Bausteine mit zugeordneten Maßnahmen und Gefährdungen

Baustein	Alt	Bausteinname	Maßnahme	Zertifikat	Zyklus	Maßnahmentitel	Gefährdung	Gefährdungstitel
B 1.0	(3.0)	IT-Sicherheitsmanagement	M 2.192	(A)	Planung	Erstellung einer IT-Sicherheitsleitlinie	G 2.66	Unzureichendes IT-Sicherheitsmanagemei
							G 2.105	Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarunger
							G 2.106	Störung der Geschäftsabläufe aufgrund von IT-Sicherheitsvorfäller
			M 2.193	(A)	Umsetzg.	Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit	G 2.66	Unzureichendes IT-Sicherheitsmanagemei
							G 2.107	Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes IT-Sicherheitsmanagemei
			M 2.195	(A)	Umsetzg.	Erstellung eines IT-Sicherheitskonzepts	G 2.66	Unzureichendes IT-Sicherheitsmanagement
			M 2.197	(A)	Umsetzg.	Integration der Mitarbeiter in den Sicherheitsprozess	G 2.66	Unzureichendes IT-Sicherheitsmanagement
			M 2.199	(A)	Betrieb	Aufrechterhaltung der IT-Sicherheit	G 2.66	Unzureichendes IT-Sicherheitsmanagemei
							G 2.107	Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes IT-Sicherheitsmanagemei
			M 2.200	(C)	Betrieb	Managementreporte und -bewertungen der IT-Sicherhei	G 2.66	Unzureichendes IT-Sicherheitsmanagement
			M 2.201	(C)	Betrieb	Dokumentation des IT-Sicherheitsprozesses	G 2.66	Unzureichendes IT-Sicherheitsmanagement
			M 2.335	(A)	Planung	Festlegung der IT-Sicherheitsziele und strategie	G 2.66	Unzureichendes IT-Sicherheitsmanagemei
							G 2.106	Störung der Geschäftsabläufe aufgrund von IT-Sicherheitsvorfäller
							G 2.107	Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes IT-Sicherheitsmanagemei
			M 2.336	(A)	Planung	Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene	G 2.66	Unzureichendes IT-Sicherheitsmanagemei
							G 2.105	Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarunger
							G 2.106	Störung der Geschäftsabläufe aufgrund von IT-Sicherheitsvorfäller
							G 2.107	Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes IT-Sicherheitsmanagemei
			M 2.337	(A)	Umsetzg.	Integration der IT-Sicherheit in organisationsweite Abläufe und Prozesse	G 2.66	Unzureichendes IT-Sicherheitsmanagement
			M 2.338	(Z)	Umsetzg.	Erstellung von zielgruppengerechten IT-Sicherheitsrichtlinier	G 2.66	Unzureichendes IT-Sicherheitsmanagement
			M 2.339	(Z)	Umsetzg.	Wirtschaftlicher Einsatz von Ressourcen für IT-Sicherheit	G 2.105	Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarunger
							G 2.107	Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes IT-Sicherheitsmanagemei
			M 2.340	(A)	Betrieb	Beachtung rechtlicher Rahmenbedingunger	G 2.105	Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarunger
B 1.1	(3.1)	Organisation	M 2.1	(A)	Planung	Festlegung von Verantwortlichkeiten	G 2.1	Fehlende oder unzureichende Regelunge

						und Regelungen für den IT-Einsatz	G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.8	Unkontrollierter Einsatz von Betriebsmittel
			M 2.2	(C)	Planung	Betriebsmittelverwaltung	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.5	Fehlende oder unzureichende Wartun
			M 2.4	(B)	Planung	Regelungen für Wartungs- und Reparaturarbeiten	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.5	Fehlende oder unzureichende Wartun
							G 2.8	Unkontrollierter Einsatz von Betriebsmittel
			M 2.5	(A)	Planung	Aufgabenverteilung und Funktionstrennung	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
			M 2.6	(A)	Betrieb	Vergabe von Zutrittsberechtigungen	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 2.7	Unerlaubte Ausübung von Rechte
			M 2.7	(A)	Betrieb	Vergabe von Zugangsberechtigungen	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte
			M 2.8	(A)	Betrieb	Vergabe von Zugriffsrechten	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte
			M 2.13	(A)	Aussnd.	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmittel	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.8	Unkontrollierter Einsatz von Betriebsmittel
			M 2.14	(A)	Betrieb	Schlüsselverwaltung	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
			M 2.16	(B)	Betrieb	Beaufsichtigung oder Begleitung von Fremdpersonen	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.12	Abhören von Telefongesprächen und Datenübertragunger
							G 5.13	Abhören von Räume
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
							G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
							G 5.102	Sabotage
			M 2.18	(Z)	Betrieb	Kontrollgänge	G 1.4	Feuer
							G 1.5	Wasser
							G 1.7	Unzulässige Temperatur und Luftfeuch

							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.6	Anschlag
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
							G 5.102	Sabotage
			M 2.37	(Z)	Betrieb	"Der aufgeräumte Arbeitsplatz'	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
			M 2.39	(B)	Betrieb	Reaktion auf Verletzungen der Sicherheitspolitik	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 2.7	Unerlaubte Ausübung von Rechte
			M 2.40	(A)	Planung	Rechtzeitige Beteiligung des Personal-/Betriebsrates	G 2.1	Fehlende oder unzureichende Regelungen
			M 2.177	(Z)	Betrieb	Sicherheit bei Umzüger	G 2.1	Fehlende oder unzureichende Regelunge
			M 2.225	(B)	Planung	Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte
B 1.2	(3.2)	Personal	M 3.1	(A)	Umsetzg.	Geregelte Einarbeitung/Einweisung neuer Mitarbeiter	G 2.2	Unzureichende Kenntnis über Regelunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-Systen
							G 5.42	Social Engineering
							G 5.104	Ausspähen von Informatione
			M 3.2	(A)	Umsetzg.	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen	G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
			M 3.3	(A)	Betrieb	Vertretungsregelunger	G 1.1	Personalausfal
			M 3.4	(A)	Betrieb	Schulung vor Programmnutzung	G 2.2	Unzureichende Kenntnis über Regelunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-Systen
							G 3.9	Fehlerhafte Administration des IT-System

							G 3.36	Fehlinterpretation von Ereignissen
							G 3.37	Unproduktive Suchzeiten
							G 3.43	Ungeeigneter Umgang mit Passwörtern
							G 3.44	Sorglosigkeit im Umgang mit Informationen
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
							G 5.2	Manipulation an Daten oder Software
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 3.5	(A)	Betrieb	Schulung zu IT-Sicherheitsmaßnahmen	G 2.2	Unzureichende Kenntnis über Regelungen
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
							G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
							G 3.8	Fehlerhafte Nutzung des IT-Systems
							G 3.43	Ungeeigneter Umgang mit Passwörtern
							G 3.44	Sorglosigkeit im Umgang mit Informationen
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
							G 5.2	Manipulation an Daten oder Software
							G 5.23	Computer-Viren
							G 5.42	Social Engineering
							G 5.43	Makro-Viren
							G 5.80	Hoax
							G 5.104	Ausspähen von Informationen
			M 3.6	(A)	Aussnd.	Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
							G 5.2	Manipulation an Daten oder Software
			M 3.7	(Z)	Betrieb	Anlaufstelle bei persönlichen Problemen	G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
							G 5.2	Manipulation an Daten oder Software
			M 3.8	(Z)	Betrieb	Vermeidung von Störungen des Betriebsklimas	G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
							G 5.2	Manipulation an Daten oder Software
			M 3.10	(A)	Umsetzg.	Auswahl eines vertrauenswürdigen Administrators und Vertreters	G 1.1	Personalausfall
							G 2.7	Unerlaubte Ausübung von Rechten
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
							G 3.9	Fehlerhafte Administration des IT-Systems
							G 3.43	Ungeeigneter Umgang mit Passwörtern
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
							G 5.2	Manipulation an Daten oder Software
			M 3.11	(A)	Betrieb	Schulung des Wartungs- und Administrationspersonals	G 1.2	Ausfall des IT-Systems
							G 2.2	Unzureichende Kenntnis über Regelungen
							G 2.7	Unerlaubte Ausübung von Rechten
							G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
							G 3.8	Fehlerhafte Nutzung des IT-Systems

							G 3.9	Fehlerhafte Administration des IT-System
							G 3.36	Fehlinterpretation von Ereignissen
							G 3.43	Ungeeigneter Umgang mit Passwörtern
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
			M 3.33	(Z)	Umsetzg.	Sicherheitsüberprüfung von Mitarbeitern	G 2.7	Unerlaubte Ausübung von Rechte
							G 5.20	Missbrauch von Administratorrechte
			M 3.50	(Z)	Beschaff.	Auswahl von Personal	G 1.1	Personalausfal
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
			M 3.51	(Z)	Planung	Geeignetes Konzept für Personaleinsatz und -qualifizierung	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-Systen
							G 3.9	Fehlerhafte Administration des IT-System
B 1.3	(3.3)	Notfallvorsorgekonzept	M 6.1	(A)	Planung	Erstellung einer Übersicht über Verfügbarkeitsanforderunger	G 1.2	Ausfall des IT-Systems
			M 6.2	(A)	Planung	Notfall-Definition, Notfall-Verantwortliche	G 1.2	Ausfall des IT-Systems
			M 6.3	(C)	Planung	Erstellung eines Notfall-Handbuche	G 1.2	Ausfall des IT-System
			M 6.4	(B)	Umsetzg.	Dokumentation der Kapazitätsanforderungen der IT-Anwendunger	G 1.2	Ausfall des IT-Systems
			M 6.5	(B)	Umsetzg.	Definition des eingeschränkten IT-Betriebs	G 1.2	Ausfall des IT-Systems
			M 6.6	(B)	Umsetzg.	Untersuchung interner und externer Ausweichmöglichkeiter	G 1.2	Ausfall des IT-Systems
			M 6.7	(A)	Umsetzg.	Regelung der Verantwortung im Notfall	G 1.2	Ausfall des IT-Systems
			M 6.8	(A)	Umsetzg.	Alarmierungsplar	G 1.2	Ausfall des IT-System
			M 6.9	(C)	Umsetzg.	Notfall-Pläne für ausgewählte Schadensereignisse	G 1.2	Ausfall des IT-Systems
			M 6.10	(C)	Umsetzg.	Notfall-Plan für DFÜ-Ausfa	G 1.2	Ausfall des IT-System
			M 6.11	(B)	Umsetzg.	Erstellung eines Wiederanlaufplan	G 1.2	Ausfall des IT-System
			M 6.12	(C)	Betrieb	Durchführung von Notfallübunge	G 1.2	Ausfall des IT-System
			M 6.13	(A)	Umsetzg.	Erstellung eines Datensicherungsplans	G 1.2	Ausfall des IT-Systems
			M 6.14	(B)	Beschaff.	Ersatzbeschaffungsplar	G 1.2	Ausfall des IT-System
			M 6.15	(Z)	Beschaff.	Lieferantenvereinbarunger	G 1.2	Ausfall des IT-System
			M 6.16	(Z)	Umsetzg.	Abschließen von Versicherunge	G 1.2	Ausfall des IT-System
			M 6.75	(Z)	Planung	Redundante Kommunikationsverbindunger	G 1.2	Ausfall des IT-Systems
B 1.4	(3.4)	Datensicherungskonzept	M 2.41	(A)	Umsetzg.	Verpflichtung der Mitarbeiter zur Datensicherunc	G 4.13	Verlust gespeicherter Daten

			M 2.137	(A)	Beschaff.	Beschaffung eines geeigneten Datensicherungssystems	G 4.13	Verlust gespeicherter Daten
			M 6.20	(A)	Betrieb	Geeignete Aufbewahrung der Backup-Datenträger	G 4.13	Verlust gespeicherter Daten
			M 6.21	(C)	Umsetzg.	Sicherungskopie der eingesetzten Software	G 4.13	Verlust gespeicherter Daten
			M 6.22	(A)	Betrieb	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherunger	G 4.13	Verlust gespeicherter Daten
			M 6.32	(A)	Betrieb	Regelmäßige Datensicherung	G 4.13	Verlust gespeicherter Dater
			M 6.33	(B)	Planung	Entwicklung eines Datensicherungskonzepts	G 4.13	Verlust gespeicherter Daten
			M 6.34	(B)	Planung	Erhebung der Einflussfaktoren der Datensicherunc	G 4.13	Verlust gespeicherter Daten
			M 6.35	(B)	Planung	Festlegung der Verfahrensweise für die Datensicherunc	G 4.13	Verlust gespeicherter Daten
			M 6.36	(A)	Planung	Festlegung des Minimaldatensicherungskonzeptes	G 4.13	Verlust gespeicherter Daten
			M 6.37	(A)	Umsetzg.	Dokumentation der Datensicherung	G 4.13	Verlust gespeicherter Dater
			M 6.41	(A)	Notfallv	Übungen zur Datenrekonstruktio	G 4.13	Verlust gespeicherter Dater
B 1.6	(3.6)	Computer-Virenschutzkonzept	M 2.154	(A)	Planung	Erstellung eines Computer-Virenschutzkonzepts	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.8	Unkontrollierter Einsatz von Betriebsmitte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
			M 2.155	(A)	Planung	Identifikation potentiell von Computer-Viren betroffener IT-Systeme	G 2.8	Unkontrollierter Einsatz von Betriebsmitte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
			M 2.156	(A)	Planung	Auswahl einer geeigneten Computer-Virenschutz-Strategie	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
			M 2.157	(A)	Beschaff.	Auswahl eines geeigneten Computer-Viren-Suchprogramms	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.80	Hoax
			M 2.158	(A)	Betrieb	Meldung von Computer-Virusinfektionen	G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren

							G 5.80	Hoax
			M 2.159	(A)	Betrieb	Aktualisierung der eingesetzten Computer-Viren-Suchprogramme	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.80	Hoax
			M 2.160	(A)	Planung	Regelungen zum Computer-Virenschutz	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
			M 2.224	(A)	Betrieb	Vorbeugung gegen Trojanische Pferde	G 2.1	Fehlende oder unzureichende Regelunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.21	Trojanische Pferde
			M 4.3	(A)	Betrieb	Regelmäßiger Einsatz eines Anti-Viren-Programms	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.80	Hoax
			M 4.33	(A)	Betrieb	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragun	G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.84	(A)	Umsetzg.	Nutzung der BIOS-Sicherheitsmechanismer	G 5.23	Computer-Viren
			M 4.253	(A)	Planun	Schutz vor Spywar	G 5.127	Spyware
			M 6.23	(A)	Notfallv.	Verhaltensregeln bei Auftreten eines Computer-Virus	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.2	Manipulation an Daten oder Softwar
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
B 1.7	(3.7)	Kryptokonzept	M 2.46	(A)	Umsetzg.	Geeignetes Schlüsselmanagement	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselun
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 4.34	Ausfall eines Kryptomodul
							G 4.35	Unsichere kryptographische Algorithme
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
			M 2.161	(A)	Planung	Entwicklung eines Kryptokonzepts	G 4.35	Unsichere kryptographische Algorithme

							G 5.81	Unautorisierte Benutzung eines Kryptomodu
							G 5.82	Manipulation eines Kryptomodul:
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
			M 2.162	(A)	Planung	Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte	G 5.82	Manipulation eines Kryptomodul:
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
			M 2.163	(A)	Planung	Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte	G 3.32	Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptographischen Verfahre
							G 5.82	Manipulation eines Kryptomodul:
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
			M 2.164	(A)	Planung	Auswahl eines geeigneten kryptographischen Verfahrens	G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselunc
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 4.33	Schlechte oder fehlende Authentikatio
							G 4.35	Unsichere kryptographische Algorithme
							G 5.27	Nichtanerkennung einer Nachrich
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.82	Manipulation eines Kryptomodul:
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.165	(A)	Beschaff.	Auswahl eines geeigneten kryptographischen Produktes	G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselunc
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.32	Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptographischen Verfahre
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.33	Schlechte oder fehlende Authentikatio
							G 4.34	Ausfall eines Kryptomodul:
							G 5.27	Nichtanerkennung einer Nachrich
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.81	Unautorisierte Benutzung eines Kryptomodu
							G 5.82	Manipulation eines Kryptomodul:
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.166	(A)	Planung	Regelung des Einsatzes von Kryptomodulen	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze

							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.34	Ausfall eines Kryptomodul:
							G 4.35	Unsichere kryptographische Algorithme
							G 4.36	Fehler in verschlüsselten Date
							G 5.81	Unautorisierte Benutzung eines Kryptomodu
							G 5.82	Manipulation eines Kryptomodul:
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
			M 3.23	(A)	Planung	Einführung in kryptographische Grundbegriffe	G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselunc
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.33	Fehlbedienung von Kryptomodule
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.35	Unsichere kryptographische Algorithme
							G 4.36	Fehler in verschlüsselten Date
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
			M 4.85	(Z)	Beschaff.	Geeignetes Schnittstellendesign bei Kryptomoduler	G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
			M 4.86	(A)	Umsetzg.	Sichere Rollenteilung und Konfiguration der Kryptomodule	G 2.1	Fehlende oder unzureichende Regelunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.33	Fehlbedienung von Kryptomodule
							G 5.81	Unautorisierte Benutzung eines Kryptomodu
							G 5.82	Manipulation eines Kryptomodul:
			M 4.87	(Z)	Umsetzg.	Physikalische Sicherheit von Kryptomodulen	G 4.34	Ausfall eines Kryptomodul:
							G 5.81	Unautorisierte Benutzung eines Kryptomodu
							G 5.82	Manipulation eines Kryptomodul:
							G 5.83	Kompromittierung kryptographischer Schlüsse
			M 4.88	(A)	Beschaff.	Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen	G 4.22	Software-Schwachstellen oder -Fehle
							G 5.81	Unautorisierte Benutzung eines Kryptomodu
							G 5.82	Manipulation eines Kryptomodul:
							G 5.83	Kompromittierung kryptographischer Schlüsse
			M 4.89	(Z)	Umsetzg.	Abstrahlsicherheit	G 5.82	Manipulation eines Kryptomodul:
							G 5.83	Kompromittierung kryptographischer Schlüsse
			M 4.90	(A)	Planung	Einsatz von kryptographischen Verfahren auf den verschiedener	G 3.33	Fehlbedienung von Kryptomodule
							G 4.22	Software-Schwachstellen oder -Fehle
			M 6.56	(A)	Notfallv.	Datensicherung bei Einsatz kryptographischer Verfahren	G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselunc
							G 4.34	Ausfall eines Kryptomodul:
							G 4.36	Fehler in verschlüsselten Date
							G 5.83	Kompromittierung kryptographischer Schlüsse

B 1.8	(3.8)	Behandlung von Sicherheitsvorfällen	M 6.58	(A)	Planung	Etablierung eines Managementsystems zur Behandlung von Sicherheitsvorfällen	G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfällen
			M 6.59	(A)	Planung	Festlegung von Verantwortlichkeiten bei Sicherheitsvorfäller	G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfällen
			M 6.60	(A)	Planung	Verhaltensregeln und Meldewege bei Sicherheitsvorfäller	G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfällen
			M 6.61	(C)	Planung	Eskalationsstrategie für Sicherheitsvorfälle	G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfällen
			M 6.62	(B)	Planung	Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfälle	G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfällen
			M 6.63	(A)	Betrieb	Untersuchung und Bewertung eines Sicherheitsvorfalls	G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfällen
			M 6.64	(A)	Betrieb	Behebung von Sicherheitsvorfälle	G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfälle
			M 6.65	(A)	Betrieb	Benachrichtigung betroffener Stelle	G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfälle
			M 6.66	(B)	Betrieb	Nachbereitung von Sicherheitsvorfällen	G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfällen
			M 6.67	(Z)	Planung	Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle	G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfällen
			M 6.68	(C)	Betrieb	Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfälle	G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfällen
B 1.9	(3.9)	Hard- und Software-Management	M 1.29	(Z)	Umsetzg.	Geeignete Aufstellung eines IT-Systems	G 1.4	Feuer
							G 1.5	Wasser
							G 1.8	Staub, Verschmutzung
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.5	Unbeabsichtigte Leitungsbeschädigung
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.35	Server im laufenden Betrieb ausschalte
							G 4.31	Ausfall oder Störung von Netzkomponente
							G 4.38	Ausfall von Komponenten eines Netz- und Systemmanagementsystems
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
			M 1.46	(Z)	Betrieb	Einsatz von Diebstahl-Sicherunge	G 5.4	Diebstahl
			M 2.3	(B)	Planung	Datenträgerverwaltung	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.10	Nicht fristgerecht verfügbare Datenträge
							G 5.2	Manipulation an Daten oder Softwar
			M 2.9	(A)	Planung	Nutzungsverbot nicht freigegebener	G 2.1	Fehlende oder unzureichende Regelunge

						Hard- und Software	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.43	Undokumentierte Funktionen
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.26	Analyse des Nachrichtenflusse
			M 2.10	(C)	Betrieb	Überprüfung des Hard- und Software-Bestandes	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.26	Analyse des Nachrichtenflusse
			M 2.11	(A)	Planung	Regelung des Passwortgebrauchs	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
			M 2.12	(C)	Planung	Betreuung und Beratung von IT-Benutzern	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
			M 2.22	(Z)	Betrieb	Hinterlegen des Passwortes	G 1.1	Personalausfal
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
			M 2.25	(A)	Umsetzg.	Dokumentation der Systemkonfiguration	G 1.1	Personalausfal
							G 1.2	Ausfall des IT-System
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
			M 2.26	(A)	Umsetzg.	Ernennung eines Administrators und eines Vertreters	G 1.1	Personalausfal
							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar

						G 5.9	Unberechtigte IT-Nutzun
			M 2.30	(A)	Planung	Regelung für die Einrichtung von Benutzern / Benutzergruppen	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
			M 2.34	(A)	Betrieb	Dokumentation der Veränderungen an einem bestehenden System	G 1.1	Personalausfal
							G 1.2	Ausfall des IT-System
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.2	Manipulation an Daten oder Softwar
			M 2.35	(B)	Betrieb	Informationsbeschaffung über Sicherheitslücken des Systems	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 4.8	Bekanntwerden von Softwareschwachstelle
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.35	Unsichere kryptographische Algorithme
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemer
							G 5.82	Manipulation eines Kryptomodul
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
							G 5.87	Web-Spoofing
			M 2.38	(B)	Umsetzg.	Aufteilung der Administrationstätigkeiten	G 1.1	Personalausfal
							G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.9	Unberechtigte IT-Nutzun
			M 2.62	(B)	Beschaff.	Software-Abnahme- und Freigabe-Verfahren	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.43	Undokumentierte Funktione
			M 2.64	(A)	Betrieb	Kontrolle der Protokolldateien	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen

							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.22	Fehlende Auswertung von Protokolldate
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
			M 2.65	(C)	Betrieb	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System	G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 3.17	Kein ordnungsgemäßer PC-Benutzerwechs
			M 2.69	(B)	Umsetzg.	Einrichtung von Standardarbeitsplätzen	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 4.22	Software-Schwachstellen oder -Fehle
			M 2.110	(A)	Betrieb	Datenschutzaspekte bei der Protokollierung	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
			M 2.111	(A)	Umsetzg.	Bereithalten von Handbüchern	G 2.2	Unzureichende Kenntnis über Regelunge
							G 3.44	Sorglosigkeit im Umgang mit Informatione
			M 2.138	(B)	Umsetzg.	Strukturierte Datenhaltun	G 3.44	Sorglosigkeit im Umgang mit Informatione
			M 2.167	(B)	Aussnd.	Sicheres Löschen von Datenträgern	G 2.1	Fehlende oder unzureichende Regelunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
			M 2.182	(A)	Betrieb	Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.22	Fehlende Auswertung von Protokolldate
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
			M 2.204	(A)	Umsetzg.	Verhinderung ungesicherter Netzzugänge	G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.2	Manipulation an Daten oder Softwar
			M 2.214	(A)	Planung	Konzeption des IT-Betriebs	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
			M 2.215	(B)	Betrieb	Fehlerbehandlun	G 3.44	Sorglosigkeit im Umgang mit Informatione
			M 2.216	(C)	Planung	Genehmigungsverfahren für IT-Komponenten	G 2.1	Fehlende oder unzureichende Regelungen
			M 2.217	(B)	Planung	Sorgfältige Einstufung und Umgang mi	G 2.1	Fehlende oder unzureichende Regelunge

						Informationen, Anwendungen und Systemen	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.44	Sorglosigkeit im Umgang mit Informatione
			M 2.218	(C)	Planung	Regelung der Mitnahme von Datenträgern und IT-Komponente	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.10	Nicht fristgerecht verfügbare Datenträge
			M 2.219	(A)	Betrieb	Kontinuierliche Dokumentation der Informationsverarbeitung	G 2.1	Fehlende oder unzureichende Regelunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
			M 2.220	(A)	Planung	Richtlinien für die Zugriffs- bzw. Zugangskontrolle	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
			M 2.221	(B)	Planung	Änderungsmanagement	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
			M 2.223	(B)	Planung	Sicherheitsvorgaben für die Nutzung von Standardsoftware	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.43	Undokumentierte Funktionel
			M 2.226	(A)	Planung	Regelungen für den Einsatz von Fremdpersonal	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
			M 3.26	(A)	Betrieb	Einweisung des Personals in den sicheren Umgang mit IT	G 2.2	Unzureichende Kenntnis über Regelunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 5.21	Trojanische Pferde
			M 4.1	(A)	Umsetzg.	Passwortschutz für IT-Systeme	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
			M 4.7	(A)	Umsetzg.	Änderung voreingestellter Passwörter	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemer
			M 4.65	(C)	Umsetzg.	Test neuer Hard- und Software	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 4.22	Software-Schwachstellen oder -Fehle

							G 4.43	Undokumentierte Funktione
							G 5.21	Trojanische Pferde
			M 4.78	(A)	Betrieb	Sorgfältige Durchführung von Konfigurationsänderungen	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 4.22	Software-Schwachstellen oder -Fehle
			M 4.84	(A)	Umsetzg.	Nutzung der BIOS-Sicherheitsmechanismen	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.2	Manipulation an Daten oder Softwar
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.107	(B)	Betrieb	Nutzung von Hersteller-Ressourcen	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Net
							G 3.11	Fehlerhafte Konfiguration von sendma
			M 4.109	(Z)	Betrieb	Software-Reinstallation bei Arbeitsplatzrechnern	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.21	Trojanische Pferde
			M 4.133	(Z)	Planung	Geeignete Auswahl von Authentikationsmechanismer	G 5.2	Manipulation an Daten oder Software
			M 4.134	(C)	Planung	Wahl geeigneter Datenformate	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
			M 4.135	(A)	Umsetzg.	Restriktive Vergabe von Zugriffsrechten auf Systemdateien	G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
							G 5.2	Manipulation an Daten oder Softwar
			M 4.234	(B)	Aussnd.	Aussonderung von IT-Systemen	G 4.13	Verlust gespeicherter Dater
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 4.254	(Z)	Betrieb	Sicherer Einsatz von drahtlosen Tastaturen und Mäusen	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 5.68	(Z)	Planung	Einsatz von Verschlüsselungsverfahren zur Netzkommunikation	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
			M 5.77	(Z)	Planung	Bildung von Teilnetzen	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
							G 5.2	Manipulation an Daten oder Softwar
			M 5.87	(C)	Planung	Vereinbarung über die Anbindung an	G 2.1	Fehlende oder unzureichende Regelunge

						Netze Dritter	G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
							G 5.2	Manipulation an Daten oder Softwar
			M 5.88	(C)	Planung	Vereinbarung über Datenaustausch mit Dritten	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 3.44	Sorglosigkeit im Umgang mit Informatione
			M 6.21	(C)	Notfallv.	Sicherungskopie der eingesetzten Software	G 1.2	Ausfall des IT-System
							G 1.4	Feuer
							G 1.5	Wasser
							G 1.8	Staub, Verschmutzun
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-Systen
							G 4.1	Ausfall der Stromversorgun
							G 4.7	Defekte Datenträger
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 6.27	(C)	Notfallv	Sicheres Update des BIOS	G 1.2	Ausfall des IT-System
B 1.10	(9.1)	Standardsoftware	M 2.66	(Z)	Beschaff.	Beachtung des Beitrags der Zertifizierung für die Beschaffung	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 4.8	Bekanntwerden von Softwareschwachstelle
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.21	Trojanische Pferde
			M 2.79	(A)	Planung	Festlegung der Verantwortlichkeiten im Bereich Standardsoftware	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
			M 2.80	(A)	Planung	Erstellung eines Anforderungskatalogs für Standardsoftware	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
							G 2.27	Fehlende oder unzureichende Dokumentatio
							G 4.22	Software-Schwachstellen oder -Fehle
			M 2.81	(A)	Beschaff.	Vorauswahl eines geeigneten Standardsoftwareproduktes	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren

							G 2.27	Fehlende oder unzureichende Dokumentatio
							G 4.22	Software-Schwachstellen oder -Fehle
			M 2.82	(B)	Planung	Entwicklung eines Testplans für Standardsoftware	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
							G 2.27	Fehlende oder unzureichende Dokumentatio
							G 2.29	Softwaretest mit Produktionsdater
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 2.83	(B)	Umsetzg.	Testen von Standardsoftware	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
							G 2.27	Fehlende oder unzureichende Dokumentatio
							G 2.29	Softwaretest mit Produktionsdater
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 2.84	(A)	Umsetzg.	Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 4.22	Software-Schwachstellen oder -Fehle
			M 2.85	(A)	Umsetzg.	Freigabe von Standardsoftware	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
							G 2.28	Verstöße gegen das Urheberrech
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
			M 2.86	(B)	Umsetzg.	Sicherstellen der Integrität von Standardsoftware	G 4.22	Software-Schwachstellen oder -Fehle
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 2.87	(A)	Umsetzg.	Installation und Konfiguration von Standardsoftware	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.21	Trojanische Pferde
			M 2.88	(A)	Betrieb	Lizenzverwaltung und Versionskontrolle von Standardsoftware	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.28	Verstöße gegen das Urheberrech
			M 2.89	(C)	Aussnd.	Deinstallation von Standardsoftwar	G 2.28	Verstöße gegen das Urheberrech
			M 2.90	(A)	Umsetzg.	Überprüfung der Lieferung	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.27	Fehlende oder unzureichende Dokumentatio
			M 4.34	(Z)	Planung	Einsatz von Verschlüsselung, Checksummen oder Digitalen	G 4.22	Software-Schwachstellen oder -Fehle
							G 5.21	Trojanische Pferde

						Signaturen	G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.42	(Z)	Umsetzg.	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung	G 1.2	Ausfall des IT-Systems
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.17	Kein ordnungsgemäßer PC-Benutzerwechse
							G 4.7	Defekte Datenträger
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
B 1.11	(3.10)	Outsourcing	M 2.40	(Z)	Planung	Rechtzeitige Beteiligung des Personal-/Betriebsrates	G 2.88	Störung des Betriebsklimas durch ein Outsourcing-Vorhaben
			M 2.42	(A)	Planung	Festlegung der möglichen Kommunikationspartner	G 2.1	Fehlende oder unzureichende Regelunge
							G 5.42	Social Engineering
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 2.221	(A)	Betrieb	Änderungsmanagement	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
							G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
							G 2.89	Mangelhafte IT-Sicherheit in der Outsourcing-Einführungsphase
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
							G 5.107	Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister
			M 2.226	(A)	Planung	Regelungen für den Einsatz von Fremdpersonal	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
			M 2.250	(A)	Planung	Festlegung einer Outsourcing-Strategie	G 2.66	Unzureichendes IT-Sicherheitsmanageme
							G 2.83	Fehlerhafte Outsourcing-Strategi
							G 2.86	Abhängigkeit von einem Outsourcing-Dienstleiste
			M 2.251	(A)	Planung	Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaber	G 2.84	Unzulängliche vertragliche Regelungen mit einem externen Dienstleiste
							G 2.86	Abhängigkeit von einem Outsourcing-Dienstleiste
			M 2.252	(A)	Beschaff.	Wahl eines geeigneten Outsourcing-	G 2.86	Abhängigkeit von einem Outsourcing-Dienstleiste

						Dienstleisters	G 2.88	Störung des Betriebsklimas durch ein Outsourcing-Vorhaben
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 4.48	Ausfall der Systeme eines Outsourcing-Dienstleister
							G 5.107	Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister
			M 2.253	(A)	Umsetzg.	Vertragsgestaltung mit dem Outsourcing-Dienstleister	G 1.10	Ausfall eines Weitverkehrsnetze
							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
							G 2.66	Unzureichendes IT-Sicherheitsmanagemer
							G 2.84	Unzulängliche vertragliche Regelungen mit einem externen Dienstleiste
							G 2.85	Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens
							G 2.86	Abhängigkeit von einem Outsourcing-Dienstleiste
							G 2.88	Störung des Betriebsklimas durch ein Outsourcing-Vorhaben
							G 2.90	Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.254	(A)	Planung	Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben	G 1.10	Ausfall eines Weitverkehrsnetze
							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
							G 2.47	Ungesicherter Akten- und Datenträgertranspo
							G 2.66	Unzureichendes IT-Sicherheitsmanagemer
							G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
							G 2.90	Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 4.33	Schlechte oder fehlende Authentikatio
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.20	Missbrauch von Administratorrechte
							G 5.42	Social Engineering
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
							G 5.107	Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister

