NIS2UmsuCG	NIS2 Requirement	IT-ACT No.	IT-ACT-Anforderung	ISO 27001	ISO Requirement
§30	**Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen**				
§30 (1) Satz 1	Maßnahmen basierend auf Risiko-Exposition und gesellschaftlichen und wirtschaftlichen Auswirkungen		Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die nach Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die	4.3	4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems
				A.5.4	A.5.4 Verantwortlichkeiten der Leitung
				A.5.29	A.5.29 Informationssicherheit bei Störungen
				A.5.30	A.5.30 IKT-Bereitschaft für Business Continuity
§30 (1) Satz 3	Dokumentation der NIS2 Risiko-Management Maßnahmen			6.1.3	6.1.3 Informationssicherheitsrisikobehandlung
				8.3	8.3 Informationssicherheitsrisikobehandlung
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
§30 (2) Nr. 1	**Konzepte für IT-Sicherheit (ISMS)**	**1**	**Richtlinie zur Sicherheit von Netzwerk- und Informationssystemen**	**Title**	
§30 (2) Nr. 1	Konzepte für IT-Sicherheit (ISMS)	1.1.1	Richtlinien zur Sicherheit von Netzwerk- und Informationssystemen, einschließlich Sicherheitsansatz, Strategie und Ziele, Risikotoleranz, Verpflichtungen, themenspezifische Richtlinien, formelle Genehmigung durch Leitungsgremien	A.5.1	A.5.1 Informationssicherheitsrichtlinien
				A.5.2	A.5.2 Informationssicherheitsrollen und -verantwortlichkeiten
				A.5.4	A.5.4 Verantwortlichkeiten der Leitung
§30 (2) Nr. 1	Konzepte für IT-Sicherheit (ISMS)	1.1.2	Überprüfen und aktualisieren Sie (durch die Leitungsgremien) das Netzwerk- und Informationssystem sowie weitere Richtlinien regelmäßig und nach bedeutenden Vorfällen und Änderungen.	6.2	6.2 Informationssicherheitsziele und Planung zu deren Erreichung
				9.3	9.3 Managementbewertung
				A.5.1	A.5.1 Informationssicherheitsrichtlinien
				A.5.2	A.5.2 Informationssicherheitsrollen und -verantwortlichkeiten
				A.5.4	A.5.4 Verantwortlichkeiten der Leitung
		1.2	**Rollen, Verantwortlichkeiten und Befugnisse**	**Title**	
§30 (2) Nr. 1	Konzepte für IT-Sicherheit (ISMS)	1.2.1	Definieren Sie Rollen, Verantwortlichkeiten und Befugnisse für die Netzwerk- und Informationssystemsicherheit und kommunizieren Sie	4.3	4.3 Festlegen des Anwendungsbereichs des
				A.5.3	A.5.3 Aufgabentrennung
				A.5.4	A.5.4 Verantwortlichkeiten der Leitung
§30 (2) Nr. 1	Konzepte für IT-Sicherheit (ISMS)	1.2.2	Fordern Sie von Mitarbeitern und Drittanbietern die Umsetzung von Sicherheitsrichtlinien	4.3	4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems
				A.5.3	A.5.3 Aufgabentrennung
				A.5.4	A.5.4 Verantwortlichkeiten der Leitung
				A.5.19	A.5.19 Informationssicherheit in Lieferantenbeziehungen
				A.5.20	A.5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen
				A.5.21	A.5.21 Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie(IKT)
				A.5.23	A.5.23 Informationssicherheit für die Nutzung von Cloud-Diensten
§30 (2) Nr. 1	Konzepte für IT-Sicherheit (ISMS)	1.2.3	Direkte Berichterstattung (CISO) an die Leitungsgremien zur Netzwerk- und Informationssystemsicherheit	9.3	9.3 Managementbewertung
§30 (2) Nr. 1	Konzepte für IT-Sicherheit (ISMS)	1.2.4	Dedizierte Rollen für die Netzwerk- und Informationssystemsicherheit	5.3	5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation
				A.5.3	A.5.3 Aufgabentrennung
				A.5.4	A.5.4 Verantwortlichkeiten der Leitung
