beschaffung
					M 4.59	(A)	Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten
					M 4.60	(A)	Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten
					M 5.29	(C)	Gelegentliche Kontrolle programmierter Zieladressen und Protokolle
					M 5.47	(Z)	Einrichten einer Closed User Group
					M 5.48	(A)	Authentisierung mittels CLIP/COLP
					M 5.49	(A)	Callback basierend auf CLIP/COLP
					M 5.50	(A)	Authentisierung mittels PAP/CHAP
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 1.43	(A)	Gesicherte Aufstellung aktiver Netzkomponenten
					M 2.42	(A)	Festlegung der möglichen Kommunikationspartner
					M 2.46	(Z)	Geeignetes Schlüsselmanagement
					M 4.59	(A)	Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten
					M 4.60	(A)	Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten
					M 4.61	(A)	Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten
					M 5.47	(Z)	Einrichten einer Closed User Group
					M 5.48	(A)	Authentisierung mittels CLIP/COLP
					M 5.49	(A)	Callback basierend auf CLIP/COLP

					M 5.50	(A)	Authentisierung mittels PAP/CHAP
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 1.43	(A)	Gesicherte Aufstellung aktiver Netzkomponenten
					M 4.7	(A)	Änderung voreingestellter Passwörter
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 2.64	(A)	Kontrolle der Protokolldateien
			G 3.13	Übertragung falscher oder nicht gewünschter Datensätze	M 2.106	(A)	Auswahl geeigneter ISDN-Karten in der Beschaffung
					M 5.29	(C)	Gelegentliche Kontrolle programmierter Zieladressen und Protokolle
			G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten	M 2.107	(A)	Dokumentation der ISDN-Karten-Konfiguration
			G 4.6	Spannungsschwankungen/Überspannung/Unterspannung	M 1.25	(B)	Überspannungsschutz
			G 4.25	Nicht getrennte Verbindungen	M 2.106	(A)	Auswahl geeigneter ISDN-Karten in der Beschaffung
			G 5.2	Manipulation an Daten oder Software	M 1.43	(A)	Gesicherte Aufstellung aktiver Netzkomponenten
					M 2.64	(A)	Kontrolle der Protokolldateien
					M 2.108	(Z)	Verzicht auf Fernwartung der ISDN-Netzkoppelelemente
					M 2.109	(A)	Rechtevergabe für den Fernzugriff
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 4.59	(A)	Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten
					M 4.60	(A)	Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten
					M 4.61	(A)	Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten
					M 4.62	(Z)	Einsatz eines D-Kanal-Filters
					M 5.32	(A)	Sicherer Einsatz von Kommunikationssoftware
					M 5.47	(Z)	Einrichten einer Closed User Group
					M 5.48	(A)	Authentisierung mittels CLIP/COLP
					M 5.49	(A)	Callback basierend auf CLIP/COLP
					M 5.50	(A)	Authentisierung mittels PAP/CHAP
			G 5.7	Abhören von Leitungen	M 2.46	(Z)	Geeignetes Schlüsselmanagement
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 4.61	(A)	Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten
			G 5.8	Manipulation an Leitungen	M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 4.60	(A)	Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten
			G 5.9	Unberechtigte IT-Nutzung	M 1.43	(A)	Gesicherte Aufstellung aktiver Netzkomponenten
					M 2.64	(A)	Kontrolle der Protokolldateien
					M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.59	(A)	Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten
					M 4.60	(A)	Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten
					M 4.61	(A)	Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten

					M 4.62	(Z)	Einsatz eines D-Kanal-Filters
					M 5.32	(A)	Sicherer Einsatz von Kommunikationssoftware
					M 5.47	(Z)	Einrichten einer Closed User Group
					M 5.48	(A)	Authentisierung mittels CLIP/COLP
					M 5.49	(A)	Callback basierend auf CLIP/COLP
					M 5.50	(A)	Authentisierung mittels PAP/CHAP
			G 5.10	Missbrauch von Fernwartungszugängen	M 1.43	(A)	Gesicherte Aufstellung aktiver Netzkomponenten
					M 2.108	(Z)	Verzicht auf Fernwartung der ISDN-Netzkoppelelemente
					M 2.109	(A)	Rechtevergabe für den Fernzugriff
					M 5.47	(Z)	Einrichten einer Closed User Group
					M 5.48	(A)	Authentisierung mittels CLIP/COLP
					M 5.49	(A)	Callback basierend auf CLIP/COLP
					M 5.50	(A)	Authentisierung mittels PAP/CHAP
			G 5.14	Gebührenbetrug	M 2.64	(A)	Kontrolle der Protokolldateien
					M 2.108	(Z)	Verzicht auf Fernwartung der ISDN-Netzkoppelelemente
					M 2.109	(A)	Rechtevergabe für den Fernzugriff
					M 4.59	(A)	Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten
					M 4.60	(A)	Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten
					M 4.61	(A)	Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten
					M 4.62	(Z)	Einsatz eines D-Kanal-Filters
					M 5.29	(C)	Gelegentliche Kontrolle programmierter Zieladressen und Protokolle
					M 5.47	(Z)	Einrichten einer Closed User Group
					M 5.48	(A)	Authentisierung mittels CLIP/COLP
					M 5.49	(A)	Callback basierend auf CLIP/COLP
					M 5.50	(A)	Authentisierung mittels PAP/CHAP
			G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal	M 1.43	(A)	Gesicherte Aufstellung aktiver Netzkomponenten
			G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal	M 1.43	(A)	Gesicherte Aufstellung aktiver Netzkomponenten
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 2.64	(A)	Kontrolle der Protokolldateien
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 5.32	(A)	Sicherer Einsatz von Kommunikationssoftware
			G 5.25	Maskerade	M 4.61	(A)	Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten
					M 4.62	(Z)	Einsatz eines D-Kanal-Filters
					M 5.49	(A)	Callback basierend auf CLIP/COLP
					M 5.50	(A)	Authentisierung mittels PAP/CHAP
			G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten	M 2.106	(A)	Auswahl geeigneter ISDN-Karten in der Beschaffung
					M 2.108	(Z)	Verzicht auf Fernwartung der ISDN-Netzkoppelelemente
					M 2.109	(A)	Rechtevergabe für den Fernzugriff
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 4.59	(A)	Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten
					M 4.60	(A)	Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten

					M 4.61	(A)	Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten
					M 5.32	(A)	Sicherer Einsatz von Kommunikationssoftware
			G 5.48	IP-Spoofing	M 5.48	(A)	Authentisierung mittels CLIP/COLP
					M 5.49	(A)	Callback basierend auf CLIP/COLP
			G 5.61	Missbrauch von Remote-Zugängen für Managementfunktionen von Routern	M 2.64	(A)	Kontrolle der Protokolldateien
					M 2.108	(Z)	Verzicht auf Fernwartung der ISDN-Netzkoppelelemente
					M 2.109	(A)	Rechtevergabe für den Fernzugriff
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
			G 5.62	Missbrauch von Ressourcen über abgesetzte IT-Systeme	M 2.42	(A)	Festlegung der möglichen Kommunikationspartner
					M 2.64	(A)	Kontrolle der Protokolldateien
					M 2.108	(Z)	Verzicht auf Fernwartung der ISDN-Netzkoppelelemente
					M 2.109	(A)	Rechtevergabe für den Fernzugriff
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
			G 5.63	Manipulationen über den ISDN-D-Kanal	M 2.64	(A)	Kontrolle der Protokolldateien
					M 4.62	(Z)	Einsatz eines D-Kanal-Filters
B 5.1	(6.3)	Peer-to-Peer-Dienste	G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten	M 2.67	(A)	Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste
					M 4.45	(A)	Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW
					M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
			G 2.65	Komplexität der SAMBA-Konfiguration	M 5.82	(A)	Sicherer Einsatz von SAMBA
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.67	(A)	Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste
					M 2.68	(B)	Sicherheitskontrollen durch die Benutzer beim Einsatz von Peer-to-Peer-Diensten
					M 2.94	(B)	Freigabe von Verzeichnissen unter Windows NT
					M 4.45	(A)	Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
					M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
			G 3.18	Freigabe von Verzeichnissen, Druckern oder der Ablagemappe	M 2.67	(A)	Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste
					M 2.68	(B)	Sicherheitskontrollen durch die Benutzer beim Einsatz von Peer-to-Peer-Diensten
					M 2.94	(B)	Freigabe von Verzeichnissen unter Windows NT
					M 3.19	(A)	Einweisung in den richtigen Einsatz der Sicherheitsfunktionen von Peer-to-Peer-Diensten
					M 4.45	(A)	Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW
					M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP

			G 3.19	Speichern von Passwörtern unter WfW und Windows 95	M 2.67	(A)	Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste
					M 3.19	(A)	Einweisung in den richtigen Einsatz der Sicherheitsfunktionen von Peer-to-Peer-Diensten
					M 4.45	(A)	Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW
					M 4.46	(A)	Nutzung des Anmeldepasswortes unter WfW und Windows 95
			G 3.20	Ungewollte Freigabe des Leserechtes bei Schedule+	M 4.45	(A)	Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW
			G 5.45	Ausprobieren von Passwörtern unter WfW und Windows 95	M 2.67	(A)	Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste
					M 2.68	(B)	Sicherheitskontrollen durch die Benutzer beim Einsatz von Peer-to-Peer-Diensten
					M 2.94	(B)	Freigabe von Verzeichnissen unter Windows NT
					M 3.19	(A)	Einweisung in den richtigen Einsatz der Sicherheitsfunktionen von Peer-to-Peer-Diensten
					M 4.58	(B)	Freigabe von Verzeichnissen unter Windows 95
			G 5.46	Maskerade unter WfW	M 2.67	(A)	Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste
					M 3.19	(A)	Einweisung in den richtigen Einsatz der Sicherheitsfunktionen von Peer-to-Peer-Diensten
			G 5.47	Löschen des Post-Office unter WfW	M 4.58	(B)	Freigabe von Verzeichnissen unter Windows 95
B 5.2	(7.1)	Datenträgeraustausch	G 1.7	Unzulässige Temperatur und Luftfeuchte	M 1.36	(A)	Sichere Aufbewahrung der Datenträger vor und nach Versand
					M 2.44	(A)	Sichere Verpackung der Datenträger
			G 1.8	Staub, Verschmutzung	M 1.36	(A)	Sichere Aufbewahrung der Datenträger vor und nach Versand
					M 2.44	(A)	Sichere Verpackung der Datenträger
			G 1.9	Datenverlust durch starke Magnetfelder	M 2.44	(A)	Sichere Verpackung der Datenträger
					M 6.38	(A)	Sicherungskopie der übermittelten Daten
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.3	(B)	Datenträgerverwaltung
			G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel	M 5.22	(B)	Kompatibilitätsprüfung des Sender- und Empfängersystems
			G 2.10	Nicht fristgerecht verfügbare Datenträger	M 2.3	(B)	Datenträgerverwaltung
					M 2.43	(A)	Ausreichende Kennzeichnung der Datenträger beim Versand
					M 2.45	(A)	Regelung des Datenträgeraustausches
					M 3.14	(B)	Einweisung des Personals in den geregelten Ablauf eines Datenträgeraustausches
					M 5.22	(B)	Kompatibilitätsprüfung des Sender- und Empfängersystems
					M 5.23	(A)	Auswahl einer geeigneten Versandart für den Datenträger
			G 2.17	Mangelhafte Kennzeichnung der Datenträger	M 2.43	(A)	Ausreichende Kennzeichnung der Datenträger beim Versand
					M 3.14	(B)	Einweisung des Personals in den geregelten Ablauf eines Datenträgeraustausches