			M 2.255	(A)	Umsetzg.	Sichere Migration bei Outsourcing-Vorhaben	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
							G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechter
							G 2.89	Mangelhafte IT-Sicherheit in der Outsourcing-Einführungsphase
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.42	Social Engineering
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.256	(A)	Betrieb	Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.20	Missbrauch von Administratorrechte
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.307	(A)	Aussnd.	Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.84	Unzulängliche vertragliche Regelungen mit einem externen Dienstleiste
							G 2.85	Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens
							G 2.86	Abhängigkeit von einem Outsourcing-Dienstleiste
			M 3.33	(Z)	Betrieb	Sicherheitsüberprüfung von Mitarbeitern	G 2.7	Unerlaubte Ausübung von Rechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
							G 5.107	Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister
			M 5.87	(A)	Umsetzg.	Vereinbarung über die Anbindung an Netze Dritter	G 2.1	Fehlende oder unzureichende Regelunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 5.88	(A)	Umsetzg.	Vereinbarung über Datenaustausch mit Dritten	G 2.1	Fehlende oder unzureichende Regelunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 6.70	(A)	Notfallv.	Erstellen eines Notfallplans für den	G 1.10	Ausfall eines Weitverkehrsnetze

						Ausfall des RAS-Systems	G 2.90	Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister
			M 6.83	(A)	Notfallv.	Notfallvorsorge beim Outsourcing	G 1.10	Ausfall eines Weitverkehrsnetze
							G 2.93	Unzureichendes Notfallvorsorgekonzept beim Outsourcinc
							G 4.34	Ausfall eines Kryptomodul:
							G 4.48	Ausfall der Systeme eines Outsourcing-Dienstleister
B 1.12	(9.5)	Archivierung	M 1.59	(B)	Umsetzg.	Geeignete Aufstellung von Archivsystemen	G 1.7	Unzulässige Temperatur und Luftfeuch
							G 1.9	Datenverlust durch starke Magnetfelde
							G 1.14	Datenverlust durch starkes Lich
							G 2.82	Fehlerhafte Planung des Aufstellungsortes von Archivsystemer
							G 3.35	Server im laufenden Betrieb ausschalte
							G 4.31	Ausfall oder Störung von Netzkomponente
							G 5.2	Manipulation an Daten oder Softwar
							G 5.6	Anschlag
							G 5.82	Manipulation eines Kryptomodul:
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.102	Sabotage
							G 5.105	Verhinderung der Dienste von Archivsysteme
			M 1.60	(A)	Betrieb	Geeignete Lagerung von Archivmedier	G 1.7	Unzulässige Temperatur und Luftfeuch
							G 1.9	Datenverlust durch starke Magnetfelde
							G 1.14	Datenverlust durch starkes Lich
							G 4.7	Defekte Datenträger
							G 4.13	Verlust gespeicherter Dater
							G 5.2	Manipulation an Daten oder Softwar
							G 5.6	Anschlag
							G 5.29	Unberechtigtes Kopieren der Datenträge
							G 5.82	Manipulation eines Kryptomodul:
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.102	Sabotage
							G 5.105	Verhinderung der Dienste von Archivsysteme
			M 2.242	(A)	Planung	Zielsetzung der elektronischen Archivierung	G 2.73	Fehlende Revisionsmöglichkeit von Archivsysteme
							G 2.82	Fehlerhafte Planung des Aufstellungsortes von Archivsystemer
			M 2.243	(A)	Planung	Entwicklung des Archivierungskonzepts	G 2.76	Unzureichende Dokumentation von Archivzugriffe
							G 2.77	Unzulängliche Übertragung von Papierdaten in elektronische Archive
							G 2.78	Unzulängliche Auffrischung von Datenbeständen bei der Archivierunc
							G 2.79	Unzureichende Erneuerung von digitalen Signaturen bei der Archivierunc
							G 2.80	Unzureichende Durchführung von Revisionen bei der Archivierunc

							G 2.81	Unzureichende Vernichtung von Datenträgern bei der Archivierung
			M 2.244	(A)	Planung	Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung	G 2.73	Fehlende Revisionsmöglichkeit von Archivsysteme
							G 2.74	Unzureichende Ordnungskriterien für Archiv
							G 2.75	Mangelnde Kapazität von Archivdatenträger
							G 2.76	Unzureichende Dokumentation von Archivzugriffe
							G 2.77	Unzulängliche Übertragung von Papierdaten in elektronische Archive
							G 2.78	Unzulängliche Auffrischung von Datenbeständen bei der Archivierung
							G 2.79	Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung
							G 2.81	Unzureichende Vernichtung von Datenträgern bei der Archivierung
							G 2.82	Fehlerhafte Planung des Aufstellungsortes von Archivsystemer
			M 2.245	(A)	Planung	Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung	G 2.76	Unzureichende Dokumentation von Archivzugriffe
							G 2.77	Unzulängliche Übertragung von Papierdaten in elektronische Archive
							G 2.78	Unzulängliche Auffrischung von Datenbeständen bei der Archivierung
							G 2.81	Unzureichende Vernichtung von Datenträgern bei der Archivierung
			M 2.246	(A)	Planung	Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung	G 2.76	Unzureichende Dokumentation von Archivzugriffe
							G 2.77	Unzulängliche Übertragung von Papierdaten in elektronische Archive
							G 2.78	Unzulängliche Auffrischung von Datenbeständen bei der Archivierung
							G 2.79	Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung
							G 2.80	Unzureichende Durchführung von Revisionen bei der Archivierung
							G 2.81	Unzureichende Vernichtung von Datenträgern bei der Archivierung
			M 2.257	(C)	Betrieb	Überwachung der Speicherressourcen von Archivmedier	G 2.75	Mangelnde Kapazität von Archivdatenträger
							G 4.20	Datenverlust bei erschöpftem Speichermedium
			M 2.258	(A)	Betrieb	Konsistente Indizierung von Dokumenten bei der Archivierung	G 2.74	Unzureichende Ordnungskriterien für Archiv
							G 4.45	Verzögerte Archivauskunf
			M 2.259	(Z)	Planung	Einführung eines übergeordneten Dokumentenmanagements	G 4.45	Verzögerte Archivauskunft
			M 2.260	(B)	Betrieb	Regelmäßige Revision des Archivierungsprozesses	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.74	Unzureichende Ordnungskriterien für Archiv
							G 2.77	Unzulängliche Übertragung von Papierdaten in elektronische Archive

							G 2.80	Unzureichende Durchführung von Revisionen bei der Archivierung
							G 3.55	Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsysteme
			M 2.261	(B)	Betrieb	Regelmäßige Marktbeobachtung von Archivsystemen	G 2.72	Unzureichende Migration von Archivsysteme
							G 2.75	Mangelnde Kapazität von Archivdatenträger
							G 3.54	Verwendung ungeeigneter Datenträger bei der Archivierung
							G 4.47	Veralten von Kryptoverfahre
			M 2.262	(A)	Planung	Regelung der Nutzung von Archivsystemer	G 2.7	Unerlaubte Ausübung von Rechten
			M 2.263	(A)	Betrieb	Regelmäßige Aufbereitung von archivierten Datenbeständen	G 2.72	Unzureichende Migration von Archivsysteme
							G 2.79	Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung
							G 4.13	Verlust gespeicherter Dater
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.264	(B)	Betrieb	Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung	G 4.47	Veralten von Kryptoverfahren
			M 2.265	(Z)	Planung	Geeigneter Einsatz digitaler Signaturen bei der Archivierung	G 2.79	Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung
							G 4.47	Veralten von Kryptoverfahre
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.266	(C)	Umsetzg.	Regelmäßige Erneuerung technischer Archivsystem-Komponenten	G 2.72	Unzureichende Migration von Archivsysteme
							G 4.7	Defekte Datenträger
							G 4.13	Verlust gespeicherter Dater
							G 4.20	Datenverlust bei erschöpftem Speichermediun
							G 4.45	Verzögerte Archivauskunf
			M 3.2	(A)	Umsetzg.	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.77	Unzulängliche Übertragung von Papierdaten in elektronische Archive
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.55	Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsysteme
							G 5.2	Manipulation an Daten oder Softwar
			M 3.34	(A)	Umsetzg.	Einweisung in die Administration des Archivsystems	G 2.78	Unzulängliche Auffrischung von Datenbeständen bei der Archivierung
							G 2.81	Unzureichende Vernichtung von Datenträgern bei der Archivierung
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze

							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.55	Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsysteme
							G 5.6	Anschlag
							G 5.106	Unberechtigtes Überschreiben oder Löschen von Archivmedien
			M 3.35	(A)	Umsetzg.	Einweisung der Benutzer in die Bedienung des Archivsystems	G 2.77	Unzulängliche Übertragung von Papierdaten in elektronische Archive
							G 2.78	Unzulängliche Auffrischung von Datenbeständen bei der Archivierung
							G 2.79	Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung
							G 2.81	Unzureichende Vernichtung von Datenträgern bei der Archivierung
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.55	Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsysteme
							G 5.6	Anschlag
			M 4.168	(A)	Beschaff.	Auswahl eines geeigneten Archivsystems	G 2.73	Fehlende Revisionsmöglichkeit von Archivsysteme
							G 2.75	Mangelnde Kapazität von Archivdatenträger
							G 3.54	Verwendung ungeeigneter Datenträger bei der Archivierung
							G 4.26	Ausfall einer Datenbank
							G 4.31	Ausfall oder Störung von Netzkomponente
							G 4.45	Verzögerte Archivauskunf
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.169	(A)	Beschaff.	Verwendung geeigneter Archivmedier	G 5.85	Integritätsverlust schützenswerter Information
			M 4.170	(A)	Beschaff.	Auswahl geeigneter Datenformate für die Archivierung von Dokumente	G 5.85	Integritätsverlust schützenswerter Informationen
			M 4.171	(A)	Betrieb	Schutz der Integrität der Index-Datenbank von Archivsystemen	G 2.74	Unzureichende Ordnungskriterien für Archiv
							G 3.35	Server im laufenden Betrieb ausschalte
							G 4.26	Ausfall einer Datenbank
							G 4.30	Verlust der Datenbankintegrität/-konsisten
							G 4.31	Ausfall oder Störung von Netzkomponente
							G 4.45	Verzögerte Archivauskunf
							G 4.46	Fehlerhafte Synchronisierung von Indexdaten bei der Archivierung
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.172	(C)	Betrieb	Protokollierung der Archivzugriffe	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.75	Mangelnde Kapazität von Archivdatenträger
							G 2.76	Unzureichende Dokumentation von Archivzugriffe
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze

							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.35	Server im laufenden Betrieb ausschalte
							G 3.55	Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsysteme
							G 4.7	Defekte Datenträger
							G 4.13	Verlust gespeicherter Dater
							G 4.20	Datenverlust bei erschöpftem Speichermediun
							G 4.45	Verzögerte Archivauskunf
							G 5.2	Manipulation an Daten oder Softwar
							G 5.6	Anschlag
							G 5.29	Unberechtigtes Kopieren der Datenträge
							G 5.82	Manipulation eines Kryptomodul
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.102	Sabotage
							G 5.105	Verhinderung der Dienste von Archivsysteme
							G 5.106	Unberechtigtes Überschreiben oder Löschen von Archivmedien
			M 4.173	(B)	Betrieb	Regelmäßige Funktions- und Recoverytests bei der Archivierun	G 4.7	Defekte Datenträger
							G 4.13	Verlust gespeicherter Dater
			M 6.84	(A)	Notfallv.	Regelmäßige Datensicherung der System- und Archivdaten	G 1.2	Ausfall des IT-System
							G 1.9	Datenverlust durch starke Magnetfelde
							G 1.14	Datenverlust durch starkes Lich
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.35	Server im laufenden Betrieb ausschalte
							G 3.54	Verwendung ungeeigneter Datenträger bei der Archivierun
							G 4.7	Defekte Datenträger
							G 4.13	Verlust gespeicherter Dater
							G 4.26	Ausfall einer Datenban
							G 4.30	Verlust der Datenbankintegrität/-konsisten
							G 4.31	Ausfall oder Störung von Netzkomponente
							G 5.2	Manipulation an Daten oder Softwar
							G 5.6	Anschlag
							G 5.102	Sabotage
							G 5.106	Unberechtigtes Überschreiben oder Löschen von Archivmedien
B 1.13	(3.11)	IT-Sicherheitssensibilisierung und -schulung	M 2.198	(A)	Betrieb	Sensibilisierung der Mitarbeiter für IT-Sicherheit	G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.102	Unzureichende Sensibilisierung für IT-Sicherhe
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme

							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 3.77	Mangelhafte Akzeptanz von IT-Sicherheitsmaßnahm
							G 5.42	Social Engineering
							G 5.104	Ausspähen von Informatione
			M 2.312	(A)	Planung	Konzeption eines Schulungs- und Sensibilisierungsprogramms zur IT-Sicherheit	G 2.102	Unzureichende Sensibilisierung für IT-Sicherhe
							G 2.103	Unzureichende Schulung der Mitarbeite
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 3.77	Mangelhafte Akzeptanz von IT-Sicherheitsmaßnahm
			M 3.4	(A)	Betrieb	Schulung vor Programmnutzung	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.8	Fehlerhafte Nutzung des IT-Systems
							G 3.44	Sorglosigkeit im Umgang mit Informatione
			M 3.5	(A)	Umsetzg.	Schulung zu IT-Sicherheitsmaßnahmen	G 2.2	Unzureichende Kenntnis über Regelunge
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 3.77	Mangelhafte Akzeptanz von IT-Sicherheitsmaßnahm
			M 3.11	(A)	Betrieb	Schulung des Wartungs- und Administrationspersonals	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.104	Ausspähen von Informatione
			M 3.26	(A)	Betrieb	Einweisung des Personals in den sicheren Umgang mit IT	G 2.2	Unzureichende Kenntnis über Regelunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-Systems
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.42	Social Engineering
							G 5.104	Ausspähen von Informatione
			M 3.44	(A)	Planung	Sensibilisierung des Managements für IT-Sicherheit	G 2.102	Unzureichende Sensibilisierung für IT-Sicherhe
							G 2.103	Unzureichende Schulung der Mitarbeite
							G 3.77	Mangelhafte Akzeptanz von IT-Sicherheitsmaßnahm
			M 3.45	(A)	Umsetzg.	Planung von Schulungsinhalten zur IT-Sicherheit	G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-Systems
							G 3.9	Fehlerhafte Administration des IT-System

							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 3.77	Mangelhafte Akzeptanz von IT-Sicherheitsmaßnahm
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.42	Social Engineering
							G 5.104	Ausspähen von Informatione
			M 3.46	(A)	Umsetzg.	Ansprechpartner zu Sicherheitsfragen	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 3.8	Fehlerhafte Nutzung des IT-Syster
							G 3.44	Sorglosigkeit im Umgang mit Informatione
			M 3.47	(Z)	Betrieb	Durchführung von Planspielen zur IT-Sicherheit	G 2.102	Unzureichende Sensibilisierung für IT-Sicherhe
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 3.77	Mangelhafte Akzeptanz von IT-Sicherheitsmaßnahm
							G 5.42	Social Engineering
			M 3.48	(A)	Beschaff.	Auswahl von Trainern oder Schulungsanbietern	G 2.102	Unzureichende Sensibilisierung für IT-Sicherhe
							G 2.103	Unzureichende Schulung der Mitarbeite
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.77	Mangelhafte Akzeptanz von IT-Sicherheitsmaßnahm
			M 3.49	(B)	Umsetzg.	Schulung zur Vorgehensweise nach IT-Grundschutz	G 2.102	Unzureichende Sensibilisierung für IT-Sicherhe
							G 2.103	Unzureichende Schulung der Mitarbeite
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 5.42	Social Engineering
B 2.1	(4.1)	Gebäude	M 1.1	(A)	Umsetzg.	Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften	G 1.3	Blitz
							G 1.4	Feuer
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 1.2	(A)	Umsetzg.	Regelungen für Zutritt zu Verteilern	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 1.3	(A)	Planung	Angepasste Aufteilung der Stromkreise	G 1.4	Feuer
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 1.4	(B)	Planung	Blitzschutzeinrichtungen	G 1.3	Blitz
							G 1.4	Feuer
			M 1.5	(Z)	Planung	Galvanische Trennung von Außenleitunger	G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 1.6	(A)	Umsetzg.	Einhaltung von Brandschutzvorschriften	G 1.4	Feuer

							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 1.7	(A)	Planung	Handfeuerlöscher	G 1.4	Feuer
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 1.8	(A)	Planung	Raumbelegung unter Berücksichtigung von Brandlaster	G 1.4	Feuer
			M 1.10	(Z)	Planung	Verwendung von Sicherheitstüren und -fenstern	G 1.4	Feuer
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.6	Anschlag
			M 1.11	(A)	Planung	Lagepläne der Versorgungsleitungen	G 1.4	Feuer
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 1.12	(A)	Planung	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.6	Anschlag
			M 1.13	(Z)	Planung	Anordnung schützenswerter Gebäudeteile	G 1.3	Blitz
							G 1.4	Feuer
							G 1.5	Wasser
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.6	Anschlag
			M 1.14	(Z)	Planung	Selbsttätige Entwässerung	G 1.5	Wasser
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 1.15	(A)	Betrieb	Geschlossene Fenster und Türen	G 1.5	Wasser
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.6	Anschlag
			M 1.16	(Z)	Planung	Geeignete Standortauswahl	G 1.3	Blitz
							G 1.5	Wasser
							G 5.5	Vandalismus
							G 5.6	Anschlag
			M 1.17	(Z)	Umsetzg.	Pförtnerdienst	G 2.1	Fehlende oder unzureichende Regelunge

							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.4	Diebstahl
			M 1.18	(Z)	Planung	Gefahrenmeldeanlage	G 1.4	Feuer
							G 1.5	Wasser
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.6	Anschlag
			M 1.19	(Z)	Planung	Einbruchsschutz	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
			M 2.14	(A)	Betrieb	Schlüsselverwaltung	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 2.15	(B)	Betrieb	Brandschutzbegehungen	G 1.4	Feuer
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 2.17	(A)	Umsetzg.	Zutrittsregelung und -kontrolle	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.4	Diebstahl
			M 2.308	(Z)	Aussnd.	Auszug aus Gebäuden	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.4	Diebstahl
			M 2.334	(Z)	Planung	Auswahl eines geeigneten Gebäudes	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 4.1	Ausfall der Stromversorgun
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.6	Anschlag
			M 6.17	(A)	Notfallv.	Alarmierungsplan und Brandschutzübungen	G 1.4	Feuer
							G 5.5	Vandalismus
							G 5.6	Anschlag
B 2.2	(4.2)	Verkabelung	M 1.9	(A)	Umsetzg.	Brandabschottung von Trassen	G 1.6	Kabelbrand
							G 4.4	Leitungsbeeinträchtigung durch Umfeldfaktore
			M 1.20	(A)	Planung	Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht	G 1.6	Kabelbrand
							G 3.5	Unbeabsichtigte Leitungsbeschädigun
							G 4.4	Leitungsbeeinträchtigung durch Umfeldfaktore
							G 4.5	Übersprechen
							G 5.7	Abhören von Leitunge
							G 5.8	Manipulation an Leitunge
			M 1.21	(A)	Planung	Ausreichende Trassendimensionierung	G 2.11	Unzureichende Trassendimensionierun
							G 3.5	Unbeabsichtigte Leitungsbeschädigun
							G 4.4	Leitungsbeeinträchtigung durch Umfeldfaktore
							G 4.5	Übersprechen

							G 5.8	Manipulation an Leitungen
			M 1.22	(Z)	Planung	Materielle Sicherung von Leitungen und Verteilern	G 2.13	Unzureichend geschützte Verteile
							G 3.5	Unbeabsichtigte Leitungsbeschädigung
							G 5.7	Abhören von Leitungen
							G 5.8	Manipulation an Leitungen
			M 1.39	(Z)	Umsetzg.	Verhinderung von Ausgleichsströmen auf Schirmungen	G 4.21	Ausgleichsströme auf Schirmungen
			M 2.19	(B)	Umsetzg.	Neutrale Dokumentation in den Verteilern	G 2.12	Unzureichende Dokumentation der Verkabelun
							G 2.13	Unzureichend geschützte Verteile
							G 3.4	Unzulässige Kabelverbindungen
							G 5.7	Abhören von Leitungen
							G 5.8	Manipulation an Leitungen
			M 2.20	(Z)	Betrieb	Kontrolle bestehender Verbindungen	G 2.13	Unzureichend geschützte Verteile
							G 3.4	Unzulässige Kabelverbindungen
							G 5.7	Abhören von Leitungen
							G 5.8	Manipulation an Leitungen
			M 5.1	(B)	Betrieb	Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen	G 3.4	Unzulässige Kabelverbindungen
							G 4.4	Leitungsbeeinträchtigung durch Umfeldfaktore
							G 4.5	Übersprechen
							G 5.7	Abhören von Leitungen
							G 5.8	Manipulation an Leitungen
			M 5.2	(A)	Planung	Auswahl einer geeigneten Netz-Topographie	G 2.11	Unzureichende Trassendimensionierun
							G 2.32	Unzureichende Leitungskapazitäte
							G 5.8	Manipulation an Leitungen
			M 5.3	(A)	Planung	Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht	G 2.11	Unzureichende Trassendimensionierun
							G 2.32	Unzureichende Leitungskapazitäte
							G 5.8	Manipulation an Leitungen
			M 5.4	(A)	Umsetzg.	Dokumentation und Kennzeichnung der Verkabelung	G 2.12	Unzureichende Dokumentation der Verkabelun
							G 3.4	Unzulässige Kabelverbindungen
							G 3.5	Unbeabsichtigte Leitungsbeschädigung
			M 5.5	(A)	Umsetzg.	Schadensmindernde Kabelführung	G 3.5	Unbeabsichtigte Leitungsbeschädigung
							G 4.4	Leitungsbeeinträchtigung durch Umfeldfaktore
							G 4.5	Übersprechen
							G 5.8	Manipulation an Leitungen
			M 6.18	(Z)	Notfallv.	Redundante Leitungsführung	G 2.11	Unzureichende Trassendimensionierun
							G 3.5	Unbeabsichtigte Leitungsbeschädigung
							G 4.4	Leitungsbeeinträchtigung durch Umfeldfaktore
B 2.3	(4.3.1)	Büroraum	M 1.15	(A)	Betrieb	Geschlossene Fenster und Türen	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.23	(A)	Betrieb	Abgeschlossene Türen	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh

							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.46	(Z)	Betrieb	Einsatz von Diebstahl-Sicherungen	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.4	Diebstahl
			M 2.17	(A)	Umsetzg.	Zutrittsregelung und -kontrolle	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 3.9	(Z)	Planung	Ergonomischer Arbeitsplatz	G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
B 2.4	(4.3.2)	Serverraum	M 1.3	(A)	Planung	Angepasste Aufteilung der Stromkreise	G 1.4	Feuer
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
			M 1.7	(A)	Planung	Handfeuerlöscher	G 1.4	Feuer
							G 4.2	Ausfall interner Versorgungsnetz
			M 1.10	(C)	Planung	Verwendung von Sicherheitstüren und -fenstern	G 1.4	Feuer
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.15	(A)	Betrieb	Geschlossene Fenster und Türen	G 1.5	Wasser
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.18	(Z)	Planung	Gefahrenmeldeanlage	G 1.4	Feuer
							G 1.5	Wasser
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 4.2	Ausfall interner Versorgungsnetz
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.23	(A)	Betrieb	Abgeschlossene Türen	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar

							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.24	(C)	Planung	Vermeidung von wasserführenden Leitungen	G 1.5	Wasser
			M 1.25	(B)	Planung	Überspannungsschutz	G 1.4	Feuer
							G 4.1	Ausfall der Stromversorgun
							G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
			M 1.26	(Z)	Planung	Not-Aus-Schalter	G 1.4	Feuer
							G 1.5	Wasser
			M 1.27	(B)	Planung	Klimatisierung	G 1.7	Unzulässige Temperatur und Luftfeuch
			M 1.28	(B)	Planung	Lokale unterbrechungsfreie Stromversorgung	G 4.1	Ausfall der Stromversorgun
							G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
			M 1.31	(Z)	Planung	Fernanzeige von Störungen	G 1.4	Feuer
							G 1.5	Wasser
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
			M 1.52	(Z)	Planung	Redundanzen in der technischen Infrastruktur	G 1.4	Feuer
							G 1.5	Wasser
							G 1.7	Unzulässige Temperatur und Luftfeuch
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.58	(A)	Planung	Technische und organisatorische Vorgaben für Serverräume	G 1.4	Feuer
							G 1.5	Wasser
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
			M 1.62	(C)	Planung	Brandschutz von Patchfeldern	G 1.4	Feuer
							G 1.16	Ausfall von Patchfeldern durch Bran
			M 2.17	(A)	Umsetzg.	Zutrittsregelung und -kontrolle	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 2.21	(A)	Umsetzg.	Rauchverbo	G 1.4	Feuer

B 2.5	(4.3.3)	Datenträgerarchiv	M 1.7	(A)	Planung	Handfeuerlösche	G 1.4	Feuer
			M 1.10	(C)	Planung	Verwendung von Sicherheitstüren und -fenstern	G 1.4	Feuer
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.15	(A)	Betrieb	Geschlossene Fenster und Türen	G 1.5	Wasser
							G 1.8	Staub, Verschmutzun
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.18	(Z)	Planung	Gefahrenmeldeanlage	G 1.4	Feuer
							G 1.5	Wasser
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.23	(A)	Betrieb	Abgeschlossene Türen	G 1.8	Staub, Verschmutzun
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.24	(Z)	Planung	Vermeidung von wasserführenden Leitungen	G 1.5	Wasser
			M 1.27	(Z)	Planung	Klimatisierung	G 1.7	Unzulässige Temperatur und Luftfeuch
			M 2.17	(A)	Umsetzg.	Zutrittsregelung und -kontrolle	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 2.21	(A)	Umsetzg.	Rauchverbot	G 1.4	Feuer
							G 1.8	Staub, Verschmutzun
B 2.6	(4.3.4)	Raum für technische Infrastruktur	M 1.3	(A)	Planung	Angepasste Aufteilung der Stromkreise	G 1.4	Feuer
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
			M 1.7	(A)	Planung	Handfeuerlöscher	G 1.4	Feuer
							G 4.2	Ausfall interner Versorgungsnetz
			M 1.10	(Z)	Planung	Verwendung von Sicherheitstüren und -fenstern	G 1.4	Feuer
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl

							G 5.5	Vandalismus
			M 1.15	(A)	Betrieb	Geschlossene Fenster und Türen	G 1.5	Wasser
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.18	(Z)	Planung	Gefahrenmeldeanlage	G 1.4	Feuer
							G 1.5	Wasser
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.23	(A)	Betrieb	Abgeschlossene Türen	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.24	(Z)	Planung	Vermeidung von wasserführenden Leitungen	G 1.5	Wasser
			M 1.25	(A)	Planung	Überspannungsschutz	G 1.4	Feuer
							G 4.1	Ausfall der Stromversorgun
							G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
			M 1.26	(Z)	Planung	Not-Aus-Schalter	G 1.4	Feuer
							G 1.5	Wasser
			M 1.27	(B)	Planung	Klimatisierung	G 1.7	Unzulässige Temperatur und Luftfeuch
			M 1.31	(Z)	Planung	Fernanzeige von Störungen	G 1.4	Feuer
							G 1.5	Wasser
							G 5.3	Unbefugtes Eindringen in ein Gebäud
			M 2.17	(A)	Umsetzg.	Zutrittsregelung und -kontrolle	G 1.4	Feuer
							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 2.21	(A)	Umsetzg.	Rauchverbot	G 1.4	Feuer
B 2.7	(4.4)	Schutzschrank	M 1.7	(B)	Planung	Handfeuerlöscher	G 1.4	Feuer
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 1.15	(A)	Betrieb	Geschlossene Fenster und Türen	G 1.4	Feuer
							G 1.5	Wasser
							G 1.8	Staub, Verschmutzun

							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 1.18	(Z)	Planung	Gefahrenmeldeanlage	G 1.4	Feuer
							G 1.5	Wasser
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
			M 1.24	(Z)	Planung	Vermeidung von wasserführenden Leitungen	G 1.5	Wasser
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 1.25	(B)	Planung	Überspannungsschutz	G 1.4	Feuer
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 1.26	(A)	Planung	Not-Aus-Schalter	G 1.4	Feuer
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 1.27	(B)	Planung	Klimatisierung	G 1.7	Unzulässige Temperatur und Luftfeuch
							G 1.8	Staub, Verschmutzun
			M 1.28	(B)	Planung	Lokale unterbrechungsfreie Stromversorgung	G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
			M 1.31	(Z)	Planung	Fernanzeige von Störungen	G 1.4	Feuer
							G 1.5	Wasser
							G 1.7	Unzulässige Temperatur und Luftfeuch
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
			M 1.40	(A)	Umsetzg.	Geeignete Aufstellung von Schutzschränken	G 1.7	Unzulässige Temperatur und Luftfeuch
							G 1.8	Staub, Verschmutzun
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge

						G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
			M 1.41	(Z)	Planung	Schutz gegen elektromagnetische Einstrahlung	G 4.4	Leitungsbeeinträchtigung durch Umfeldfaktoren
			M 2.17	(C)	Umsetzg.	Zutrittsregelung und -kontrolle	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
			M 2.21	(A)	Umsetzg.	Rauchverbot	G 1.4	Feuer
							G 1.8	Staub, Verschmutzun
			M 2.95	(A)	Beschaff.	Beschaffung geeigneter Schutzschränke	G 1.4	Feuer
							G 1.5	Wasser
							G 1.7	Unzulässige Temperatur und Luftfeuch
							G 1.8	Staub, Verschmutzun
							G 3.21	Fehlbedienung von Codeschlösser
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.53	Bewusste Fehlbedienung von Schutzschränken aus Bequemlichkeit
			M 2.96	(A)	Betrieb	Verschluss von Schutzschränken	G 1.4	Feuer
							G 1.5	Wasser
							G 1.7	Unzulässige Temperatur und Luftfeuch
							G 1.8	Staub, Verschmutzun
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.4	Diebstahl
							G 5.5	Vandalismus
			M 2.97	(A)	Betrieb	Korrekter Umgang mit Codeschlössern	G 3.21	Fehlbedienung von Codeschlösser
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.53	Bewusste Fehlbedienung von Schutzschränken aus Bequemlichkeit
			M 2.311	(A)	Planung	Planung von Schutzschränken	G 4.3	Ausfall vorhandener Sicherungseinrichtunge
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
			M 3.20	(A)	Umsetzg.	Einweisung in die Bedienung von Schutzschränken	G 1.4	Feuer
							G 1.5	Wasser
							G 1.7	Unzulässige Temperatur und Luftfeuch
							G 1.8	Staub, Verschmutzun
							G 3.21	Fehlbedienung von Codeschlösser
							G 4.1	Ausfall der Stromversorgun

							G 4.2	Ausfall interner Versorgungsnetz
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.53	Bewusste Fehlbedienung von Schutzschränken aus Beguemlichkeit
B 2.8	(4.5)	Häuslicher Arbeitsplatz	M 1.15	(A)	Betrieb	Geschlossene Fenster und Türen	G 1.5	Wasser
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.69	Erhöhte Diebstahlgefahr am häuslichen Arbeitspla
							G 5.70	Manipulation durch Familienangehörige und Besuch
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 1.19	(Z)	Planung	Einbruchsschutz	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.69	Erhöhte Diebstahlgefahr am häuslichen Arbeitspla
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 1.23	(A)	Betrieb	Abgeschlossene Türen	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.69	Erhöhte Diebstahlgefahr am häuslichen Arbeitspla
							G 5.70	Manipulation durch Familienangehörige und Besuch
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 1.44	(A)	Planung	Geeignete Einrichtung eines häuslichen Arbeitsplatzes	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
			M 1.45	(A)	Betrieb	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträge	G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 2.13	(A)	Aussnd.	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.48	Ungeeignete Entsorgung der Datenträger und Dokumente
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 2.37	(C)	Betrieb	"Der aufgeräumte Arbeitsplatz"	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.2	Manipulation an Daten oder Softwar
							G 5.69	Erhöhte Diebstahlgefahr am häuslichen Arbeitspla
							G 5.70	Manipulation durch Familienangehörige und Besuch
							G 5.71	Vertraulichkeitsverlust schützenswerter Information

			M 2.112	(A)	Umsetzg.	Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institutic	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.47	Ungesicherter Akten- und Datenträgertranspo
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 2.136	(A)	Betrieb	Einhaltung von Regelungen bzgl. Arbeitsplatz und Arbeitsumgebung	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
			M 3.9	(Z)	Planung	Ergonomischer Arbeitsplatz	G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
B 2.9	(4.6)	Rechenzentrum	M 1.3	(A)	Planung	Angepasste Aufteilung der Stromkreise	G 1.2	Ausfall des IT-Systems
							G 1.4	Feuer
							G 1.6	Kabelbrand
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 4.1	Ausfall der Stromversorgun
			M 1.7	(A)	Planung	Handfeuerlöscher	G 1.4	Feuer
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
			M 1.10	(C)	Planung	Verwendung von Sicherheitstüren und -fenstern	G 1.4	Feuer
							G 1.11	Technische Katastrophen im Umfeld
			M 1.12	(A)	Planung	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile	G 1.12	Beeinträchtigung durch Großveranstaltunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.6	Anschlag
			M 1.13	(Z)	Planung	Anordnung schützenswerter Gebäudeteile	G 1.5	Wasser
							G 1.12	Beeinträchtigung durch Großveranstaltunge
							G 1.13	Sturm
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.6	Anschlag
			M 1.15	(A)	Betrieb	Geschlossene Fenster und Türen	G 1.5	Wasser
							G 1.7	Unzulässige Temperatur und Luftfeuch
							G 1.8	Staub, Verschmutzun
							G 1.12	Beeinträchtigung durch Großveranstaltunge
							G 1.13	Sturm
							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl

							G 5.5	Vandalismus
							G 5.6	Anschlag
							G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
			M 1.18	(B)	Planung	Gefahrenmeldeanlage	G 1.5	Wasser
							G 1.12	Beeinträchtigung durch Großveranstaltunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
			M 1.23	(A)	Betrieb	Abgeschlossene Türen	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.6	Anschlag
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
							G 5.102	Sabotage
			M 1.24	(C)	Planung	Vermeidung von wasserführenden Leitungen	G 1.5	Wasser
			M 1.25	(A)	Planung	Überspannungsschutz	G 1.2	Ausfall des IT-System
							G 1.3	Blitz
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 4.1	Ausfall der Stromversorgun
			M 1.26	(B)	Planung	Not-Aus-Schalte	G 1.4	Feuer
			M 1.27	(B)	Planung	Klimatisierung	G 1.2	Ausfall des IT-System
							G 1.7	Unzulässige Temperatur und Luftfeuch
							G 1.8	Staub, Verschmutzun
			M 1.31	(Z)	Planung	Fernanzeige von Störungen	G 1.4	Feuer
							G 1.5	Wasser
							G 4.1	Ausfall der Stromversorgun
							G 4.2	Ausfall interner Versorgungsnetz
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl

			M 1.47	(B)	Planung	Eigener Brandabschnitt	G 1.4	Feuer
							G 1.11	Technische Katastrophen im Umfel
			M 1.48	(B)	Planung	Brandmeldeanlage	G 1.4	Feuer
							G 1.6	Kabelbrand
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 4.2	Ausfall interner Versorgungsnetz
			M 1.49	(A)	Planung	Technische und organisatorische Vorgaben für das Rechenzentrum	G 1.11	Technische Katastrophen im Umfel
							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 2.11	Unzureichende Trassendimensionierun
			M 1.50	(C)	Planung	Rauchschut	G 1.4	Feuer
			M 1.51	(A)	Umsetzg.	Brandlastreduzierung	G 1.4	Feuer
			M 1.52	(Z)	Planung	Redundanzen in der technischen Infrastruktur	G 1.2	Ausfall des IT-System
							G 1.7	Unzulässige Temperatur und Luftfeuch
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 1.53	(Z)	Planung	Videoüberwachung	G 1.12	Beeinträchtigung durch Großveranstaltunge
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl
							G 5.5	Vandalismus
							G 5.6	Anschlag
							G 5.102	Sabotage
			M 1.54	(Z)	Planung	Brandfrühesterkennung / Löschtechnik	G 1.4	Feuer
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
			M 1.55	(Z)	Planung	Perimeterschutz	G 1.12	Beeinträchtigung durch Großveranstaltunge
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.5	Vandalismus
							G 5.6	Anschlag
							G 5.102	Sabotage
			M 1.56	(A)	Planung	Sekundär-Energieversorgung	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.11	Unzureichende Trassendimensionierun
							G 4.1	Ausfall der Stromversorgun
			M 1.57	(A)	Umsetzg.	Aktuelle Infrastruktur- und Baupläne	G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.12	Unzureichende Dokumentation der Verkabelun
			M 1.62	(C)	Planung	Brandschutz von Patchfeldern	G 1.4	Feuer
							G 1.16	Ausfall von Patchfeldern durch Bran
			M 2.17	(A)	Umsetzg.	Zutrittsregelung und -kontrolle	G 1.12	Beeinträchtigung durch Großveranstaltunge
							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 5.3	Unbefugtes Eindringen in ein Gebäud
							G 5.4	Diebstahl

							G 5.5	Vandalismus
							G 5.102	Sabotage
			M 2.21	(A)	Umsetzg.	Rauchverbot	G 1.4	Feuer
							G 1.8	Staub, Verschmutzun
							G 2.1	Fehlende oder unzureichende Regelunge
			M 2.212	(B)	Umsetzg.	Organisatorische Vorgaben für die Gebäudereinigung	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
			M 2.213	(A)	Umsetzg.	Wartung der technischen Infrastruktur	G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 4.3	Ausfall vorhandener Sicherungseinrichtunge
			M 6.16	(Z)	Notfallv.	Abschließen von Versicherungen	G 1.3	Blitz
							G 1.4	Feuer
							G 1.5	Wasser
							G 1.13	Sturm
			M 6.17	(A)	Notfallv.	Alarmierungsplan und Brandschutzübungen	G 1.4	Feuer
							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
			M 6.74	(Z)	Notfallv	Notfallarchiv	G 2.11	Unzureichende Trassendimensionierun
B 2.10	(4.7)	Mobiler Arbeitsplatz	M 1.15	(A)	Betrieb	Geschlossene Fenster und Türen	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.4	Diebstahl
			M 1.23	(A)	Betrieb	Abgeschlossene Türen	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.4	Diebstahl
			M 1.45	(A)	Betrieb	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger	G 2.47	Ungesicherter Akten- und Datenträgertranspo
							G 2.48	Ungeeignete Entsorgung der Datenträger und Dokumente
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 1.46	(Z)	Betrieb	Einsatz von Diebstahl-Sicherunge	G 5.4	Diebstahl
			M 1.61	(A)	Planung	Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes	G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebur
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.4	Diebstahl
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 2.13	(A)	Aussnd.	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.48	Ungeeignete Entsorgung der Datenträger und Dokumente
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 2.37	(C)	Betrieb	"Der aufgeräumte Arbeitsplatz"	G 2.48	Ungeeignete Entsorgung der Datenträger und Dokumente
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 2.136	(A)	Betrieb	Einhaltung von Regelungen bzgl.	G 2.1	Fehlende oder unzureichende Regelunge

						Arbeitsplatz und Arbeitsumgebung	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
			M 2.218	(A)	Planung	Regelung der Mitnahme von Datenträgern und IT-Komponenten	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.47	Ungesicherter Akten- und Datenträgertranspo
							G 2.48	Ungeeignete Entsorgung der Datenträger und Dokumente
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 5.2	Manipulation an Daten oder Softwar
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 2.309	(C)	Planung	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung	G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebur
							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.47	Ungesicherter Akten- und Datenträgertranspo
							G 2.48	Ungeeignete Entsorgung der Datenträger und Dokumente
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.43	Ungeeigneter Umgang mit Passwörter
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 4.251	(A)	Betrieb	Arbeiten mit fremden IT-Systemen	G 2.1	Fehlende oder unzureichende Regelunge
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 5.2	Manipulation an Daten oder Softwar
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
B 2.11	(4.8)	Besprechungs-, Veranstaltungs- und Schulungsräume	M 1.6	(A)	Umsetzg.	Einhaltung von Brandschutzvorschriften	G 4.2	Ausfall interner Versorgungsnetze
			M 1.15	(A)	Betrieb	Geschlossene Fenster und Türe	G 5.4	Diebstahl
			M 2.16	(B)	Betrieb	Beaufsichtigung oder Begleitung von Fremdpersonen	G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 4.1	Ausfall der Stromversorgun
							G 5.4	Diebstahl
			M 2.69	(B)	Umsetzg.	Einrichtung von Standardarbeitsplätzen	G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
			M 2.204	(A)	Umsetzg.	Verhinderung ungesicherter Netzzugänge	G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
			M 2.331	(A)	Planung	Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
							G 2.104	Inkompatibilität zwischen fremder und eigener

							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.78	Fliegende Verkabelung
			M 2.332	(B)	Planung	Einrichtung von Besprechungs-, Vortrags- und Schulungsräumen	G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
							G 4.1	Ausfall der Stromversorgung
							G 4.2	Ausfall interner Versorgungsnetz
			M 2.333	(A)	Umsetzg.	Sichere Nutzung von Besprechungs-, Vortrags- und Schulungsräumen	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.104	Inkompatibilität zwischen fremder und eigener
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.4	Diebstahl
			M 3.9	(Z)	Planung	Ergonomischer Arbeitsplatz	G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
							G 3.78	Fliegende Verkabelung
			M 4.109	(C)	Betrieb	Software-Reinstallation bei Arbeitsplatzrechnern	G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
			M 4.252	(C)	Umsetzg.	Sichere Konfiguration von Schulungsrechnern	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
			M 5.77	(Z)	Planung	Bildung von Teilnetzen	G 2.104	Inkompatibilität zwischen fremder und eigener
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
			M 5.124	(C)	Planung	Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
B 3.101	(6.1)	Allgemeiner Server	M 1.28	(B)	Planung	Lokale unterbrechungsfreie Stromversorgung	G 1.2	Ausfall des IT-System
							G 3.5	Unbeabsichtigte Leitungsbeschädigung
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 4.1	Ausfall der Stromversorgung
							G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
			M 2.22	(A)	Betrieb	Hinterlegen des Passwortes	G 1.1	Personalausfal
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
			M 2.31	(A)	Betrieb	Dokumentation der zugelassenen Benutzer und Rechteprofile	G 1.1	Personalausfal
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.9	Unberechtigte IT-Nutzun
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
			M 2.32	(Z)	Umsetzg.	Einrichtung einer eingeschränkten Benutzerumgebung	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme

							G 3.8	Fehlerhafte Nutzung des IT-System
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.15	"Neugierige" Mitarbeiter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.21	Trojanische Pferde
							G 5.26	Analyse des Nachrichtenflusse
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.35	(B)	Betrieb	Informationsbeschaffung über Sicherheitslücken des Systems	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.138	(B)	Umsetzg.	Strukturierte Datenhaltung	G 3.31	Unstrukturierte Datenhaltun
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.204	(A)	Betrieb	Verhinderung ungesicherter Netzzugänge	G 2.7	Unerlaubte Ausübung von Rechte
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitunge
							G 5.9	Unberechtigte IT-Nutzun
			M 2.273	(A)	Betrieb	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	G 4.22	Software-Schwachstellen oder -Fehle
							G 4.39	Software-Konzeptionsfehle
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.314	(Z)	Planung	Verwendung von hochverfügbaren Architekturen für Serve	G 1.2	Ausfall des IT-Systems
			M 2.315	(A)	Planung	Planung des Servereinsatzes	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.9	Fehlerhafte Administration des IT-System

							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.39	Software-Konzeptionsfehle
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.316	(A)	Planung	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server	G 1.1	Personalausfal
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitunge
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.317	(C)	Beschaff.	Beschaffungskriterien für einen Server	G 4.22	Software-Schwachstellen oder -Fehle
							G 4.39	Software-Konzeptionsfehle
			M 2.318	(A)	Umsetzg.	Sichere Installation eines Servers	G 1.2	Ausfall des IT-System
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.39	Software-Konzeptionsfehle
							G 5.7	Abhören von Leitunge
							G 5.26	Analyse des Nachrichtenflusse
			M 2.319	(C)	Aussnd.	Migration eines Servers	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.39	Software-Konzeptionsfehle
			M 2.320	(A)	Aussnd.	Geregelte Außerbetriebnahme eines Servers	G 5.9	Unberechtigte IT-Nutzun
							G 5.15	"Neugierige" Mitarbeiter
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 4.7	(A)	Umsetzg.	Änderung voreingestellter Passwörter	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitunge
							G 5.9	Unberechtigte IT-Nutzun

							G 5.15	"Neugierige" Mitarbeiter
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.40	Abhören von Räumen mittels Rechner mit Mikrofo
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.15	(A)	Umsetzg.	Gesichertes Login	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.15	"Neugierige" Mitarbeiter
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.16	(A)	Umsetzg.	Zugangsbeschränkungen für Accounts und / oder Terminals	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.7	Abhören von Leitunge
							G 5.9	Unberechtigte IT-Nutzun
							G 5.19	Missbrauch von Benutzerrechte
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.17	(A)	Umsetzg.	Sperren und Löschen nicht benötigter Accounts und Terminals	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.24	(A)	Betrieb	Sicherstellung einer konsistenten Systemverwaltung	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System

							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.7	Abhören von Leitungen
							G 5.20	Missbrauch von Administratorrechte
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.40	(C)	Umsetzg.	Verhinderung der unautorisierten Nutzung des Rechnermikrofon	G 5.40	Abhören von Räumen mittels Rechner mit Mikrofo
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 4.93	(B)	Betrieb	Regelmäßige Integritätsprüfung	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.21	Trojanische Pferde
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.237	(A)	Umsetzg.	Sichere Grundkonfiguration eines IT-Systems	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitungen
							G 5.9	Unberechtigte IT-Nutzun
							G 5.15	"Neugierige" Mitarbeiter
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.40	Abhören von Räumen mittels Rechner mit Mikrofo
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.238	(A)	Betrieb	Einsatz eines lokalen Paketfilters	G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
			M 4.239	(A)	Betrieb	Sicherer Betrieb eines Servers	G 1.1	Personalausfal
							G 1.2	Ausfall des IT-System
							G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System

							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitunge
							G 5.9	Unberechtigte IT-Nutzun
							G 5.15	"Neugierige" Mitarbeiter
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.26	Analyse des Nachrichtenflusse
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.240	(Z)	Betrieb	Einrichten einer Testumgebung für einen Server	G 1.2	Ausfall des IT-System
							G 2.7	Unerlaubte Ausübung von Rechte
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-Syster
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 5.8	(B)	Betrieb	Regelmäßiger Sicherheitscheck des Netzes	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-Syster
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitunge
							G 5.9	Unberechtigte IT-Nutzun
							G 5.26	Analyse des Nachrichtenflusse
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 5.9	(A)	Betrieb	Protokollierung am Server	G 1.2	Ausfall des IT-System
							G 2.7	Unerlaubte Ausübung von Rechte
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.9	Fehlerhafte Administration des IT-System

							G 4.7	Defekte Datenträger
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 5.10	(A)	Planung	Restriktive Rechtevergabe	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-Syster
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitunge
							G 5.9	Unberechtigte IT-Nutzun
							G 5.15	"Neugierige" Mitarbeiter
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 5.37	(B)	Planung	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz	G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäter
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.15	"Neugierige" Mitarbeiter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 6.24	(A)	Notfallv.	Erstellen eines Notfall-Bootmediums	G 3.9	Fehlerhafte Administration des IT-System
							G 4.13	Verlust gespeicherter Dater
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
			M 6.96	(A)	Notfallv.	Notfallvorsorge für einen Server	G 1.1	Personalausfal
							G 1.2	Ausfall des IT-System
							G 4.7	Defekte Datenträger
							G 4.13	Verlust gespeicherter Dater
							G 4.22	Software-Schwachstellen oder -Fehle
B 3.102	(6.2)	Server unter Unix	M 2.33	(C)	Planung	Aufteilung der Administrationstätigkeiten unter Unix	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp

			M 4.9	(A)	Umsetzg.	Einsatz der Sicherheitsmechanismen von X-Windows	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
							G 5.89	Hijacking von Netz-Verbindunge
			M 4.13	(A)	Planung	Sorgfältige Vergabe von IDs	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 4.14	(A)	Umsetzg.	Obligatorischer Passwortschutz unter Unix	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Clien
							G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 4.18	(A)	Planung	Administrative und technische Absicherung des Zugangs zum Monitor und Single-User-Modus	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
			M 4.19	(A)	Umsetzg.	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
							G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 4.20	(B)	Umsetzg.	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
							G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 4.21	(A)	Umsetzg.	Verhinderung des unautorisierten Erlangens von Administratorrechten	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.10	Falsches Exportieren von Dateisystemen unter Un
							G 3.11	Fehlerhafte Konfiguration von sendma
							G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Clien
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
			M 4.22	(C)	Umsetzg.	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Clien
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien

						G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 4.23	(A)	Umsetzg.	Sicherer Aufruf ausführbarer Dateien	G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 4.25	(A)	Betrieb	Einsatz der Protokollierung im Unix-System	G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 4.26	(B)	Betrieb	Regelmäßiger Sicherheitscheck des Unix-Systems	G 3.10	Falsches Exportieren von Dateisystemen unter Un
							G 3.11	Fehlerhafte Konfiguration von sendma
							G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 4.105	(A)	Umsetzg.	Erste Maßnahmen nach einer Unix-Standardinstallatior	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
			M 4.106	(A)	Umsetzg.	Aktivieren der Systemprotokollierung	G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 5.16	(B)	Planung	Übersicht über Netzdienste	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
			M 5.17	(A)	Umsetzg.	Einsatz der Sicherheitsmechanismen von NFS	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.10	Falsches Exportieren von Dateisystemen unter Un
			M 5.18	(A)	Umsetzg.	Einsatz der Sicherheitsmechanismen von NIS	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Clien
			M 5.19	(A)	Umsetzg.	Einsatz der Sicherheitsmechanismen von sendmail	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.11	Fehlerhafte Konfiguration von sendma
							G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 5.20	(A)	Umsetzg.	Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.10	Falsches Exportieren von Dateisystemen unter Un
			M 5.21	(A)	Umsetzg.	Sicherer Einsatz von telnet, ftp, tftp und rexec	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.10	Falsches Exportieren von Dateisystemen unter Un
			M 5.34	(Z)	Planung	Einsatz von Einmalpasswörtern	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 5.35	(A)	Umsetzg.	Einsatz der Sicherheitsmechanismen von UUCP	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 5.36	(Z)	Planung	Verschlüsselung unter Unix und Windows NT	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 5.89	Hijacking von Netz-Verbindunge

			M 5.38	(B)	Planung	Sichere Einbindung von DOS-PCs in ein Unix-Net	G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Net
			M 5.64	(Z)	Planung	Secure Shel	G 5.89	Hijacking von Netz-Verbindunge
			M 5.72	(A)	Umsetzg.	Deaktivieren nicht benötigter Netzdienste	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
			M 5.82	(A)	Planung	Sicherer Einsatz von SAMBA	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 2.65	Komplexität der SAMBA-Konfiguratior
			M 5.83	(Z)	Planung	Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 5.89	Hijacking von Netz-Verbindunge
			M 6.31	(A)	Notfallv.	Verhaltensregeln nach Verlust der Systemintegrität	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
B 3.103	(6.4)	Server unter Windows NT	M 2.91	(A)	Planung	Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz	G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Net
							G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäter
							G 2.30	Unzureichende Domänenplanun
							G 2.31	Unzureichender Schutz des Windows NT Systen
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemer
			M 2.92	(B)	Betrieb	Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz	G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Net
							G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäter
							G 2.31	Unzureichender Schutz des Windows NT Systen
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
			M 2.93	(A)	Planung	Planung des Windows NT Netzes	G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Net
							G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäter
							G 2.30	Unzureichende Domänenplanun
							G 2.31	Unzureichender Schutz des Windows NT Systen

						G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
						G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
						G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 2.94	(B)	Umsetzg.	Freigabe von Verzeichnissen unter Windows NT	G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Net
							G 2.31	Unzureichender Schutz des Windows NT System
			M 4.48	(A)	Umsetzg.	Passwortschutz unter Windows NT/2000/XP	G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Net
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.49	(A)	Umsetzg.	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System	G 2.31	Unzureichender Schutz des Windows NT System
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.50	(Z)	Planung	Strukturierte Systemverwaltung unter Windows NT	G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Net
							G 2.31	Unzureichender Schutz des Windows NT System
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.51	(Z)	Planung	Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT	G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Net
							G 2.31	Unzureichender Schutz des Windows NT System
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.52	(A)	Umsetzg.	Geräteschutz unter Windows NT/2000/XP	G 2.31	Unzureichender Schutz des Windows NT System
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.53	(A)	Umsetzg.	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT	G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Net
							G 2.31	Unzureichender Schutz des Windows NT System
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen

			M 4.54	(A)	Betrieb	Protokollierung unter Windows NT	G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Net
							G 2.31	Unzureichender Schutz des Windows NT Systen
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemer
			M 4.55	(A)	Umsetzg.	Sichere Installation von Windows NT	G 2.31	Unzureichender Schutz des Windows NT Systen
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemer
			M 4.56	(B)	Betrieb	Sicheres Löschen unter Windows-Betriebssystemen	G 2.31	Unzureichender Schutz des Windows NT Systems
			M 4.57	(A)	Umsetzg.	Deaktivieren der automatischen CD-ROM-Erkennung	G 4.23	Automatische CD-ROM-Erkennun
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.75	(A)	Umsetzg.	Schutz der Registrierung unter Windows NT/2000/XP	G 2.31	Unzureichender Schutz des Windows NT Systen
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemer
			M 4.76	(B)	Planung	Sichere Systemversion von Windows NT	G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemer
			M 4.77	(A)	Umsetzg.	Schutz der Administratorkonten unter Windows NT	G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemer
			M 5.36	(Z)	Planung	Verschlüsselung unter Unix und Windows NT	G 2.31	Unzureichender Schutz des Windows NT Systen
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
			M 5.40	(B)	Planung	Sichere Einbindung von DOS-PCs in ein Windows NT Net	G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Net
			M 5.41	(C)	Planung	Sichere Konfiguration des Fernzugriffs unter Windows NT	G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Net
							G 2.31	Unzureichender Schutz des Windows NT Systen
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
			M 5.42	(C)	Planung	Sichere Konfiguration der TCP/IP-	G 2.31	Unzureichender Schutz des Windows NT Systen

						Netzverwaltung unter Windows NT	G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
			M 5.43	(B)	Planung	Sichere Konfiguration der TCP/IP-Netzdienste unter Windows NT	G 2.31	Unzureichender Schutz des Windows NT System
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
			M 6.42	(A)	Notfallv.	Erstellung von Rettungsdisketten für Windows NT	G 2.31	Unzureichender Schutz des Windows NT System
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 6.43	(Z)	Notfallv.	Einsatz redundanter Windows NT/2000 Server	G 2.31	Unzureichender Schutz des Windows NT Systems
			M 6.44	(A)	Notfallv.	Datensicherung unter Windows NT	G 2.31	Unzureichender Schutz des Windows NT System
							G 5.43	Makro-Viren
B 3.104	(6.5)	Server unter Novell Netware 3.x	M 1.42	(A)	Umsetzg.	Gesicherte Aufstellung von Novell Netware Servern	G 1.2	Ausfall des IT-Systems
							G 2.33	Nicht gesicherter Aufstellungsort von Novell Netware Servern
							G 5.54	Vorsätzliches Herbeiführen eines Abnormal En
							G 5.58	"Hacking Novell Netware
			M 2.98	(A)	Umsetzg.	Sichere Installation von Novell Netware Servern	G 1.2	Ausfall des IT-Systems
							G 2.34	Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen
							G 4.1	Ausfall der Stromversorgung
			M 2.99	(A)	Planung	Sichere Einrichtung von Novell Netware Servern	G 1.2	Ausfall des IT-Systems
							G 2.34	Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen
							G 4.1	Ausfall der Stromversorgung
							G 5.58	"Hacking Novell Netware
			M 2.100	(A)	Betrieb	Sicherer Betrieb von Novell Netware Servern	G 1.2	Ausfall des IT-Systems
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.54	Vorsätzliches Herbeiführen eines Abnormal En
							G 5.55	Login Bypass
							G 5.56	Temporär frei zugängliche Account
							G 5.58	"Hacking Novell Netware
							G 5.59	Missbrauch von Administratorrechten unter Novell Netware 3.x
			M 2.101	(B)	Betrieb	Revision von Novell Netware Servern	G 2.34	Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen
							G 5.56	Temporär frei zugängliche Account
							G 5.57	Netzanalyse-Tools
							G 5.58	"Hacking Novell Netware
							G 5.59	Missbrauch von Administratorrechten unter Novell Netware 3.x
			M 2.102	(Z)	Umsetzg.	Verzicht auf die Aktivierung der Remote Console	G 5.58	"Hacking Novell Netware"

B 3.105	(6.6)	Server unter Novell Netware 4.x	M 1.42	(A)	Umsetzg.	Gesicherte Aufstellung von Novell Netware Servern	G 2.33	Nicht gesicherter Aufstellungsort von Novell Netware Servern
							G 5.58	"Hacking Novell Netware
			M 2.102	(Z)	Umsetzg.	Verzicht auf die Aktivierung der Remote Console	G 5.57	Netzanalyse-Tools
							G 5.58	"Hacking Novell Netware
			M 2.147	(A)	Umsetzg.	Sichere Migration von Novell Netware 3.x Servern in Novell Netware 4.x Netze	G 2.42	Komplexität der NDS
							G 2.43	Migration von Novell Netware 3.x nach Novell Netware Version 4
							G 5.59	Missbrauch von Administratorrechten unter Novell Netware 3.x
			M 2.148	(A)	Planung	Sichere Einrichtung von Novell Netware 4.x Netzen	G 2.34	Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen
							G 3.25	Fahrlässiges Löschen von Objekten
							G 3.26	Ungewollte Freigabe des Dateisystems
							G 3.27	Fehlerhafte Zeitsynchronisation
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.55	Login Bypass
							G 5.56	Temporär frei zugängliche Account
							G 5.58	"Hacking Novell Netware
			M 2.149	(A)	Betrieb	Sicherer Betrieb von Novell Netware 4.x Netzen	G 2.34	Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen
							G 3.25	Fahrlässiges Löschen von Objekten
							G 3.26	Ungewollte Freigabe des Dateisystems
							G 3.27	Fehlerhafte Zeitsynchronisation
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.58	"Hacking Novell Netware
			M 2.150	(B)	Betrieb	Revision von Novell Netware 4.x Netzen	G 2.34	Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen
							G 3.26	Ungewollte Freigabe des Dateisystems
			M 2.151	(A)	Planung	Entwurf eines NDS-Konzeptes	G 2.42	Komplexität der NDS
							G 3.27	Fehlerhafte Zeitsynchronisation
			M 2.152	(B)	Planung	Entwurf eines Zeitsynchronisations-Konzeptes	G 3.27	Fehlerhafte Zeitsynchronisation
			M 2.153	(A)	Planung	Dokumentation von Novell Netware 4.x Netzen	G 1.2	Ausfall des IT-Systems
			M 4.102	(Z)	Umsetzg.	C2-Sicherheit unter Novell 4.11	G 2.34	Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen
							G 5.58	"Hacking Novell Netware
			M 4.103	(Z)	Umsetzg.	DHCP-Server unter Novell Netware 4.	G 3.8	Fehlerhafte Nutzung des IT-System
			M 4.104	(Z)	Umsetzg.	LDAP Services for NDS	G 3.8	Fehlerhafte Nutzung des IT-System
			M 4.108	(Z)	Betrieb	Vereinfachtes und sicheres Netzmanagement mit DNS Services unter Novell NetWare 4.1	G 3.38	Konfigurations- und Bedienungsfehler

			M 6.55	(C)	Notfallv.	Reduzierung der Wiederanlaufzeit für Novell Netware Serve	G 1.2	Ausfall des IT-Systems
B 3.106	(6.9)	Server unter Windows 2000	M 2.227	(A)	Planung	Planung des Windows 2000 Einsatzes	G 2.68	Fehlende oder unzureichende Planung des Active Directory
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 3.49	Fehlkonfiguration des Active Director
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.228	(A)	Planung	Festlegen einer Windows 2000 Sicherheitsrichtlinie	G 2.7	Unerlaubte Ausübung von Rechte
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.229	(A)	Planung	Planung des Active Directory	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.68	Fehlende oder unzureichende Planung des Active Directory
			M 2.230	(A)	Planung	Planung der Active Directory-Administration	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.49	Fehlkonfiguration des Active Director
			M 2.231	(A)	Planung	Planung der Gruppenrichtlinien unter Windows 2000	G 2.68	Fehlende oder unzureichende Planung des Active Directory
			M 2.232	(B)	Planung	Planung der Windows 2000 CA-Struktur	G 2.7	Unerlaubte Ausübung von Rechte
							G 4.35	Unsichere kryptographische Algorithme
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.84	Gefälschte Zertifikate
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.233	(B)	Planung	Planung der Migration von Windows NT auf Windows 2000	G 2.68	Fehlende oder unzureichende Planung des Active Directory
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 3.49	Fehlkonfiguration des Active Director
							G 4.35	Unsichere kryptographische Algorithme
							G 5.7	Abhören von Leitunge
							G 5.23	Computer-Viren
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
							G 5.85	Integritätsverlust schützenswerter Information
			M 3.27	(A)	Umsetzg.	Schulung zur Active Directory-	G 2.1	Fehlende oder unzureichende Regelunge

						Verwaltung	G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.68	Fehlende oder unzureichende Planung des Active Directory
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 3.49	Fehlkonfiguration des Active Director
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.48	(A)	Umsetzg.	Passwortschutz unter Windows NT/2000/XP	G 2.7	Unerlaubte Ausübung von Rechte
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.56	(C)	Betrieb	Sicheres Löschen unter Windows-Betriebssystemen	G 2.18	Ungeordnete Zustellung der Datenträge
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 4.75	(A)	Umsetzg.	Schutz der Registrierung unter Windows NT/2000/XP	G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.136	(A)	Umsetzg.	Sichere Installation von Windows 2000	G 2.7	Unerlaubte Ausübung von Rechte
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.23	Automatische CD-ROM-Erkennun
							G 4.35	Unsichere kryptographische Algorithme
							G 5.7	Abhören von Leitunge
							G 5.23	Computer-Viren
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.137	(A)	Umsetzg.	Sichere Konfiguration von Windows 2000	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 3.49	Fehlkonfiguration des Active Director
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen

							G 4.23	Automatische CD-ROM-Erkennun
							G 4.35	Unsichere kryptographische Algorithme
							G 5.7	Abhören von Leitunge
							G 5.23	Computer-Viren
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.138	(A)	Umsetzg.	Konfiguration von Windows 2000 als Domänen-Controller	G 2.7	Unerlaubte Ausübung von Rechte
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.23	Automatische CD-ROM-Erkennun
							G 5.7	Abhören von Leitunge
							G 5.23	Computer-Viren
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.139	(A)	Umsetzg.	Konfiguration von Windows 2000 als Server	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.23	Automatische CD-ROM-Erkennun
							G 4.35	Unsichere kryptographische Algorithme
							G 5.7	Abhören von Leitunge
							G 5.23	Computer-Viren
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.140	(A)	Umsetzg.	Sichere Konfiguration wichtiger Windows 2000 Dienste	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 3.49	Fehlkonfiguration des Active Director
							G 4.23	Automatische CD-ROM-Erkennun
							G 4.35	Unsichere kryptographische Algorithme
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.141	(A)	Umsetzg.	Sichere Konfiguration des DDNS unter	G 2.7	Unerlaubte Ausübung von Rechte

						Windows 2000	G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 4.35	Unsichere kryptographische Algorithme
							G 5.7	Abhören von Leitunge
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.142	(B)	Umsetzg.	Sichere Konfiguration des WINS unter Windows 2000	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 4.23	Automatische CD-ROM-Erkennun
							G 4.35	Unsichere kryptographische Algorithme
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.143	(B)	Umsetzg.	Sichere Konfiguration des DHCP unter Windows 2000	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 4.23	Automatische CD-ROM-Erkennun
							G 4.35	Unsichere kryptographische Algorithme
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.144	(B)	Umsetzg.	Nutzung der Windows 2000 CA	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.68	Fehlende oder unzureichende Planung des Active Directory
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.145	(A)	Umsetzg.	Sichere Konfiguration von RRAS unter Windows 2000	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.35	Unsichere kryptographische Algorithme
							G 5.7	Abhören von Leitunge
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.146	(A)	Betrieb	Sicherer Betrieb von Windows 2000/XP	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 3.49	Fehlkonfiguration des Active Director
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.23	Automatische CD-ROM-Erkennun
							G 4.35	Unsichere kryptographische Algorithme

							G 5.7	Abhören von Leitungen
							G 5.23	Computer-Viren
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
							G 5.83	Kompromittierung kryptographischer Schlüssel
							G 5.84	Gefälschte Zertifikate
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.147	(Z)	Planung	Sichere Nutzung von EFS unter Windows 2000/XP	G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.148	(B)	Betrieb	Überwachung eines Windows 2000/XP Systems	G 2.7	Unerlaubte Ausübung von Rechten
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechnern
							G 3.49	Fehlkonfiguration des Active Directory
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
			M 4.149	(A)	Umsetzg.	Datei- und Freigabeberechtigungen unter Windows 2000/XP	G 2.7	Unerlaubte Ausübung von Rechten
							G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
							G 5.85	Integritätsverlust schützenswerter Information
			M 5.89	(A)	Umsetzg.	Konfiguration des sicheren Kanals unter Windows 2000/XP	G 5.7	Abhören von Leitungen
							G 5.83	Kompromittierung kryptographischer Schlüssel
							G 5.85	Integritätsverlust schützenswerter Information
			M 5.90	(Z)	Umsetzg.	Einsatz von IPSec unter Windows 2000/XP	G 5.7	Abhören von Leitungen
							G 5.83	Kompromittierung kryptographischer Schlüssel
							G 5.85	Integritätsverlust schützenswerter Information
			M 6.43	(Z)	Notfallv.	Einsatz redundanter Windows NT/2000 Server	G 1.2	Ausfall des IT-Systems
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.23	Computer-Viren
			M 6.76	(C)	Notfallv.	Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes	G 1.2	Ausfall des IT-Systems
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.23	Computer-Viren
			M 6.77	(A)	Notfallv.	Erstellung von Rettungsdisketten für Windows 2000	G 1.2	Ausfall des IT-Systems
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.23	Computer-Viren
			M 6.78	(A)	Notfallv.	Datensicherung unter Windows 2000/XP	G 1.2	Ausfall des IT-Systems
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.23	Computer-Viren
B 3.107	(6.10)	S/390- und zSeries-Mainframe	M 2.31	(B)	Planung	Dokumentation der zugelassenen Benutzer und Rechteprofile	G 5.10	Missbrauch von Fernwartungszugängen
							G 5.19	Missbrauch von Benutzerrechten
							G 5.122	Missbrauch von RACF-Attributen unter z/O
			M 2.285	(Z)	Planung	Festlegung von Standards für z/OS-Systemdefinitionen	G 2.27	Fehlende oder unzureichende Dokumentation