§30 (2) Nr. 1	Konzepte für IT-Sicherheit (ISMS)	1.2.5	Trennung widersprüchlicher Aufgaben und Verantwortlichkeiten	A.5.3	A.5.3 Aufgabentrennung
§30 (2) Nr. 1	Konzepte für IT-Sicherheit (ISMS)	1.2.6	Überprüfen und aktualisieren Sie (durch die Leitungsgremien) Rollen, Verantwortlichkeiten und Befugnisse regelmäßig sowie nach bedeutenden Vorfällen und Änderungen.	5.3	5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation
§30 (2) Nr. 1	**Konzepte zur Risiko-Analyse (IT-RM)**	**2**	**Risikomanagementpolitik**	**Title**	
				Title	
		2.1	**Rahmen für das Risikomanagement**	**Title**	
§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	2.1.1	Angemessener Rahmen für das Risikomanagement zur Sicherheit von Netzwerk- und Informationssystemen mit Bewertungen, Behandlungsplänen und Akzeptanz durch das Management oder die Risikoeigentümer sowie Berichterstattung	6.1.1	6.1.1 Allgemeines
				6.1.2	6.1.2 Informationssicherheitsrisikobeurteilung
				6.1.3	6.1.3 Informationssicherheitsrisikobehandlung
				8.2	8.2 Informationssicherheitsrisikobeurteilung
				8.3	8.3 Informationssicherheitsrisikobehandlung
§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	2.1.2	Cybersecurity-Risikomanagementprozess als integraler Bestandteil des Gesamtrisikomanagements, mit Methoden, Werkzeugen, Kriterien, All-Hazards-Ansatz, Risikoeigentümern, Kriterien, Verantwortlichkeiten, Bewusstsein	6.1.1	6.1.1 Allgemeines
				8.2	8.2 Informationssicherheitsrisikobeurteilung
				8.3	8.3 Informationssicherheitsrisikobehandlung
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	2.1.3	Überprüfen und aktualisieren Sie die Ergebnisse der Risikobewertung und die Behandlungspläne regelmäßig oder nach bedeutenden Vorfällen und Änderungen.	6.1.1	6.1.1 Allgemeines
				8.2	8.2 Informationssicherheitsrisikobeurteilung
				8.3	8.3 Informationssicherheitsrisikobehandlung
				10.1	10.1 Fortlaufende Verbesserung
		2.2	**Compliance-Überwachung**	**Title**	
§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	2.2.1	Regelmäßige Überprüfung der Einhaltung von Richtlinien, Information der Leitungsgremien	A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
				A.5.36	A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	2.2.2	Compliance-Meldesystem zur effektiven Information der Leitungsorgane über Risiken	9.2	9.2 Internes Audit
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
				A.5.36	A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
				A.5.36	A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	2.2.3	Compliance-Prüfungen in regelmäßigen Abständen oder nach wesentlichen Vorfällen und Änderungen	9.2	9.2 Internes Audit
				A.5.36	A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
				A.8.34	A.8.34 Schutz der Informationssysteme während der Überwachungsprüfung
		2.3	**Unabhängige Überprüfung der Informations- und Netzwerksicherheit**	**Title**	
§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	2.3.1	Unabhängige Überprüfungen des Sicherheitsmanagements und der Implementierung von Netzwerk- und Informationssystemen	9.2	9.2 Internes Audit
				A.5.35	A.5.35 Unabhängige Überprüfung der Informationssicherheit
				A.5.36	A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
				A.8.34	A.8.34 Schutz der Informationssysteme während der Überwachungsprüfung
§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	2.3.2	Prozesse für unabhängige Prüfungen durch Personen mit Prüfungskompetenz und Unabhängigkeit	A.5.36	A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