			G 2.18	Ungeordnete Zustellung der Datenträger	M 2.42	(B)	Festlegung der möglichen Kommunikationspartner
					M 2.43	(A)	Ausreichende Kennzeichnung der Datenträger beim Versand
					M 2.45	(A)	Regelung des Datenträgeraustausches
					M 5.23	(A)	Auswahl einer geeigneten Versandart für den Datenträger
			G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung	M 2.46	(Z)	Geeignetes Schlüsselmanagement
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 1.36	(A)	Sichere Aufbewahrung der Datenträger vor und nach Versand
					M 2.42	(B)	Festlegung der möglichen Kommunikationspartner
					M 2.45	(A)	Regelung des Datenträgeraustausches
					M 2.46	(Z)	Geeignetes Schlüsselmanagement
					M 4.32	(B)	Physikalisches Löschen der Datenträger vor und nach Verwendung
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 4.35	(Z)	Verifizieren der zu übertragenden Daten vor Versand
					M 5.23	(A)	Auswahl einer geeigneten Versandart für den Datenträger
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.45	(A)	Regelung des Datenträgeraustausches
					M 3.14	(B)	Einweisung des Personals in den geregelten Ablauf eines Datenträgeraustausches
			G 3.12	Verlust der Datenträger beim Versand	M 2.43	(A)	Ausreichende Kennzeichnung der Datenträger beim Versand
					M 2.44	(A)	Sichere Verpackung der Datenträger
					M 5.23	(A)	Auswahl einer geeigneten Versandart für den Datenträger
					M 6.38	(A)	Sicherungskopie der übermittelten Daten
			G 3.13	Übertragung falscher oder nicht gewünschter Datensätze	M 2.45	(A)	Regelung des Datenträgeraustausches
					M 3.14	(B)	Einweisung des Personals in den geregelten Ablauf eines Datenträgeraustausches
					M 4.32	(B)	Physikalisches Löschen der Datenträger vor und nach Verwendung
					M 4.35	(Z)	Verifizieren der zu übertragenden Daten vor Versand
			G 4.7	Defekte Datenträger	M 2.44	(A)	Sichere Verpackung der Datenträger
					M 6.38	(A)	Sicherungskopie der übermittelten Daten
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 1.36	(A)	Sichere Aufbewahrung der Datenträger vor und nach Versand
					M 2.44	(A)	Sichere Verpackung der Datenträger
					M 5.23	(A)	Auswahl einer geeigneten Versandart für den Datenträger
			G 5.2	Manipulation an Daten oder Software	M 1.36	(A)	Sichere Aufbewahrung der Datenträger vor und nach Versand
					M 2.3	(B)	Datenträgerverwaltung
					M 2.44	(A)	Sichere Verpackung der Datenträger
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 5.23	(A)	Auswahl einer geeigneten Versandart für den Datenträger
					M 6.38	(A)	Sicherungskopie der übermittelten Daten

			G 5.4	Diebstahl	M 1.36	(A)	Sichere Aufbewahrung der Datenträger vor und nach Versand
					M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 5.23	(A)	Auswahl einer geeigneten Versandart für den Datenträger
					M 6.38	(A)	Sicherungskopie der übermittelten Daten
			G 5.9	Unberechtigte IT-Nutzung	M 1.36	(A)	Sichere Aufbewahrung der Datenträger vor und nach Versand
					M 2.44	(A)	Sichere Verpackung der Datenträger
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 5.23	(A)	Auswahl einer geeigneten Versandart für den Datenträger
			G 5.23	Computer-Viren	M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 5.23	(A)	Auswahl einer geeigneten Versandart für den Datenträger
					M 6.38	(A)	Sicherungskopie der übermittelten Daten
			G 5.29	Unberechtigtes Kopieren der Datenträger	M 1.36	(A)	Sichere Aufbewahrung der Datenträger vor und nach Versand
					M 2.44	(A)	Sichere Verpackung der Datenträger
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 5.23	(A)	Auswahl einer geeigneten Versandart für den Datenträger
			G 5.43	Makro-Viren	M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 6.38	(A)	Sicherungskopie der übermittelten Daten
B 5.3	(7.4)	E-Mail	G 2.1	Fehlende oder unzureichende Regelungen	M 2.274	(A)	Vertretungsregelungen bei E-Mail-Nutzung
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.30	(A)	Regelung für die Einrichtung von Benutzern / Benutzergruppen
					M 2.118	(A)	Konzeption der sicheren E-Mail-Nutzung
					M 2.119	(A)	Regelung für den Einsatz von E-Mail
					M 5.56	(A)	Sicherer Betrieb eines Mailservers
					M 5.57	(A)	Sichere Konfiguration der Mail-Clients
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	M 2.30	(A)	Regelung für die Einrichtung von Benutzern / Benutzergruppen
					M 2.118	(A)	Konzeption der sicheren E-Mail-Nutzung
					M 2.119	(A)	Regelung für den Einsatz von E-Mail
					M 2.120	(A)	Einrichtung einer Poststelle
					M 5.22	(B)	Kompatibilitätsprüfung des Sender- und Empfängersystems
					M 5.56	(A)	Sicherer Betrieb eines Mailservers
			G 2.19	Unzureichendes Schlüsselmanagement bei	M 2.46	(Z)	Geeignetes Schlüsselmanagement

				Verschlüsselung	M 2.118	(A)	Konzeption der sicheren E-Mail-Nutzung
					M 2.119	(A)	Regelung für den Einsatz von E-Mail
			G 2.54	Vertraulichkeitsverlust durch Restinformationen	M 2.118	(A)	Konzeption der sicheren E-Mail-Nutzung
					M 2.119	(A)	Regelung für den Einsatz von E-Mail
					M 4.64	(C)	Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen
			G 2.55	Ungeordnete E-Mail-Nutzung	M 2.42	(B)	Festlegung der möglichen Kommunikationspartner
					M 2.118	(A)	Konzeption der sicheren E-Mail-Nutzung
					M 2.119	(A)	Regelung für den Einsatz von E-Mail
					M 2.120	(A)	Einrichtung einer Poststelle
					M 2.122	(B)	Einheitliche E-Mail-Adressen
					M 2.274	(A)	Vertretungsregelungen bei E-Mail-Nutzung
					M 2.275	(Z)	Einrichtung funktionsbezogener E-Mailadressen
					M 5.57	(A)	Sichere Konfiguration der Mail-Clients
			G 2.56	Mangelhafte Beschreibung von Dateien	M 2.118	(A)	Konzeption der sicheren E-Mail-Nutzung
					M 2.119	(A)	Regelung für den Einsatz von E-Mail
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 2.42	(B)	Festlegung der möglichen Kommunikationspartner
					M 2.46	(Z)	Geeignetes Schlüsselmanagement
					M 2.119	(A)	Regelung für den Einsatz von E-Mail
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 5.32	(A)	Sicherer Einsatz von Kommunikationssoftware
					M 5.63	(Z)	Einsatz von GnuPG oder PGP
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.42	(B)	Festlegung der möglichen Kommunikationspartner
					M 2.118	(A)	Konzeption der sicheren E-Mail-Nutzung
					M 2.119	(A)	Regelung für den Einsatz von E-Mail
					M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
					M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
					M 5.32	(A)	Sicherer Einsatz von Kommunikationssoftware
					M 5.57	(A)	Sichere Konfiguration der Mail-Clients
			G 3.8	Fehlerhafte Nutzung des IT-Systems	M 2.119	(A)	Regelung für den Einsatz von E-Mail
					M 5.32	(A)	Sicherer Einsatz von Kommunikationssoftware
			G 3.13	Übertragung falscher oder nicht gewünschter Datensätze	M 2.119	(A)	Regelung für den Einsatz von E-Mail
					M 5.32	(A)	Sicherer Einsatz von Kommunikationssoftware
			G 4.13	Verlust gespeicherter Daten	M 6.90	(C)	Datensicherung und Archivierung von E-Mails
			G 4.20	Datenverlust bei erschöpftem Speichermedium	M 2.121	(B)	Regelmäßiges Löschen von E-Mails
					M 5.53	(B)	Schutz vor Mailbomben
					M 5.54	(B)	Schutz vor Mailüberlastung und Spam
					M 5.55	(B)	Kontrolle von Alias-Dateien und Verteilerlisten
					M 5.56	(A)	Sicherer Betrieb eines Mailservers
					M 6.38	(A)	Sicherungskopie der übermittelten Daten
			G 4.32	Nichtzustellung einer Nachricht	M 2.120	(A)	Einrichtung einer Poststelle
					M 5.22	(B)	Kompatibilitätsprüfung des Sender- und Empfängersystems
					M 5.56	(A)	Sicherer Betrieb eines Mailservers
					M 6.38	(A)	Sicherungskopie der übermittelten Daten

			G 4.37	Mangelnde Authentizität und Vertraulichkeit von E-Mail	M 5.67	(Z)	Verwendung eines Zeitstempel-Dienstes
					M 5.108	(Z)	Kryptographische Absicherung von E-Mail
					M 5.110	(Z)	Absicherung von E-Mail mit SPHINX (S/MIME)
			G 5.2	Manipulation an Daten oder Software	M 2.123	(B)	Auswahl eines Mailproviders
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
					M 5.56	(A)	Sicherer Betrieb eines Mailservers
					M 5.63	(Z)	Einsatz von GnuPG oder PGP
					M 6.38	(A)	Sicherungskopie der übermittelten Daten
			G 5.7	Abhören von Leitungen	M 2.46	(Z)	Geeignetes Schlüsselmanagement
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 5.63	(Z)	Einsatz von GnuPG oder PGP
			G 5.9	Unberechtigte IT-Nutzung	M 5.56	(A)	Sicherer Betrieb eines Mailservers
					M 5.57	(A)	Sichere Konfiguration der Mail-Clients
			G 5.21	Trojanische Pferde	M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 5.56	(A)	Sicherer Betrieb eines Mailservers
					M 5.63	(Z)	Einsatz von GnuPG oder PGP
					M 5.109	(Z)	Einsatz eines E-Mail-Scanners auf dem Mailserver
			G 5.23	Computer-Viren	M 2.42	(B)	Festlegung der möglichen Kommunikationspartner
					M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 4.199	(B)	Vermeidung gefährlicher Dateiformate
					M 5.56	(A)	Sicherer Betrieb eines Mailservers
					M 5.63	(Z)	Einsatz von GnuPG oder PGP
					M 5.109	(Z)	Einsatz eines E-Mail-Scanners auf dem Mailserver
			G 5.24	Wiedereinspielen von Nachrichten	M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 5.63	(Z)	Einsatz von GnuPG oder PGP
			G 5.25	Maskerade	M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 5.63	(Z)	Einsatz von GnuPG oder PGP
			G 5.26	Analyse des Nachrichtenflusses	M 2.123	(B)	Auswahl eines Mailproviders
			G 5.27	Nichtanerkennung einer Nachricht	M 2.123	(B)	Auswahl eines Mailproviders
			G 5.28	Verhinderung von Diensten	M 5.53	(B)	Schutz vor Mailbomben
					M 5.54	(B)	Schutz vor Mailüberlastung und Spam
					M 5.56	(A)	Sicherer Betrieb eines Mailservers
			G 5.43	Makro-Viren	M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 4.44	(A)	Prüfung eingehender Dateien auf Makro-Viren
					M 4.199	(B)	Vermeidung gefährlicher Dateiformate