			M 2.286	(Z)	Planung	Planung und Einsatz von zSeries-Systemen	G 2.99	Unzureichende oder fehlerhafte Konfiguration der zSerie Systemumgebunc
			M 2.287	(Z)	Planung	Batch-Job-Planung für z/OS-System	G 3.75	Mangelhafte Kontrolle der Batch-Jobs bei z/O
			M 2.288	(B)	Planung	Erstellung von Sicherheitsrichtlinien für z/OS-Systeme	G 2.27	Fehlende oder unzureichende Dokumentatio
							G 3.72	Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF
							G 5.2	Manipulation an Daten oder Softwar
							G 5.19	Missbrauch von Benutzerrechte
							G 5.119	Benutzung fremder Kennungen unter z/OS-System
							G 5.122	Missbrauch von RACF-Attributen unter z/O
			M 2.289	(A)	Umsetzg.	Einsatz restriktiver z/OS-Kennungen	G 5.19	Missbrauch von Benutzerrechte
							G 5.122	Missbrauch von RACF-Attributen unter z/O
			M 2.290	(Z)	Umsetzg.	Einsatz von RACF-Exits	G 5.118	Unbefugtes Erlangen höherer Rechte im RAC
							G 5.119	Benutzung fremder Kennungen unter z/OS-System
							G 5.122	Missbrauch von RACF-Attributen unter z/O
			M 2.291	(C)	Betrieb	Sicherheits-Berichtswesen und -Audits unter z/OS	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.116	Manipulation der z/OS-Systemsteuerun
							G 5.117	Verschleiern von Manipulationen unter z/O
							G 5.119	Benutzung fremder Kennungen unter z/OS-System
			M 2.292	(B)	Betrieb	Überwachung von z/OS-Systemen	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.74	Unzureichender Schutz der z/OS-Systemeinstellungen v dynamischen Änderunge
							G 3.75	Mangelhafte Kontrolle der Batch-Jobs bei z/O
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.119	Benutzung fremder Kennungen unter z/OS-System
							G 5.122	Missbrauch von RACF-Attributen unter z/O
			M 2.293	(C)	Betrieb	Wartung von zSeries-Systemen	G 2.27	Fehlende oder unzureichende Dokumentatio
							G 4.22	Software-Schwachstellen oder -Fehle
			M 2.294	(Z)	Betrieb	Synchronisierung von z/OS-Passwörtern und RACF-Kommandos	G 3.73	Fehlbedienung der z/OS-Systemfunktionen
			M 2.295	(A)	Planung	Systemverwaltung von z/OS-Systemen	G 3.9	Fehlerhafte Administration des IT-System
							G 3.70	Unzureichender Dateischutz des z/OS-System
							G 5.122	Missbrauch von RACF-Attributen unter z/O
			M 2.296	(Z)	Planung	Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren	G 3.70	Unzureichender Dateischutz des z/OS-System
							G 5.119	Benutzung fremder Kennungen unter z/OS-System
			M 2.297	(B)	Aussnd.	Deinstallation von z/OS-Systeme	G 2.54	Vertraulichkeitsverlust durch Restinformatione
			M 3.39	(A)	Planung	Einführung in die zSeries-Plattform	G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.9	Fehlerhafte Administration des IT-System
			M 3.40	(A)	Planung	Einführung in das z/OS-Betriebssystem	G 3.67	Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems

							G 3.68	Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers
							G 3.69	Fehlerhafte Konfiguration der Unix System Services unte z/OS
							G 3.70	Unzureichender Dateischutz des z/OS-System
							G 3.72	Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF
							G 3.73	Fehlbedienung der z/OS-Systemfunktione
			M 3.41	(A)	Planung	Einführung in Linux und z/VM für zSeries-Systeme	G 5.120	Manipulation der Linux/zSeries Systemsteuerung
			M 3.42	(A)	Umsetzg.	Schulung des z/OS-Bedienungspersonals	G 3.67	Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems
							G 3.68	Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers
							G 3.69	Fehlerhafte Konfiguration der Unix System Services unte z/OS
							G 3.70	Unzureichender Dateischutz des z/OS-System
							G 3.71	Fehlerhafte Systemzeit bei z/OS-Systeme
							G 3.72	Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF
							G 3.73	Fehlbedienung der z/OS-Systemfunktione
			M 4.207	(A)	Umsetzg.	Einsatz und Sicherung systemnaher z/OS-Terminals	G 3.73	Fehlbedienung der z/OS-Systemfunktione
							G 3.74	Unzureichender Schutz der z/OS-Systemeinstellungen v dynamischen Änderunge
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.116	Manipulation der z/OS-Systemsteuerun
							G 5.120	Manipulation der Linux/zSeries Systemsteuerur
			M 4.208	(B)	Umsetzg.	Absichern des Start-Vorgangs von z/OS-Systemer	G 3.73	Fehlbedienung der z/OS-Systemfunktione
							G 5.116	Manipulation der z/OS-Systemsteuerun
			M 4.209	(A)	Umsetzg.	Sichere Grundkonfiguration von z/OS-Systemen	G 3.67	Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems
							G 3.68	Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers
							G 3.69	Fehlerhafte Konfiguration der Unix System Services unte z/OS
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.21	Trojanische Pferde
			M 4.210	(B)	Betrieb	Sicherer Betrieb des z/OS-Betriebssystems	G 3.73	Fehlbedienung der z/OS-Systemfunktione
							G 3.75	Mangelhafte Kontrolle der Batch-Jobs bei z/O
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.50	Überlastung des z/OS-Betriebssystem
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde

							G 5.116	Manipulation der z/OS-Systemsteuerun
							G 5.120	Manipulation der Linux/zSeries Systemsteuerur
			M 4.211	(A)	Umsetzg.	Einsatz des z/OS-Sicherheitssystems RACF	G 2.54	Vertraulichkeitsverlust durch Restinformatione
							G 3.38	Konfigurations- und Bedienungsfehle
							G 3.70	Unzureichender Dateischutz des z/OS-Systen
							G 3.72	Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.21	Trojanische Pferde
							G 5.118	Unbefugtes Erlangen höherer Rechte im RAC
			M 4.212	(Z)	Umsetzg.	Absicherung von Linux für zSeries	G 3.70	Unzureichender Dateischutz des z/OS-Systen
							G 3.73	Fehlbedienung der z/OS-Systemfunktione
							G 3.74	Unzureichender Schutz der z/OS-Systemeinstellungen v dynamischen Änderunge
							G 5.116	Manipulation der z/OS-Systemsteuerun
							G 5.120	Manipulation der Linux/zSeries Systemsteuerur
			M 4.213	(A)	Umsetzg.	Absichern des Login-Vorgangs unter z/OS	G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.19	Missbrauch von Benutzerrechte
							G 5.21	Trojanische Pferde
							G 5.121	Angriffe über TCP/IP auf z/OS-System
			M 4.214	(B)	Betrieb	Datenträgerverwaltung unter z/OS-Systemen	G 3.70	Unzureichender Dateischutz des z/OS-Systems
			M 4.215	(B)	Betrieb	Absicherung sicherheitskritischer z/OS-Dienstprogramme	G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.70	Unzureichender Dateischutz des z/OS-Systen
							G 5.2	Manipulation an Daten oder Softwar
							G 5.118	Unbefugtes Erlangen höherer Rechte im RAC
							G 5.121	Angriffe über TCP/IP auf z/OS-System
			M 4.216	(C)	Umsetzg.	Festlegung der Systemgrenzen von z/OS	G 4.50	Überlastung des z/OS-Betriebssystems
			M 4.217	(C)	Umsetzg.	Workload Management für z/OS-Systeme	G 4.50	Überlastung des z/OS-Betriebssystems
			M 4.218	(Z)	Betrieb	Hinweise zur Zeichensatzkonvertierung bei z/OS-Systemen	G 3.66	Fehlerhafte Zeichensatzkonvertierung beim Einsatz von z/OS
			M 4.219	(C)	Umsetzg.	Lizenzschlüssel-Management für z/OS-Software	G 2.27	Fehlende oder unzureichende Dokumentatio
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.28	Verhinderung von Dienste
			M 4.220	(B)	Umsetzg.	Absicherung von Unix System Services bei z/OS-Systemer	G 3.69	Fehlerhafte Konfiguration der Unix System Services unte z/OS
			M 4.221	(C)	Planung	Parallel-Sysplex unter z/O	G 3.71	Fehlerhafte Systemzeit bei z/OS-Systeme

			M 5.113	(Z)	Umsetzg.	Einsatz des VTAM Session Management Exit unter z/O	G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
			M 5.114	(B)	Umsetzg.	Absicherung der z/OS-Tracefunktionen	G 5.57	Netzanalyse-Tools
			M 6.67	(A)	Notfallv.	Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.116	Manipulation der z/OS-Systemsteuerun
							G 5.117	Verschleiern von Manipulationen unter z/O
							G 5.119	Benutzung fremder Kennungen unter z/OS-System
			M 6.93	(A)	Notfallv.	Notfallvorsorge für z/OS-Systeme	G 2.27	Fehlende oder unzureichende Dokumentatio
							G 3.73	Fehlbedienung der z/OS-Systemfunktione
							G 4.22	Software-Schwachstellen oder -Fehle
B 3.201	(5.99)	Allgemeiner Client	M 2.22	(A)	Betrieb	Hinterlegen des Passwortes	G 1.1	Personalausfal
			M 2.23	(Z)	Planung	Herausgabe einer PC-Richtlinie	G 2.1	Fehlende oder unzureichende Regelunge
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 2.25	(A)	Umsetzg.	Dokumentation der Systemkonfiguratior	G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
			M 2.204	(A)	Betrieb	Verhinderung ungesicherter Netzzugänge	G 2.7	Unerlaubte Ausübung von Rechte
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitunge
							G 5.9	Unberechtigte IT-Nutzun
			M 2.273	(A)	Betrieb	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 2.321	(A)	Planung	Planung des Einsatzes von Client-Server-Netzen	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.40	Abhören von Räumen mittels Rechner mit Mikrofo

							G 5.43	Makro-Viren
			M 2.322	(A)	Planung	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-Systen
							G 3.17	Kein ordnungsgemäßer PC-Benutzerwechse
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 2.323	(A)	Aussnd.	Geregelte Außerbetriebnahme eines Clients	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 4.13	Verlust gespeicherter Dater
							G 5.9	Unberechtigte IT-Nutzun
			M 3.18	(A)	Betrieb	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung	G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 3.17	Kein ordnungsgemäßer PC-Benutzerwechse
							G 5.2	Manipulation an Daten oder Softwar
			M 4.2	(A)	Umsetzg.	Bildschirmsperre	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.17	Kein ordnungsgemäßer PC-Benutzerwechse
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
			M 4.3	(A)	Betrieb	Regelmäßiger Einsatz eines Anti-Viren-Programms	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.4	(C)	Betrieb	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-Systen

							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.40	(A)	Umsetzg.	Verhinderung der unautorisierten Nutzung des Rechnermikrofon	G 5.40	Abhören von Räumen mittels Rechner mit Mikrofon
			M 4.41	(C)	Betrieb	Einsatz angemessener Sicherheitsprodukte für IT-Systeme	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
			M 4.93	(B)	Betrieb	Regelmäßige Integritätsprüfung	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.200	(Z)	Betrieb	Umgang mit USB-Speichermedien	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.234	(A)	Aussnd.	Aussonderung von IT-Systeme	G 5.9	Unberechtigte IT-Nutzun
			M 4.236	(Z)	Betrieb	Zentrale Administration von Laptops	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.237	(A)	Umsetzg.	Sichere Grundkonfiguration eines IT-Systems	G 2.7	Unerlaubte Ausübung von Rechte
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.7	Abhören von Leitunge

							G 5.20	Missbrauch von Administratorrechte
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.238	(A)	Betrieb	Einsatz eines lokalen Paketfilters	G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
			M 4.241	(A)	Betrieb	Sicherer Betrieb von Clients	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.40	Abhören von Räumen mittels Rechner mit Mikrof
							G 5.43	Makro-Viren
			M 4.242	(Z)	Umsetzg.	Einrichten einer Referenzinstallation für Clients	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.40	Abhören von Räumen mittels Rechner mit Mikrof
							G 5.43	Makro-Viren
			M 5.37	(B)	Planung	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz	G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäter
							G 3.9	Fehlerhafte Administration des IT-System
			M 5.45	(B)	Betrieb	Sicherheit von WWW-Browsern	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 6.24	(A)	Notfallv.	Erstellen eines Notfall-Bootmediums	G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 6.32	(A)	Notfallv.	Regelmäßige Datensicherung	G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl

							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
B 3.202	(5.99)	Allgemeines nicht vernetztes IT-System	M 2.22	(Z)	Betrieb	Hinterlegen des Passwortes	G 1.1	Personalausfal
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
			M 2.23	(Z)	Planung	Herausgabe einer PC-Richtlinie	G 2.1	Fehlende oder unzureichende Regelunge
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 2.63	(A)	Planung	Einrichten der Zugriffsrechte	G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 5.20	Missbrauch von Administratorrechte
							G 5.21	Trojanische Pferde
			M 3.18	(A)	Betrieb	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung	G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 3.17	Kein ordnungsgemäßer PC-Benutzerwechse
			M 4.2	(A)	Umsetzg.	Bildschirmsperre	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.4	(Z)	Betrieb	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern	G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-Systen
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.7	(A)	Umsetzg.	Änderung voreingestellter Passwörter	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
			M 4.15	(A)	Umsetzg.	Gesichertes Login	G 2.7	Unerlaubte Ausübung von Rechte

							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
			M 4.30	(A)	Betrieb	Nutzung der in Anwendungsprogrammen angebotener Sicherheitsfunktionen	G 1.1	Personalausfal
							G 1.2	Ausfall des IT-System
							G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-Systen
							G 4.1	Ausfall der Stromversorgun
							G 4.7	Defekte Datenträger
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.40	(C)	Betrieb	Verhinderung der unautorisierten Nutzung des Rechnermikrofon	G 5.40	Abhören von Räumen mittels Rechner mit Mikrofon
			M 4.41	(Z)	Planung	Einsatz angemessener Sicherheitsprodukte für IT-Systeme	G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 5.19	Missbrauch von Benutzerrechte
			M 6.20	(A)	Notfallv.	Geeignete Aufbewahrung der Backup-Datenträger	G 1.2	Ausfall des IT-System
							G 1.4	Feuer
							G 1.5	Wasser
							G 1.8	Staub, Verschmutzun
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-Systen
							G 4.1	Ausfall der Stromversorgun
							G 4.7	Defekte Datenträger
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 6.22	(A)	Notfallv.	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen	G 1.2	Ausfall des IT-System
							G 1.4	Feuer
							G 1.5	Wasser
							G 1.8	Staub, Verschmutzun

							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 4.7	Defekte Datenträger
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 6.32	(A)	Notfallv.	Regelmäßige Datensicherung	G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
B 3.203	(5.3)	Laptop	M 1.33	(A)	Betrieb	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz	G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebur
							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.8	Unkontrollierter Einsatz von Betriebsmittel
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 4.52	Datenverlust bei mobilem Einsat
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.22	Diebstahl bei mobiler Nutzung des IT-System
			M 1.34	(A)	Betrieb	Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.8	Unkontrollierter Einsatz von Betriebsmittel
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
			M 1.35	(Z)	Betrieb	Sammelaufbewahrung tragbarer IT-Systeme	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.8	Unkontrollierter Einsatz von Betriebsmittel
							G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PC
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
			M 1.46	(Z)	Betrieb	Einsatz von Diebstahl-Sicherunge	G 5.4	Diebstahl
			M 2.36	(B)	Betrieb	Geregelte Übergabe und Rücknahme	G 2.8	Unkontrollierter Einsatz von Betriebsmittel

						eines tragbaren PC	G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PC
							G 5.9	Unberechtigte IT-Nutzun
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 2.218	(B)	Planung	Regelung der Mitnahme von Datenträgern und IT-Komponenten	G 1.2	Ausfall des IT-System
							G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebur
							G 2.8	Unkontrollierter Einsatz von Betriebsmittel
							G 4.52	Datenverlust bei mobilem Einsat
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.124	Missbrauch der Informationen von mobilen Endgerät
							G 5.125	Unberechtigte Datenweitergabe über mobile Endgerät
			M 2.306	(B)	Aussnd.	Verlustmeldun	G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 2.309	(A)	Planung	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.8	Unkontrollierter Einsatz von Betriebsmittel
							G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PC
							G 3.8	Fehlerhafte Nutzung des IT-Syster
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.124	Missbrauch der Informationen von mobilen Endgerät
							G 5.125	Unberechtigte Datenweitergabe über mobile Endgerät
							G 5.126	Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten
			M 2.310	(A)	Beschaff.	Geeignete Auswahl von Laptops	G 2.7	Unerlaubte Ausübung von Rechte
							G 5.9	Unberechtigte IT-Nutzun
							G 5.126	Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten
			M 4.3	(A)	Betrieb	Regelmäßiger Einsatz eines Anti-Viren-Programms	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.27	(A)	Betrieb	Zugriffsschutz am Laptop	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
			M 4.28	(Z)	Betrieb	Software-Reinstallation bei Benutzerwechsel eines Laptops	G 2.8	Unkontrollierter Einsatz von Betriebsmittel
							G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PC
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren

			M 4.29	(Z)	Planung	Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.8	Unkontrollierter Einsatz von Betriebsmitteln
							G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PC
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.22	Diebstahl bei mobiler Nutzung des IT-System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 4.31	(A)	Betrieb	Sicherstellung der Energieversorgung im mobilen Einsatz	G 1.2	Ausfall des IT-System
							G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebur
							G 4.9	Ausfall der internen Stromversorgun
							G 4.52	Datenverlust bei mobilem Einsat
			M 4.40	(A)	Umsetzg.	Verhinderung der unautorisierten Nutzung des Rechnermikrofon	G 5.123	Abhören von Raumgesprächen über mobile Endgeräte
			M 4.235	(B)	Betrieb	Abgleich der Datenbestände von Laptops	G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.76	Fehler bei der Synchronisation mobiler Endgerät
							G 4.13	Verlust gespeicherter Dater
							G 4.19	Informationsverlust bei erschöpftem Speichermediu
			M 4.236	(Z)	Betrieb	Zentrale Administration von Laptops	G 2.8	Unkontrollierter Einsatz von Betriebsmitteln
							G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PC
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.38	Konfigurations- und Bedienungsfehle
			M 4.255	(A)	Betrieb	Nutzung von IrDA-Schnittstellen	G 3.8	Fehlerhafte Nutzung des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.124	Missbrauch der Informationen von mobilen Endgeräte
							G 5.125	Unberechtigte Datenweitergabe über mobile Endgerät
			M 5.91	(A)	Betrieb	Einsatz von Personal Firewalls für Internet-PCs	G 3.38	Konfigurations- und Bedienungsfehle
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.18	Systematisches Ausprobieren von Passwörter
			M 5.121	(A)	Betrieb	Sichere Kommunikation von unterwegs	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.124	Missbrauch der Informationen von mobilen Endgeräte
							G 5.125	Unberechtigte Datenweitergabe über mobile Endgerät
			M 5.122	(A)	Betrieb	Sicherer Anschluss von Laptops an lokale Netze	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren

			M 6.71	(A)	Notfallv.	Datensicherung bei mobiler Nutzung des IT-Systems	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 4.13	Verlust gespeicherter Dater
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
B 3.204	(5.2)	Client unter Unix	M 2.31	(A)	Betrieb	Dokumentation der zugelassenen Benutzer und Rechteprofile	G 1.1	Personalausfal
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
							G 5.9	Unberechtigte IT-Nutzun
							G 5.19	Missbrauch von Benutzerrechte
			M 2.32	(Z)	Umsetzg.	Einrichtung einer eingeschränkten Benutzerumgebung	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Clien
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
			M 2.33	(Z)	Planung	Aufteilung der Administrationstätigkeiten unter Unix	G 1.1	Personalausfal
							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.9	Unberechtigte IT-Nutzun
							G 5.20	Missbrauch von Administratorrechte
			M 4.9	(A)	Umsetzg.	Einsatz der Sicherheitsmechanismen von X-Windows	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme

							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
			M 4.13	(A)	Planung	Sorgfältige Vergabe von IDs	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
			M 4.14	(A)	Umsetzg.	Obligatorischer Passwortschutz unter Unix	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Clien
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.21	Trojanische Pferde
			M 4.16	(C)	Umsetzg.	Zugangsbeschränkungen für Accounts und / oder Terminals	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 4.8	Bekanntwerden von Softwareschwachstelle
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.9	Unberechtigte IT-Nutzun
							G 5.19	Missbrauch von Benutzerrechte
			M 4.17	(A)	Umsetzg.	Sperren und Löschen nicht benötigter Accounts und Terminals	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz

							G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.19	Missbrauch von Benutzerrechte
			M 4.18	(A)	Planung	Administrative und technische Absicherung des Zugangs zum Monitor und Single-User-Modus	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-Syster
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.20	Missbrauch von Administratorrechte
			M 4.19	(A)	Umsetzg.	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.8	Fehlerhafte Nutzung des IT-Syster
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
			M 4.20	(B)	Umsetzg.	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.8	Fehlerhafte Nutzung des IT-Syster
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.19	Missbrauch von Benutzerrechte
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
			M 4.21	(A)	Umsetzg.	Verhinderung des unautorisierten Erlangens von Administratorrechten	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date

							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Clien
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.20	Missbrauch von Administratorrechte
			M 4.22	(Z)	Umsetzg.	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Clien
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
							G 5.2	Manipulation an Daten oder Softwar
							G 5.19	Missbrauch von Benutzerrechte
			M 4.23	(B)	Umsetzg.	Sicherer Aufruf ausführbarer Dateien	G 2.7	Unerlaubte Ausübung von Rechte
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
			M 4.25	(A)	Betrieb	Einsatz der Protokollierung im Unix-System	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.21	Trojanische Pferde
			M 4.26	(C)	Betrieb	Regelmäßiger Sicherheitscheck des Unix-Systems	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
			M 4.105	(A)	Umsetzg.	Erste Maßnahmen nach einer Unix-	G 2.7	Unerlaubte Ausübung von Rechte

						Standardinstallation	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
			M 4.106	(B)	Umsetzg.	Aktivieren der Systemprotokollierung	G 2.7	Unerlaubte Ausübung von Rechte
							G 5.18	Systematisches Ausprobieren von Passwörter
			M 5.17	(A)	Umsetzg.	Einsatz der Sicherheitsmechanismen von NFS	G 2.7	Unerlaubte Ausübung von Rechten
			M 5.18	(A)	Umsetzg.	Einsatz der Sicherheitsmechanismen von NIS	G 2.7	Unerlaubte Ausübung von Rechte
							G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Clien
			M 5.19	(A)	Umsetzg.	Einsatz der Sicherheitsmechanismen von sendmail	G 2.7	Unerlaubte Ausübung von Rechte
							G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 5.20	(A)	Umsetzg.	Einsatz der Sicherheitsmechanismen von rlogin, rsh und rc	G 2.7	Unerlaubte Ausübung von Rechten
			M 5.21	(A)	Umsetzg.	Sicherer Einsatz von telnet, ftp, tftp und rexec	G 2.7	Unerlaubte Ausübung von Rechten
			M 5.34	(Z)	Planung	Einsatz von Einmalpasswörtern	G 2.7	Unerlaubte Ausübung von Rechte
							G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 5.35	(A)	Umsetzg.	Einsatz der Sicherheitsmechanismen von UUCP	G 2.7	Unerlaubte Ausübung von Rechte
							G 5.41	Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
			M 5.36	(Z)	Planung	Verschlüsselung unter Unix und Windows NT	G 2.7	Unerlaubte Ausübung von Rechte
							G 5.89	Hijacking von Netz-Verbindunge
			M 5.64	(Z)	Planung	Secure Shel	G 5.89	Hijacking von Netz-Verbindunge
			M 5.72	(A)	Umsetzg.	Deaktivieren nicht benötigter Netzdienste	G 1.8	Staub, Verschmutzun
							G 2.7	Unerlaubte Ausübung von Rechte
							G 5.9	Unberechtigte IT-Nutzun
			M 6.31	(A)	Notfallv.	Verhaltensregeln nach Verlust der Systemintegrität	G 1.2	Ausfall des IT-System
							G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
							G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitunge

							G 5.8	Manipulation an Leitunge
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
B 3.205	(5.5)	Client unter Windows NT	M 2.31	(B)	Betrieb	Dokumentation der zugelassenen Benutzer und Rechteprofile	G 1.1	Personalausfal
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 2.32	(Z)	Umsetzg.	Einrichtung einer eingeschränkten Benutzerumgebung	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.31	Unzureichender Schutz des Windows NT System
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.17	(B)	Umsetzg.	Sperren und Löschen nicht benötigter Accounts und Terminals	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.31	Unzureichender Schutz des Windows NT System
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
			M 4.48	(A)	Planung	Passwortschutz unter Windows NT/2000/XP	G 2.31	Unzureichender Schutz des Windows NT System
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.49	(A)	Planung	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System	G 2.31	Unzureichender Schutz des Windows NT System
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
			M 4.50	(Z)	Planung	Strukturierte Systemverwaltung unter Windows NT	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.31	Unzureichender Schutz des Windows NT System
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun

							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.51	(Z)	Planung	Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT	G 2.31	Unzureichender Schutz des Windows NT System
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.52	(B)	Umsetzg.	Geräteschutz unter Windows NT/2000/XP	G 2.7	Unerlaubte Ausübung von Rechten
							G 2.31	Unzureichender Schutz des Windows NT System
							G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
							G 5.2	Manipulation an Daten oder Software
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.53	(A)	Planung	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT	G 2.7	Unerlaubte Ausübung von Rechten
							G 2.31	Unzureichender Schutz des Windows NT System
							G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
							G 5.2	Manipulation an Daten oder Software
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.54	(Z)	Umsetzg.	Protokollierung unter Windows NT	G 2.7	Unerlaubte Ausübung von Rechten
							G 2.31	Unzureichender Schutz des Windows NT System
							G 5.2	Manipulation an Daten oder Software
							G 5.9	Unberechtigte IT-Nutzung
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.55	(B)	Umsetzg.	Sichere Installation von Windows NT	G 2.7	Unerlaubte Ausübung von Rechten
							G 2.31	Unzureichender Schutz des Windows NT System
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.56	(B)	Betrieb	Sicheres Löschen unter Windows-Betriebssystemen	G 2.7	Unerlaubte Ausübung von Rechten
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
			M 4.57	(A)	Umsetzg.	Deaktivieren der automatischen CD-ROM-Erkennung	G 4.23	Automatische CD-ROM-Erkennung
							G 5.21	Trojanische Pferde

							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.75	(A)	Umsetzg.	Schutz der Registrierung unter Windows NT/2000/XP	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.31	Unzureichender Schutz des Windows NT System
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.76	(C)	Planung	Sichere Systemversion von Windows NT	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.77	(A)	Umsetzg.	Schutz der Administratorkonten unter Windows NT	G 5.9	Unberechtigte IT-Nutzun
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 6.42	(A)	Notfallv.	Erstellung von Rettungsdisketten für Windows NT	G 1.2	Ausfall des IT-Systems
							G 2.31	Unzureichender Schutz des Windows NT System
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 6.44	(A)	Notfallv.	Datensicherung unter Windows NT	G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.1	Ausfall der Stromversorgun
							G 4.7	Defekte Datenträger
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
B 3.206	(5.6)	Client unter Windows 95	M 2.63	(A)	Planung	Einrichten der Zugriffsrechte	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz

							G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.60	Umgehen der Systemrichtlinie
			M 2.65	(Z)	Betrieb	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 2.36	Ungeeignete Einschränkung der Benutzerumgebur
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.17	Kein ordnungsgemäßer PC-Benutzerwechse
							G 5.60	Umgehen der Systemrichtlinie
			M 2.103	(A)	Planung	Einrichten von Benutzerprofilen unter Windows 95	G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 3.17	Kein ordnungsgemäßer PC-Benutzerwechse
							G 5.60	Umgehen der Systemrichtlinie
			M 2.104	(Z)	Planung	Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 2.36	Ungeeignete Einschränkung der Benutzerumgebur
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.17	Kein ordnungsgemäßer PC-Benutzerwechse
							G 3.22	Fehlerhafte Änderung der Registrierun
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.60	Umgehen der Systemrichtlinie
			M 3.18	(A)	Betrieb	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung	G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 3.17	Kein ordnungsgemäßer PC-Benutzerwechse
							G 5.60	Umgehen der Systemrichtlinie

			M 4.41	(Z)	Planung	Einsatz angemessener Sicherheitsprodukte für IT-Systeme	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.22	Fehlende Auswertung von Protokolldate
							G 2.35	Fehlende Protokollierung unter Windows 9
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.17	Kein ordnungsgemäßer PC-Benutzerwechse
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.60	Umgehen der Systemrichtlinie
			M 4.56	(B)	Betrieb	Sicheres Löschen unter Windows-Betriebssystemen	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.17	Kein ordnungsgemäßer PC-Benutzerwechse
							G 5.2	Manipulation an Daten oder Softwar
			M 4.57	(A)	Umsetzg.	Deaktivieren der automatischen CD-ROM-Erkennung	G 4.23	Automatische CD-ROM-Erkennun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.74	(A)	Planung	Vernetzte Windows 95 Rechner	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 5.2	Manipulation an Daten oder Softwar
			M 6.45	(A)	Notfallv.	Datensicherung unter Windows 95	G 1.2	Ausfall des IT-System
							G 1.4	Feuer
							G 1.5	Wasser
							G 1.8	Staub, Verschmutzun
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.22	Fehlerhafte Änderung der Registrierun
							G 4.24	Dateinamenkonvertierung bei Datensicherungen unter Windows 95
							G 5.21	Trojanische Pferde
			M 6.46	(A)	Notfallv.	Erstellung von Rettungsdisketten für Windows 95	G 1.2	Ausfall des IT-System
							G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr

							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.22	Fehlerhafte Änderung der Registrierun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
B 3.207	(5.7)	Client unter Windows 2000	M 2.31	(B)	Betrieb	Dokumentation der zugelassenen Benutzer und Rechteprofile	G 1.1	Personalausfal
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.9	Unberechtigte IT-Nutzun
			M 2.32	(Z)	Umsetzg.	Einrichtung einer eingeschränkten Benutzerumgebung	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 2.227	(A)	Planung	Planung des Windows 2000 Einsatzes	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.9	Unberechtigte IT-Nutzun
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
			M 2.228	(A)	Planung	Festlegen einer Windows 2000 Sicherheitsrichtlinie	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.9	Unberechtigte IT-Nutzun
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
			M 2.231	(A)	Planung	Planung der Gruppenrichtlinien unter Windows 2000	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System

			M 3.28	(A)	Umsetzg.	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer	G 1.2	Ausfall des IT-System
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
			M 4.17	(A)	Umsetzg.	Sperren und Löschen nicht benötigter Accounts und Terminals	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
			M 4.48	(A)	Umsetzg.	Passwortschutz unter Windows NT/2000/XP	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.49	(A)	Umsetzg.	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.52	(A)	Umsetzg.	Geräteschutz unter Windows NT/2000/XP	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.2	Manipulation an Daten oder Softwar
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.57	(A)	Umsetzg.	Deaktivieren der automatischen CD-ROM-Erkennung	G 4.23	Automatische CD-ROM-Erkennun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren

			M 4.75	(A)	Umsetzg.	Schutz der Registrierung unter Windows NT/2000/XP	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.136	(A)	Umsetzg.	Sichere Installation von Windows 2000	G 1.2	Ausfall des IT-Systems
							G 2.7	Unerlaubte Ausübung von Rechten
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.8	Bekanntwerden von Softwareschwachstellen
							G 5.2	Manipulation an Daten oder Software
							G 5.9	Unberechtigte IT-Nutzung
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.147	(Z)	Betrieb	Sichere Nutzung von EFS unter Windows 2000/XP	G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.148	(B)	Betrieb	Überwachung eines Windows 2000/XP Systems	G 2.7	Unerlaubte Ausübung von Rechten
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.2	Manipulation an Daten oder Software
							G 5.9	Unberechtigte IT-Nutzung
							G 5.18	Systematisches Ausprobieren von Passwörtern
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.149	(A)	Umsetzg.	Datei- und Freigabeberechtigungen unter Windows 2000/XP	G 2.7	Unerlaubte Ausübung von Rechten
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 5.2	Manipulation an Daten oder Software
							G 5.9	Unberechtigte IT-Nutzung
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 4.150	(A)	Umsetzg.	Konfiguration von Windows 2000 als Workstation	G 2.7	Unerlaubte Ausübung von Rechten
							G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 5.2	Manipulation an Daten oder Software
							G 5.9	Unberechtigte IT-Nutzung