				A.8.34	A.8.34 Schutz der Informationssysteme während der Überwachungsprüfung
§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	2.3.3	Berichterstattung an die Leitungsorgane über die Überwachung der Einhaltung der Vorschriften und über Korrekturmaßnahmen	A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
				A.5.36	A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	2.3.4	Unabhängige Überprüfungen in regelmäßigen Abständen oder nach wesentlichen Vorfällen und Änderungen	9.2	9.2 Internes Audit
				A.5.36	A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
				A.8.34	A.8.34 Schutz der Informationssysteme während der Überwachungsprüfung
§30 (2) Nr. 2	**Bewältigung von Sicherheitsvorfällen**	**3**	**Vorfallmanagement**	**Title**	
		3.1	**Richtlinie zur Vorfallbehandlung**	**Title**	
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.1.1	Richtlinie zur Vorfallbehandlung mit Rollen und Prozessen zur Erkennung, Analyse und Reaktion auf Vorfälle	A.5.24	A.5.24 Planung und Vorbereitung der Handhabung von Informations-sicherheitsvorfällen
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.1.2	Die in Punkt 3.1.1 genannte Strategie muss Folgendes umfassen: (a) ein Kategorisierungssystem für Vorfälle; (b) wirksame Kommunikationspläne,	A.6.8	A.6.8 Meldung von Informationssicherheitsereignissen
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.1.3	Überprüfung und Aktualisierung der Rollen und Prozesse der Richtlinie zur Vorfallbehandlung	A.5.24	A.5.24 Planung und Vorbereitung der Handhabung von Informations-sicherheitsvorfällen
				A.6.8	A.6.8 Meldung von Informationssicherheitsereignissen
				A.5.1	A.5.1 Informationssicherheitsrichtlinien
		3.2	**Überwachung und Protokollierung**	**Title**	
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.2.1	Verfahren und Werkzeuge zur Überwachung von Aktivitäten und zur Erkennung von Ereignissen	A.5.28	A.5.28 Sammeln von Beweismaterial
				A.6.8	A.6.8 Meldung von Informationssicherheitsereignissen
				A.8.15	A.8.15 Protokollierung
				A.8.16	A.8.16 Überwachung von Aktivitäten
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.2.2	Automatisiertes und kontinuierliches Monitoring, sofern möglich	A.5.28	A.5.28 Sammeln von Beweismaterial

				A.6.8	A.6.8 Meldung von Informationssicherheitsereignissen
				A.8.15	A.8.15 Protokollierung
				A.8.16	A.8.16 Überwachung von Aktivitäten
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.2.3	Dokumentation und Überprüfung von Protokollen, einschließlich vieler Details (vom Netzwerkverkehr bis zum Zugriff auf Einrichtungen)	A.8.15	A.8.15 Protokollierung
				A.8.16	A.8.16 Überwachung von Aktivitäten
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.2.4	Überprüfung der Protokolle anhand von Schwellenwerten und möglichen automatisierten Alarmen mit entsprechender Reaktion	A.5.28	A.5.28 Sammeln von Beweismaterial
				A.6.8	A.6.8 Meldung von Informationssicherheitsereignissen
				A.8.15	A.8.15 Protokollierung
				A.8.16	A.8.16 Überwachung von Aktivitäten
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.2.5	Zentrale Speicherung und Sicherung von Protokollen	A.8.9	A.8.9 Konfigurationsmanagement
				A.8.13	A.8.13 Sicherung von Information
				A.8.15	A.8.15 Protokollierung