					M 5.56	(A)	Sicherer Betrieb eines Mailservers
					M 5.63	(Z)	Einsatz von GnuPG oder PGP
					M 5.109	(Z)	Einsatz eines E-Mail-Scanners auf dem Mailserver
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 5.108	(Z)	Kryptographische Absicherung von E-Mail
					M 5.110	(Z)	Absicherung von E-Mail mit SPHINX (S/MIME)
			G 5.72	Mißbräuchliche E-Mail-Nutzung	M 2.30	(A)	Regelung für die Einrichtung von Benutzern / Benutzergruppen
			G 5.73	Vortäuschen eines falschen Absenders	M 2.122	(B)	Einheitliche E-Mail-Adressen
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 5.63	(Z)	Einsatz von GnuPG oder PGP
			G 5.74	Manipulation von Alias-Dateien oder Verteilerlisten	M 5.55	(B)	Kontrolle von Alias-Dateien und Verteilerlisten
					M 5.56	(A)	Sicherer Betrieb eines Mailservers
			G 5.75	Überlastung durch eingehende E-Mails	M 2.121	(B)	Regelmäßiges Löschen von E-Mails
					M 2.123	(B)	Auswahl eines Mailproviders
					M 5.53	(B)	Schutz vor Mailbomben
					M 5.54	(B)	Schutz vor Mailüberlastung und Spam
					M 5.56	(A)	Sicherer Betrieb eines Mailservers
			G 5.76	Mailbomben	M 2.123	(B)	Auswahl eines Mailproviders
					M 5.53	(B)	Schutz vor Mailbomben
					M 5.54	(B)	Schutz vor Mailüberlastung und Spam
					M 5.56	(A)	Sicherer Betrieb eines Mailservers
			G 5.77	Mitlesen von E-Mails	M 2.123	(B)	Auswahl eines Mailproviders
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 5.56	(A)	Sicherer Betrieb eines Mailservers
					M 5.63	(Z)	Einsatz von GnuPG oder PGP
			G 5.85	Integritätsverlust schützenswerter Informationen	M 5.108	(Z)	Kryptographische Absicherung von E-Mail
					M 5.110	(Z)	Absicherung von E-Mail mit SPHINX (S/MIME)
			G 5.110	Web-Bugs	M 4.199	(B)	Vermeidung gefährlicher Dateiformate
			G 5.111	Missbrauch aktiver Inhalte in E-Mails	M 4.199	(B)	Vermeidung gefährlicher Dateiformate
					M 5.109	(Z)	Einsatz eines E-Mail-Scanners auf dem Mailserver
B 5.4	(7.5)	Webserver	G 2.1	Fehlende oder unzureichende Regelungen	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 2.173	(A)	Festlegung einer WWW-Sicherheitsstrategie
					M 2.175	(A)	Aufbau eines WWW-Servers
					M 2.271	(A)	Festlegung einer Sicherheitsstrategie für den WWW-Zugang
					M 6.88	(B)	Erstellen eines Notfallplans für den Webserver
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	M 2.174	(A)	Sicherer Betrieb eines WWW-Servers
					M 4.93	(B)	Regelmäßige Integritätsprüfung
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.173	(A)	Festlegung einer WWW-Sicherheitsstrategie
					M 2.271	(A)	Festlegung einer Sicherheitsstrategie für den WWW-Zugang
					M 4.94	(A)	Schutz der WWW-Dateien
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 2.173	(A)	Festlegung einer WWW-Sicherheitsstrategie
					M 2.175	(A)	Aufbau eines WWW-Servers

					M 2.272	(A)	Einrichtung eines WWW-Redaktionsteams
					M 4.78	(A)	Sorgfältige Durchführung von Konfigurationsänderungen
			G 2.28	Verstöße gegen das Urheberrecht	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 2.173	(A)	Festlegung einer WWW-Sicherheitsstrategie
					M 2.175	(A)	Aufbau eines WWW-Servers
					M 2.272	(A)	Einrichtung eines WWW-Redaktionsteams
					M 4.99	(C)	Schutz gegen nachträgliche Veränderungen von Informationen
			G 2.32	Unzureichende Leitungskapazitäten	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 2.176	(B)	Geeignete Auswahl eines Internet Service Providers
			G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 2.173	(A)	Festlegung einer WWW-Sicherheitsstrategie
					M 2.174	(A)	Sicherer Betrieb eines WWW-Servers
					M 5.64	(Z)	Secure Shell
			G 2.96	Veraltete oder falsche Informationen in einem Webangebot	M 2.272	(A)	Einrichtung eines WWW-Redaktionsteams
			G 2.100	Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen	M 2.298	(Z)	Verwaltung von Internet-Domainnamen
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 2.173	(A)	Festlegung einer WWW-Sicherheitsstrategie
					M 2.174	(A)	Sicherer Betrieb eines WWW-Servers
					M 2.176	(B)	Geeignete Auswahl eines Internet Service Providers
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 4.64	(C)	Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.94	(A)	Schutz der WWW-Dateien
					M 4.95	(A)	Minimales Betriebssystem
					M 4.99	(C)	Schutz gegen nachträgliche Veränderungen von Informationen
					M 5.64	(Z)	Secure Shell
					M 5.66	(Z)	Verwendung von SSL
					M 5.69	(A)	Schutz vor aktiven Inhalten
			G 3.37	Unproduktive Suchzeiten	M 2.176	(B)	Geeignete Auswahl eines Internet Service Providers
			G 3.38	Konfigurations- und Bedienungsfehler	M 2.174	(A)	Sicherer Betrieb eines WWW-Servers
					M 4.78	(A)	Sorgfältige Durchführung von Konfigurationsänderungen
					M 4.95	(A)	Minimales Betriebssystem
					M 4.97	(Z)	Ein Dienst pro Server
			G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 2.176	(B)	Geeignete Auswahl eines Internet Service Providers
					M 4.95	(A)	Minimales Betriebssystem
					M 4.97	(Z)	Ein Dienst pro Server
					M 4.98	(A)	Kommunikation durch Paketfilter auf Minimum beschränken
					M 5.64	(Z)	Secure Shell
					M 5.66	(Z)	Verwendung von SSL
					M 5.69	(A)	Schutz vor aktiven Inhalten

			G 4.22	Software-Schwachstellen oder -Fehler	M 2.273	(A)	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 4.64	(C)	Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen
					M 4.78	(A)	Sorgfältige Durchführung von Konfigurationsänderungen
			G 4.39	Software-Konzeptionsfehler	M 4.95	(A)	Minimales Betriebssystem
					M 4.97	(Z)	Ein Dienst pro Server
					M 5.64	(Z)	Secure Shell
					M 5.66	(Z)	Verwendung von SSL
					M 5.69	(A)	Schutz vor aktiven Inhalten
			G 5.2	Manipulation an Daten oder Software	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 2.173	(A)	Festlegung einer WWW-Sicherheitsstrategie
					M 2.174	(A)	Sicherer Betrieb eines WWW-Servers
					M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.94	(A)	Schutz der WWW-Dateien
					M 4.95	(A)	Minimales Betriebssystem
					M 4.97	(Z)	Ein Dienst pro Server
					M 4.98	(A)	Kommunikation durch Paketfilter auf Minimum beschränken
					M 4.176	(B)	Auswahl einer Authentisierungsmethode für Webangebote
					M 4.177	(B)	Sicherstellung der Integrität und Authentizität von Softwarepaketen
					M 5.64	(Z)	Secure Shell
					M 5.66	(Z)	Verwendung von SSL
					M 5.69	(A)	Schutz vor aktiven Inhalten
			G 5.19	Missbrauch von Benutzerrechten	M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.176	(B)	Auswahl einer Authentisierungsmethode für Webangebote
			G 5.20	Missbrauch von Administratorrechten	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 2.174	(A)	Sicherer Betrieb eines WWW-Servers
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 5.64	(Z)	Secure Shell
			G 5.21	Trojanische Pferde	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 2.174	(A)	Sicherer Betrieb eines WWW-Servers
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 4.95	(A)	Minimales Betriebssystem
					M 4.177	(B)	Sicherstellung der Integrität und Authentizität von Softwarepaketen
			G 5.23	Computer-Viren	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung

					M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
			G 5.28	Verhinderung von Diensten	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 4.95	(A)	Minimales Betriebssystem
					M 4.97	(Z)	Ein Dienst pro Server
					M 4.98	(A)	Kommunikation durch Paketfilter auf Minimum beschränken
			G 5.43	Makro-Viren	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 2.174	(A)	Sicherer Betrieb eines WWW-Servers
					M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
			G 5.48	IP-Spoofing	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 5.64	(Z)	Secure Shell
			G 5.78	DNS-Spoofing	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 2.176	(B)	Geeignete Auswahl eines Internet Service Providers
					M 4.96	(Z)	Abschaltung von DNS
					M 5.59	(A)	Schutz vor DNS-Spoofing
			G 5.87	Web-Spoofing	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 5.66	(Z)	Verwendung von SSL
					M 5.69	(A)	Schutz vor aktiven Inhalten
			G 5.88	Missbrauch aktiver Inhalte	M 2.172	(A)	Entwicklung eines Konzeptes für die WWW-Nutzung
					M 2.173	(A)	Festlegung einer WWW-Sicherheitsstrategie
					M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
					M 4.78	(A)	Sorgfältige Durchführung von Konfigurationsänderungen
					M 4.93	(B)	Regelmäßige Integritätsprüfung
					M 5.64	(Z)	Secure Shell
					M 5.66	(Z)	Verwendung von SSL
					M 5.69	(A)	Schutz vor aktiven Inhalten
B 5.5	(7.7)	Lotus Notes	G 1.1	Personalausfall	M 2.206	(A)	Planung des Einsatzes von Lotus Notes
					M 2.209	(B)	Planung des Einsatzes von Lotus Notes im Intranet
					M 2.210	(B)	Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff
					M 2.211	(A)	Planung des Einsatzes von Lotus Notes in einer DMZ
					M 6.73	(B)	Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems
			G 1.2	Ausfall des IT-Systems	M 2.206	(A)	Planung des Einsatzes von Lotus Notes
					M 2.209	(B)	Planung des Einsatzes von Lotus Notes im Intranet
					M 2.210	(B)	Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff
					M 2.211	(A)	Planung des Einsatzes von Lotus Notes in einer DMZ
					M 6.73	(B)	Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems

			G 2.1	Fehlende oder unzureichende Regelungen	M 2.206	(A)	Planung des Einsatzes von Lotus Notes
					M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 2.209	(B)	Planung des Einsatzes von Lotus Notes im Intranet
					M 2.210	(B)	Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff
					M 2.211	(A)	Planung des Einsatzes von Lotus Notes in einer DMZ
			G 2.2	Unzureichende Kenntnis über Regelungen	M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 3.24	(A)	Schulung zur Lotus Notes Systemarchitektur für Administratoren
					M 3.25	(A)	Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer
					M 4.132	(C)	Überwachen eines Lotus Notes-Systems
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 2.208	(A)	Planung der Domänen und der Zertifikatshierarchie von Lotus Notes
					M 4.116	(A)	Sichere Installation von Lotus Notes
					M 4.117	(A)	Sichere Konfiguration eines Lotus Notes Servers
					M 4.119	(A)	Einrichten von Zugangsbeschränkungen auf Lotus Notes Server
					M 4.120	(A)	Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken
					M 4.121	(A)	Konfiguration der Zugriffsrechte auf das Namens- und Adressbuch von Lotus Notes
					M 4.124	(A)	Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes
					M 4.125	(A)	Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken
					M 4.128	(A)	Sicherer Betrieb von Lotus Notes
					M 4.130	(A)	Sicherheitsmaßnahmen nach dem Anlegen neuer Lotus Notes Datenbanken
					M 4.132	(C)	Überwachen eines Lotus Notes-Systems
			G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PCs	M 4.126	(A)	Sichere Konfiguration eines Lotus Notes Clients
					M 4.127	(A)	Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes
					M 4.129	(A)	Sicherer Umgang mit Notes-ID-Dateien
					M 4.131	(Z)	Verschlüsselung von Lotus Notes Datenbanken
			G 2.18	Ungeordnete Zustellung der Datenträger	M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 3.24	(A)	Schulung zur Lotus Notes Systemarchitektur für Administratoren
					M 3.25	(A)	Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer
					M 4.129	(A)	Sicherer Umgang mit Notes-ID-Dateien
			G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung	M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 2.208	(A)	Planung der Domänen und der Zertifikatshierarchie von Lotus Notes

					M 3.24	(A)	Schulung zur Lotus Notes Systemarchitektur für Administratoren
					M 3.25	(A)	Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer
					M 5.84	(Z)	Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation
					M 5.85	(Z)	Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail
					M 5.86	(C)	Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes
			G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen	M 2.206	(A)	Planung des Einsatzes von Lotus Notes
					M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 4.117	(A)	Sichere Konfiguration eines Lotus Notes Servers
					M 4.118	(A)	Konfiguration als Lotus Notes Server
					M 4.119	(A)	Einrichten von Zugangsbeschränkungen auf Lotus Notes Server
					M 4.122	(B)	Konfiguration für den Browser-Zugriff auf Lotus Notes
					M 4.123	(B)	Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes
					M 4.124	(A)	Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes
					M 4.125	(A)	Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken
					M 4.126	(A)	Sichere Konfiguration eines Lotus Notes Clients
					M 4.127	(A)	Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes
					M 4.128	(A)	Sicherer Betrieb von Lotus Notes
					M 4.129	(A)	Sicherer Umgang mit Notes-ID-Dateien
					M 4.132	(C)	Überwachen eines Lotus Notes-Systems
			G 2.40	Komplexität des Datenbankzugangs/-zugriffs	M 2.206	(A)	Planung des Einsatzes von Lotus Notes
					M 2.209	(B)	Planung des Einsatzes von Lotus Notes im Intranet
					M 2.210	(B)	Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff
					M 2.211	(A)	Planung des Einsatzes von Lotus Notes in einer DMZ
					M 4.118	(A)	Konfiguration als Lotus Notes Server
					M 4.120	(A)	Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken
					M 4.132	(C)	Überwachen eines Lotus Notes-Systems
			G 2.49	Fehlende oder unzureichende Schulung der Telearbeiter	M 3.25	(A)	Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 3.24	(A)	Schulung zur Lotus Notes Systemarchitektur für Administratoren
					M 4.116	(A)	Sichere Installation von Lotus Notes
					M 4.117	(A)	Sichere Konfiguration eines Lotus Notes Servers
					M 4.118	(A)	Konfiguration als Lotus Notes Server

					M 4.119	(A)	Einrichten von Zugangsbeschränkungen auf Lotus Notes Server
					M 4.120	(A)	Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken
					M 4.121	(A)	Konfiguration der Zugriffsrechte auf das Namens- und Adressbuch von Lotus Notes
					M 4.122	(B)	Konfiguration für den Browser-Zugriff auf Lotus Notes
					M 4.125	(A)	Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken
					M 4.128	(A)	Sicherer Betrieb von Lotus Notes
					M 4.132	(C)	Überwachen eines Lotus Notes-Systems
					M 6.73	(B)	Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems
			G 3.43	Ungeeigneter Umgang mit Passwörtern	M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 3.24	(A)	Schulung zur Lotus Notes Systemarchitektur für Administratoren
					M 3.25	(A)	Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer
					M 4.124	(A)	Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes
					M 4.129	(A)	Sicherer Umgang mit Notes-ID-Dateien
			G 3.44	Sorglosigkeit im Umgang mit Informationen	M 3.24	(A)	Schulung zur Lotus Notes Systemarchitektur für Administratoren
					M 3.25	(A)	Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer
					M 4.129	(A)	Sicherer Umgang mit Notes-ID-Dateien
			G 3.46	Fehlkonfiguration eines Lotus Notes Servers	M 2.206	(A)	Planung des Einsatzes von Lotus Notes
					M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 2.208	(A)	Planung der Domänen und der Zertifikatshierarchie von Lotus Notes
					M 2.209	(B)	Planung des Einsatzes von Lotus Notes im Intranet
					M 2.211	(A)	Planung des Einsatzes von Lotus Notes in einer DMZ
					M 4.116	(A)	Sichere Installation von Lotus Notes
					M 4.117	(A)	Sichere Konfiguration eines Lotus Notes Servers
					M 4.118	(A)	Konfiguration als Lotus Notes Server
					M 4.119	(A)	Einrichten von Zugangsbeschränkungen auf Lotus Notes Server
					M 4.120	(A)	Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken
					M 4.121	(A)	Konfiguration der Zugriffsrechte auf das Namens- und Adressbuch von Lotus Notes
					M 4.128	(A)	Sicherer Betrieb von Lotus Notes
					M 4.129	(A)	Sicherer Umgang mit Notes-ID-Dateien
					M 4.130	(A)	Sicherheitsmaßnahmen nach dem Anlegen neuer Lotus Notes Datenbanken
					M 4.131	(Z)	Verschlüsselung von Lotus Notes Datenbanken
					M 4.132	(C)	Überwachen eines Lotus Notes-Systems

					M 5.84	(Z)	Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation
					M 5.85	(Z)	Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail
					M 5.86	(C)	Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes
					M 6.73	(B)	Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems
			G 3.47	Fehlkonfiguration des Browser-Zugriffs auf Lotus Notes	M 2.206	(A)	Planung des Einsatzes von Lotus Notes
					M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 2.208	(A)	Planung der Domänen und der Zertifikatshierarchie von Lotus Notes
					M 2.210	(B)	Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff
					M 2.211	(A)	Planung des Einsatzes von Lotus Notes in einer DMZ
					M 4.116	(A)	Sichere Installation von Lotus Notes
					M 4.117	(A)	Sichere Konfiguration eines Lotus Notes Servers
					M 4.122	(B)	Konfiguration für den Browser-Zugriff auf Lotus Notes
					M 4.123	(B)	Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes
					M 4.124	(A)	Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes
					M 4.125	(A)	Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken
					M 4.128	(A)	Sicherer Betrieb von Lotus Notes
					M 4.132	(C)	Überwachen eines Lotus Notes-Systems
					M 5.86	(C)	Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes
					M 6.73	(B)	Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems
			G 4.26	Ausfall einer Datenbank	M 6.49	(A)	Datensicherung einer Datenbank
			G 4.28	Verlust von Daten einer Datenbank	M 6.49	(A)	Datensicherung einer Datenbank
			G 4.35	Unsichere kryptographische Algorithmen	M 2.208	(A)	Planung der Domänen und der Zertifikatshierarchie von Lotus Notes
					M 4.123	(B)	Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes
					M 4.124	(A)	Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes
					M 5.84	(Z)	Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation
					M 5.85	(Z)	Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail
					M 5.86	(C)	Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes
			G 5.7	Abhören von Leitungen	M 5.84	(Z)	Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation

					M 5.85	(Z)	Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail
					M 5.86	(C)	Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes
			G 5.8	Manipulation an Leitungen	M 5.84	(Z)	Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation
					M 5.85	(Z)	Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail
					M 5.86	(C)	Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes
					M 6.73	(B)	Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems
			G 5.22	Diebstahl bei mobiler Nutzung des IT-Systems	M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 3.24	(A)	Schulung zur Lotus Notes Systemarchitektur für Administratoren
					M 3.25	(A)	Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer
					M 4.126	(A)	Sichere Konfiguration eines Lotus Notes Clients
					M 4.127	(A)	Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes
					M 4.131	(Z)	Verschlüsselung von Lotus Notes Datenbanken
					M 4.132	(C)	Überwachen eines Lotus Notes-Systems
					M 6.73	(B)	Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 3.24	(A)	Schulung zur Lotus Notes Systemarchitektur für Administratoren
					M 3.25	(A)	Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer
					M 4.116	(A)	Sichere Installation von Lotus Notes
					M 4.117	(A)	Sichere Konfiguration eines Lotus Notes Servers
					M 4.121	(A)	Konfiguration der Zugriffsrechte auf das Namens- und Adressbuch von Lotus Notes
					M 4.123	(B)	Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes
					M 4.129	(A)	Sicherer Umgang mit Notes-ID-Dateien
					M 4.131	(Z)	Verschlüsselung von Lotus Notes Datenbanken
					M 4.132	(C)	Überwachen eines Lotus Notes-Systems
					M 5.84	(Z)	Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation
					M 5.85	(Z)	Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail
					M 5.86	(C)	Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes
			G 5.77	Mitlesen von E-Mails	M 4.131	(Z)	Verschlüsselung von Lotus Notes Datenbanken
					M 5.84	(Z)	Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation

					M 5.85	(Z)	Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail
					M 5.86	(C)	Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes
			G 5.83	Kompromittierung kryptographischer Schlüssel	M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 2.208	(A)	Planung der Domänen und der Zertifikatshierarchie von Lotus Notes
					M 4.131	(Z)	Verschlüsselung von Lotus Notes Datenbanken
					M 5.84	(Z)	Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation
					M 5.85	(Z)	Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail
					M 5.86	(C)	Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes
			G 5.84	Gefälschte Zertifikate	M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 2.208	(A)	Planung der Domänen und der Zertifikatshierarchie von Lotus Notes
					M 4.119	(A)	Einrichten von Zugangsbeschränkungen auf Lotus Notes Server
					M 4.129	(A)	Sicherer Umgang mit Notes-ID-Dateien
					M 4.132	(C)	Überwachen eines Lotus Notes-Systems
					M 6.73	(B)	Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems
			G 5.85	Integritätsverlust schützenswerter Informationen	M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 4.129	(A)	Sicherer Umgang mit Notes-ID-Dateien
					M 4.131	(Z)	Verschlüsselung von Lotus Notes Datenbanken
					M 4.132	(C)	Überwachen eines Lotus Notes-Systems
					M 5.84	(Z)	Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation
					M 5.85	(Z)	Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail
					M 5.86	(C)	Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes
					M 6.73	(B)	Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems
			G 5.100	Missbrauch aktiver Inhalte beim Zugriff auf Lotus Notes	M 2.206	(A)	Planung des Einsatzes von Lotus Notes
					M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 2.208	(A)	Planung der Domänen und der Zertifikatshierarchie von Lotus Notes
					M 2.209	(B)	Planung des Einsatzes von Lotus Notes im Intranet
					M 3.24	(A)	Schulung zur Lotus Notes Systemarchitektur für Administratoren
					M 3.25	(A)	Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer
					M 4.126	(A)	Sichere Konfiguration eines Lotus Notes Clients
					M 4.132	(C)	Überwachen eines Lotus Notes-Systems