			M 6.77	(A)	Notfallv.	Erstellung von Rettungsdisketten für Windows 2000	G 1.2	Ausfall des IT-System
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-Syster
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.7	Defekte Datenträger
							G 5.2	Manipulation an Daten oder Softwar
			M 6.78	(A)	Notfallv.	Datensicherung unter Windows 2000/XP	G 1.2	Ausfall des IT-System
							G 1.4	Feuer
							G 1.5	Wasser
							G 1.8	Staub, Verschmutzun
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-Syster
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.1	Ausfall der Stromversorgun
							G 4.7	Defekte Datenträger
							G 4.8	Bekanntwerden von Softwareschwachstelle
							G 4.23	Automatische CD-ROM-Erkennun
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
B 3.208	(5.8)	Internet-PC	M 2.234	(A)	Planung	Konzeption von Internet-PCs	G 1.2	Ausfall des IT-System
							G 2.1	Fehlende oder unzureichende Regelunge
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.38	Konfigurations- und Bedienungsfehle
			M 2.235	(A)	Planung	Richtlinien für die Nutzung von Internet-PCs	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.38	Konfigurations- und Bedienungsfehle
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.88	Missbrauch aktiver Inhalt
			M 2.313	(A)	Betrieb	Sichere Anmeldung bei Internet-Diensten	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
			M 4.3	(A)	Betrieb	Regelmäßiger Einsatz eines Anti-Viren-Programms	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.2	Manipulation an Daten oder Softwar

						G 5.21	Trojanische Pferde
						G 5.23	Computer-Viren
						G 5.43	Makro-Viren
			M 4.41	(Z)	Planung	Einsatz angemessener Sicherheitsprodukte für IT-Systeme	G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.44	(A)	Betrieb	Prüfung eingehender Dateien auf Makro-Viren	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.2	Manipulation an Daten oder Softwar
							G 5.43	Makro-Viren
			M 4.151	(B)	Umsetzg.	Sichere Installation von Internet-PCs	G 1.2	Ausfall des IT-System
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.38	Konfigurations- und Bedienungsfehle
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.152	(B)	Betrieb	Sicherer Betrieb von Internet-PCs	G 1.2	Ausfall des IT-System
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.38	Konfigurations- und Bedienungsfehle
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 5.59	(C)	Umsetzg.	Schutz vor DNS-Spoofin	G 5.78	DNS-Spoofing
			M 5.66	(B)	Planung	Verwendung von SSL	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 5.48	IP-Spoofing
							G 5.87	Web-Spoofing
							G 5.88	Missbrauch aktiver Inhalt
			M 5.91	(Z)	Planung	Einsatz von Personal Firewalls für Internet-PCs	G 3.38	Konfigurations- und Bedienungsfehle
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.91	Abschalten von Sicherheitsmechanismen für den RAS-Zugang
			M 5.92	(B)	Planung	Sichere Internet-Anbindung von Internet-PCs	G 3.38	Konfigurations- und Bedienungsfehle
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.78	DNS-Spoofing
			M 5.93	(A)	Betrieb	Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.88	Missbrauch aktiver Inhalt

			M 5.94	(A)	Betrieb	Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 5.95	(B)	Betrieb	Sicherer E-Commerce bei der Nutzung von Internet-PCs	G 1.2	Ausfall des IT-Systems
							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzerr
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.87	Web-Spoofing
			M 5.96	(A)	Betrieb	Sichere Nutzung von Webmail	G 5.48	IP-Spoofing
							G 5.88	Missbrauch aktiver Inhalte
							G 5.103	Missbrauch von Webmai
			M 5.98	(C)	Umsetzg.	Schutz vor Missbrauch kostenpflichtiger Einwahlnummern	G 5.21	Trojanische Pferde
							G 5.88	Missbrauch aktiver Inhalte
			M 6.79	(A)	Notfallv.	Datensicherung beim Einsatz von Internet-PCs	G 1.2	Ausfall des IT-Systems
							G 3.38	Konfigurations- und Bedienungsfehle
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
B 3.209	(5.9)	Client unter Windows XP	M 2.32	(Z)	Umsetzg.	Einrichtung einer eingeschränkten Benutzerumgebung	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemer
			M 2.324	(A)	Planung	Einführung von Windows XP planen	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.9	Unberechtigte IT-Nutzun
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
			M 2.325	(A)	Planung	Planung der Windows XP Sicherheitsrichtlinie	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 5.9	Unberechtigte IT-Nutzun
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
			M 2.326	(A)	Planung	Planung der Windows XP	G 2.7	Unerlaubte Ausübung von Rechte

						Gruppenrichtlinien	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
			M 2.327	(B)	Planung	Sicherheit beim Fernzugriff unter Windows XP	G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 5.7	Abhören von Leitungen
							G 5.9	Unberechtigte IT-Nutzun
			M 2.328	(B)	Planung	Einsatz von Windows XP auf mobilen Rechnern	G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.85	Integritätsverlust schützenswerter Information
			M 2.329	(A)	Betrieb	Einführung von Windows XP SP2	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.8	Bekanntwerden von Softwareschwachstelle
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
			M 2.330	(B)	Betrieb	Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
			M 3.28	(A)	Planung	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer	G 1.2	Ausfall des IT-Systems
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
			M 4.48	(A)	Planung	Passwortschutz unter Windows	G 2.7	Unerlaubte Ausübung von Rechte

						G 3.2	Fahrlässige Zerstörung von Gerät oder Date
						G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
						G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
						G 5.2	Manipulation an Daten oder Softwar
						G 5.9	Unberechtigte IT-Nutzun
						G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemer
			M 4.49	(A)	Betrieb	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System	G 2.7
							G 3.3
							G 3.6
							G 5.2
							G 5.9
							G 5.52
							G 5.79
			M 4.52	(A)	Betrieb	Geräteschutz unter Windows NT/2000/XP	G 2.7
							G 3.2
							G 3.3
							G 5.2
							G 5.52
							G 5.79
			M 4.56	(C)	Betrieb	Sicheres Löschen unter Windows-Betriebssystemen	G 5.71
			M 4.57	(A)	Planung	Deaktivieren der automatischen CD-ROM-Erkennung	G 4.23
							G 5.21
							G 5.23
							G 5.43
			M 4.75	(A)	Planung	Schutz der Registrierung unter Windows NT/2000/XP	G 2.9
							G 3.8
							G 5.52
							G 5.79
			M 4.146	(A)	Betrieb	Sicherer Betrieb von Windows 2000/XP	G 4.23
							G 5.7
							G 5.23
							G 5.52
							G 5.71
							G 5.83
							G 5.85

			M 4.147	(Z)	Planung	Sichere Nutzung von EFS unter Windows 2000/XP	G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.148	(B)	Betrieb	Überwachung eines Windows 2000/XP Systems	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.149	(A)	Planung	Datei- und Freigabeberechtigungen unter Windows 2000/XP	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.243	(Z)	Planung	Windows XP Verwaltungswerkzeuge	G 3.9	Fehlerhafte Administration des IT-System
			M 4.244	(A)	Planung	Sichere Windows XP Systemkonfiguration	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 4.23	Automatische CD-ROM-Erkennun
							G 5.2	Manipulation an Daten oder Softwar
			M 4.245	(A)	Planung	Basiseinstellungen für Windows XP GPOs	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 5.2	Manipulation an Daten oder Softwar
			M 4.246	(A)	Planung	Konfiguration der Systemdienste unter Windows XP	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 5.2	Manipulation an Daten oder Softwar

			M 4.247	(A)	Planung	Restriktive Berechtigungsvergabe unter Windows XP	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.22	Fehlerhafte Änderung der Registrierun
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
			M 4.248	(A)	Umsetzg.	Sichere Installation von Windows XP	G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 4.8	Bekanntwerden von Softwareschwachstelle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
			M 4.249	(A)	Betrieb	Windows XP Systeme aktuell halten	G 2.7	Unerlaubte Ausübung von Rechte
							G 4.8	Bekanntwerden von Softwareschwachstelle
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 5.37	(B)	Planung	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz	G 5.7	Abhören von Leitungen
							G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.85	Integritätsverlust schützenswerter Information
			M 5.89	(A)	Umsetzg.	Konfiguration des sicheren Kanals unter Windows 2000/XP	G 5.7	Abhören von Leitungen
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.85	Integritätsverlust schützenswerter Information
			M 5.90	(Z)	Umsetzg.	Einsatz von IPSec unter Windows 2000/XP	G 5.7	Abhören von Leitungen
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.85	Integritätsverlust schützenswerter Information
			M 5.123	(B)	Planung	Absicherung der Netzwerkkommunikation unter Windows XP	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.48	Fehlkonfiguration von Windows 2000/XP Rechner
							G 5.7	Abhören von Leitungen
							G 5.9	Unberechtigte IT-Nutzun
			M 6.76	(C)	Notfallv.	Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes	G 1.2	Ausfall des IT-Systems
							G 3.9	Fehlerhafte Administration des IT-System
							G 5.23	Computer-Viren

			M 6.78	(A)	Notfallv.	Datensicherung unter Windows 2000/XP	G 1.2	Ausfall des IT-System
							G 1.4	Feuer
							G 1.5	Wasser
							G 1.8	Staub, Verschmutzun
							G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahm
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.8	Fehlerhafte Nutzung des IT-Syster
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.1	Ausfall der Stromversorgun
							G 4.7	Defekte Datenträger
							G 4.8	Bekanntwerden von Softwareschwachstelle
							G 4.23	Automatische CD-ROM-Erkennun
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
B 3.301	(7.3)	Sicherheitsgateway (Firewall)	M 2.70	(A)	Planung	Entwicklung eines Konzepts für Sicherheitsgateways	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.25	Maskerade
							G 5.28	Verhinderung von Dienste
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
			M 2.71	(A)	Planung	Festlegung einer Policy für ein Sicherheitsgateway	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.38	Konfigurations- und Bedienungsfehle
							G 4.8	Bekanntwerden von Softwareschwachstelle
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.25	Maskerade
							G 5.28	Verhinderung von Dienste
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
			M 2.73	(A)	Beschaff.	Auswahl geeigneter Grundstrukturen für Sicherheitsgateways	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze

						G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
						G 5.2	Manipulation an Daten oder Softwar
						G 5.9	Unberechtigte IT-Nutzun
			M 2.74	(A)	Beschaff.	Geeignete Auswahl eines Paketfilters	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.48	IP-Spoofing
							G 5.49	Missbrauch des Source-Routing
							G 5.50	Missbrauch des ICMP-Protokolls
							G 5.51	Missbrauch der Routing-Protokolle
			M 2.75	(A)	Beschaff.	Geeignete Auswahl eines Application-Level-Gateways	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.48	IP-Spoofing
							G 5.49	Missbrauch des Source-Routing
							G 5.50	Missbrauch des ICMP-Protokolls
							G 5.51	Missbrauch der Routing-Protokolle
			M 2.76	(A)	Umsetzg.	Auswahl und Einrichtung geeigneter Filterregeln	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.48	IP-Spoofing
							G 5.49	Missbrauch des Source-Routing
							G 5.50	Missbrauch des ICMP-Protokolls
							G 5.51	Missbrauch der Routing-Protokolle
			M 2.77	(A)	Umsetzg.	Integration von Servern in das Sicherheitsgateway	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
			M 2.78	(A)	Betrieb	Sicherer Betrieb eines Sicherheitsgateways	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.38	Konfigurations- und Bedienungsfehle
							G 4.8	Bekanntwerden von Softwareschwachstelle

							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.20	Datenverlust bei erschöpftem Speichermedium
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.25	Maskerade
							G 5.28	Verhinderung von Dienste
							G 5.78	DNS-Spoofing
			M 2.299	(A)	Beschaff.	Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.38	Konfigurations- und Bedienungsfehle
			M 2.300	(C)	Aussnd.	Sichere Außerbetriebnahme oder Ersatz von Komponenten eines Sicherheitsgateways	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
			M 2.301	(Z)	Planung	Outsourcing des Sicherheitsgateway	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.38	Konfigurations- und Bedienungsfehle
			M 2.302	(Z)	Betrieb	Sicherheitsgateways und Hochverfügbarkei	G 5.28	Verhinderung von Diensten
			M 3.43	(C)	Umsetzg.	Schulung der Administratoren des Sicherheitsgateways	G 3.9	Fehlerhafte Administration des IT-System
							G 3.38	Konfigurations- und Bedienungsfehle
			M 4.47	(A)	Betrieb	Protokollierung der Sicherheitsgateway-Aktivitäten	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.38	Konfigurations- und Bedienungsfehle
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.20	Datenverlust bei erschöpftem Speichermedium
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.24	Wiedereinspielen von Nachrichte
							G 5.25	Maskerade
							G 5.28	Verhinderung von Dienste
			M 4.93	(B)	Betrieb	Regelmäßige Integritätsprüfung	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.2	Manipulation an Daten oder Softwar
			M 4.100	(C)	Betrieb	Sicherheitsgateways und aktive Inhalte	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze

							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
			M 4.101	(C)	Betrieb	Sicherheitsgateways und Verschlüsselung	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.2	Manipulation an Daten oder Softwar
			M 4.222	(B)	Betrieb	Festlegung geeigneter Einstellungen von Sicherheitsproxies	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
			M 4.223	(B)	Betrieb	Integration von Proxy-Servern in das Sicherheitsgateway	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
			M 4.224	(Z)	Betrieb	Integration von Virtual Private Networks in ein Sicherheitsgateway	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
			M 4.225	(Z)	Betrieb	Einsatz eines Protokollierungsservers in einem Sicherheitsgateway	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
			M 4.226	(Z)	Betrieb	Integration von Virenscannern in ein Sicherheitsgateway	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
			M 4.227	(C)	Betrieb	Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
			M 5.39	(A)	Betrieb	Sicherer Einsatz der Protokolle und Dienste	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Clien
							G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Clien
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.24	Wiedereinspielen von Nachrichte
							G 5.25	Maskerade
							G 5.48	IP-Spoofing
							G 5.49	Missbrauch des Source-Routin
							G 5.50	Missbrauch des ICMP-Protokolls
							G 5.51	Missbrauch der Routing-Protokolle
							G 5.78	DNS-Spoofing
			M 5.46	(A)	Betrieb	Einsatz von Stand-alone-Systemen zur Nutzung des Internets	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.38	Konfigurations- und Bedienungsfehle

						G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
						G 4.20	Datenverlust bei erschöpftem Speichermedium
						G 4.22	Software-Schwachstellen oder -Fehle
						G 4.39	Software-Konzeptionsfehle
						G 5.2	Manipulation an Daten oder Softwar
						G 5.9	Unberechtigte IT-Nutzun
						G 5.18	Systematisches Ausprobieren von Passwörter
						G 5.28	Verhinderung von Dienste
						G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
			M 5.59	(A)	Betrieb	Schutz vor DNS-Spoofin	G 5.78	DNS-Spoofing
			M 5.70	(A)	Betrieb	Adreßumsetzung - NAT (Network Address Translation)	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.28	Verhinderung von Dienste
			M 5.71	(Z)	Betrieb	Intrusion Detection und Intrusion Response Systeme	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.38	Konfigurations- und Bedienungsfehle
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.22	Software-Schwachstellen oder -Fehle
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.28	Verhinderung von Dienste
							G 5.49	Missbrauch des Source-Routin
							G 5.50	Missbrauch des ICMP-Protokolls
							G 5.51	Missbrauch der Routing-Protokolle
			M 5.115	(Z)	Betrieb	Integration eines Webservers in ein Sicherheitsgateway	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
			M 5.116	(Z)	Betrieb	Integration eines E-Mailservers in ein Sicherheitsgateway	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
			M 5.117	(Z)	Betrieb	Integration eines Datenbank-Servers in ein Sicherheitsgateway	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
			M 5.118	(Z)	Betrieb	Integration eines DNS-Servers in ein Sicherheitsgateway	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 5.78	DNS-Spoofing
			M 5.119	(Z)	Betrieb	Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes

			M 5.120	(A)	Betrieb	Behandlung von ICMP am Sicherheitsgateway	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 5.50	Missbrauch des ICMP-Protokolls
			M 6.94	(C)	Notfallv.	Notfallvorsorge bei Sicherheitsgateways	G 2.101	Unzureichende Notfallvorsorge bei einem Sicherheitsgateway
B 3.302	(7.11)	Router und Switches	M 1.43	(A)	Umsetzg.	Gesicherte Aufstellung aktiver Netzkomponenter	G 5.4	Diebstahl
			M 2.276	(Z)	Planung	Funktionsweise eines Routers	G 2.98	Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switche
			M 2.277	(Z)	Planung	Funktionsweise eines Switches	G 2.98	Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switche
			M 2.278	(Z)	Planung	Typische Einsatzszenarien von Routern und Switches	G 2.98	Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switche
			M 2.279	(A)	Planung	Erstellung einer Sicherheitsrichtlinie für Router und Switches	G 2.1	Fehlende oder unzureichende Regelungen
			M 2.280	(C)	Beschaff.	Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.44	Inkompatible aktive und passive Netzkomponente
							G 2.98	Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switche
			M 2.281	(A)	Betrieb	Dokumentation der Systemkonfiguration von Routern und Switches	G 2.27	Fehlende oder unzureichende Dokumentation
			M 2.282	(A)	Betrieb	Regelmäßige Kontrolle von Routern und Switches	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
			M 2.283	(B)	Betrieb	Software-Pflege auf Routern und Switches	G 4.8	Bekanntwerden von Softwareschwachstellen
			M 2.284	(C)	Aussnd.	Sichere Außerbetriebnahme von Routern und Switche	G 2.54	Vertraulichkeitsverlust durch Restinformationen
			M 3.38	(B)	Umsetzg.	Administratorenschulung für Router und Switches	G 3.64	Fehlerhafte Konfiguration von Routern und Switch
							G 3.65	Fehlerhafte Administration von Routern und Switche
			M 4.201	(A)	Umsetzg.	Sichere lokale Grundkonfiguration von Routern und Switches	G 3.64	Fehlerhafte Konfiguration von Routern und Switch
							G 4.49	Unsichere Default-Einstellungen auf Routern und Switches
			M 4.202	(A)	Umsetzg.	Sichere Netz-Grundkonfiguration von Routern und Switches	G 3.64	Fehlerhafte Konfiguration von Routern und Switch
							G 4.49	Unsichere Default-Einstellungen auf Routern und Switches
							G 5.112	Manipulation von ARP-Tabelle
							G 5.113	MAC-Spoofing
							G 5.115	Überwindung der Grenzen zwischen VLAN
			M 4.203	(A)	Umsetzg.	Konfigurations-Checkliste für Router und Switches	G 3.64	Fehlerhafte Konfiguration von Routern und Switch
							G 4.49	Unsichere Default-Einstellungen auf Routern und Switches
			M 4.204	(C)	Betrieb	Sichere Administration von Routern und Switches	G 3.65	Fehlerhafte Administration von Routern und Switche
							G 5.112	Manipulation von ARP-Tabelle
							G 5.114	Missbrauch von Spanning Tree

							G 5.115	Überwindung der Grenzen zwischen VLAN
			M 4.205	(C)	Betrieb	Protokollierung bei Routern und Switches	G 2.22	Fehlende Auswertung von Protokolldaten
			M 4.206	(C)	Betrieb	Sicherung von Switch-Ports	G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
			M 5.111	(C)	Umsetzg.	Einrichtung von Access Control Lists auf Routern	G 3.65	Fehlerhafte Administration von Routern und Switches
			M 5.112	(C)	Betrieb	Sicherheitsaspekte von Routing-Protokollen	G 5.51	Missbrauch der Routing-Protokolle
			M 6.91	(C)	Notfallv.	Datensicherung und Recovery bei Routern und Switches	G 3.65	Fehlerhafte Administration von Routern und Switches
			M 6.92	(C)	Notfallv.	Notfallvorsorge bei Routern und Switches	G 3.65	Fehlerhafte Administration von Routern und Switches
B 3.401	(8.1)	TK-Anlage	M 1.12	(B)	Planung	Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
							G 5.13	Abhören von Räumen
			M 1.13	(Z)	Planung	Anordnung schützenswerter Gebäudeteile	G 1.4	Feuer
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.13	Abhören von Räumen
			M 1.25	(B)	Planung	Überspannungsschutz	G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
			M 1.28	(B)	Planung	Lokale unterbrechungsfreie Stromversorgung	G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
			M 1.30	(A)	Umsetzg.	Absicherung der Datenträger mit TK-Gebührendaten	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
							G 5.14	Gebührenbetrug
			M 2.27	(Z)	Planung	Verzicht auf Fernwartung der TK-Anlage	G 5.12	Abhören von Telefongesprächen und Datenübertragunger
							G 5.13	Abhören von Räumen
							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
			M 2.28	(Z)	Planung	Bereitstellung externer TK-Beratungskapazität	G 3.7	Ausfall der TK-Anlage durch Fehlbedienun
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
			M 2.29	(B)	Umsetzg.	Bedienungsanleitung der TK-Anlage für	G 3.7	Ausfall der TK-Anlage durch Fehlbedienun

						die Benutzer	G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
							G 5.13	Abhören von Räumen
							G 5.14	Gebührenbetrug
							G 5.15	"Neugierige" Mitarbeiter
			M 2.105	(A)	Beschaff.	Beschaffung von TK-Anlagen	G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
			M 3.12	(B)	Betrieb	Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne	G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
							G 5.12	Abhören von Telefongesprächen und Datenübertragunger
							G 5.13	Abhören von Räumen
							G 5.14	Gebührenbetrug
							G 5.15	"Neugierige" Mitarbeiter
			M 3.13	(B)	Betrieb	Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen	G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
							G 5.12	Abhören von Telefongesprächen und Datenübertragunger
							G 5.13	Abhören von Räumen
							G 5.14	Gebührenbetrug
							G 5.15	"Neugierige" Mitarbeiter
			M 4.5	(B)	Betrieb	Protokollierung der TK-Administrationsarbeiten	G 3.7	Ausfall der TK-Anlage durch Fehlbedienun
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
							G 5.12	Abhören von Telefongesprächen und Datenübertragunger
							G 5.13	Abhören von Räumen
							G 5.14	Gebührenbetrug
							G 5.15	"Neugierige" Mitarbeiter
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
			M 4.6	(C)	Betrieb	Revision der TK-Anlagenkonfiguration	G 3.7	Ausfall der TK-Anlage durch Fehlbedienun
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh

							G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
							G 5.12	Abhören von Telefongesprächen und Datenübertragunger
							G 5.13	Abhören von Räumer
							G 5.14	Gebührenbetruc
							G 5.15	"Neugierige" Mitarbeiter
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
				M 4.7	(A)	Umsetzg.	Änderung voreingestellter Passwörter	G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
								G 5.12	Abhören von Telefongesprächen und Datenübertragunger
								G 5.13	Abhören von Räumer
								G 5.14	Gebührenbetruc
								G 5.15	"Neugierige" Mitarbeiter
								G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
								G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
								G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
				M 4.8	(A)	Planung	Schutz des TK-Bedienplatzes	G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
								G 5.12	Abhören von Telefongesprächen und Datenübertragunger
								G 5.13	Abhören von Räumer
								G 5.14	Gebührenbetruc
								G 5.15	"Neugierige" Mitarbeiter
								G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
								G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
				M 4.10	(Z)	Umsetzg.	Passwortschutz für TK-Endgeräte	G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
								G 5.12	Abhören von Telefongesprächen und Datenübertragunger
								G 5.13	Abhören von Räumer
								G 5.14	Gebührenbetruc
								G 5.15	"Neugierige" Mitarbeiter

							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
			M 4.11	(B)	Umsetzg.	Absicherung der TK-Anlagen-Schnittstellen	G 3.7	Ausfall der TK-Anlage durch Fehlbedienun
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
							G 5.12	Abhören von Telefongesprächen und Datenübertragunger
							G 5.13	Abhören von Räume
							G 5.14	Gebührenbetruc
							G 5.15	"Neugierige" Mitarbeiter
							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
			M 4.12	(A)	Umsetzg.	Sperren nicht benötigter TK-Leistungsmerkmale	G 3.7	Ausfall der TK-Anlage durch Fehlbedienun
							G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
							G 5.12	Abhören von Telefongesprächen und Datenübertragunger
							G 5.13	Abhören von Räume
							G 5.14	Gebührenbetruc
							G 5.15	"Neugierige" Mitarbeiter
							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
			M 4.62	(Z)	Planung	Einsatz eines D-Kanal-Filters	G 5.14	Gebührenbetruc
							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
			M 5.14	(A)	Umsetzg.	Absicherung interner Remote-Zugänge	G 3.7	Ausfall der TK-Anlage durch Fehlbedienun
							G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
							G 5.12	Abhören von Telefongesprächen und Datenübertragunger
							G 5.13	Abhören von Räume
							G 5.15	"Neugierige" Mitarbeiter
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
			M 5.15	(A)	Umsetzg.	Absicherung externer Remote-Zugänge	G 3.7	Ausfall der TK-Anlage durch Fehlbedienun
							G 5.11	Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
							G 5.12	Abhören von Telefongesprächen und Datenübertragunger
							G 5.13	Abhören von Räume
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal

							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
			M 6.10	(B)	Notfallv.	Notfall-Plan für DFÜ-Ausfall	G 3.7	Ausfall der TK-Anlage durch Fehlbedienun
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
			M 6.26	(B)	Notfallv.	Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten	G 1.4	Feuer
							G 3.7	Ausfall der TK-Anlage durch Fehlbedienun
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
			M 6.28	(Z)	Notfallv.	Vereinbarung über Lieferzeiten "lebensnotwendiger" TK-Baugruppen	G 1.4	Feuer
							G 3.7	Ausfall der TK-Anlage durch Fehlbedienun
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
			M 6.29	(Z)	Notfallv.	TK-Basisanschluss für Notrufe	G 1.4	Feuer
							G 3.7	Ausfall der TK-Anlage durch Fehlbedienun
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
			M 6.30	(Z)	Notfallv.	Katastrophenschaltung	G 1.4	Feuer
							G 3.7	Ausfall der TK-Anlage durch Fehlbedienun
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
							G 5.44	Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlage
B 3.402	(8.2)	Faxgerät	M 1.37	(A)	Umsetzg.	Geeignete Aufstellung eines Faxgerätes	G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
							G 5.31	Unbefugtes Lesen von Faxsendunge
							G 5.32	Auswertung von Restinformationen in Faxgeräten und Faxserverr
							G 5.33	Vortäuschen eines falschen Absenders bei Faxsendunger
							G 5.34	Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes
			M 2.47	(B)	Umsetzg.	Ernennung eines Fax-Verantwortlichen	G 2.20	Unzureichende oder falsche Versorgung mit Verbrauchsgüterr
							G 5.31	Unbefugtes Lesen von Faxsendunge

							G 5.32	Auswertung von Restinformationen in Faxgeräten und Faxserverr
							G 5.34	Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes
			M 2.48	(Z)	Betrieb	Festlegung berechtigter Faxbediener	G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
							G 5.31	Unbefugtes Lesen von Faxsendunge
							G 5.33	Vortäuschen eines falschen Absenders bei Faxsendunger
							G 5.34	Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes
			M 2.49	(A)	Beschaff.	Beschaffung geeigneter Faxgeräte	G 4.14	Verblassen spezieller Faxpapiere
							G 4.15	Fehlerhafte Faxübertragun
							G 5.35	Überlastung durch Faxsendunge
			M 2.50	(B)	Aussnd.	Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteile	G 5.32	Auswertung von Restinformationen in Faxgeräten und Faxserverr
			M 2.51	(Z)	Betrieb	Fertigung von Kopien eingehender Faxsendunger	G 4.14	Verblassen spezieller Faxpapiere
			M 2.52	(C)	Betrieb	Versorgung und Kontrolle der Verbrauchsgüter	G 2.20	Unzureichende oder falsche Versorgung mit Verbrauchsgüterr
			M 2.53	(Z)	Betrieb	Abschalten des Faxgerätes außerhalb der Bürozeiten	G 2.20	Unzureichende oder falsche Versorgung mit Verbrauchsgüterr
							G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
							G 5.31	Unbefugtes Lesen von Faxsendunge
							G 5.32	Auswertung von Restinformationen in Faxgeräten und Faxserverr
							G 5.34	Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes
							G 5.35	Überlastung durch Faxsendunge
			M 3.15	(A)	Umsetzg.	Informationen für alle Mitarbeiter über die Faxnutzung	G 3.14	Fehleinschätzung der Rechtsverbindlichkeit eines Fa
							G 4.15	Fehlerhafte Faxübertragun
							G 5.7	Abhören von Leitunger
							G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
							G 5.31	Unbefugtes Lesen von Faxsendunge
							G 5.33	Vortäuschen eines falschen Absenders bei Faxsendunger
							G 5.34	Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes
			M 4.36	(Z)	Umsetzg.	Sperren bestimmter Faxempfänger-Rufnummern	G 4.15	Fehlerhafte Faxübertragun
							G 5.34	Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes
			M 4.37	(Z)	Umsetzg.	Sperren bestimmter Absender-Faxnummern	G 2.20	Unzureichende oder falsche Versorgung mit Verbrauchsgüterr

							G 5.33	Vortäuschen eines falschen Absenders bei Faxsendunger
							G 5.35	Überlastung durch Faxsendunge
			M 4.43	(Z)	Betrieb	Faxgerät mit automatischer Eingangskuvertierung	G 5.31	Unbefugtes Lesen von Faxsendunge
							G 5.32	Auswertung von Restinformationen in Faxgeräten und Faxserverr
			M 5.24	(Z)	Betrieb	Nutzung eines geeigneten Faxvorblattes	G 4.15	Fehlerhafte Faxübertragun
							G 5.33	Vortäuschen eines falschen Absenders bei Faxsendunger
			M 5.25	(A)	Betrieb	Nutzung von Sende- und Empfangsprotokollen	G 4.15	Fehlerhafte Faxübertragun
							G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
							G 5.33	Vortäuschen eines falschen Absenders bei Faxsendunger
							G 5.34	Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes
			M 5.26	(Z)	Betrieb	Telefonische Ankündigung einer Faxsendung	G 5.31	Unbefugtes Lesen von Faxsendunge
							G 5.33	Vortäuschen eines falschen Absenders bei Faxsendunger
			M 5.27	(Z)	Betrieb	Telefonische Rückversicherung über korrekten Faxempfang	G 4.15	Fehlerhafte Faxübertragun
							G 5.34	Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes
			M 5.28	(Z)	Betrieb	Telefonische Rückversicherung über korrekten Faxabsender	G 4.15	Fehlerhafte Faxübertragun
							G 5.33	Vortäuschen eines falschen Absenders bei Faxsendunger
			M 5.29	(C)	Betrieb	Gelegentliche Kontrolle programmierter Zieladressen und Protokolle	G 4.15	Fehlerhafte Faxübertragun
							G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
							G 5.31	Unbefugtes Lesen von Faxsendunge
							G 5.34	Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes
			M 6.39	(C)	Notfallv.	Auflistung von Händleradressen zur Fa Wiederbeschaffung	G 2.20	Unzureichende oder falsche Versorgung mit Verbrauchsgüterr
B 3.403	(8.3)	Anrufbeantworter	M 2.11	(A)	Planung	Regelung des Passwortgebrauchs	G 5.37	Ermitteln des Sicherungscodes
							G 5.38	Missbrauch der Fernabfrage
			M 2.54	(A)	Beschaff.	Beschaffung geeigneter Anrufbeantworter	G 3.15	Fehlbedienung eines Anrufbeantworter
							G 4.1	Ausfall der Stromversorgun
							G 4.19	Informationsverlust bei erschöpftem Speichermediu
							G 5.36	Absichtliche Überlastung des Anrufbeantworter
							G 5.38	Missbrauch der Fernabfrage
			M 2.55	(Z)	Umsetzg.	Einsatz eines Sicherungscodes	G 5.38	Missbrauch der Fernabfrage
			M 2.56	(A)	Betrieb	Vermeidung schutzbedürftiger Informationen auf dem Anrufbeantworte	G 5.38	Missbrauch der Fernabfrage
			M 2.57	(A)	Betrieb	Regelmäßiges Abhören und Löschen	G 4.19	Informationsverlust bei erschöpftem Speichermediu

						aufgezeichneter Gespräche	G 5.38	Missbrauch der Fernabfrage
			M 2.58	(Z)	Umsetzg.	Begrenzung der Sprechdaue	G 5.36	Absichtliche Überlastung des Anrufbeantworter
			M 3.16	(A)	Umsetzg.	Einweisung in die Bedienung des Anrufbeantworters	G 2.1	Fehlende oder unzureichende Regelunge
							G 3.15	Fehlbedienung eines Anrufbeantworter
			M 4.38	(A)	Umsetzg.	Abschalten nicht benötigter Leistungsmerkmale	G 3.15	Fehlbedienung eines Anrufbeantworter
							G 5.38	Missbrauch der Fernabfrage
			M 4.39	(Z)	Betrieb	Abschalten des Anrufbeantworters bei Anwesenheit	G 3.15	Fehlbedienung eines Anrufbeantworter
							G 5.36	Absichtliche Überlastung des Anrufbeantworter
							G 5.38	Missbrauch der Fernabfrage
			M 6.40	(A)	Notfallv.	Regelmäßige Batterieprüfung/-wechsel	G 2.5	Fehlende oder unzureichende Wartun
							G 4.18	Entladene oder überalterte Notstromversorgung im Anrufbeantworte
B 3.404	(8.6)	Mobiltelefon	M 2.188	(A)	Planung	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 3.45	Unzureichende Identifikationsprüfung von Kommunikationspartnerr
							G 4.41	Nicht-Verfügbarkeit des Mobilfunknetze
							G 5.2	Manipulation an Daten oder Softwar
							G 5.80	Hoax
							G 5.94	Kartenmissbrauch
							G 5.95	Abhören von Raumgesprächen über Mobiltelefon
							G 5.96	Manipulation von Mobiltelefone
							G 5.97	Unberechtigte Datenweitergabe über Mobiltelefon
							G 5.98	Abhören von Mobiltelefonate
							G 5.99	Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefoner
							G 5.126	Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten
			M 2.189	(A)	Betrieb	Sperrung des Mobiltelefons bei Verlust	G 5.4	Diebstahl
							G 5.94	Kartenmissbrauch
			M 2.190	(Z)	Beschaff.	Einrichtung eines Mobiltelefon-Pools	G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.43	Ungeeigneter Umgang mit Passwörter
							G 4.42	Ausfall des Mobiltelefons oder des PDAs
							G 5.94	Kartenmissbrauch
			M 4.114	(A)	Umsetzg.	Nutzung der Sicherheitsmechanismen von Mobiltelefonen	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.43	Ungeeigneter Umgang mit Passwörter
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.94	Kartenmissbrauch