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.2.6	Synchronisierte Zeitquellen auf Systemen und Liste der Protokollierungsressourcen	A.8.17	A.8.17 Uhrensynchronisation
				A.8.9	A.8.9 Konfigurationsmanagement
				A.8.15	A.8.15 Protokollierung
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.2.7	Regelmäßige Überprüfung der Protokollierungsverfahren und der Vermögensliste	9.1	9.1 Überwachung, Messung, Analyse und Bewertung
				A.5.36	A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
		3.3	**Ereignisberichterstattung**	**Title**	
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.3.1	Warnmeldemechanismus für Mitarbeiter, Lieferanten und Kunden	A.5.2	A.5.2 Informationssicherheitsrollen und -verantwortlichkeiten
				A.5.24	A.5.24 Planung und Vorbereitung der Handhabung von Informations-sicherheitsvorfällen
				A.5.25	A.5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse
				A.5.26	A.5.26 Reaktion auf Informationssicherheitsvorfälle
				A.6.8	A.6.8 Meldung von Informationssicherheitsereignissen
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.3.2	Kommunikation und Schulung des Warnmechanismus	A.5.24	A.5.24 Planung und Vorbereitung der Handhabung von Informations-sicherheitsvorfällen
				A.5.24	A.5.24 Planung und Vorbereitung der Handhabung von Informations-sicherheitsvorfällen
		3.4	**Ereignisbewertung und -klassifizierung**	**Title**	
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.4.1	Bewertung von Ereignissen zur Bestimmung der Art und Schwere von Vorfällen	A.5.25	A.5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.4.2	Bewertung von Ereignissen zur Bestimmung der Art und Schwere von Vorfällen	A.5.28	A.5.28 Sammeln von Beweismaterial
				A.6.8	A.6.8 Meldung von Informationssicherheitsereignissen
				A.8.15	A.8.15 Protokollierung
		3.5	**Reaktion auf Vorfälle**	**Title**	
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.5.1	Verfahren zur Reaktion auf Vorfälle	A.5.24	A.5.24 Planung und Vorbereitung der Handhabung von Informations-sicherheitsvorfällen
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.5.2	Die Verfahren zur Reaktion auf einen Vorfall müssen die folgenden Schritte umfassen: a) Eindämmung des Vorfalls, um eine Ausbreitung seiner Folgen zu verhindern; b) Beseitigung, um eine Fortsetzung oder ein erneutes Auftreten des Vorfalls zu verhindern; c) Wiederherstellung nach dem Vorfall, falls	A.5.25	A.5.25 Beurteilung und Entscheidung über
				A.5.26	A.5.26 Reaktion auf Informationssicherheitsvorfälle
				A.5.28	A.5.28 Sammeln von Beweismaterial
				A.6.8	A.6.8 Meldung von Informationssicherheitsereignissen
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.5.3	Kommunikationspläne mit CSIRT und Stakeholdern	A.5.24	A.5.24 Planung und Vorbereitung der Handhabung von Informations-sicherheitsvorfällen
				A.6.8	A.6.8 Meldung von Informationssicherheitsereignissen
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.5.4	Protokollierung und Prüfung von Vorfallaktivitäten und -verfahren	A.5.24	A.5.24 Planung und Vorbereitung der Handhabung von Informations-sicherheitsvorfällen
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.5.5	The relevant entities shall test at planned intervals their incident response procedures	A.5.28	A.5.28 Sammeln von Beweismaterial
				A.5.30	A.5.30 IKT-Bereitschaft für Business Continuity
		3.6	**Überprüfungen nach Vorfällen**	**Title**	