					M 6.73	(B)	Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems
			G 5.101	"Hacking Lotus Notes"	M 2.206	(A)	Planung des Einsatzes von Lotus Notes
					M 2.207	(A)	Festlegen einer Sicherheitsrichtlinie für Lotus Notes
					M 2.211	(A)	Planung des Einsatzes von Lotus Notes in einer DMZ
					M 4.124	(A)	Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes
					M 4.125	(A)	Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken
					M 4.128	(A)	Sicherer Betrieb von Lotus Notes
					M 4.132	(C)	Überwachen eines Lotus Notes-Systems
B 5.6	(8.5)	Faxserver	G 2.7	Unerlaubte Ausübung von Rechten	M 2.178	(A)	Erstellung einer Sicherheitsleitlinie für die Faxnutzung
					M 2.179	(A)	Regelungen für den Faxserver-Einsatz
					M 5.73	(A)	Sicherer Betrieb eines Faxservers
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	M 2.180	(A)	Einrichten einer Fax-Poststelle
					M 5.73	(A)	Sicherer Betrieb eines Faxservers
					M 5.74	(A)	Pflege der Faxserver-Adressbücher und der Verteillisten
			G 2.22	Fehlende Auswertung von Protokolldaten	M 2.179	(A)	Regelungen für den Faxserver-Einsatz
					M 2.180	(A)	Einrichten einer Fax-Poststelle
					M 5.25	(A)	Nutzung von Sende- und Empfangsprotokollen
					M 5.73	(A)	Sicherer Betrieb eines Faxservers
			G 2.63	Ungeordnete Faxnutzung	M 2.178	(A)	Erstellung einer Sicherheitsleitlinie für die Faxnutzung
					M 2.179	(A)	Regelungen für den Faxserver-Einsatz
					M 2.180	(A)	Einrichten einer Fax-Poststelle
					M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung
					M 4.36	(Z)	Sperren bestimmter Faxempfänger-Rufnummern
					M 4.37	(Z)	Sperren bestimmter Absender-Faxnummern
					M 5.74	(A)	Pflege der Faxserver-Adressbücher und der Verteillisten
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.178	(A)	Erstellung einer Sicherheitsleitlinie für die Faxnutzung
					M 2.179	(A)	Regelungen für den Faxserver-Einsatz
			G 3.14	Fehleinschätzung der Rechtsverbindlichkeit eines Fax	M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung
			G 4.15	Fehlerhafte Faxübertragung	M 5.24	(Z)	Nutzung eines geeigneten Faxvorblattes
					M 5.26	(Z)	Telefonische Ankündigung einer Faxsendung
					M 5.27	(Z)	Telefonische Rückversicherung über korrekten Faxempfang
					M 5.28	(Z)	Telefonische Rückversicherung über korrekten Faxabsender
			G 4.20	Datenverlust bei erschöpftem Speichermedium	M 2.180	(A)	Einrichten einer Fax-Poststelle
					M 2.181	(A)	Auswahl eines geeigneten Faxservers
					M 5.73	(A)	Sicherer Betrieb eines Faxservers
					M 6.69	(B)	Notfallvorsorge und Ausfallsicherheit bei Faxservern
			G 5.2	Manipulation an Daten oder Software	M 5.73	(A)	Sicherer Betrieb eines Faxservers
			G 5.7	Abhören von Leitungen	M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung
			G 5.9	Unberechtigte IT-Nutzung	M 2.178	(A)	Erstellung einer Sicherheitsleitlinie für die Faxnutzung
					M 2.179	(A)	Regelungen für den Faxserver-Einsatz
					M 2.180	(A)	Einrichten einer Fax-Poststelle

					M 5.73	(A)	Sicherer Betrieb eines Faxservers
			G 5.24	Wiedereinspielen von Nachrichten	M 5.25	(A)	Nutzung von Sende- und Empfangsprotokollen
			G 5.25	Maskerade	M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung
			G 5.27	Nichtanerkennung einer Nachricht	M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung
			G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers	M 2.178	(A)	Erstellung einer Sicherheitsleitlinie für die Faxnutzung
					M 2.179	(A)	Regelungen für den Faxserver-Einsatz
					M 2.180	(A)	Einrichten einer Fax-Poststelle
					M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung
					M 5.25	(A)	Nutzung von Sende- und Empfangsprotokollen
					M 5.73	(A)	Sicherer Betrieb eines Faxservers
			G 5.31	Unbefugtes Lesen von Faxsendungen	M 2.178	(A)	Erstellung einer Sicherheitsleitlinie für die Faxnutzung
					M 2.179	(A)	Regelungen für den Faxserver-Einsatz
					M 2.180	(A)	Einrichten einer Fax-Poststelle
					M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung
					M 5.73	(A)	Sicherer Betrieb eines Faxservers
					M 5.74	(A)	Pflege der Faxserver-Adressbücher und der Verteillisten
			G 5.32	Auswertung von Restinformationen in Faxgeräten und Faxservern	M 2.179	(A)	Regelungen für den Faxserver-Einsatz
					M 2.180	(A)	Einrichten einer Fax-Poststelle
					M 5.73	(A)	Sicherer Betrieb eines Faxservers
			G 5.33	Vortäuschen eines falschen Absenders bei Faxsendungen	M 5.24	(Z)	Nutzung eines geeigneten Faxvorblattes
					M 5.28	(Z)	Telefonische Rückversicherung über korrekten Faxabsender
			G 5.35	Überlastung durch Faxsendungen	M 2.178	(A)	Erstellung einer Sicherheitsleitlinie für die Faxnutzung
					M 2.179	(A)	Regelungen für den Faxserver-Einsatz
					M 2.180	(A)	Einrichten einer Fax-Poststelle
					M 2.181	(A)	Auswahl eines geeigneten Faxservers
					M 5.73	(A)	Sicherer Betrieb eines Faxservers
					M 5.75	(Z)	Schutz vor Überlastung des Faxservers
					M 6.69	(B)	Notfallvorsorge und Ausfallsicherheit bei Faxservern
			G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten	M 2.181	(A)	Auswahl eines geeigneten Faxservers
					M 5.73	(A)	Sicherer Betrieb eines Faxservers
			G 5.90	Manipulation von Adressbüchern und Verteillisten	M 2.179	(A)	Regelungen für den Faxserver-Einsatz
					M 2.180	(A)	Einrichten einer Fax-Poststelle
					M 3.15	(A)	Informationen für alle Mitarbeiter über die Faxnutzung
					M 5.26	(Z)	Telefonische Ankündigung einer Faxsendung
					M 5.27	(Z)	Telefonische Rückversicherung über korrekten Faxempfang
					M 5.74	(A)	Pflege der Faxserver-Adressbücher und der Verteillisten
B 5.7	(9.2)	Datenbanken	G 1.1	Personalausfall	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.34	(A)	Dokumentation der Veränderungen an einem bestehenden System
					M 2.126	(A)	Erstellung eines Datenbanksicherheitskonzeptes
			G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel	M 2.80	(A)	Erstellung eines Anforderungskatalogs für Standardsoftware
					M 2.124	(A)	Geeignete Auswahl einer Datenbank-Software
					M 2.126	(A)	Erstellung eines Datenbanksicherheitskonzeptes

					M 2.135	(C)	Gesicherte Datenübernahme in eine Datenbank
					M 6.51	(B)	Wiederherstellung einer Datenbank
			G 2.22	Fehlende Auswertung von Protokolldaten	M 2.126	(A)	Erstellung eines Datenbanksicherheitskonzeptes
					M 2.131	(C)	Aufteilung von Administrationstätigkeiten bei Datenbanksystemen
					M 2.133	(A)	Kontrolle der Protokolldateien eines Datenbanksystems
			G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren	M 2.80	(A)	Erstellung eines Anforderungskatalogs für Standardsoftware
			G 2.38	Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen	M 2.125	(A)	Installation und Konfiguration einer Datenbank
					M 2.126	(A)	Erstellung eines Datenbanksicherheitskonzeptes
					M 2.127	(B)	Inferenzprävention
					M 2.128	(A)	Zugangskontrolle einer Datenbank
					M 2.129	(A)	Zugriffskontrolle einer Datenbank
					M 2.131	(C)	Aufteilung von Administrationstätigkeiten bei Datenbanksystemen
					M 4.69	(B)	Regelmäßiger Sicherheitscheck der Datenbank
			G 2.39	Komplexität eines DBMS	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.34	(A)	Dokumentation der Veränderungen an einem bestehenden System
					M 2.124	(A)	Geeignete Auswahl einer Datenbank-Software
					M 2.126	(A)	Erstellung eines Datenbanksicherheitskonzeptes
					M 2.134	(B)	Richtlinien für Datenbank-Anfragen
			G 2.40	Komplexität des Datenbankzugangs/-zugriffs	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.127	(B)	Inferenzprävention
					M 2.128	(A)	Zugangskontrolle einer Datenbank
					M 2.129	(A)	Zugriffskontrolle einer Datenbank
					M 2.132	(A)	Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen
					M 2.134	(B)	Richtlinien für Datenbank-Anfragen
					M 4.68	(A)	Sicherstellung einer konsistenten Datenbankverwaltung
			G 2.41	Mangelhafte Organisation des Wechsels von Datenbank-Benutzern	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.65	(B)	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
					M 2.128	(A)	Zugangskontrolle einer Datenbank
					M 2.129	(A)	Zugriffskontrolle einer Datenbank
					M 2.132	(A)	Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen
			G 2.57	Nicht ausreichende Speichermedien für den Notfall	M 6.51	(B)	Wiederherstellung einer Datenbank
			G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	M 2.127	(B)	Inferenzprävention
					M 2.128	(A)	Zugangskontrolle einer Datenbank
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.67	(A)	Sperren und Löschen nicht benötigter Datenbank-Accounts

					M 6.49	(A)	Datensicherung einer Datenbank
			G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.65	(B)	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
					M 2.127	(B)	Inferenzprävention
					M 2.128	(A)	Zugangskontrolle einer Datenbank
					M 2.129	(A)	Zugriffskontrolle einer Datenbank
					M 2.131	(C)	Aufteilung von Administrationstätigkeiten bei Datenbanksystemen
					M 2.132	(A)	Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen
					M 4.67	(A)	Sperren und Löschen nicht benötigter Datenbank-Accounts
					M 4.68	(A)	Sicherstellung einer konsistenten Datenbankverwaltung
					M 4.69	(B)	Regelmäßiger Sicherheitscheck der Datenbank
			G 3.23	Fehlerhafte Administration eines DBMS	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.126	(A)	Erstellung eines Datenbanksicherheitskonzeptes
					M 2.128	(A)	Zugangskontrolle einer Datenbank
					M 2.131	(C)	Aufteilung von Administrationstätigkeiten bei Datenbanksystemen
					M 4.68	(A)	Sicherstellung einer konsistenten Datenbankverwaltung
					M 4.69	(B)	Regelmäßiger Sicherheitscheck der Datenbank
			G 3.24	Unbeabsichtigte Datenmanipulation	M 2.134	(B)	Richtlinien für Datenbank-Anfragen
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.67	(A)	Sperren und Löschen nicht benötigter Datenbank-Accounts
					M 6.49	(A)	Datensicherung einer Datenbank
					M 6.50	(A)	Archivierung von Datenbeständen
					M 6.51	(B)	Wiederherstellung einer Datenbank
			G 4.26	Ausfall einer Datenbank	M 2.31	(A)	Dokumentation der zugelassenen Benutzer und Rechteprofile
					M 2.34	(A)	Dokumentation der Veränderungen an einem bestehenden System
					M 2.126	(A)	Erstellung eines Datenbanksicherheitskonzeptes
					M 4.70	(C)	Durchführung einer Datenbanküberwachung
					M 6.48	(A)	Verhaltensregeln nach Verlust der Datenbankintegrität
					M 6.49	(A)	Datensicherung einer Datenbank
					M 6.50	(A)	Archivierung von Datenbeständen
					M 6.51	(B)	Wiederherstellung einer Datenbank
			G 4.27	Unterlaufen von Zugriffskontrollen über ODBC	M 4.69	(B)	Regelmäßiger Sicherheitscheck der Datenbank
					M 4.70	(C)	Durchführung einer Datenbanküberwachung
					M 5.58	(B)	Installation von ODBC-Treibern
			G 4.28	Verlust von Daten einer Datenbank	M 2.135	(C)	Gesicherte Datenübernahme in eine Datenbank
					M 4.70	(C)	Durchführung einer Datenbanküberwachung
					M 6.49	(A)	Datensicherung einer Datenbank