							G 5.96	Manipulation von Mobiltelefone
			M 4.115	(B)	Betrieb	Sicherstellung der Energieversorgung von Mobiltelefoner	G 4.42	Ausfall des Mobiltelefons oder des PDAs
			M 4.255	(A)	Betrieb	Nutzung von IrDA-Schnittstellen	G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 5.2	Manipulation an Daten oder Softwar
							G 5.97	Unberechtigte Datenweitergabe über Mobiltelefon
			M 5.78	(Z)	Betrieb	Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzun	G 5.99	Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen
			M 5.79	(Z)	Betrieb	Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzun	G 5.99	Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefoner
			M 5.80	(Z)	Betrieb	Schutz vor Abhören der Raumgespräche über Mobiltelefon	G 5.95	Abhören von Raumgesprächen über Mobiltelefone
			M 5.81	(B)	Betrieb	Sichere Datenübertragung über Mobiltelefone	G 2.2	Unzureichende Kenntnis über Regelunge
							G 5.4	Diebstahl
			M 6.72	(C)	Notfallv.	Ausfallvorsorge bei Mobiltelefonen	G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.96	Manipulation von Mobiltelefone
B 3.405	(8.7)	PDA	M 1.33	(A)	Betrieb	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz	G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebur
							G 4.42	Ausfall des Mobiltelefons oder des PDAs
							G 4.52	Datenverlust bei mobilem Einsat
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.22	Diebstahl bei mobiler Nutzung des IT-System
			M 2.218	(C)	Planung	Regelung der Mitnahme von Datenträgern und IT-Komponenten	G 4.42	Ausfall des Mobiltelefons oder des PDAs
							G 4.52	Datenverlust bei mobilem Einsat
							G 5.2	Manipulation an Daten oder Softwar
							G 5.22	Diebstahl bei mobiler Nutzung des IT-System
							G 5.124	Missbrauch der Informationen von mobilen Endgeräte
							G 5.125	Unberechtigte Datenweitergabe über mobile Endgerät
			M 2.303	(A)	Planung	Festlegung einer Strategie für den Einsatz von PDAs	G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 3.76	Fehler bei der Synchronisation mobiler Endgerät
							G 4.51	Unzureichende Sicherheitsmechanismen bei PDA
							G 5.124	Missbrauch der Informationen von mobilen Endgeräte
			M 2.304	(A)	Planung	Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung	G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.43	Ungeeigneter Umgang mit Passwörter
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 3.45	Unzureichende Identifikationsprüfung von Kommunikationspartnerr
							G 3.76	Fehler bei der Synchronisation mobiler Endgerät
							G 4.51	Unzureichende Sicherheitsmechanismen bei PDA
							G 5.9	Unberechtigte IT-Nutzun

							G 5.23	Computer-Viren
							G 5.123	Abhören von Raumgesprächen über mobile Endgerät
							G 5.124	Missbrauch der Informationen von mobilen Endgeräte
							G 5.125	Unberechtigte Datenweitergabe über mobile Endgerät
							G 5.126	Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten
			M 2.305	(B)	Beschaff.	Geeignete Auswahl von PDAs	G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebur
							G 3.76	Fehler bei der Synchronisation mobiler Endgerät
							G 4.51	Unzureichende Sicherheitsmechanismen bei PDA
							G 4.52	Datenverlust bei mobilem Einsat
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.124	Missbrauch der Informationen von mobilen Endgeräte
			M 2.306	(A)	Aussnd.	Verlustmeldung	G 2.7	Unerlaubte Ausübung von Rechte
							G 5.9	Unberechtigte IT-Nutzun
			M 4.3	(A)	Betrieb	Regelmäßiger Einsatz eines Anti-Viren-Programms	G 5.2	Manipulation an Daten oder Softwar
							G 5.23	Computer-Viren
			M 4.31	(A)	Betrieb	Sicherstellung der Energieversorgung im mobilen Einsatz	G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebur
							G 4.42	Ausfall des Mobiltelefons oder des PDAs
							G 4.52	Datenverlust bei mobilem Einsat
			M 4.228	(A)	Betrieb	Nutzung der Sicherheitsmechanismen von PDAs	G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebur
							G 4.52	Datenverlust bei mobilem Einsat
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.124	Missbrauch der Informationen von mobilen Endgeräte
							G 5.125	Unberechtigte Datenweitergabe über mobile Endgerät
			M 4.229	(C)	Betrieb	Sicherer Betrieb von PDAs	G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebur
							G 3.76	Fehler bei der Synchronisation mobiler Endgerät
							G 4.51	Unzureichende Sicherheitsmechanismen bei PDA
							G 4.52	Datenverlust bei mobilem Einsat
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.124	Missbrauch der Informationen von mobilen Endgeräte
							G 5.125	Unberechtigte Datenweitergabe über mobile Endgerät
			M 4.230	(Z)	Betrieb	Zentrale Administration von PDAs	G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.43	Ungeeigneter Umgang mit Passwörter
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 3.76	Fehler bei der Synchronisation mobiler Endgerät
							G 4.42	Ausfall des Mobiltelefons oder des PDAs
							G 4.51	Unzureichende Sicherheitsmechanismen bei PDA
							G 4.52	Datenverlust bei mobilem Einsat

							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.124	Missbrauch der Informationen von mobilen Endgeräte
							G 5.125	Unberechtigte Datenweitergabe über mobile Endgerät
			M 4.231	(Z)	Beschaff.	Einsatz zusätzlicher Sicherheitswerkzeuge für PDAs	G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebur
							G 2.7	Unerlaubte Ausübung von Rechte
							G 3.43	Ungeeigneter Umgang mit Passwörter
							G 4.51	Unzureichende Sicherheitsmechanismen bei PDA
							G 4.52	Datenverlust bei mobilem Einsat
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.124	Missbrauch der Informationen von mobilen Endgeräte
							G 5.125	Unberechtigte Datenweitergabe über mobile Endgerät
			M 4.232	(Z)	Betrieb	Sichere Nutzung von Zusatzspeicherkarten	G 2.7	Unerlaubte Ausübung von Rechte
							G 4.52	Datenverlust bei mobilem Einsat
							G 5.2	Manipulation an Daten oder Softwar
							G 5.124	Missbrauch der Informationen von mobilen Endgeräte
			M 4.255	(A)	Betrieb	Nutzung von IrDA-Schnittstellen	G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 4.51	Unzureichende Sicherheitsmechanismen bei PDA
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.124	Missbrauch der Informationen von mobilen Endgeräte
							G 5.125	Unberechtigte Datenweitergabe über mobile Endgerät
			M 5.121	(B)	Umsetzg.	Sichere Kommunikation von unterwegs	G 2.7	Unerlaubte Ausübung von Rechte
							G 4.51	Unzureichende Sicherheitsmechanismen bei PDA
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.124	Missbrauch der Informationen von mobilen Endgeräte
							G 5.125	Unberechtigte Datenweitergabe über mobile Endgerät
			M 6.95	(C)	Notfallv.	Ausfallvorsorge und Datensicherung bei PDAs	G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebur
							G 3.76	Fehler bei der Synchronisation mobiler Endgerät
							G 4.52	Datenverlust bei mobilem Einsat
B 4.1	(6.7)	Heterogene Netze	M 2.139	(A)	Planung	Ist-Aufnahme der aktuellen Netzsituation	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.45	Konzeptionelle Schwächen des Netze
							G 2.46	Überschreiten der zulässigen Kabel- bzw. Buslänge oder der Ringgröße
							G 3.29	Fehlende oder ungeeignete Segmentierun
							G 5.4	Diebstahl
			M 2.140	(Z)	Planung	Analyse der aktuellen Netzsituation	G 2.32	Unzureichende Leitungskapazitäte
							G 2.45	Konzeptionelle Schwächen des Netze
							G 2.46	Überschreiten der zulässigen Kabel- bzw. Buslänge oder der Ringgröße
							G 3.9	Fehlerhafte Administration des IT-System

							G 3.28	Ungeeignete Konfiguration der aktiven Netzkomponenten
							G 3.29	Fehlende oder ungeeignete Segmentierung
							G 5.4	Diebstahl
			M 2.141	(B)	Planung	Entwicklung eines Netzkonzeptes	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.27	Fehlende oder unzureichende Dokumentatio
							G 2.32	Unzureichende Leitungskapazitäte
							G 2.44	Inkompatible aktive und passive Netzkomponente
							G 2.45	Konzeptionelle Schwächen des Netze
							G 3.29	Fehlende oder ungeeignete Segmentierung
							G 4.31	Ausfall oder Störung von Netzkomponente
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitunge
							G 5.8	Manipulation an Leitunge
							G 5.28	Verhinderung von Dienste
							G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
							G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktione
							G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
			M 2.142	(B)	Planung	Entwicklung eines Netz-Realisierungsplans	G 2.32	Unzureichende Leitungskapazitäte
							G 2.46	Überschreiten der zulässigen Kabel- bzw. Buslänge oder der Ringgröße
							G 3.5	Unbeabsichtigte Leitungsbeschädigun
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktione
			M 4.7	(A)	Umsetzg.	Änderung voreingestellter Passwörter	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
							G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktione
			M 4.79	(A)	Planung	Sichere Zugriffsmechanismen bei lokaler Administration	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun

							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
							G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktionen
							G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
			M 4.80	(B)	Planung	Sichere Zugriffsmechanismen bei Fernadministration	G 2.22	Fehlende Auswertung von Protokolldaten
							G 2.44	Inkompatible aktive und passive Netzkomponente
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.28	Ungeeignete Konfiguration der aktiven Netzkomponenten
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
							G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktionen
			M 4.81	(B)	Betrieb	Audit und Protokollierung der Aktivitäten im Netz	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.28	Ungeeignete Konfiguration der aktiven Netzkomponenten
							G 5.8	Manipulation an Leitunge
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.28	Verhinderung von Dienste
							G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
							G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktionen
							G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
			M 4.82	(A)	Umsetzg.	Sichere Konfiguration der aktiven Netzkomponenten	G 2.32	Unzureichende Leitungskapazitäte
							G 2.44	Inkompatible aktive und passive Netzkomponente
							G 3.28	Ungeeignete Konfiguration der aktiven Netzkomponenten
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.28	Verhinderung von Dienste
							G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz

							G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktionen
							G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
			M 4.83	(C)	Betrieb	Update/Upgrade von Soft- und Hardware im Netzbereich	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.32	Unzureichende Leitungskapazitäte
							G 2.44	Inkompatible aktive und passive Netzkomponente
							G 2.45	Konzeptionelle Schwächen des Netze
							G 2.46	Überschreiten der zulässigen Kabel- bzw. Buslänge oder der Ringgröße
							G 3.5	Unbeabsichtigte Leitungsbeschädigung
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
			M 5.2	(A)	Planung	Auswahl einer geeigneten Netz-Topographie	G 3.9	Fehlerhafte Administration des IT-System
							G 5.5	Vandalismus
							G 5.6	Anschlag
							G 5.7	Abhören von Leitungen
							G 5.8	Manipulation an Leitungen
							G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
							G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
			M 5.7	(A)	Umsetzg.	Netzverwaltung	G 2.32	Unzureichende Leitungskapazitäte
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.9	Unberechtigte IT-Nutzun
							G 5.20	Missbrauch von Administratorrechte
			M 5.13	(A)	Planung	Geeigneter Einsatz von Elementen zur Netzkopplung	G 1.2	Ausfall des IT-System
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
			M 5.60	(A)	Planung	Auswahl einer geeigneten Backbone-Technologie	G 2.32	Unzureichende Leitungskapazitäte
							G 2.45	Konzeptionelle Schwächen des Netze
							G 2.46	Überschreiten der zulässigen Kabel- bzw. Buslänge oder der Ringgröße
							G 3.5	Unbeabsichtigte Leitungsbeschädigung
							G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
			M 5.61	(A)	Planung	Geeignete physikalische Segmentierung	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.27	Fehlende oder unzureichende Dokumentatio
							G 2.32	Unzureichende Leitungskapazitäte
							G 2.44	Inkompatible aktive und passive Netzkomponente
							G 2.45	Konzeptionelle Schwächen des Netze
							G 3.5	Unbeabsichtigte Leitungsbeschädigung
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.7	Abhören von Leitungen

							G 5.8	Manipulation an Leitungen
							G 5.28	Verhinderung von Diensten
							G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
							G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktionen
							G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
			M 5.62	(Z)	Planung	Geeignete logische Segmentierung	G 2.7	Unerlaubte Ausübung von Rechten
							G 2.32	Unzureichende Leitungskapazitäten
							G 2.44	Inkompatible aktive und passive Netzkomponenten
							G 2.45	Konzeptionelle Schwächen des Netzes
							G 2.46	Überschreiten der zulässigen Kabel- bzw. Buslänge oder der Ringgröße
							G 3.5	Unbeabsichtigte Leitungsbeschädigung
							G 3.29	Fehlende oder ungeeignete Segmentierung
							G 5.7	Abhören von Leitungen
							G 5.8	Manipulation an Leitungen
							G 5.28	Verhinderung von Diensten
							G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
							G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktionen
							G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
			M 5.77	(Z)	Planung	Bildung von Teilnetzen	G 2.7	Unerlaubte Ausübung von Rechten
							G 2.32	Unzureichende Leitungskapazitäten
							G 2.45	Konzeptionelle Schwächen des Netzes
							G 3.5	Unbeabsichtigte Leitungsbeschädigung
							G 5.7	Abhören von Leitungen
							G 5.8	Manipulation an Leitungen
							G 5.28	Verhinderung von Diensten
							G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
							G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktionen
			M 6.52	(A)	Notfallv.	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten	G 1.2	Ausfall des IT-Systems
							G 1.3	Blitz
							G 1.4	Feuer
							G 1.5	Wasser
							G 1.7	Unzulässige Temperatur und Luftfeuchte
							G 1.8	Staub, Verschmutzung
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.9	Fehlerhafte Administration des IT-System

							G 3.28	Ungeeignete Konfiguration der aktiven Netzkomponenten
							G 4.1	Ausfall der Stromversorgun
							G 4.31	Ausfall oder Störung von Netzkomponente
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
			M 6.53	(Z)	Notfallv.	Redundante Auslegung der Netzkomponenten	G 1.2	Ausfall des IT-System
							G 1.3	Blitz
							G 1.4	Feuer
							G 1.5	Wasser
							G 1.7	Unzulässige Temperatur und Luftfeuch
							G 1.8	Staub, Verschmutzun
							G 2.32	Unzureichende Leitungskapazitäte
							G 2.45	Konzeptionelle Schwächen des Netze
							G 3.5	Unbeabsichtigte Leitungsbeschädigun
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.1	Ausfall der Stromversorgun
							G 4.31	Ausfall oder Störung von Netzkomponente
							G 5.28	Verhinderung von Dienste
			M 6.54	(B)	Notfallv.	Verhaltensregeln nach Verlust der Netzintegrität	G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-Syster
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.31	Ausfall oder Störung von Netzkomponente
B 4.2	(6.8)	Netz- und Systemmanagement	M 2.143	(A)	Planung	Entwicklung eines Netzmanagementkonzeptes	G 2.60	Fehlende oder unzureichende Strategie für das Netz- und Systemmanagemen
							G 3.34	Ungeeignete Konfiguration des Managementsystem
			M 2.144	(A)	Planung	Geeignete Auswahl eines Netzmanagement-Protokolls	G 2.60	Fehlende oder unzureichende Strategie für das Netz- und Systemmanagemen
			M 2.145	(B)	Beschaff.	Anforderungen an ein Netzmanagement-Tool	G 2.32	Unzureichende Leitungskapazitäte
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.31	Ausfall oder Störung von Netzkomponente
							G 5.8	Manipulation an Leitunge
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.28	Verhinderung von Dienste
							G 5.66	Unberechtigter Anschluss von IT-Systemen an ein Netz
							G 5.67	Unberechtigte Ausführung von Netzmanagement-Funktione
			M 2.146	(A)	Betrieb	Sicherer Betrieb eines Netzmanagementsystems	G 1.7	Unzulässige Temperatur und Luftfeuch
							G 2.27	Fehlende oder unzureichende Dokumentatio
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.28	Ungeeignete Konfiguration der aktiven Netzkomponenten
							G 3.36	Fehlinterpretation von Ereignisse

							G 5.2	Manipulation an Daten oder Softwar
			M 2.168	(A)	Planung	IT-System-Analyse vor Einführung eine Systemmanagementsystems	G 2.60	Fehlende oder unzureichende Strategie für das Netz- und Systemmanagemen
			M 2.169	(A)	Planung	Entwickeln einer Systemmanagementstrategie	G 2.59	Betreiben von nicht angemeldeten Komponente
							G 2.60	Fehlende oder unzureichende Strategie für das Netz- und Systemmanagemen
							G 2.61	Unberechtigte Sammlung personenbezogener Date
							G 3.34	Ungeeignete Konfiguration des Managementsystem
			M 2.170	(A)	Beschaff.	Anforderungen an ein Systemmanagementsysten	G 2.60	Fehlende oder unzureichende Strategie für das Netz- und Systemmanagemen
			M 2.171	(A)	Beschaff.	Geeignete Auswahl eines Systemmanagement-Produktes	G 2.60	Fehlende oder unzureichende Strategie für das Netz- und Systemmanagemen
							G 2.61	Unberechtigte Sammlung personenbezogener Date
							G 3.34	Ungeeignete Konfiguration des Managementsystem
							G 4.38	Ausfall von Komponenten eines Netz- und Systemmanagementsystems
			M 4.91	(A)	Umsetzg.	Sichere Installation eines Systemmanagementsystems	G 2.59	Betreiben von nicht angemeldeten Komponente
							G 2.61	Unberechtigte Sammlung personenbezogener Date
							G 3.34	Ungeeignete Konfiguration des Managementsystem
							G 3.35	Server im laufenden Betrieb ausschalte
							G 5.86	Manipulation von Managementparameter
			M 4.92	(A)	Betrieb	Sicherer Betrieb eines Systemmanagementsystems	G 1.1	Personalausfal
							G 1.2	Ausfall des IT-System
							G 2.59	Betreiben von nicht angemeldeten Komponente
							G 2.61	Unberechtigte Sammlung personenbezogener Date
							G 3.34	Ungeeignete Konfiguration des Managementsystem
							G 3.35	Server im laufenden Betrieb ausschalte
							G 3.36	Fehlinterpretation von Ereignisse
							G 5.86	Manipulation von Managementparameter
			M 6.57	(C)	Notfallv.	Erstellen eines Notfallplans für den Ausfall des Managementsystems	G 1.2	Ausfall des IT-System
							G 3.35	Server im laufenden Betrieb ausschalte
							G 4.38	Ausfall von Komponenten eines Netz- und Systemmanagementsystems
							G 5.86	Manipulation von Managementparameter
B 4.3	(7.2)	Modem	M 1.25	(Z)	Planung	Überspannungsschutz	G 1.2	Ausfall des IT-System
							G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
			M 1.38	(A)	Umsetzg.	Geeignete Aufstellung eines Modems	G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.5	Unbeabsichtigte Leitungsbeschädigun
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
			M 2.42	(B)	Planung	Festlegung der möglichen Kommunikationspartner	G 3.2	Fahrlässige Zerstörung von Gerät oder Date
							G 3.5	Unbeabsichtigte Leitungsbeschädigun
							G 5.2	Manipulation an Daten oder Softwar
							G 5.23	Computer-Viren

			M 2.46	(Z)	Planung	Geeignetes Schlüsselmanagement	G 5.7	Abhören von Leitungen
							G 5.12	Abhören von Telefongesprächen und Datenübertragungen
			M 2.59	(A)	Beschaff.	Auswahl eines geeigneten Modems in der Beschaffung	G 5.7	Abhören von Leitungen
							G 5.8	Manipulation an Leitungen
							G 5.10	Missbrauch von Fernwartungszugängen
			M 2.60	(A)	Betrieb	Sichere Administration eines Modems	G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
							G 5.2	Manipulation an Daten oder Software
							G 5.9	Unberechtigte IT-Nutzung
							G 5.10	Missbrauch von Fernwartungszugängen
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten
			M 2.61	(A)	Planung	Regelung des Modem-Einsatzes	G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
							G 5.2	Manipulation an Daten oder Software
							G 5.9	Unberechtigte IT-Nutzung
							G 5.10	Missbrauch von Fernwartungszugängen
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten
			M 2.204	(A)	Umsetzg.	Verhinderung ungesicherter Netzzugänge	G 5.2	Manipulation an Daten oder Software
							G 5.7	Abhören von Leitungen
							G 5.9	Unberechtigte IT-Nutzung
			M 3.17	(A)	Betrieb	Einweisung des Personals in die Modem-Benutzung	G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
							G 3.5	Unbeabsichtigte Leitungsbeschädigung
			M 4.7	(A)	Umsetzg.	Änderung voreingestellter Passwörter	G 5.2	Manipulation an Daten oder Software
							G 5.9	Unberechtigte IT-Nutzung
							G 5.10	Missbrauch von Fernwartungszugängen
							G 5.18	Systematisches Ausprobieren von Passwörtern
							G 5.25	Maskerade
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten
			M 4.33	(A)	Betrieb	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung	G 5.23	Computer-Viren
			M 4.34	(Z)	Planung	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen	G 5.7	Abhören von Leitungen
							G 5.8	Manipulation an Leitungen
							G 5.12	Abhören von Telefongesprächen und Datenübertragungen
			M 5.30	(Z)	Umsetzg.	Aktivierung einer vorhandenen Callback-Option	G 5.9	Unberechtigte IT-Nutzung
							G 5.10	Missbrauch von Fernwartungszugängen
							G 5.18	Systematisches Ausprobieren von Passwörtern
							G 5.25	Maskerade

							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
			M 5.31	(A)	Umsetzg.	Geeignete Modem-Konfiguration	G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
			M 5.32	(A)	Planung	Sicherer Einsatz von Kommunikationssoftware	G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
			M 5.33	(A)	Betrieb	Absicherung der per Modem durchgeführten Fernwartung	G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.25	Maskerade
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
			M 5.44	(Z)	Betrieb	Einseitiger Verbindungsaufbau	G 5.2	Manipulation an Daten oder Softwar
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.25	Maskerade
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
B 4.4	(7.6)	Remote Access	M 2.183	(A)	Planung	Durchführung einer RAS-Anforderungsanalyse	G 1.2	Ausfall des IT-System
							G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselun
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 2.44	Inkompatible aktive und passive Netzkomponente
							G 3.39	Fehlerhafte Administration des RAS-System
							G 4.40	Ungeeignete Ausrüstung der Betriebsumgebung des RAS-Clients
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 2.184	(A)	Planung	Entwicklung eines RAS-Konzeptes	G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselun
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 2.64	Fehlende Regelungen für das RAS-Syste
							G 3.39	Fehlerhafte Administration des RAS-System
							G 3.40	Ungeeignete Nutzung von Authentisierungsdiensten bei Remote Access
							G 3.41	Fehlverhalten bei der Nutzung von RAS-Dienste
							G 3.42	Unsichere Konfiguration der RAS-Client

							G 4.40	Ungeeignete Ausrüstung der Betriebsumgebung des RAS-Clients
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 2.185	(A)	Planung	Auswahl einer geeigneten RAS-Systemarchitektur	G 1.2	Ausfall des IT-System
							G 2.44	Inkompatible aktive und passive Netzkomponente
							G 3.39	Fehlerhafte Administration des RAS-System
							G 3.40	Ungeeignete Nutzung von Authentisierungsdiensten bei Remote Access
							G 3.42	Unsichere Konfiguration der RAS-Client
							G 4.40	Ungeeignete Ausrüstung der Betriebsumgebung des RAS-Clients
							G 5.7	Abhören von Leitungen
							G 5.8	Manipulation an Leitungen
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.83	Kompromittierung kryptographischer Schlüssel
			M 2.186	(A)	Beschaff.	Geeignete Auswahl eines RAS-Produktes	G 1.2	Ausfall des IT-System
							G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung
							G 2.44	Inkompatible aktive und passive Netzkomponente
							G 3.39	Fehlerhafte Administration des RAS-System
							G 3.42	Unsichere Konfiguration der RAS-Client
							G 4.35	Unsichere kryptographische Algorithme
			M 2.187	(A)	Planung	Festlegen einer RAS-Sicherheitsrichtlinie	G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PC
							G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung
							G 2.64	Fehlende Regelungen für das RAS-Syster
							G 3.41	Fehlverhalten bei der Nutzung von RAS-Dienste
							G 3.42	Unsichere Konfiguration der RAS-Client
							G 3.43	Ungeeigneter Umgang mit Passwörtern
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 4.35	Unsichere kryptographische Algorithme
							G 5.7	Abhören von Leitungen
							G 5.8	Manipulation an Leitungen
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.91	Abschalten von Sicherheitsmechanismen für den RAS-Zugang
							G 5.92	Nutzung des RAS-Clients als RAS-Serve
							G 5.93	Erlauben von Fremdnutzung von RAS-Komponente
			M 2.205	(A)	Planung	Übertragung und Abruf personenbezogener Dater	G 2.64	Fehlende Regelungen für das RAS-System
			M 4.110	(A)	Umsetzg.	Sichere Installation des RAS-Systems	G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung

							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunger
							G 2.44	Inkompatible aktive und passive Netzkomponente
							G 4.40	Ungeeignete Ausrüstung der Betriebsumgebung des RAS-Clients
							G 5.7	Abhören von Leitunger
							G 5.8	Manipulation an Leitunger
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
			M 4.111	(A)	Umsetzg.	Sichere Konfiguration des RAS-Systems	G 1.2	Ausfall des IT-System
							G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselunc
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunger
							G 3.39	Fehlerhafte Administration des RAS-System
							G 3.42	Unsichere Konfiguration der RAS-Client
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.91	Abschalten von Sicherheitsmechanismen für den RAS-Zugang
							G 5.92	Nutzung des RAS-Clients als RAS-Serve
			M 4.112	(A)	Betrieb	Sicherer Betrieb des RAS-Systems	G 1.2	Ausfall des IT-System
							G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselunc
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunger
							G 3.39	Fehlerhafte Administration des RAS-System
							G 3.40	Ungeeignete Nutzung von Authentisierungsdiensten bei Remote Access
							G 3.41	Fehlverhalten bei der Nutzung von RAS-Dienste
							G 3.42	Unsichere Konfiguration der RAS-Client
							G 3.43	Ungeeigneter Umgang mit Passwörter
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 4.35	Unsichere kryptographische Algorithme
							G 4.40	Ungeeignete Ausrüstung der Betriebsumgebung des RAS-Clients
							G 5.22	Diebstahl bei mobiler Nutzung des IT-Syster
							G 5.91	Abschalten von Sicherheitsmechanismen für den RAS-Zugang
							G 5.92	Nutzung des RAS-Clients als RAS-Serve
							G 5.93	Erlauben von Fremdnutzung von RAS-Komponente
			M 4.113	(Z)	Planung	Nutzung eines Authentisierungsservers beim RAS-Einsatz	G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunger
							G 3.40	Ungeeignete Nutzung von Authentisierungsdiensten bei Remote Access

			M 4.233	(B)	Aussnd.	Sperrung nicht mehr benötigter RAS-Zugänge	G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
			M 5.76	(Z)	Planung	Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikatior	G 5.7	Abhören von Leitunge
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 6.70	(B)	Notfallv.	Erstellen eines Notfallplans für den Ausfall des RAS-Systems	G 1.2	Ausfall des IT-System
							G 5.22	Diebstahl bei mobiler Nutzung des IT-System
			M 6.71	(B)	Notfallv.	Datensicherung bei mobiler Nutzung des IT-Systems	G 1.2	Ausfall des IT-System
							G 5.22	Diebstahl bei mobiler Nutzung des IT-System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.83	Kompromittierung kryptographischer Schlüsse
B 4.5	(8.4)	LAN-Anbindung eines IT-Systems über ISDN	M 1.25	(B)	Planung	Überspannungsschutz	G 1.2	Ausfall des IT-System
							G 4.6	Spannungsschwankungen/Überspannung/Unterspannung
			M 1.43	(A)	Umsetzg.	Gesicherte Aufstellung aktiver Netzkomponenten	G 1.2	Ausfall des IT-System
							G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räum
							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
			M 2.42	(A)	Planung	Festlegung der möglichen Kommunikationspartner	G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 5.62	Missbrauch von Ressourcen über abgesetzte IT-Systeme
			M 2.46	(Z)	Planung	Geeignetes Schlüsselmanagement	G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselun
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 5.7	Abhören von Leitunge
			M 2.64	(A)	Betrieb	Kontrolle der Protokolldateien	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.22	Fehlende Auswertung von Protokolldate
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.8	Fehlerhafte Nutzung des IT-System

							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.14	Gebührenbetrug
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.61	Missbrauch von Remote-Zugängen für Managementfunktionen von Route
							G 5.62	Missbrauch von Ressourcen über abgesetzte IT-Systeme
							G 5.63	Manipulationen über den ISDN-D-Kana
			M 2.106	(A)	Beschaff.	Auswahl geeigneter ISDN-Karten in der Beschaffung	G 1.2	Ausfall des IT-System
							G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
							G 4.25	Nicht getrennte Verbindunge
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
			M 2.107	(A)	Umsetzg.	Dokumentation der ISDN-Karten-Konfiguration	G 1.2	Ausfall des IT-System
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
			M 2.108	(Z)	Planung	Verzicht auf Fernwartung der ISDN-Netzkoppelelemente	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 5.2	Manipulation an Daten oder Softwar
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.14	Gebührenbetrug
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
							G 5.61	Missbrauch von Remote-Zugängen für Managementfunktionen von Route
							G 5.62	Missbrauch von Ressourcen über abgesetzte IT-Systeme
			M 2.109	(A)	Umsetzg.	Rechtevergabe für den Fernzugriff	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 5.2	Manipulation an Daten oder Softwar
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.14	Gebührenbetrug
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
							G 5.61	Missbrauch von Remote-Zugängen für Managementfunktionen von Route

						G 5.62	Missbrauch von Ressourcen über abgesetzte IT-Systeme
			M 2.204	(A)	Umsetzg.	Verhinderung ungesicherter Netzzugänge	G 2.7	Unerlaubte Ausübung von Rechte
							G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitunge
							G 5.9	Unberechtigte IT-Nutzun
			M 4.7	(A)	Umsetzg.	Änderung voreingestellter Passwörter	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
			M 4.34	(Z)	Planung	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen	G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitunge
							G 5.8	Manipulation an Leitunge
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
							G 5.61	Missbrauch von Remote-Zugängen für Managementfunktionen von Route
							G 5.62	Missbrauch von Ressourcen über abgesetzte IT-Systeme
			M 4.59	(A)	Umsetzg.	Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 2.32	Unzureichende Leitungskapazitäte
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.14	Gebührenbetruc
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
			M 4.60	(A)	Umsetzg.	Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 5.2	Manipulation an Daten oder Softwar
							G 5.8	Manipulation an Leitunge
							G 5.9	Unberechtigte IT-Nutzun
							G 5.14	Gebührenbetruc
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter

			M 4.61	(A)	Umsetzg.	Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitunge
							G 5.9	Unberechtigte IT-Nutzun
							G 5.14	Gebührenbetruc
							G 5.25	Maskerade
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
			M 4.62	(Z)	Planung	Einsatz eines D-Kanal-Filters	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.14	Gebührenbetruc
							G 5.25	Maskerade
							G 5.63	Manipulationen über den ISDN-D-Kana
			M 5.29	(C)	Betrieb	Gelegentliche Kontrolle programmierter Zieladressen und Protokolle	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
							G 5.14	Gebührenbetruc
			M 5.32	(A)	Planung	Sicherer Einsatz von Kommunikationssoftware	G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
			M 5.47	(Z)	Planung	Einrichten einer Closed User Group	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.14	Gebührenbetruc
			M 5.48	(A)	Umsetzg.	Authentisierung mittels CLIP/COLP	G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 5.2	Manipulation an Daten oder Softwar