					M 6.50	(A)	Archivierung von Datenbeständen
					M 6.51	(B)	Wiederherstellung einer Datenbank
			G 4.29	Datenverlust einer Datenbank bei erschöpftem Speichermedium	M 2.126	(A)	Erstellung eines Datenbanksicherheitskonzeptes
					M 2.135	(C)	Gesicherte Datenübernahme in eine Datenbank
					M 4.70	(C)	Durchführung einer Datenbanküberwachung
					M 4.73	(C)	Festlegung von Obergrenzen für selektierbare Datensätze
					M 6.49	(A)	Datensicherung einer Datenbank
					M 6.50	(A)	Archivierung von Datenbeständen
					M 6.51	(B)	Wiederherstellung einer Datenbank
			G 4.30	Verlust der Datenbankintegrität/-konsistenz	M 2.130	(A)	Gewährleistung der Datenbankintegrität
					M 2.135	(C)	Gesicherte Datenübernahme in eine Datenbank
					M 4.68	(A)	Sicherstellung einer konsistenten Datenbankverwaltung
					M 4.70	(C)	Durchführung einer Datenbanküberwachung
					M 6.48	(A)	Verhaltensregeln nach Verlust der Datenbankintegrität
					M 6.49	(A)	Datensicherung einer Datenbank
					M 6.50	(A)	Archivierung von Datenbeständen
					M 6.51	(B)	Wiederherstellung einer Datenbank
			G 5.9	Unberechtigte IT-Nutzung	M 2.128	(A)	Zugangskontrolle einer Datenbank
					M 2.129	(A)	Zugriffskontrolle einer Datenbank
					M 2.133	(A)	Kontrolle der Protokolldateien eines Datenbanksystems
					M 3.18	(A)	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.67	(A)	Sperren und Löschen nicht benötigter Datenbank-Accounts
					M 4.69	(B)	Regelmäßiger Sicherheitscheck der Datenbank
					M 4.71	(C)	Restriktive Handhabung von Datenbank-Links
					M 4.72	(Z)	Datenbank-Verschlüsselung
					M 6.49	(A)	Datensicherung einer Datenbank
			G 5.10	Missbrauch von Fernwartungszugängen	M 2.128	(A)	Zugangskontrolle einer Datenbank
					M 2.133	(A)	Kontrolle der Protokolldateien eines Datenbanksystems
					M 4.67	(A)	Sperren und Löschen nicht benötigter Datenbank-Accounts
					M 4.69	(B)	Regelmäßiger Sicherheitscheck der Datenbank
					M 4.72	(Z)	Datenbank-Verschlüsselung
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 2.128	(A)	Zugangskontrolle einer Datenbank
					M 2.133	(A)	Kontrolle der Protokolldateien eines Datenbanksystems
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.69	(B)	Regelmäßiger Sicherheitscheck der Datenbank
			G 5.64	Manipulation an Daten oder Software bei Datenbanksystemen	M 2.127	(B)	Inferenzprävention
					M 2.129	(A)	Zugriffskontrolle einer Datenbank
					M 4.7	(A)	Änderung voreingestellter Passwörter
					M 4.67	(A)	Sperren und Löschen nicht benötigter Datenbank-Accounts
					M 4.68	(A)	Sicherstellung einer konsistenten Datenbankverwaltung
					M 4.69	(B)	Regelmäßiger Sicherheitscheck der Datenbank
					M 4.71	(C)	Restriktive Handhabung von Datenbank-Links

					M 4.72	(Z)	Datenbank-Verschlüsselung
					M 6.49	(A)	Datensicherung einer Datenbank
					M 6.50	(A)	Archivierung von Datenbeständen
			G 5.65	Verhinderung der Dienste eines Datenbanksystems	M 2.134	(B)	Richtlinien für Datenbank-Anfragen
					M 4.69	(B)	Regelmäßiger Sicherheitscheck der Datenbank
					M 4.73	(C)	Festlegung von Obergrenzen für selektierbare Datensätze
B 5.8	(9.3)	Telearbeit	G 1.1	Personalausfall	M 2.113	(A)	Regelungen für Telearbeit
					M 2.114	(A)	Informationsfluss zwischen Telearbeiter und Institution
					M 3.22	(B)	Vertretungsregelung für Telearbeit
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.113	(A)	Regelungen für Telearbeit
					M 2.115	(B)	Betreuungs- und Wartungskonzept für Telearbeitsplätze
					M 2.116	(A)	Geregelte Nutzung der Kommunikationsmöglichkeiten
					M 2.117	(A)	Regelung der Zugriffsmöglichkeiten des Telearbeiters
					M 2.205	(C)	Übertragung und Abruf personenbezogener Daten
					M 2.241	(C)	Durchführung einer Anforderungsanalyse für den Telearbeitsplatz
					M 3.22	(B)	Vertretungsregelung für Telearbeit
			G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	M 2.113	(A)	Regelungen für Telearbeit
			G 2.5	Fehlende oder unzureichende Wartung	M 2.115	(B)	Betreuungs- und Wartungskonzept für Telearbeitsplätze
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.117	(A)	Regelung der Zugriffsmöglichkeiten des Telearbeiters
					M 2.205	(C)	Übertragung und Abruf personenbezogener Daten
					M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
			G 2.22	Fehlende Auswertung von Protokolldaten	M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
			G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes	M 2.116	(A)	Geregelte Nutzung der Kommunikationsmöglichkeiten
					M 2.205	(C)	Übertragung und Abruf personenbezogener Daten
					M 2.241	(C)	Durchführung einer Anforderungsanalyse für den Telearbeitsplatz
					M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
			G 2.49	Fehlende oder unzureichende Schulung der Telearbeiter	M 2.205	(C)	Übertragung und Abruf personenbezogener Daten
					M 3.21	(A)	Sicherheitstechnische Einweisung und Fortbildung des Telearbeiters

			G 2.50	Verzögerungen durch temporär eingeschränkte Erreichbarkeit der	M 2.113	(A)	Regelungen für Telearbeit
					M 2.114	(A)	Informationsfluss zwischen Telearbeiter und Institution
			G 2.51	Mangelhafte Einbindung des Telearbeiters in den Informationsfluss	M 2.114	(A)	Informationsfluss zwischen Telearbeiter und Institution
			G 2.52	Erhöhte Reaktionszeiten bei IT-Systemausfall	M 6.47	(B)	Datensicherung bei der Telearbeit
			G 2.53	Unzureichende Vertretungsregelungen für Telearbeit	M 3.21	(A)	Sicherheitstechnische Einweisung und Fortbildung des Telearbeiters
					M 3.22	(B)	Vertretungsregelung für Telearbeit
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 2.114	(A)	Informationsfluss zwischen Telearbeiter und Institution
					M 2.115	(B)	Betreuungs- und Wartungskonzept für Telearbeitsplätze
					M 2.116	(A)	Geregelte Nutzung der Kommunikationsmöglichkeiten
					M 2.117	(A)	Regelung der Zugriffsmöglichkeiten des Telearbeiters
					M 2.205	(C)	Übertragung und Abruf personenbezogener Daten
					M 3.21	(A)	Sicherheitstechnische Einweisung und Fortbildung des Telearbeiters
					M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
			G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen	M 2.113	(A)	Regelungen für Telearbeit
					M 2.114	(A)	Informationsfluss zwischen Telearbeiter und Institution
					M 2.116	(A)	Geregelte Nutzung der Kommunikationsmöglichkeiten
					M 2.117	(A)	Regelung der Zugriffsmöglichkeiten des Telearbeiters
					M 2.205	(C)	Übertragung und Abruf personenbezogener Daten
					M 3.21	(A)	Sicherheitstechnische Einweisung und Fortbildung des Telearbeiters
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
					M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
					M 6.47	(B)	Datensicherung bei der Telearbeit
			G 3.9	Fehlerhafte Administration des IT-Systems	M 2.117	(A)	Regelung der Zugriffsmöglichkeiten des Telearbeiters
					M 2.205	(C)	Übertragung und Abruf personenbezogener Daten
					M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 6.47	(B)	Datensicherung bei der Telearbeit
			G 3.13	Übertragung falscher oder nicht gewünschter Datensätze	M 2.116	(A)	Geregelte Nutzung der Kommunikationsmöglichkeiten
					M 2.205	(C)	Übertragung und Abruf personenbezogener Daten
					M 2.241	(C)	Durchführung einer Anforderungsanalyse für den Telearbeitsplatz

					M 3.21	(A)	Sicherheitstechnische Einweisung und Fortbildung des Telearbeiters
			G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten	M 2.117	(A)	Regelung der Zugriffsmöglichkeiten des Telearbeiters
					M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
			G 3.30	Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners	M 2.113	(A)	Regelungen für Telearbeit
					M 2.116	(A)	Geregelte Nutzung der Kommunikationsmöglichkeiten
					M 2.117	(A)	Regelung der Zugriffsmöglichkeiten des Telearbeiters
					M 2.205	(C)	Übertragung und Abruf personenbezogener Daten
			G 4.13	Verlust gespeicherter Daten	M 2.241	(C)	Durchführung einer Anforderungsanalyse für den Telearbeitsplatz
					M 6.47	(B)	Datensicherung bei der Telearbeit
			G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör	M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 6.47	(B)	Datensicherung bei der Telearbeit
			G 5.2	Manipulation an Daten oder Software	M 2.114	(A)	Informationsfluss zwischen Telearbeiter und Institution
					M 2.116	(A)	Geregelte Nutzung der Kommunikationsmöglichkeiten
					M 2.117	(A)	Regelung der Zugriffsmöglichkeiten des Telearbeiters
					M 2.205	(C)	Übertragung und Abruf personenbezogener Daten
					M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
					M 6.38	(B)	Sicherungskopie der übermittelten Daten
					M 6.47	(B)	Datensicherung bei der Telearbeit
			G 5.7	Abhören von Leitungen	M 2.205	(C)	Übertragung und Abruf personenbezogener Daten
			G 5.9	Unberechtigte IT-Nutzung	M 2.241	(C)	Durchführung einer Anforderungsanalyse für den Telearbeitsplatz
					M 6.47	(B)	Datensicherung bei der Telearbeit
			G 5.10	Missbrauch von Fernwartungszugängen	M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
			G 5.19	Missbrauch von Benutzerrechten	M 2.205	(C)	Übertragung und Abruf personenbezogener Daten

					M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
					M 6.47	(B)	Datensicherung bei der Telearbeit
			G 5.20	Missbrauch von Administratorrechten	M 2.205	(C)	Übertragung und Abruf personenbezogener Daten
					M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
					M 6.47	(B)	Datensicherung bei der Telearbeit
			G 5.21	Trojanische Pferde	M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
					M 6.47	(B)	Datensicherung bei der Telearbeit
			G 5.23	Computer-Viren	M 6.38	(B)	Sicherungskopie der übermittelten Daten
			G 5.24	Wiedereinspielen von Nachrichten	M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
			G 5.25	Maskerade	M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
			G 5.43	Makro-Viren	M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
					M 4.63	(A)	Sicherheitstechnische Anforderungen an den Telearbeitsrechner
					M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
					M 6.47	(B)	Datensicherung bei der Telearbeit
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 2.116	(A)	Geregelte Nutzung der Kommunikationsmöglichkeiten
					M 2.205	(C)	Übertragung und Abruf personenbezogener Daten
					M 2.241	(C)	Durchführung einer Anforderungsanalyse für den Telearbeitsplatz
					M 3.21	(A)	Sicherheitstechnische Einweisung und Fortbildung des Telearbeiters

					M 5.51	(A)	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
					M 5.52	(A)	Sicherheitstechnische Anforderungen an den Kommunikationsrechner
B 5.9	(9.4)	Novell eDirectory	G 1.2	Ausfall des IT-Systems	M 4.153	(A)	Sichere Installation von Novell eDirectory
					M 6.80	(A)	Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes
					M 6.81	(A)	Erstellen von Datensicherungen für Novell eDirectory
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.238	(A)	Festlegung einer Sicherheitsrichtlinie für Novell eDirectory
			G 2.2	Unzureichende Kenntnis über Regelungen	M 3.29	(A)	Schulung zur Administration von Novell eDirectory
					M 3.30	(A)	Schulung zum Einsatz von Novell eDirectory Clientsoftware
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.236	(A)	Planung des Einsatzes von Novell eDirectory
					M 2.239	(A)	Planung des Einsatzes von Novell eDirectory im Intranet
					M 2.240	(A)	Planung des Einsatzes von Novell eDirectory im Extranet
					M 4.157	(A)	Einrichten von Zugriffsberechtigungen auf Novell eDirectory
					M 4.158	(B)	Einrichten des LDAP-Zugriffs auf Novell eDirectory
			G 2.69	Fehlende oder unzureichende Planung des Einsatzes von Novell eDirectory	M 2.236	(A)	Planung des Einsatzes von Novell eDirectory
					M 2.239	(A)	Planung des Einsatzes von Novell eDirectory im Intranet
					M 2.240	(A)	Planung des Einsatzes von Novell eDirectory im Extranet
			G 2.70	Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Novell eDirectory	M 2.237	(B)	Planung der Partitionierung und Replikation im Novell eDirectory
			G 2.71	Fehlerhafte oder unzureichende Planung des LDAP-Zugriffs auf Novell eDirectory	M 2.240	(A)	Planung des Einsatzes von Novell eDirectory im Extranet
			G 3.9	Fehlerhafte Administration des IT-Systems	M 3.29	(A)	Schulung zur Administration von Novell eDirectory
					M 4.159	(A)	Sicherer Betrieb von Novell eDirectory
			G 3.13	Übertragung falscher oder nicht gewünschter Datensätze	M 5.97	(B)	Absicherung der Kommunikation mit Novell eDirectory
			G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten	M 3.29	(A)	Schulung zur Administration von Novell eDirectory
					M 4.157	(A)	Einrichten von Zugriffsberechtigungen auf Novell eDirectory
					M 4.158	(B)	Einrichten des LDAP-Zugriffs auf Novell eDirectory
			G 3.34	Ungeeignete Konfiguration des Managementsystems	M 4.155	(A)	Sichere Konfiguration von Novell eDirectory
			G 3.35	Server im laufenden Betrieb ausschalten	M 4.159	(A)	Sicherer Betrieb von Novell eDirectory
					M 6.80	(A)	Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes
					M 6.81	(A)	Erstellen von Datensicherungen für Novell eDirectory
			G 3.36	Fehlinterpretation von Ereignissen	M 4.160	(B)	Überwachen von Novell eDirectory
			G 3.38	Konfigurations- und Bedienungsfehler	M 3.29	(A)	Schulung zur Administration von Novell eDirectory
					M 3.30	(A)	Schulung zum Einsatz von Novell eDirectory Clientsoftware
					M 4.155	(A)	Sichere Konfiguration von Novell eDirectory
					M 4.156	(A)	Sichere Konfiguration der Novell eDirectory Clientsoftware
					M 4.159	(A)	Sicherer Betrieb von Novell eDirectory
			G 3.43	Ungeeigneter Umgang mit Passwörtern	M 3.30	(A)	Schulung zum Einsatz von Novell eDirectory Clientsoftware

			G 3.50	Fehlkonfiguration von Novell eDirectory	M 3.29	(A)	Schulung zur Administration von Novell eDirectory
					M 4.155	(A)	Sichere Konfiguration von Novell eDirectory
			G 3.51	Falsche Vergabe von Zugriffsrechten im Novell eDirectory	M 3.29	(A)	Schulung zur Administration von Novell eDirectory
					M 4.155	(A)	Sichere Konfiguration von Novell eDirectory
					M 4.157	(A)	Einrichten von Zugriffsberechtigungen auf Novell eDirectory
			G 3.52	Fehlkonfiguration des Intranet-Clientzugriffs auf Novell eDirectory	M 3.29	(A)	Schulung zur Administration von Novell eDirectory
					M 4.155	(A)	Sichere Konfiguration von Novell eDirectory
					M 4.157	(A)	Einrichten von Zugriffsberechtigungen auf Novell eDirectory
					M 5.97	(B)	Absicherung der Kommunikation mit Novell eDirectory
			G 3.53	Fehlkonfiguration des LDAP-Zugriffs auf Novell eDirectory	M 3.29	(A)	Schulung zur Administration von Novell eDirectory
					M 4.155	(A)	Sichere Konfiguration von Novell eDirectory
					M 4.156	(A)	Sichere Konfiguration der Novell eDirectory Clientsoftware
					M 4.158	(B)	Einrichten des LDAP-Zugriffs auf Novell eDirectory
					M 5.97	(B)	Absicherung der Kommunikation mit Novell eDirectory
			G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen	M 4.154	(A)	Sichere Installation der Novell eDirectory Clientsoftware
			G 4.13	Verlust gespeicherter Daten	M 2.236	(A)	Planung des Einsatzes von Novell eDirectory
					M 6.81	(A)	Erstellen von Datensicherungen für Novell eDirectory
			G 4.33	Schlechte oder fehlende Authentikation	M 2.240	(A)	Planung des Einsatzes von Novell eDirectory im Extranet
					M 4.154	(A)	Sichere Installation der Novell eDirectory Clientsoftware
					M 4.156	(A)	Sichere Konfiguration der Novell eDirectory Clientsoftware
					M 4.157	(A)	Einrichten von Zugriffsberechtigungen auf Novell eDirectory
					M 4.158	(B)	Einrichten des LDAP-Zugriffs auf Novell eDirectory
					M 4.159	(A)	Sicherer Betrieb von Novell eDirectory
			G 4.34	Ausfall eines Kryptomoduls	M 6.81	(A)	Erstellen von Datensicherungen für Novell eDirectory
			G 4.44	Ausfall von Novell eDirectory	M 4.153	(A)	Sichere Installation von Novell eDirectory
					M 6.80	(A)	Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes
					M 6.81	(A)	Erstellen von Datensicherungen für Novell eDirectory
			G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes	M 4.157	(A)	Einrichten von Zugriffsberechtigungen auf Novell eDirectory
					M 4.160	(B)	Überwachen von Novell eDirectory
			G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal	M 4.157	(A)	Einrichten von Zugriffsberechtigungen auf Novell eDirectory
					M 4.160	(B)	Überwachen von Novell eDirectory
			G 5.18	Systematisches Ausprobieren von Passwörtern	M 2.240	(A)	Planung des Einsatzes von Novell eDirectory im Extranet
					M 4.157	(A)	Einrichten von Zugriffsberechtigungen auf Novell eDirectory
					M 4.160	(B)	Überwachen von Novell eDirectory
			G 5.19	Missbrauch von Benutzerrechten	M 4.160	(B)	Überwachen von Novell eDirectory
			G 5.20	Missbrauch von Administratorrechten	M 4.160	(B)	Überwachen von Novell eDirectory
			G 5.65	Verhinderung der Dienste eines Datenbanksystems	M 4.155	(A)	Sichere Konfiguration von Novell eDirectory
					M 4.159	(A)	Sicherer Betrieb von Novell eDirectory
					M 4.160	(B)	Überwachen von Novell eDirectory
			G 5.78	DNS-Spoofing	M 5.97	(B)	Absicherung der Kommunikation mit Novell eDirectory
			G 5.81	Unautorisierte Benutzung eines Kryptomoduls	M 2.237	(B)	Planung der Partitionierung und Replikation im Novell eDirectory
					M 4.155	(A)	Sichere Konfiguration von Novell eDirectory
					M 4.159	(A)	Sicherer Betrieb von Novell eDirectory
B 5.10	(7.8)	Internet Information Server	G 2.1	Fehlende oder unzureichende Regelungen	M 2.267	(A)	Planen des IIS-Einsatzes

		M 2.268	(A)	Festlegung einer IIS-Sicherheitsrichtlinie
		M 6.85	(C)	Erstellung eines Notfallplans für den Ausfall des IIS
G 2.94	Unzureichende Planung des IIS-Einsatzes	M 2.267	(A)	Planen des IIS-Einsatzes
G 3.56	Fehlerhafte Einbindung des IIS in die Systemumgebung	M 2.267	(A)	Planen des IIS-Einsatzes
		M 2.268	(A)	Festlegung einer IIS-Sicherheitsrichtlinie
		M 3.36	(A)	Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS
		M 4.175	(A)	Sichere Konfiguration von Windows NT/2000 für den IIS
		M 5.101	(B)	Entfernen nicht benötigter ODBC-Treiber beim IIS-Einsatz
		M 5.103	(B)	Entfernen sämtlicher Netzwerkfreigaben beim IIS-Einsatz
G 3.57	Fehlerhafte Konfiguration des Betriebssystems für den IIS	M 4.174	(A)	Vorbereitung der Installation von Windows NT/2000 für den IIS
		M 4.175	(A)	Sichere Konfiguration von Windows NT/2000 für den IIS
		M 5.101	(B)	Entfernen nicht benötigter ODBC-Treiber beim IIS-Einsatz
		M 5.103	(B)	Entfernen sämtlicher Netzwerkfreigaben beim IIS-Einsatz
		M 5.104	(C)	Konfiguration des TCP/IP-Filters beim IIS-Einsatz
G 3.58	Fehlkonfiguration eines IIS	M 3.36	(A)	Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS
		M 4.181	(A)	Ausführen des IIS in einem separaten Prozess
G 3.59	Unzureichende Kenntnisse über aktuelle Sicherheitslücken und Prüfwerkzeuge für den IIS	M 3.36	(A)	Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS
G 4.13	Verlust gespeicherter Daten	M 6.87	(A)	Datensicherung auf dem IIS
G 4.22	Software-Schwachstellen oder -Fehler	M 4.182	(B)	Überwachen des IIS-Systems
		M 4.187	(A)	Entfernen der FrontPage Server-Erweiterung des IIS
		M 4.189	(B)	Schutz vor unzulässigen Programmaufrufen beim IIS-Einsatz
		M 5.104	(C)	Konfiguration des TCP/IP-Filters beim IIS-Einsatz
G 4.39	Software-Konzeptionsfehler	M 4.188	(B)	Prüfen der Benutzereingaben beim IIS-Einsatz
G 5.2	Manipulation an Daten oder Software	M 4.178	(A)	Absicherung der Administrator- und Benutzerkonten beim IIS-Einsatz
		M 4.179	(A)	Schutz von sicherheitskritischen Dateien beim IIS-Einsatz
		M 5.103	(B)	Entfernen sämtlicher Netzwerkfreigaben beim IIS-Einsatz
G 5.20	Missbrauch von Administratorrechten	M 4.178	(A)	Absicherung der Administrator- und Benutzerkonten beim IIS-Einsatz
G 5.28	Verhinderung von Diensten	M 4.181	(A)	Ausführen des IIS in einem separaten Prozess
		M 4.182	(B)	Überwachen des IIS-Systems
		M 4.183	(A)	Sicherstellen der Verfügbarkeit und Performance des IIS
		M 5.105	(C)	Vorbeugen vor SYN-Attacken auf den IIS
G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 4.180	(A)	Konfiguration der Authentisierungsmechanismen für den Zugriff auf den IIS
G 5.84	Gefälschte Zertifikate	M 5.106	(A)	Entfernen nicht vertrauenswürdiger Root-Zertifikate beim IIS-Einsatz
G 5.88	Missbrauch aktiver Inhalte	M 4.188	(B)	Prüfen der Benutzereingaben beim IIS-Einsatz
G 5.108	Ausnutzen von systemspezifischen Schwachstellen des IIS	M 4.182	(B)	Überwachen des IIS-Systems
		M 4.184	(A)	Deaktivieren nicht benötigter Dienste beim IIS-Einsatz