							G 5.9	Unberechtigte IT-Nutzun
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.14	Gebührenbetruc
							G 5.48	IP-Spoofing
			M 5.49	(A)	Umsetzg.	Callback basierend auf CLIP/COLP	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.14	Gebührenbetruc
							G 5.25	Maskerade
							G 5.48	IP-Spoofing
			M 5.50	(A)	Umsetzg.	Authentisierung mittels PAP/CHAP	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.14	Gebührenbetruc
							G 5.25	Maskerade
B 5.1	(6.3)	Peer-to-Peer-Dienste	M 2.67	(A)	Planung	Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste	G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäter
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.18	Freigabe von Verzeichnissen, Druckern oder der Ablagemappe
							G 3.19	Speichern von Passwörtern unter WfW und Windows 95
							G 5.45	Ausprobieren von Passwörtern unter WfW und Windows 95
							G 5.46	Maskerade unter WfW
			M 2.68	(B)	Betrieb	Sicherheitskontrollen durch die Benutzer beim Einsatz von Peer-to-Peer-Diensten	G 3.9	Fehlerhafte Administration des IT-System
							G 3.18	Freigabe von Verzeichnissen, Druckern oder der Ablagemappe
							G 5.45	Ausprobieren von Passwörtern unter WfW und Windows 95
			M 2.94	(B)	Umsetzg.	Freigabe von Verzeichnissen unter	G 3.9	Fehlerhafte Administration des IT-System

						Windows NT	G 3.18	Freigabe von Verzeichnissen, Druckern oder der Ablagemappe
							G 5.45	Ausprobieren von Passwörtern unter WfW und Windows 95
			M 3.19	(A)	Umsetzg.	Einweisung in den richtigen Einsatz der Sicherheitsfunktionen von Peer-to-Peer-Diensten	G 3.18	Freigabe von Verzeichnissen, Druckern oder der Ablagemappe
							G 3.19	Speichern von Passwörtern unter WfW und Windows 95
							G 5.45	Ausprobieren von Passwörtern unter WfW und Windows 95
							G 5.46	Maskerade unter WfW
			M 4.45	(A)	Umsetzg.	Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW	G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäter
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.18	Freigabe von Verzeichnissen, Druckern oder der Ablagemappe
							G 3.19	Speichern von Passwörtern unter WfW und Windows 95
							G 3.20	Ungewollte Freigabe des Leserechtes bei Schedule-
			M 4.46	(A)	Betrieb	Nutzung des Anmeldepasswortes unter WfW und Windows 9	G 3.19	Speichern von Passwörtern unter WfW und Windows 95
			M 4.58	(B)	Betrieb	Freigabe von Verzeichnissen unter Windows 95	G 5.45	Ausprobieren von Passwörtern unter WfW und Windows 95
							G 5.47	Löschen des Post-Office unter WfW
			M 4.149	(A)	Umsetzg.	Datei- und Freigabeberechtigungen unter Windows 2000/XP	G 3.9	Fehlerhafte Administration des IT-System
							G 3.18	Freigabe von Verzeichnissen, Druckern oder der Ablagemappe
			M 5.37	(B)	Planung	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz	G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäter
							G 3.9	Fehlerhafte Administration des IT-System
			M 5.82	(A)	Betrieb	Sicherer Einsatz von SAMBA	G 2.65	Komplexität der SAMBA-Konfiguratior
B 5.2	(7.1)	Datenträgeraustausch	M 1.36	(A)	Betrieb	Sichere Aufbewahrung der Datenträger vor und nach Versand	G 1.7	Unzulässige Temperatur und Luftfeuch
							G 1.8	Staub, Verschmutzun
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.29	Unberechtigtes Kopieren der Datenträge
			M 2.3	(B)	Planung	Datenträgerverwaltung	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.10	Nicht fristgerecht verfügbare Datenträge
							G 5.2	Manipulation an Daten oder Softwar

			M 2.42	(B)	Planung	Festlegung der möglichen Kommunikationspartner	G 2.18	Ungeordnete Zustellung der Datenträge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
			M 2.43	(A)	Betrieb	Ausreichende Kennzeichnung der Datenträger beim Versand	G 2.10	Nicht fristgerecht verfügbare Datenträge
							G 2.17	Mangelhafte Kennzeichnung der Datenträge
							G 2.18	Ungeordnete Zustellung der Datenträge
							G 3.12	Verlust der Datenträger beim Versanc
			M 2.44	(A)	Betrieb	Sichere Verpackung der Datenträger	G 1.7	Unzulässige Temperatur und Luftfeuch
							G 1.8	Staub, Verschmutzunc
							G 1.9	Datenverlust durch starke Magnetfelde
							G 3.12	Verlust der Datenträger beim Versanc
							G 4.7	Defekte Datenträger
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwarc
							G 5.9	Unberechtigte IT-Nutzun
							G 5.29	Unberechtigtes Kopieren der Datenträge
			M 2.45	(A)	Planung	Regelung des Datenträgeraustausches	G 2.10	Nicht fristgerecht verfügbare Datenträge
							G 2.18	Ungeordnete Zustellung der Datenträge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
			M 2.46	(Z)	Planung	Geeignetes Schlüsselmanagement	G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselunc
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
			M 3.14	(B)	Betrieb	Einweisung des Personals in den geregelten Ablauf eines Datenträgeraustausches	G 2.10	Nicht fristgerecht verfügbare Datenträge
							G 2.17	Mangelhafte Kennzeichnung der Datenträge
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
			M 4.32	(B)	Aussnd.	Physikalisches Löschen der Datenträger vor und nach Verwendung	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
			M 4.33	(A)	Betrieb	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragunc	G 5.4	Diebstahl
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.34	(Z)	Planung	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 5.2	Manipulation an Daten oder Softwarc
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.23	Computer-Viren

							G 5.29	Unberechtigtes Kopieren der Datenträge
							G 5.43	Makro-Viren
			M 4.35	(Z)	Betrieb	Verifizieren der zu übertragenden Daten vor Versand	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
			M 5.22	(B)	Umsetzg.	Kompatibilitätsprüfung des Sender- und Empfängersystems	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.10	Nicht fristgerecht verfügbare Datenträge
			M 5.23	(A)	Umsetzg.	Auswahl einer geeigneten Versandart für den Datenträger	G 2.10	Nicht fristgerecht verfügbare Datenträge
							G 2.18	Ungeordnete Zustellung der Datenträge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.12	Verlust der Datenträger beim Versand
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.9	Unberechtigte IT-Nutzun
							G 5.23	Computer-Viren
							G 5.29	Unberechtigtes Kopieren der Datenträge
			M 6.38	(A)	Notfallv.	Sicherungskopie der übermittelten Daten	G 1.9	Datenverlust durch starke Magnetfelde
							G 3.12	Verlust der Datenträger beim Versand
							G 4.7	Defekte Datenträger
							G 5.2	Manipulation an Daten oder Softwar
							G 5.4	Diebstahl
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
B 5.3	(7.4)	E-Mail	M 2.30	(A)	Planung	Regelung für die Einrichtung von Benutzern / Benutzergruppen	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 5.72	Mißbräuchliche E-Mail-Nutzun
			M 2.42	(B)	Planung	Festlegung der möglichen Kommunikationspartner	G 2.55	Ungeordnete E-Mail-Nutzun
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.23	Computer-Viren
			M 2.46	(Z)	Planung	Geeignetes Schlüsselmanagement	G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselun
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 5.7	Abhören von Leitunge
			M 2.118	(A)	Planung	Konzeption der sicheren E-Mail-Nutzung	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselun

							G 2.54	Vertraulichkeitsverlust durch Restinformatione
							G 2.55	Ungeordnete E-Mail-Nutzun
							G 2.56	Mangelhafte Beschreibung von Dateie
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
			M 2.119	(A)	Planung	Regelung für den Einsatz von E-Mail	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselun
							G 2.54	Vertraulichkeitsverlust durch Restinformatione
							G 2.55	Ungeordnete E-Mail-Nutzun
							G 2.56	Mangelhafte Beschreibung von Dateie
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-Systen
							G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
			M 2.120	(A)	Umsetzg.	Einrichtung einer Poststelle	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.55	Ungeordnete E-Mail-Nutzun
							G 4.32	Nichtzustellung einer Nachricl
			M 2.121	(B)	Betrieb	Regelmäßiges Löschen von E-Mails	G 4.20	Datenverlust bei erschöpftem Speichermediun
							G 5.75	Überlastung durch eingehende E-Mail
			M 2.122	(B)	Planung	Einheitliche E-Mail-Adressen	G 2.55	Ungeordnete E-Mail-Nutzun
							G 5.73	Vortäuschen eines falschen Absender
			M 2.123	(B)	Beschaff.	Auswahl eines Mailproviders	G 5.2	Manipulation an Daten oder Softwar
							G 5.26	Analyse des Nachrichtenflusse
							G 5.27	Nichtanerkennung einer Nachricl
							G 5.75	Überlastung durch eingehende E-Mail
							G 5.76	Mailbomben
							G 5.77	Mitlesen von E-Mails
			M 2.274	(A)	Planung	Vertretungsregelungen bei E-Mail-Nutzun	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.55	Ungeordnete E-Mail-Nutzun
			M 2.275	(Z)	Umsetzg.	Einrichtung funktionsbezogener E-Mailadressen	G 2.55	Ungeordnete E-Mail-Nutzung
			M 4.33	(A)	Betrieb	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragun	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.34	(Z)	Betrieb	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitunge
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren

							G 5.24	Wiedereinspielen von Nachrichten
							G 5.25	Maskerade
							G 5.43	Makro-Viren
							G 5.73	Vortäuschen eines falschen Absender
							G 5.77	Mitlesen von E-Mails
			M 4.44	(A)	Betrieb	Prüfung eingehender Dateien auf Makro-Viren	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.2	Manipulation an Daten oder Softwar
							G 5.43	Makro-Viren
			M 4.64	(C)	Betrieb	Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformation	G 2.54	Vertraulichkeitsverlust durch Restinformationen
			M 4.199	(B)	Betrieb	Vermeidung gefährlicher Dateiformate	G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.110	Web-Bugs
							G 5.111	Missbrauch aktiver Inhalte in E-Mail
			M 5.22	(B)	Umsetzg.	Kompatibilitätsprüfung des Sender- und Empfängersystems	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 4.32	Nichtzustellung einer Nachricl
			M 5.32	(A)	Umsetzg.	Sicherer Einsatz von Kommunikationssoftware	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.8	Fehlerhafte Nutzung des IT-System
							G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
			M 5.53	(B)	Betrieb	Schutz vor Mailbomben	G 4.20	Datenverlust bei erschöpftem Speichermedium
							G 5.28	Verhinderung von Diensten
							G 5.75	Überlastung durch eingehende E-Mail
							G 5.76	Mailbomben
			M 5.54	(B)	Betrieb	Schutz vor Mailüberlastung und Spam	G 4.20	Datenverlust bei erschöpftem Speichermedium
							G 5.28	Verhinderung von Diensten
							G 5.75	Überlastung durch eingehende E-Mail
							G 5.76	Mailbomben
			M 5.55	(B)	Betrieb	Kontrolle von Alias-Dateien und Verteilerlisten	G 4.20	Datenverlust bei erschöpftem Speichermedium
							G 5.74	Manipulation von Alias-Dateien oder Verteilerliste
			M 5.56	(A)	Betrieb	Sicherer Betrieb eines Mailservers	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 4.20	Datenverlust bei erschöpftem Speichermedium
							G 4.32	Nichtzustellung einer Nachricl
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.28	Verhinderung von Diensten
							G 5.43	Makro-Viren

							G 5.74	Manipulation von Alias-Dateien oder Verteilerliste
							G 5.75	Überlastung durch eingehende E-Mail
							G 5.76	Mailbomben
							G 5.77	Mitlesen von E-Mails
			M 5.57	(A)	Umsetzg.	Sichere Konfiguration der Mail-Clients	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.55	Ungeordnete E-Mail-Nutzun
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.9	Unberechtigte IT-Nutzun
			M 5.63	(Z)	Planung	Einsatz von GnuPG oder PGP	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 5.2	Manipulation an Daten oder Softwar
							G 5.7	Abhören von Leitunge
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.24	Wiedereinspielen von Nachrichte
							G 5.25	Maskerade
							G 5.43	Makro-Viren
							G 5.73	Vortäuschen eines falschen Absender
							G 5.77	Mitlesen von E-Mails
			M 5.67	(Z)	Planung	Verwendung eines Zeitstempel-Dienstes	G 4.37	Mangelnde Authentizität und Vertraulichkeit von E-Mail
			M 5.108	(Z)	Planung	Kryptographische Absicherung von E-Mail	G 4.37	Mangelnde Authentizität und Vertraulichkeit von E-M
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 5.109	(Z)	Betrieb	Einsatz eines E-Mail-Scanners auf dem Mailserver	G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.111	Missbrauch aktiver Inhalte in E-Mail
			M 5.110	(Z)	Planung	Absicherung von E-Mail mit SPHINX (S/MIME)	G 4.37	Mangelnde Authentizität und Vertraulichkeit von E-M
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 6.38	(A)	Notfallv.	Sicherungskopie der übermittelten Daten	G 4.20	Datenverlust bei erschöpftem Speichermedium
							G 4.32	Nichtzustellung einer Nachricl
							G 5.2	Manipulation an Daten oder Softwar
			M 6.90	(C)	Notfallv.	Datensicherung und Archivierung von E-Mails	G 4.13	Verlust gespeicherter Daten
B 5.4	(7.5)	Webserver	M 2.172	(A)	Planung	Entwicklung eines Konzeptes für die WWW-Nutzung	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.28	Verstöße gegen das Urheberrech
							G 2.32	Unzureichende Leitungskapazitäte
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systeme

							G 5.2	Manipulation an Daten oder Softwar
							G 5.20	Missbrauch von Administratorrechte
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.28	Verhinderung von Dienste
							G 5.43	Makro-Viren
							G 5.48	IP-Spoofing
							G 5.78	DNS-Spoofing
							G 5.87	Web-Spoofing
							G 5.88	Missbrauch aktiver Inhalt
			M 2.173	(A)	Planung	Festlegung einer WWW-Sicherheitsstrategie	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.28	Verstöße gegen das Urheberrech
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 5.2	Manipulation an Daten oder Softwar
							G 5.88	Missbrauch aktiver Inhalt
			M 2.174	(A)	Betrieb	Sicherer Betrieb eines WWW-Servers	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 3.38	Konfigurations- und Bedienungsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.20	Missbrauch von Administratorrechte
							G 5.21	Trojanische Pferde
							G 5.43	Makro-Viren
			M 2.175	(A)	Planung	Aufbau eines WWW-Servers	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.28	Verstöße gegen das Urheberrech
			M 2.176	(B)	Beschaff.	Geeignete Auswahl eines Internet Service Providers	G 2.32	Unzureichende Leitungskapazitäte
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 3.37	Unproduktive Suchzeite
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.78	DNS-Spoofing
			M 2.271	(A)	Planung	Festlegung einer Sicherheitsstrategie für den WWW-Zugan	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte

			M 2.272	(A)	Planung	Einrichtung eines WWW-Redaktionsteams	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.28	Verstöße gegen das Urheberrech
							G 2.96	Veraltete oder falsche Informationen in einem Webangebot
			M 2.273	(A)	Betrieb	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	G 4.22	Software-Schwachstellen oder -Fehler
			M 2.298	(Z)	Betrieb	Verwaltung von Internet-Domainnamer	G 2.100	Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen
			M 4.33	(A)	Betrieb	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragunc	G 5.2	Manipulation an Daten oder Softwar
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
			M 4.34	(Z)	Betrieb	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.23	Computer-Viren
							G 5.43	Makro-Viren
							G 5.88	Missbrauch aktiver Inhalt
			M 4.64	(C)	Betrieb	Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformatione	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 4.22	Software-Schwachstellen oder -Fehle
			M 4.78	(A)	Betrieb	Sorgfältige Durchführung von Konfigurationsänderungen	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 3.38	Konfigurations- und Bedienungsfehle
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.88	Missbrauch aktiver Inhalt
			M 4.93	(B)	Betrieb	Regelmäßige Integritätsprüfung	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 5.2	Manipulation an Daten oder Softwar
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.21	Trojanische Pferde
							G 5.88	Missbrauch aktiver Inhalt
			M 4.94	(A)	Umsetzg.	Schutz der WWW-Dateien	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 5.2	Manipulation an Daten oder Softwar
			M 4.95	(A)	Umsetzg.	Minimales Betriebssystem	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 3.38	Konfigurations- und Bedienungsfehle

							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
							G 5.28	Verhinderung von Dienste
					M 4.96	(Z)	Umsetzg.	Abschaltung von DNS
					M 4.97	(Z)	Umsetzg.	Ein Dienst pro Server
							G 3.38	Konfigurations- und Bedienungsfehle
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.28	Verhinderung von Dienste
					M 4.98	(A)	Umsetzg.	Kommunikation durch Paketfilter auf Minimum beschränken
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 5.2	Manipulation an Daten oder Softwar
							G 5.28	Verhinderung von Dienste
					M 4.99	(C)	Umsetzg.	Schutz gegen nachträgliche Veränderungen von Informationen
							G 2.28	Verstöße gegen das Urheberrech
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
					M 4.176	(B)	Planung	Auswahl einer Authentisierungsmethode fü
							G 5.2	Manipulation an Daten oder Softwar
							G 5.19	Missbrauch von Benutzerrechte
					M 4.177	(B)	Betrieb	Sicherstellung der Integrität und Authentizität von Softwarepakete
							G 5.2	Manipulation an Daten oder Softwar
							G 5.21	Trojanische Pferde
					M 5.59	(A)	Betrieb	Schutz vor DNS-Spoofing
							G 5.78	DNS-Spoofing
					M 5.64	(Z)	Planung	Secure Shell
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.20	Missbrauch von Administratorrechte
							G 5.48	IP-Spoofing
							G 5.88	Missbrauch aktiver Inhalt
					M 5.66	(Z)	Planung	Verwendung von SSL
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.87	Web-Spoofing
							G 5.88	Missbrauch aktiver Inhalt

			M 5.69	(A)	Planung	Schutz vor aktiven Inhalten	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.39	Software-Konzeptionsfehle
							G 5.2	Manipulation an Daten oder Softwar
							G 5.87	Web-Spoofing
							G 5.88	Missbrauch aktiver Inhalt
			M 6.88	(B)	Notfallv.	Erstellen eines Notfallplans für den Webserver	G 2.1	Fehlende oder unzureichende Regelungen
B 5.5	(7.7)	Lotus Notes	M 2.206	(A)	Planung	Planung des Einsatzes von Lotus Notes	G 1.1	Personalausfal
							G 1.2	Ausfall des IT-System
							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 2.40	Komplexität des Datenbankzugangs/-zugriff
							G 3.46	Fehlkonfiguration eines Lotus Notes Server
							G 3.47	Fehlkonfiguration des Browser-Zugriffs auf Lotus Note
							G 5.100	Missbrauch aktiver Inhalte beim Zugriff auf Lotus Not
							G 5.101	"Hacking Lotus Notes'
			M 2.207	(A)	Planung	Festlegen einer Sicherheitsrichtlinie für Lotus Notes	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.18	Ungeordnete Zustellung der Datenträge
							G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselun
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.43	Ungeeigneter Umgang mit Passwörter
							G 3.46	Fehlkonfiguration eines Lotus Notes Server
							G 3.47	Fehlkonfiguration des Browser-Zugriffs auf Lotus Note
							G 5.22	Diebstahl bei mobiler Nutzung des IT-System
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
							G 5.85	Integritätsverlust schützenswerter Information
							G 5.100	Missbrauch aktiver Inhalte beim Zugriff auf Lotus Not
							G 5.101	"Hacking Lotus Notes'
			M 2.208	(A)	Planung	Planung der Domänen und der Zertifikatshierarchie von Lotus Notes	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselun
							G 3.46	Fehlkonfiguration eines Lotus Notes Server
							G 3.47	Fehlkonfiguration des Browser-Zugriffs auf Lotus Note

							G 4.35	Unsichere kryptographische Algorithme
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
							G 5.100	Missbrauch aktiver Inhalte beim Zugriff auf Lotus Not
			M 2.209	(B)	Planung	Planung des Einsatzes von Lotus Note im Intranet	G 1.1	Personalausfal
							G 1.2	Ausfall des IT-System
							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.40	Komplexität des Datenbankzugangs/-zugriff
							G 3.46	Fehlkonfiguration eines Lotus Notes Server
							G 5.100	Missbrauch aktiver Inhalte beim Zugriff auf Lotus Not
			M 2.210	(B)	Planung	Planung des Einsatzes von Lotus Note im Intranet mit Browser-Zugriff	G 1.1	Personalausfal
							G 1.2	Ausfall des IT-System
							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.40	Komplexität des Datenbankzugangs/-zugriff
							G 3.47	Fehlkonfiguration des Browser-Zugriffs auf Lotus Note
			M 2.211	(A)	Planung	Planung des Einsatzes von Lotus Note in einer DMZ	G 1.1	Personalausfal
							G 1.2	Ausfall des IT-System
							G 2.1	Fehlende oder unzureichende Regelunge
							G 2.40	Komplexität des Datenbankzugangs/-zugriff
							G 3.46	Fehlkonfiguration eines Lotus Notes Server
							G 3.47	Fehlkonfiguration des Browser-Zugriffs auf Lotus Note
							G 5.101	"Hacking Lotus Notes'
			M 3.24	(A)	Umsetzg.	Schulung zur Lotus Notes Systemarchitektur für Administratoren	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.18	Ungeordnete Zustellung der Datenträge
							G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.43	Ungeeigneter Umgang mit Passwörter
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 5.22	Diebstahl bei mobiler Nutzung des IT-System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.100	Missbrauch aktiver Inhalte beim Zugriff auf Lotus Not
			M 3.25	(A)	Umsetzg.	Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.18	Ungeordnete Zustellung der Datenträge
							G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung
							G 2.49	Fehlende oder unzureichende Schulung der Telearbeite
							G 3.43	Ungeeigneter Umgang mit Passwörter
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 5.22	Diebstahl bei mobiler Nutzung des IT-System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.100	Missbrauch aktiver Inhalte beim Zugriff auf Lotus Not

			M 4.116	(A)	Umsetzg.	Sichere Installation von Lotus Notes	G 2.7 Unerlaubte Ausübung von Rechte
							G 3.9 Fehlerhafte Administration des IT-System
							G 3.46 Fehlkonfiguration eines Lotus Notes Server
							G 3.47 Fehlkonfiguration des Browser-Zugriffs auf Lotus Note
							G 5.71 Vertraulichkeitsverlust schützenswerter Information
			M 4.117	(A)	Umsetzg.	Sichere Konfiguration eines Lotus Notes Servers	G 2.7 Unerlaubte Ausübung von Rechte
							G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.9 Fehlerhafte Administration des IT-System
							G 3.46 Fehlkonfiguration eines Lotus Notes Server
							G 3.47 Fehlkonfiguration des Browser-Zugriffs auf Lotus Note
							G 5.71 Vertraulichkeitsverlust schützenswerter Information
			M 4.118	(A)	Umsetzg.	Konfiguration als Lotus Notes Server	G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 2.40 Komplexität des Datenbankzugangs/-zugriff
							G 3.9 Fehlerhafte Administration des IT-System
							G 3.46 Fehlkonfiguration eines Lotus Notes Server
			M 4.119	(A)	Umsetzg.	Einrichten von Zugangsbeschränkungen auf Lotus Notes Server	G 2.7 Unerlaubte Ausübung von Rechte
							G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.9 Fehlerhafte Administration des IT-System
							G 3.46 Fehlkonfiguration eines Lotus Notes Server
							G 5.84 Gefälschte Zertifikate
			M 4.120	(A)	Umsetzg.	Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken	G 2.7 Unerlaubte Ausübung von Rechte
							G 2.40 Komplexität des Datenbankzugangs/-zugriff
							G 3.9 Fehlerhafte Administration des IT-System
							G 3.46 Fehlkonfiguration eines Lotus Notes Server
			M 4.121	(A)	Umsetzg.	Konfiguration der Zugriffsrechte auf das Namens- und Adressbuch von Lotus Notes	G 2.7 Unerlaubte Ausübung von Rechte
							G 3.9 Fehlerhafte Administration des IT-System
							G 3.46 Fehlkonfiguration eines Lotus Notes Server
							G 5.71 Vertraulichkeitsverlust schützenswerter Information
			M 4.122	(B)	Umsetzg.	Konfiguration für den Browser-Zugriff auf Lotus Notes	G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.9 Fehlerhafte Administration des IT-System
							G 3.47 Fehlkonfiguration des Browser-Zugriffs auf Lotus Note
			M 4.123	(B)	Umsetzg.	Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes	G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.47 Fehlkonfiguration des Browser-Zugriffs auf Lotus Note
							G 4.35 Unsichere kryptographische Algorithme
							G 5.71 Vertraulichkeitsverlust schützenswerter Information
			M 4.124	(A)	Umsetzg.	Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes	G 2.7 Unerlaubte Ausübung von Rechte
							G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.43 Ungeeigneter Umgang mit Passwörter
							G 3.47 Fehlkonfiguration des Browser-Zugriffs auf Lotus Note

							G 4.35	Unsichere kryptographische Algorithme
							G 5.101	"Hacking Lotus Notes'
			M 4.125	(A)	Umsetzg.	Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.47	Fehlkonfiguration des Browser-Zugriffs auf Lotus Note
							G 5.101	"Hacking Lotus Notes'
			M 4.126	(A)	Umsetzg.	Sichere Konfiguration eines Lotus Notes Clients	G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PC
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 5.22	Diebstahl bei mobiler Nutzung des IT-System
							G 5.100	Missbrauch aktiver Inhalte beim Zugriff auf Lotus Not
			M 4.127	(A)	Umsetzg.	Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes	G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PC
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 5.22	Diebstahl bei mobiler Nutzung des IT-System
			M 4.128	(A)	Betrieb	Sicherer Betrieb von Lotus Notes	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.46	Fehlkonfiguration eines Lotus Notes Server
							G 3.47	Fehlkonfiguration des Browser-Zugriffs auf Lotus Note
							G 5.101	"Hacking Lotus Notes'
			M 4.129	(A)	Betrieb	Sicherer Umgang mit Notes-ID-Dateien	G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PC
							G 2.18	Ungeordnete Zustellung der Datenträge
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 3.43	Ungeeigneter Umgang mit Passwörter
							G 3.44	Sorglosigkeit im Umgang mit Informatione
							G 3.46	Fehlkonfiguration eines Lotus Notes Server
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.84	Gefälschte Zertifikate
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.130	(A)	Betrieb	Sicherheitsmaßnahmen nach dem Anlegen neuer Lotus Notes	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.46	Fehlkonfiguration eines Lotus Notes Server
			M 4.131	(Z)	Planung	Verschlüsselung von Lotus Notes Datenbanken	G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PC
							G 3.46	Fehlkonfiguration eines Lotus Notes Server
							G 5.22	Diebstahl bei mobiler Nutzung des IT-System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.77	Mitlesen von E-Mails
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.132	(C)	Betrieb	Überwachen eines Lotus Notes-Systems	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen

							G 2.7	Unerlaubte Ausübung von Rechte
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindunge
							G 2.40	Komplexität des Datenbankzugangs/-zugriff
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.46	Fehlkonfiguration eines Lotus Notes Server
							G 3.47	Fehlkonfiguration des Browser-Zugriffs auf Lotus Note
							G 5.22	Diebstahl bei mobiler Nutzung des IT-System
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.84	Gefälschte Zertifikate
							G 5.85	Integritätsverlust schützenswerter Information
							G 5.100	Missbrauch aktiver Inhalte beim Zugriff auf Lotus Not
							G 5.101	"Hacking Lotus Notes'
			M 5.84	(Z)	Betrieb	Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation	G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselun
							G 3.46	Fehlkonfiguration eines Lotus Notes Server
							G 4.35	Unsichere kryptographische Algorithme
							G 5.7	Abhören von Leitunge
							G 5.8	Manipulation an Leitunge
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.77	Mitlesen von E-Mails
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.85	Integritätsverlust schützenswerter Information
			M 5.85	(Z)	Betrieb	Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail	G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselun
							G 3.46	Fehlkonfiguration eines Lotus Notes Server
							G 4.35	Unsichere kryptographische Algorithme
							G 5.7	Abhören von Leitunge
							G 5.8	Manipulation an Leitunge
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.77	Mitlesen von E-Mails
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.85	Integritätsverlust schützenswerter Information
			M 5.86	(C)	Betrieb	Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes	G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselun
							G 3.46	Fehlkonfiguration eines Lotus Notes Server
							G 3.47	Fehlkonfiguration des Browser-Zugriffs auf Lotus Note
							G 4.35	Unsichere kryptographische Algorithme
							G 5.7	Abhören von Leitunge
							G 5.8	Manipulation an Leitunge
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.77	Mitlesen von E-Mails
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.85	Integritätsverlust schützenswerter Information
			M 6.49	(A)	Notfallv.	Datensicherung einer Datenbank	G 4.26	Ausfall einer Datenbank

							G 4.28	Verlust von Daten einer Datenban
			M 6.73	(B)	Notfallv.	Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems	G 1.1	Personalausfal
							G 1.2	Ausfall des IT-System
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.46	Fehlkonfiguration eines Lotus Notes Server
							G 3.47	Fehlkonfiguration des Browser-Zugriffs auf Lotus Note
							G 5.8	Manipulation an Leitunge
							G 5.22	Diebstahl bei mobiler Nutzung des IT-System
							G 5.84	Gefälschte Zertifikate
							G 5.85	Integritätsverlust schützenswerter Information
							G 5.100	Missbrauch aktiver Inhalte beim Zugriff auf Lotus Not
B 5.6	(8.5)	Faxserver	M 2.178	(A)	Planung	Erstellung einer Sicherheitsleitlinie für die Faxnutzung	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.63	Ungeordnete Faxnutzun
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.9	Unberechtigte IT-Nutzun
							G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
							G 5.31	Unbefugtes Lesen von Faxsendunge
							G 5.35	Überlastung durch Faxsendunge
			M 2.179	(A)	Planung	Regelungen für den Faxserver-Einsatz	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.22	Fehlende Auswertung von Protokolldate
							G 2.63	Ungeordnete Faxnutzun
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.9	Unberechtigte IT-Nutzun
							G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
							G 5.31	Unbefugtes Lesen von Faxsendunge
							G 5.32	Auswertung von Restinformationen in Faxgeräten und Faxserver
							G 5.35	Überlastung durch Faxsendunge
							G 5.90	Manipulation von Adressbüchern und Verteilliste
			M 2.180	(A)	Umsetzg.	Einrichten einer Fax-Poststelle	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.22	Fehlende Auswertung von Protokolldate
							G 2.63	Ungeordnete Faxnutzun
							G 4.20	Datenverlust bei erschöpftem Speichermediun
							G 5.9	Unberechtigte IT-Nutzun
							G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
							G 5.31	Unbefugtes Lesen von Faxsendunge
							G 5.32	Auswertung von Restinformationen in Faxgeräten und Faxserver
							G 5.35	Überlastung durch Faxsendunge
							G 5.90	Manipulation von Adressbüchern und Verteilliste
			M 2.181	(A)	Beschaff.	Auswahl eines geeigneten Faxservers	G 4.20	Datenverlust bei erschöpftem Speichermediun

						G 5.35	Überlastung durch Faxsendunge
						G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter
			M 3.15	(A)	Betrieb	Informationen für alle Mitarbeiter über die Faxnutzung	G 2.63	Ungeordnete Faxnutzun
							G 3.14	Fehleinschätzung der Rechtsverbindlichkeit eines Fa
							G 5.7	Abhören von Leitunge
							G 5.25	Maskerade
							G 5.27	Nichtanerkennung einer Nachrich
							G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
							G 5.31	Unbefugtes Lesen von Faxsendunge
							G 5.90	Manipulation von Adressbüchern und Verteilliste
			M 4.36	(Z)	Umsetzg.	Sperren bestimmter Faxempfänger-Rufnummer	G 2.63	Ungeordnete Faxnutzung
			M 4.37	(Z)	Umsetzg.	Sperren bestimmter Absender-Faxnummer	G 2.63	Ungeordnete Faxnutzung
			M 5.24	(Z)	Betrieb	Nutzung eines geeigneten Faxvorblattes	G 4.15	Fehlerhafte Faxübertragun
							G 5.33	Vortäuschen eines falschen Absenders bei Faxsendunger
			M 5.25	(A)	Betrieb	Nutzung von Sende- und Empfangsprotokollen	G 2.22	Fehlende Auswertung von Protokolldate
							G 5.24	Wiedereinspielen von Nachrichte
							G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
			M 5.26	(Z)	Betrieb	Telefonische Ankündigung einer Faxsendunc	G 4.15	Fehlerhafte Faxübertragun
							G 5.90	Manipulation von Adressbüchern und Verteilliste
			M 5.27	(Z)	Betrieb	Telefonische Rückversicherung über korrekten Faxempfanc	G 4.15	Fehlerhafte Faxübertragun
							G 5.90	Manipulation von Adressbüchern und Verteilliste
			M 5.28	(Z)	Betrieb	Telefonische Rückversicherung über korrekten Faxabsender	G 4.15	Fehlerhafte Faxübertragun
							G 5.33	Vortäuschen eines falschen Absenders bei Faxsendunger
			M 5.73	(A)	Betrieb	Sicherer Betrieb eines Faxservers	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.22	Fehlende Auswertung von Protokolldate
							G 4.20	Datenverlust bei erschöpftem Speichermediu
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.30	Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
							G 5.31	Unbefugtes Lesen von Faxsendunge
							G 5.32	Auswertung von Restinformationen in Faxgeräten und Faxserver
							G 5.35	Überlastung durch Faxsendunge
							G 5.39	Eindringen in Rechnersysteme über Kommunikationskarter