					M 4.185	(A)	Absichern von virtuellen Verzeichnissen und Web-Anwendungen beim IIS-Einsatz
					M 4.186	(A)	Entfernen von Beispieldateien und Administrations-Scripts des IIS
					M 4.187	(A)	Entfernen der FrontPage Server-Erweiterung des IIS
					M 4.189	(B)	Schutz vor unzulässigen Programmaufrufen beim IIS-Einsatz
					M 4.190	(B)	Entfernen der RDS-Unterstützung des IIS
					M 5.102	(B)	Installation von URL-Filtern beim IIS-Einsatz
					M 5.104	(C)	Konfiguration des TCP/IP-Filters beim IIS-Einsatz
					M 6.86	(B)	Schutz vor schädlichem Code auf dem IIS
B 5.11	(7.9)	Apache Webserver	G 2.1	Fehlende oder unzureichende Regelungen	M 2.269	(A)	Planung des Einsatzes eines Apache Webservers
					M 6.89	(A)	Notfallvorsorge für einen Apache-Webserver
			G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	M 4.196	(A)	Sicherer Betrieb eines Apache-Webservers
			G 2.87	Verwendung unsicherer Protokolle in öffentlichen Netzen	M 2.270	(Z)	Planung des SSL-Einsatzes beim Apache Webserver (zusätzlich)
					M 5.107	(Z)	Verwendung von SSL im Apache-Webserver
			G 2.97	Unzureichende Notfallplanung bei einem Apache-Webserver	M 6.89	(A)	Notfallvorsorge für einen Apache-Webserver
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 4.195	(A)	Konfiguration der Zugriffssteuerung beim Apache-Webserver
			G 3.9	Fehlerhafte Administration des IT-Systems	M 3.37	(A)	Schulung der Administratoren eines Apache-Webservers
			G 3.38	Konfigurations- und Bedienungsfehler	M 3.37	(A)	Schulung der Administratoren eines Apache-Webservers
			G 3.62	Fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver	M 3.37	(A)	Schulung der Administratoren eines Apache-Webservers
					M 4.192	(A)	Konfiguration des Betriebssystems für einen Apache-Webserver
					M 4.193	(A)	Sichere Installation eines Apache-Webservers
			G 3.63	Fehlerhafte Konfiguration eines Apache-Webservers	M 3.37	(A)	Schulung der Administratoren eines Apache-Webservers
					M 4.193	(A)	Sichere Installation eines Apache-Webservers
					M 4.194	(A)	Sichere Grundkonfiguration eines Apache-Webservers
					M 4.195	(A)	Konfiguration der Zugriffssteuerung beim Apache-Webserver
			G 4.39	Software-Konzeptionsfehler	M 4.197	(B)	Servererweiterungen für dynamische Webseiten beim Apache-Webserver
			G 5.2	Manipulation an Daten oder Software	M 4.193	(A)	Sichere Installation eines Apache-Webservers
					M 4.198	(Z)	Installation eines Apache-Webservers in einem chroot-Käfig
			G 5.7	Abhören von Leitungen	M 5.107	(Z)	Verwendung von SSL im Apache-Webserver
			G 5.21	Trojanische Pferde	M 4.191	(A)	Überprüfung der Integrität und Authentizität der Apache-Pakete
			G 5.28	Verhinderung von Diensten	M 6.89	(A)	Notfallvorsorge für einen Apache-Webserver
			G 5.71	Vertraulichkeitsverlust schützenswerter Informationen	M 4.193	(A)	Sichere Installation eines Apache-Webservers
					M 4.195	(A)	Konfiguration der Zugriffssteuerung beim Apache-Webserver
					M 4.196	(A)	Sicherer Betrieb eines Apache-Webservers

					M 4.197	(B)	Servererweiterungen für dynamische Webseiten beim Apache-Webserver
					M 5.107	(Z)	Verwendung von SSL im Apache-Webserver
			G 5.85	Integritätsverlust schützenswerter Informationen	M 4.193	(A)	Sichere Installation eines Apache-Webservers
					M 4.195	(A)	Konfiguration der Zugriffssteuerung beim Apache-Webserver
					M 4.196	(A)	Sicherer Betrieb eines Apache-Webservers
					M 4.197	(B)	Servererweiterungen für dynamische Webseiten beim Apache-Webserver
			G 5.109	Ausnutzen systemspezifischer Schwachstellen beim Apache-Webserver	M 4.193	(A)	Sichere Installation eines Apache-Webservers
					M 4.196	(A)	Sicherer Betrieb eines Apache-Webservers
B 5.12	(7.10)	Exchange 2000 / Outlook 2000	G 1.2	Ausfall des IT-Systems	M 4.166	(A)	Sicherer Betrieb von Exchange/Outlook 2000
					M 4.167	(B)	Überwachung und Protokollierung von Exchange 2000 Systemen
					M 6.82	(C)	Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen
			G 2.1	Fehlende oder unzureichende Regelungen	M 2.248	(A)	Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000
			G 2.2	Unzureichende Kenntnis über Regelungen	M 2.248	(A)	Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000
			G 2.7	Unerlaubte Ausübung von Rechten	M 2.247	(A)	Planung des Einsatzes von Exchange/Outlook 2000
					M 2.248	(A)	Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000
					M 3.31	(A)	Schulung zur Systemarchitektur und Sicherheit von Exchange 2000 für Administratoren
					M 4.163	(A)	Zugriffsrechte auf Exchange 2000 Objekte
			G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen	M 2.247	(A)	Planung des Einsatzes von Exchange/Outlook 2000
			G 2.55	Ungeordnete E-Mail-Nutzung	M 2.247	(A)	Planung des Einsatzes von Exchange/Outlook 2000
			G 2.91	Fehlerhafte Planung der Migration von Exchange 5.5 nach Exchange 2000	M 2.249	(B)	Planung der Migration von "Exchange 5.5-Servern" nach "Exchange 2000"
			G 2.92	Fehlerhafte Regelungen für den Browser-Zugriff auf Exchange	M 4.164	(A)	Browser-Zugriff auf Exchange 2000
					M 5.99	(C)	SSL/TLS-Absicherung für Exchange 2000
			G 2.95	Fehlendes Konzept zur Anbindung anderer E-Mail-Systeme an Exchange/Outlook	M 2.247	(A)	Planung des Einsatzes von Exchange/Outlook 2000
					M 4.162	(A)	Sichere Konfiguration von Exchange 2000 Servern
			G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer	M 3.32	(A)	Schulung zu Sicherheitsmechanismen von Outlook 2000 für Benutzer
			G 3.9	Fehlerhafte Administration des IT-Systems	M 4.161	(A)	Sichere Installation von Exchange/Outlook 2000
					M 4.162	(A)	Sichere Konfiguration von Exchange 2000 Servern
					M 4.166	(A)	Sicherer Betrieb von Exchange/Outlook 2000
			G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten	M 4.163	(A)	Zugriffsrechte auf Exchange 2000 Objekte
			G 3.38	Konfigurations- und Bedienungsfehler	M 3.31	(A)	Schulung zur Systemarchitektur und Sicherheit von Exchange 2000 für Administratoren
					M 3.32	(A)	Schulung zu Sicherheitsmechanismen von Outlook 2000 für Benutzer
					M 4.165	(A)	Sichere Konfiguration von Outlook 2000

			G 3.60	Fehlkonfiguration von Exchange 2000 Servern	M 3.31	(A)	Schulung zur Systemarchitektur und Sicherheit von Exchange 2000 für Administratoren
					M 4.161	(A)	Sichere Installation von Exchange/Outlook 2000
					M 4.162	(A)	Sichere Konfiguration von Exchange 2000 Servern
					M 4.163	(A)	Zugriffsrechte auf Exchange 2000 Objekte
					M 6.82	(C)	Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen
			G 3.61	Fehlerhafte Konfiguration von Outlook 2000 Clients	M 3.32	(A)	Schulung zu Sicherheitsmechanismen von Outlook 2000 für Benutzer
					M 4.165	(A)	Sichere Konfiguration von Outlook 2000
			G 4.22	Software-Schwachstellen oder -Fehler	M 4.166	(A)	Sicherer Betrieb von Exchange/Outlook 2000
					M 4.167	(B)	Überwachung und Protokollierung von Exchange 2000 Systemen
			G 4.32	Nichtzustellung einer Nachricht	M 6.82	(C)	Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen
			G 5.9	Unberechtigte IT-Nutzung	M 4.161	(A)	Sichere Installation von Exchange/Outlook 2000
					M 4.162	(A)	Sichere Konfiguration von Exchange 2000 Servern
					M 4.167	(B)	Überwachung und Protokollierung von Exchange 2000 Systemen
			G 5.19	Missbrauch von Benutzerrechten	M 4.165	(A)	Sichere Konfiguration von Outlook 2000
			G 5.23	Computer-Viren	M 2.247	(A)	Planung des Einsatzes von Exchange/Outlook 2000
			G 5.77	Mitlesen von E-Mails	M 5.99	(C)	SSL/TLS-Absicherung für Exchange 2000
					M 5.100	(Z)	Einsatz von Verschlüsselungs- und Signaturverfahren für die Exchange 2000 Kommunikation
			G 5.83	Kompromittierung kryptographischer Schlüssel	M 5.100	(Z)	Einsatz von Verschlüsselungs- und Signaturverfahren für die Exchange 2000 Kommunikation
			G 5.84	Gefälschte Zertifikate	M 5.100	(Z)	Einsatz von Verschlüsselungs- und Signaturverfahren für die Exchange 2000 Kommunikation
			G 5.85	Integritätsverlust schützenswerter Informationen	M 5.99	(C)	SSL/TLS-Absicherung für Exchange 2000
					M 5.100	(Z)	Einsatz von Verschlüsselungs- und Signaturverfahren für die Exchange 2000 Kommunikation