			M 5.74	(A)	Betrieb	Pflege der Faxserver-Adressbücher und der Verteillisten	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 2.63	Ungeordnete Faxnutzun
							G 5.31	Unbefugtes Lesen von Faxsendunge
							G 5.90	Manipulation von Adressbüchern und Verteilliste
			M 5.75	(Z)	Betrieb	Schutz vor Überlastung des Faxservers	G 5.35	Überlastung durch Faxsendungen
			M 6.69	(B)	Notfallv.	Notfallvorsorge und Ausfallsicherheit bei Faxserverr	G 4.20	Datenverlust bei erschöpftem Speichermediun
							G 5.35	Überlastung durch Faxsendunge
B 5.7	(9.2)	Datenbanken	M 2.31	(A)	Betrieb	Dokumentation der zugelassenen Benutzer und Rechteprofile	G 1.1	Personalausfal
							G 2.39	Komplexität eines DBMS
							G 2.40	Komplexität des Datenbankzugangs/-zugriff
							G 2.41	Mangelhafte Organisation des Wechsels von Datenbank-Benutzerr
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.23	Fehlerhafte Administration eines DBMS
							G 4.26	Ausfall einer Datenbanl
			M 2.34	(A)	Betrieb	Dokumentation der Veränderungen an einem bestehenden System	G 1.1	Personalausfal
							G 2.39	Komplexität eines DBMS
							G 4.26	Ausfall einer Datenbanl
			M 2.65	(B)	Betrieb	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System	G 2.41	Mangelhafte Organisation des Wechsels von Datenbank-Benutzerr
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
			M 2.80	(A)	Planung	Erstellung eines Anforderungskatalogs für Standardsoftware	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
			M 2.124	(A)	Beschaff.	Geeignete Auswahl einer Datenbank-Software	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.39	Komplexität eines DBMS
			M 2.125	(A)	Umsetzg.	Installation und Konfiguration einer Datenbank	G 2.38	Fehlende oder unzureichende Aktivierung von Datenbar Sicherheitsmechanismer
			M 2.126	(A)	Planung	Erstellung eines Datenbanksicherheitskonzeptes	G 1.1	Personalausfal
							G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.22	Fehlende Auswertung von Protokolldate
							G 2.38	Fehlende oder unzureichende Aktivierung von Datenbar Sicherheitsmechanismer
							G 2.39	Komplexität eines DBMS
							G 3.23	Fehlerhafte Administration eines DBMS
							G 4.26	Ausfall einer Datenbanl
							G 4.29	Datenverlust einer Datenbank bei erschöpftem Speichermedium
			M 2.127	(B)	Umsetzg.	Inferenzprävention	G 2.38	Fehlende oder unzureichende Aktivierung von Datenbar Sicherheitsmechanismer
							G 2.40	Komplexität des Datenbankzugangs/-zugriff

							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 5.64	Manipulation an Daten oder Software bei Datenbanksystemer
					M 2.128	(A)	Umsetzg.	Zugangskontrolle einer Datenbank
							G 2.40	Komplexität des Datenbankzugangs/-zugriff
							G 2.41	Mangelhafte Organisation des Wechsels von Datenbank-Benutzerr
							G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.23	Fehlerhafte Administration eines DBMS
							G 5.9	Unberechtigte IT-Nutzun
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.18	Systematisches Ausprobieren von Passwörter
					M 2.129	(A)	Umsetzg.	Zugriffskontrolle einer Datenbank
							G 2.40	Komplexität des Datenbankzugangs/-zugriff
							G 2.41	Mangelhafte Organisation des Wechsels von Datenbank-Benutzerr
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 5.9	Unberechtigte IT-Nutzun
							G 5.64	Manipulation an Daten oder Software bei Datenbanksystemer
					M 2.130	(A)	Betrieb	Gewährleistung der Datenbankintegrität
					M 2.131	(C)	Planung	Aufteilung von Administrationstätigkeiten bei Datenbanksystemen
							G 2.38	Fehlende oder unzureichende Aktivierung von Datenbar Sicherheitsmechanismer
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.23	Fehlerhafte Administration eines DBMS
					M 2.132	(A)	Planung	Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen
							G 2.41	Mangelhafte Organisation des Wechsels von Datenbank-Benutzerr
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
					M 2.133	(A)	Betrieb	Kontrolle der Protokolldateien eines Datenbanksystems
							G 5.9	Unberechtigte IT-Nutzun
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.18	Systematisches Ausprobieren von Passwörter
					M 2.134	(B)	Planung	Richtlinien für Datenbank-Anfragen
							G 2.39	Komplexität eines DBMS

							G 2.40	Komplexität des Datenbankzugangs/-zugriff
							G 3.24	Unbeabsichtigte Datenmanipulatior
							G 5.65	Verhinderung der Dienste eines Datenbanksystem
			M 2.135	(C)	Umsetzg.	Gesicherte Datenübernahme in eine Datenbank	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 4.28	Verlust von Daten einer Datenban
							G 4.29	Datenverlust einer Datenbank bei erschöpftem Speichermedium
							G 4.30	Verlust der Datenbankintegrität/-konsisten
			M 3.18	(A)	Betrieb	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllun	G 5.9	Unberechtigte IT-Nutzung
			M 4.7	(A)	Umsetzg.	Änderung voreingestellter Passwörter	G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.24	Unbeabsichtigte Datenmanipulatior
							G 5.9	Unberechtigte IT-Nutzun
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.64	Manipulation an Daten oder Software bei Datenbanksystemer
			M 4.67	(A)	Umsetzg.	Sperren und Löschen nicht benötigter Datenbank-Accounts	G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.24	Unbeabsichtigte Datenmanipulatior
							G 5.9	Unberechtigte IT-Nutzun
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.64	Manipulation an Daten oder Software bei Datenbanksystemer
			M 4.68	(A)	Betrieb	Sicherstellung einer konsistenten Datenbankverwaltung	G 2.40	Komplexität des Datenbankzugangs/-zugriff
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.23	Fehlerhafte Administration eines DBMS
							G 4.30	Verlust der Datenbankintegrität/-konsisten
							G 5.64	Manipulation an Daten oder Software bei Datenbanksystemer
			M 4.69	(B)	Betrieb	Regelmäßiger Sicherheitscheck der Datenbank	G 2.38	Fehlende oder unzureichende Aktivierung von Datenbar Sicherheitsmechanismer
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.23	Fehlerhafte Administration eines DBMS
							G 4.27	Unterlaufen von Zugriffskontrollen über ODB
							G 5.9	Unberechtigte IT-Nutzun
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.64	Manipulation an Daten oder Software bei Datenbanksystemer
							G 5.65	Verhinderung der Dienste eines Datenbanksystem
			M 4.70	(C)	Betrieb	Durchführung einer Datenbanküberwachung	G 4.26	Ausfall einer Datenbanl
							G 4.27	Unterlaufen von Zugriffskontrollen über ODB

							G 4.28	Verlust von Daten einer Datenban
							G 4.29	Datenverlust einer Datenbank bei erschöpftem Speichermedium
							G 4.30	Verlust der Datenbankintegrität/-konsisten
			M 4.71	(C)	Umsetzg.	Restriktive Handhabung von Datenban Links	G 5.9	Unberechtigte IT-Nutzun
							G 5.64	Manipulation an Daten oder Software bei Datenbanksystemer
			M 4.72	(Z)	Planung	Datenbank-Verschlüsselung	G 5.9	Unberechtigte IT-Nutzun
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.64	Manipulation an Daten oder Software bei Datenbanksystemer
			M 4.73	(C)	Planung	Festlegung von Obergrenzen für selektierbare Datensätze	G 4.29	Datenverlust einer Datenbank bei erschöpftem Speichermedium
							G 5.65	Verhinderung der Dienste eines Datenbanksystem
			M 5.58	(B)	Umsetzg.	Installation von ODBC-Treiber	G 4.27	Unterlaufen von Zugriffskontrollen über ODB
			M 6.48	(A)	Notfallv.	Verhaltensregeln nach Verlust der Datenbankintegrität	G 4.26	Ausfall einer Datenban
							G 4.30	Verlust der Datenbankintegrität/-konsisten
			M 6.49	(A)	Notfallv.	Datensicherung einer Datenbank	G 3.6	Gefährdung durch Reinigungs- oder Fremdperson
							G 3.24	Unbeabsichtigte Datenmanipulatior
							G 4.26	Ausfall einer Datenban
							G 4.28	Verlust von Daten einer Datenban
							G 4.29	Datenverlust einer Datenbank bei erschöpftem Speichermedium
							G 4.30	Verlust der Datenbankintegrität/-konsisten
							G 5.9	Unberechtigte IT-Nutzun
							G 5.64	Manipulation an Daten oder Software bei Datenbanksystemer
			M 6.50	(A)	Notfallv.	Archivierung von Datenbeständen	G 3.24	Unbeabsichtigte Datenmanipulatior
							G 4.26	Ausfall einer Datenban
							G 4.28	Verlust von Daten einer Datenban
							G 4.29	Datenverlust einer Datenbank bei erschöpftem Speichermedium
							G 4.30	Verlust der Datenbankintegrität/-konsisten
							G 5.64	Manipulation an Daten oder Software bei Datenbanksystemer
			M 6.51	(B)	Notfallv.	Wiederherstellung einer Datenbank	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmitte
							G 2.57	Nicht ausreichende Speichermedien für den Notfa
							G 3.24	Unbeabsichtigte Datenmanipulatior
							G 4.26	Ausfall einer Datenban
							G 4.28	Verlust von Daten einer Datenban
							G 4.29	Datenverlust einer Datenbank bei erschöpftem Speichermedium
							G 4.30	Verlust der Datenbankintegrität/-konsisten
B 5.8	(9.3)	Telearbeit	M 2.113	(A)	Planung	Regelungen für Telearbeit	G 1.1	Personalausfal
							G 2.1	Fehlende oder unzureichende Regelunge

							G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
							G 2.50	Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Telearbeiter
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.30	Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners
			M 2.114	(A)	Planung	Informationsfluss zwischen Telearbeiter und Institution	G 1.1	Personalausfal
							G 2.50	Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Telearbeiter
							G 2.51	Mangelhafte Einbindung des Telearbeiters in den Informationsfluss
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 5.2	Manipulation an Daten oder Softwar
			M 2.115	(B)	Planung	Betreuungs- und Wartungskonzept für Telearbeitsplätze	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.5	Fehlende oder unzureichende Wartun
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
			M 2.116	(A)	Planung	Geregelte Nutzung der Kommunikationsmöglichkeiten	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
							G 3.30	Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners
							G 5.2	Manipulation an Daten oder Softwar
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 2.117	(A)	Planung	Regelung der Zugriffsmöglichkeiten des Telearbeiters	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.30	Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners
							G 5.2	Manipulation an Daten oder Softwar
			M 2.205	(C)	Planung	Übertragung und Abruf personenbezogener Daten	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte

						G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
						G 2.49	Fehlende oder unzureichende Schulung der Telearbeiter
						G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
						G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
						G 3.9	Fehlerhafte Administration des IT-System
						G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
						G 3.30	Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners
						G 5.2	Manipulation an Daten oder Softwar
						G 5.7	Abhören von Leitunge
						G 5.19	Missbrauch von Benutzerrechte
						G 5.20	Missbrauch von Administratorrechte
						G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 2.241	(C)	Planung	G 2.1	Fehlende oder unzureichende Regelunge
					Durchführung einer Anforderungsanalyse für den Telearbeitsplatz	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
						G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
						G 4.13	Verlust gespeicherter Dater
						G 5.9	Unberechtigte IT-Nutzun
						G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 3.21	(A)	Betrieb	G 2.49	Fehlende oder unzureichende Schulung der Telearbeiter
					Sicherheitstechnische Einweisung und Fortbildung des Telearbeiters	G 2.53	Unzureichende Vertretungsregelungen für Telearb
						G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
						G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
						G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
						G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 3.22	(B)	Betrieb	G 1.1	Personalausfal
					Vertretungsregelung für Telearbeit	G 2.1	Fehlende oder unzureichende Regelunge
						G 2.53	Unzureichende Vertretungsregelungen für Telearb
			M 4.3	(A)	Betrieb	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
					Regelmäßiger Einsatz eines Anti-Viren-Programms	G 5.2	Manipulation an Daten oder Softwar
						G 5.43	Makro-Viren
			M 4.33	(A)	Betrieb	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
					Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragun		
			M 4.63	(A)	Umsetzg.	G 2.7	Unerlaubte Ausübung von Rechte
					Sicherheitstechnische Anforderungen an den Telearbeitsrechner	G 2.22	Fehlende Auswertung von Protokolldate

							G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.24	Wiedereinspielen von Nachrichte
							G 5.25	Maskerade
							G 5.43	Makro-Viren
			M 5.51	(A)	Umsetzg.	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.22	Fehlende Auswertung von Protokolldate
							G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 5.2	Manipulation an Daten oder Softwar
							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.21	Trojanische Pferde
							G 5.24	Wiedereinspielen von Nachrichte
							G 5.25	Maskerade
							G 5.43	Makro-Viren
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 5.52	(A)	Umsetzg.	Sicherheitstechnische Anforderungen an den Kommunikationsrechner	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.22	Fehlende Auswertung von Protokolldate
							G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netze
							G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutz
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 5.2	Manipulation an Daten oder Softwar

							G 5.10	Missbrauch von Fernwartungszugänge
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.21	Trojanische Pferde
							G 5.24	Wiedereinspielen von Nachrichte
							G 5.25	Maskerade
							G 5.43	Makro-Viren
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 6.38	(B)	Notfallv.	Sicherungskopie der übermittelten Daten	G 5.2	Manipulation an Daten oder Softwar
							G 5.23	Computer-Viren
			M 6.47	(B)	Notfallv.	Datensicherung bei der Telearbeit	G 2.52	Erhöhte Reaktionszeiten bei IT-Systemausfa
							G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahme
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.13	Verlust gespeicherter Dater
							G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubeh
							G 5.2	Manipulation an Daten oder Softwar
							G 5.9	Unberechtigte IT-Nutzun
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.21	Trojanische Pferde
							G 5.43	Makro-Viren
B 5.9	(9.4)	Novell eDirectory	M 2.236	(A)	Planung	Planung des Einsatzes von Novell eDirectory	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.69	Fehlende oder unzureichende Planung des Einsatzes vo Novell eDirectory
							G 4.13	Verlust gespeicherter Dater
			M 2.237	(B)	Planung	Planung der Partitionierung und Replikation im Novell eDirectory	G 2.70	Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Novell eDirecto
							G 5.81	Unautorisierte Benutzung eines Kryptomodu
			M 2.238	(A)	Planung	Festlegung einer Sicherheitsrichtlinie für Novell eDirector	G 2.1	Fehlende oder unzureichende Regelungen
			M 2.239	(A)	Planung	Planung des Einsatzes von Novell eDirectory im Intranet	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.69	Fehlende oder unzureichende Planung des Einsatzes vo Novell eDirectory
			M 2.240	(A)	Planung	Planung des Einsatzes von Novell eDirectory im Extranet	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.69	Fehlende oder unzureichende Planung des Einsatzes vo Novell eDirectory
							G 2.71	Fehlerhafte oder unzureichende Planung des LDAP-Zugriffs auf Novell eDirector
							G 4.33	Schlechte oder fehlende Authentikatio
							G 5.18	Systematisches Ausprobieren von Passwörter
			M 3.29	(A)	Umsetzg.	Schulung zur Administration von Novell eDirectory	G 2.2	Unzureichende Kenntnis über Regelunge
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter

							G 3.38	Konfigurations- und Bedienungsfehle
							G 3.50	Fehlkonfiguration von Novell eDirector
							G 3.51	Falsche Vergabe von Zugriffsrechten im Novell eDirectory
							G 3.52	Fehlkonfiguration des Intranet-Clientzugriffs auf Novell eDirectory
							G 3.53	Fehlkonfiguration des LDAP-Zugriffs auf Novell eDirectory
			M 3.30	(A)	Umsetzg.	Schulung zum Einsatz von Novell eDirectory Clientsoftware	G 2.2	Unzureichende Kenntnis über Regelunge
							G 3.38	Konfigurations- und Bedienungsfehle
							G 3.43	Ungeeigneter Umgang mit Passwörtern
			M 4.153	(A)	Umsetzg.	Sichere Installation von Novell eDirectory	G 1.2	Ausfall des IT-Systems
							G 4.44	Ausfall von Novell eDirector
			M 4.154	(A)	Umsetzg.	Sichere Installation der Novell eDirectory Clientsoftware	G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
							G 4.33	Schlechte oder fehlende Authentikatio
			M 4.155	(A)	Umsetzg.	Sichere Konfiguration von Novell eDirectory	G 3.34	Ungeeignete Konfiguration des Managementsystem
							G 3.38	Konfigurations- und Bedienungsfehle
							G 3.50	Fehlkonfiguration von Novell eDirector
							G 3.51	Falsche Vergabe von Zugriffsrechten im Novell eDirectory
							G 3.52	Fehlkonfiguration des Intranet-Clientzugriffs auf Novell eDirectory
							G 3.53	Fehlkonfiguration des LDAP-Zugriffs auf Novell eDirectory
							G 5.65	Verhinderung der Dienste eines Datenbanksystem
							G 5.81	Unautorisierte Benutzung eines Kryptomodu
			M 4.156	(A)	Umsetzg.	Sichere Konfiguration der Novell eDirectory Clientsoftware	G 3.38	Konfigurations- und Bedienungsfehle
							G 3.53	Fehlkonfiguration des LDAP-Zugriffs auf Novell eDirectory
							G 4.33	Schlechte oder fehlende Authentikatio
			M 4.157	(A)	Umsetzg.	Einrichten von Zugriffsberechtigungen auf Novell eDirectory	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.51	Falsche Vergabe von Zugriffsrechten im Novell eDirectory
							G 3.52	Fehlkonfiguration des Intranet-Clientzugriffs auf Novell eDirectory
							G 4.33	Schlechte oder fehlende Authentikatio
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
							G 5.18	Systematisches Ausprobieren von Passwörter
			M 4.158	(B)	Umsetzg.	Einrichten des LDAP-Zugriffs auf Nove	G 2.7	Unerlaubte Ausübung von Rechte

						eDirectory	G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.53	Fehlkonfiguration des LDAP-Zugriffs auf Novell eDirectory
							G 4.33	Schlechte oder fehlende Authentikatio
			M 4.159	(A)	Betrieb	Sicherer Betrieb von Novell eDirectory	G 3.9	Fehlerhafte Administration des IT-System
							G 3.35	Server im laufenden Betrieb ausschalte
							G 3.38	Konfigurations- und Bedienungsfehle
							G 4.33	Schlechte oder fehlende Authentikatio
							G 5.65	Verhinderung der Dienste eines Datenbanksystem
							G 5.81	Unautorisierte Benutzung eines Kryptomodu
			M 4.160	(B)	Betrieb	Überwachen von Novell eDirectory	G 3.36	Fehlinterpretation von Ereignisse
							G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Persona
							G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
							G 5.18	Systematisches Ausprobieren von Passwörter
							G 5.19	Missbrauch von Benutzerrechte
							G 5.20	Missbrauch von Administratorrechte
							G 5.65	Verhinderung der Dienste eines Datenbanksystem
			M 5.97	(B)	Betrieb	Absicherung der Kommunikation mit Novell eDirectory	G 3.13	Übertragung falscher oder nicht gewünschter Datensätze
							G 3.52	Fehlkonfiguration des Intranet-Clientzugriffs auf Novell eDirectory
							G 3.53	Fehlkonfiguration des LDAP-Zugriffs auf Novell eDirectory
							G 5.78	DNS-Spoofing
			M 6.80	(A)	Notfallv.	Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes	G 1.2	Ausfall des IT-System
							G 3.35	Server im laufenden Betrieb ausschalte
							G 4.44	Ausfall von Novell eDirector
			M 6.81	(A)	Notfallv.	Erstellen von Datensicherungen für Novell eDirectory	G 1.2	Ausfall des IT-System
							G 3.35	Server im laufenden Betrieb ausschalte
							G 4.13	Verlust gespeicherter Dater
							G 4.34	Ausfall eines Kryptomodul
							G 4.44	Ausfall von Novell eDirector
B 5.10	(7.8)	Internet Information Server	M 2.267	(A)	Planung	Planen des IIS-Einsatzes	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.94	Unzureichende Planung des IIS-Einsatze
							G 3.56	Fehlerhafte Einbindung des IIS in die Systemumgebung
			M 2.268	(A)	Planung	Festlegung einer IIS-Sicherheitsrichtlinie	G 2.1	Fehlende oder unzureichende Regelunge
							G 3.56	Fehlerhafte Einbindung des IIS in die Systemumgebung
			M 3.36	(A)	Umsetzg.	Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS	G 3.56	Fehlerhafte Einbindung des IIS in die Systemumgebung
							G 3.58	Fehlkonfiguration eines IIS

						G 3.59	Unzureichende Kenntnisse über aktuelle Sicherheitslücken und Prüfwerkzeuge für den I
			M 4.174	(A)	Umsetzg.	Vorbereitung der Installation von Windows NT/2000 für den IIS	G 3.57	Fehlerhafte Konfiguration des Betriebssystems für den IIS
			M 4.175	(A)	Umsetzg.	Sichere Konfiguration von Windows NT/2000 für den IIS	G 3.56	Fehlerhafte Einbindung des IIS in die Systemumgebung
							G 3.57	Fehlerhafte Konfiguration des Betriebssystems für den IIS
			M 4.178	(A)	Umsetzg.	Absicherung der Administrator- und Benutzerkonten beim IIS-Einsat	G 5.2	Manipulation an Daten oder Softwar
							G 5.20	Missbrauch von Administratorrechte
			M 4.179	(A)	Umsetzg.	Schutz von sicherheitskritischen Dateien beim IIS-Einsatz	G 5.2	Manipulation an Daten oder Software
			M 4.180	(A)	Umsetzg.	Konfiguration der Authentisierungsmechanismen für den Zugriff auf den IIS	G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
			M 4.181	(A)	Umsetzg.	Ausführen des IIS in einem separaten Prozess	G 3.58	Fehlkonfiguration eines IIS
							G 5.28	Verhinderung von Dienste
			M 4.182	(B)	Betrieb	Überwachen des IIS-Systems	G 4.22	Software-Schwachstellen oder -Fehle
							G 5.28	Verhinderung von Dienste
							G 5.108	Ausnutzen von systemspezifischen Schwachstellen des IIS
			M 4.183	(A)	Betrieb	Sicherstellen der Verfügbarkeit und Performance des IIS	G 5.28	Verhinderung von Diensten
			M 4.184	(A)	Umsetzg.	Deaktivieren nicht benötigter Dienste beim IIS-Einsatz	G 5.108	Ausnutzen von systemspezifischen Schwachstellen des IIS
			M 4.185	(A)	Umsetzg.	Absichern von virtuellen Verzeichnisse und Web-Anwendungen beim IIS-Einsatz	G 5.108	Ausnutzen von systemspezifischen Schwachstellen des IIS
			M 4.186	(A)	Umsetzg.	Entfernen von Beispieldateien und Administrations-Scripts des IIS	G 5.108	Ausnutzen von systemspezifischen Schwachstellen des IIS
			M 4.187	(A)	Umsetzg.	Entfernen der FrontPage Server-Erweiterung des IIS	G 4.22	Software-Schwachstellen oder -Fehle
							G 5.108	Ausnutzen von systemspezifischen Schwachstellen des IIS
			M 4.188	(B)	Umsetzg.	Prüfen der Benutzereingaben beim IIS-Einsatz	G 4.39	Software-Konzeptionsfehle
							G 5.88	Missbrauch aktiver Inhalt
			M 4.189	(B)	Umsetzg.	Schutz vor unzulässigen Programmaufrufen beim IIS-Einsatz	G 4.22	Software-Schwachstellen oder -Fehle
							G 5.108	Ausnutzen von systemspezifischen Schwachstellen des IIS
			M 4.190	(B)	Umsetzg.	Entfernen der RDS-Unterstützung des IIS	G 5.108	Ausnutzen von systemspezifischen Schwachstellen des IIS
			M 5.101	(B)	Umsetzg.	Entfernen nicht benötigter ODBC-Treiber beim IIS-Einsatz	G 3.56	Fehlerhafte Einbindung des IIS in die Systemumgebung
							G 3.57	Fehlerhafte Konfiguration des Betriebssystems für den IIS

			M 5.102	(B)	Umsetzg.	Installation von URL-Filtern beim IIS-Einsatz	G 5.108	Ausnutzen von systemspezifischen Schwachstellen des IIS
			M 5.103	(B)	Umsetzg.	Entfernen sämtlicher Netzwerkfreigaben beim IIS-Einsatz	G 3.56	Fehlerhafte Einbindung des IIS in die Systemumgebung
							G 3.57	Fehlerhafte Konfiguration des Betriebssystems für den IIS
							G 5.2	Manipulation an Daten oder Softwar
			M 5.104	(C)	Umsetzg.	Konfiguration des TCP/IP-Filters beim IIS-Einsatz	G 3.57	Fehlerhafte Konfiguration des Betriebssystems für den IIS
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.108	Ausnutzen von systemspezifischen Schwachstellen des IIS
			M 5.105	(C)	Umsetzg.	Vorbeugen vor SYN-Attacken auf den IIS	G 5.28	Verhinderung von Diensten
			M 5.106	(A)	Umsetzg.	Entfernen nicht vertrauenswürdiger Root-Zertifikate beim IIS-Einsat	G 5.84	Gefälschte Zertifikate
			M 6.85	(C)	Notfallv.	Erstellung eines Notfallplans für den Ausfall des IIS	G 2.1	Fehlende oder unzureichende Regelungen
			M 6.86	(B)	Umsetzg.	Schutz vor schädlichem Code auf dem IIS	G 5.108	Ausnutzen von systemspezifischen Schwachstellen des IIS
			M 6.87	(A)	Notfallv	Datensicherung auf dem IIS	G 4.13	Verlust gespeicherter Dater
B 5.11	(7.9)	Apache Webserver	M 2.269	(A)	Planung	Planung des Einsatzes eines Apache Webservers	G 2.1	Fehlende oder unzureichende Regelungen
			M 2.270	(Z)	Planung	Planung des SSL-Einsatzes beim Apache Webserver (zusätzlich	G 2.87	Verwendung unsicherer Protokolle in öffentlichen Netzen
			M 3.37	(A)	Umsetzg.	Schulung der Administratoren eines Apache-Webservers	G 3.9	Fehlerhafte Administration des IT-System
							G 3.38	Konfigurations- und Bedienungsfehle
							G 3.62	Fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver
							G 3.63	Fehlerhafte Konfiguration eines Apache-Webserver
			M 4.191	(A)	Beschaff.	Überprüfung der Integrität und Authentizität der Apache-Pakete	G 5.21	Trojanische Pferde
			M 4.192	(A)	Umsetzg.	Konfiguration des Betriebssystems für einen Apache-Webserver	G 3.62	Fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver
			M 4.193	(A)	Umsetzg.	Sichere Installation eines Apache-Webservers	G 3.62	Fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver
							G 3.63	Fehlerhafte Konfiguration eines Apache-Webserver
							G 5.2	Manipulation an Daten oder Softwar
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
							G 5.109	Ausnutzen systemspezifischer Schwachstellen beim Apache-Webserver
			M 4.194	(A)	Umsetzg.	Sichere Grundkonfiguration eines Apache-Webservers	G 3.63	Fehlerhafte Konfiguration eines Apache-Webservers

			M 4.195	(A)	Umsetzg.	Konfiguration der Zugriffssteuerung beim Apache-Webserver	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.63	Fehlerhafte Konfiguration eines Apache-Webserver
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.196	(A)	Betrieb	Sicherer Betrieb eines Apache-Webservers	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
							G 5.109	Ausnutzen systemspezifischer Schwachstellen beim Apache-Webserver
			M 4.197	(B)	Umsetzg.	Servererweiterungen für dynamische Webseiten beim Apache-Webserver	G 4.39	Software-Konzeptionsfehle
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
							G 5.85	Integritätsverlust schützenswerter Information
			M 4.198	(Z)	Umsetzg.	Installation eines Apache-Webservers in einem chroot-Käfig	G 5.2	Manipulation an Daten oder Software
			M 5.107	(Z)	Umsetzg.	Verwendung von SSL im Apache-Webserver	G 2.87	Verwendung unsicherer Protokolle in öffentlichen Netzen
							G 5.7	Abhören von Leitungen
							G 5.71	Vertraulichkeitsverlust schützenswerter Information
			M 6.89	(A)	Notfallv.	Notfallvorsorge für einen Apache-Webserver	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.97	Unzureichende Notfallplanung bei einem Apache-Webserver
							G 5.28	Verhinderung von Diensten
B 5.12	(7.10)	Exchange 2000 / Outlook 2000	M 2.247	(A)	Planung	Planung des Einsatzes von Exchange/Outlook 2000	G 2.7	Unerlaubte Ausübung von Rechte
							G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen
							G 2.55	Ungeordnete E-Mail-Nutzun
							G 2.95	Fehlendes Konzept zur Anbindung anderer E-Mail-Systeme an Exchange/Outloo
							G 5.23	Computer-Viren
			M 2.248	(A)	Planung	Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000	G 2.1	Fehlende oder unzureichende Regelunge
							G 2.2	Unzureichende Kenntnis über Regelunge
							G 2.7	Unerlaubte Ausübung von Rechte
			M 2.249	(B)	Planung	Planung der Migration von "Exchange 5.5-Servern" nach "Exchange 2000	G 2.91	Fehlerhafte Planung der Migration von Exchange 5.5 nach Exchange 200
			M 3.31	(A)	Umsetzg.	Schulung zur Systemarchitektur und Sicherheit von Exchange 2000 für Administratoren	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.38	Konfigurations- und Bedienungsfehle
							G 3.60	Fehlkonfiguration von Exchange 2000 Server
			M 3.32	(A)	Umsetzg.	Schulung zu Sicherheitsmechanismen von Outlook 2000 für Benutzer	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutze
							G 3.38	Konfigurations- und Bedienungsfehle
							G 3.61	Fehlerhafte Konfiguration von Outlook 2000 Client
			M 4.161	(A)	Umsetzg.	Sichere Installation von Exchange/Outlook 2000	G 3.9	Fehlerhafte Administration des IT-System
							G 3.60	Fehlkonfiguration von Exchange 2000 Server

							G 5.9	Unberechtigte IT-Nutzun
			M 4.162	(A)	Umsetzg.	Sichere Konfiguration von Exchange 2000 Servern	G 2.95	Fehlendes Konzept zur Anbindung anderer E-Mail-Systeme an Exchange/Outloo
							G 3.9	Fehlerhafte Administration des IT-System
							G 3.60	Fehlkonfiguration von Exchange 2000 Server
							G 5.9	Unberechtigte IT-Nutzun
			M 4.163	(A)	Umsetzg.	Zugriffsrechte auf Exchange 2000 Objekte	G 2.7	Unerlaubte Ausübung von Rechte
							G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechter
							G 3.60	Fehlkonfiguration von Exchange 2000 Server
			M 4.164	(A)	Umsetzg.	Browser-Zugriff auf Exchange 2000	G 2.92	Fehlerhafte Regelungen für den Browser-Zugriff auf Exchange
			M 4.165	(A)	Umsetzg.	Sichere Konfiguration von Outlook 2000	G 3.38	Konfigurations- und Bedienungsfehle
							G 3.61	Fehlerhafte Konfiguration von Outlook 2000 Client
							G 5.19	Missbrauch von Benutzerrechte
			M 4.166	(A)	Betrieb	Sicherer Betrieb von Exchange/Outlook 2000	G 1.2	Ausfall des IT-Systems
							G 3.9	Fehlerhafte Administration des IT-System
							G 4.22	Software-Schwachstellen oder -Fehle
			M 4.167	(B)	Betrieb	Überwachung und Protokollierung von Exchange 2000 Systemen	G 1.2	Ausfall des IT-Systems
							G 4.22	Software-Schwachstellen oder -Fehle
							G 5.9	Unberechtigte IT-Nutzun
			M 5.99	(C)	Umsetzg.	SSL/TLS-Absicherung für Exchange 2000	G 2.92	Fehlerhafte Regelungen für den Browser-Zugriff auf Exchange
							G 5.77	Mitlesen von E-Mails
							G 5.85	Integritätsverlust schützenswerter Information
			M 5.100	(Z)	Betrieb	Einsatz von Verschlüsselungs- und Signaturverfahren für die Exchange 2000 Kommunikation	G 5.77	Mitlesen von E-Mails
							G 5.83	Kompromittierung kryptographischer Schlüsse
							G 5.84	Gefälschte Zertifikate
							G 5.85	Integritätsverlust schützenswerter Information
			M 6.82	(C)	Notfallv.	Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen	G 1.2	Ausfall des IT-Systems
							G 3.60	Fehlkonfiguration von Exchange 2000 Server
							G 4.32	Nichtzustellung einer Nachricl