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.6.1	Überprüfungen nach Vorfällen, um die Grundursachen zu ermitteln und gewonnene Erkenntnisse zu gewinnen, um die Netzwerk- und IT-Sicherheit zu verbessern und Risiken zu reduzieren	A.5.26	A.5.26 Reaktion auf Informationssicherheitsvorfälle
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.6.2	Die betreffenden Stellen stellen sicher, dass die Überprüfungen nach Vorfällen dazu beitragen, ihren Ansatz zur Netz- und Informationssicherheit, zu Risikobehandlungsmaßnahmen und zu Verfahren zur Behandlung, Erkennung und Reaktion auf Vorfälle zu verbessern.	A.5.27	A.5.27 Erkenntnisse aus Informationssicherheitsvorfällen
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	3.6.3	Regelmäßige Überprüfungen, ob Überprüfungen nach Vorfällen durchgeführt wurden	A.5.26	A.5.26 Reaktion auf Informationssicherheitsvorfälle
§30 (2) Nr. 3	**Geschäftskontinuitäts- und Krisenmanagement**				
		4.1	**Geschäftskontinuitäts- und Krisenmanagement**	**Title**	
§30 (2) Nr. 3	Aufrechterhaltung Betrieb (BCM)	4.1.1	Auf Risikobewertungen basierender Geschäftskontinuitäts- und Notfallwiederherstellungsplan zur Verwendung für die Wiederherstellung	partial	
§30 (2) Nr. 3	Aufrechterhaltung Betrieb (BCM)	4.1.2	Der Betrieb der betreffenden Einheiten wird gemäß dem Geschäftskontinuitäts- und Notfallwiederherstellungsplan wiederhergestellt. Der Plan muss die Ergebnisse der Risikobewertung berücksichtigen und Folgendes umfassen: a) Zweck, Umfang und Zielgruppe; b) Rollen und Zuständigkeiten; c) wichtige	A.5.29	A.5.29 Informationssicherheit bei Störungen
				A.5.30	A.5.30 IKT-Bereitschaft für Business Continuity
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
§30 (2) Nr. 3	Aufrechterhaltung Betrieb (BCM)	4.1.3	Business Impact Analysis (BIA) zur Bewertung störender Auswirkungen und Festlegung der daraus resultierenden Kontinuitätsanforderungen	partial	
				A.5.29	A.5.29 Informationssicherheit bei Störungen
				A.5.30	A.5.30 IKT-Bereitschaft für Business Continuity
§30 (2) Nr. 3	Wiederherstellung nach Notfällen (DR und IT-SCM)	4.1.4	Test und Überprüfung der Geschäftskontinuität und Notfallwiederherstellung mit Updates und gewonnenen Erkenntnissen	partial	
				A.5.30	A.5.30 IKT-Bereitschaft für Business Continuity
		4.2	**Backup-Management (und Redundanz)**	**Title**	
§30 (2) Nr. 3	Backup-Management	4.2.1	Backups von Informationen mit ausreichenden Ressourcen, Einrichtungen und Personal	A.8.13	A.8.13 Sicherung von Information
				A.8.14	A.8.14 Redundanz von informationsverarbeitenden Einrichtungen
§30 (2) Nr. 3	Backup-Management	4.2.2	Auf Risikobewertung basierende Backup-Pläne und Geschäftskontinuitätspläne mit Zeit (RTO/RPO), Standorten, Zugriffskontrollen usw.	A.8.13	A.8.13 Sicherung von Information
				A.8.14	A.8.14 Redundanz von informationsverarbeitenden Einrichtungen
§30 (2) Nr. 3	Backup-Management	4.2.3	Regelmäßige Integritätsprüfungen von Backups	A.8.13	A.8.13 Sicherung von Information
				A.8.16	A.8.16 Überwachung von Aktivitäten
§30 (2) Nr. 3	Backup-Management	4.2.4	Mindestens teilweise Redundanz für NIS, Vermögenswerte und Einrichtungen, Personal, Kommunikation	A.8.14	A.8.14 Redundanz von informationsverarbeitenden Einrichtungen
§30 (2) Nr. 3	Backup-Management	4.2.5	Überwachung und Anpassung von Ressourcen unter Berücksichtigung von Backup- und Redundanzanforderungen	A.8.13	A.8.13 Sicherung von Information
				A.8.6	A.8.6 Kapazitätssteuerung
§30 (2) Nr. 3	Backup-Management	4.2.6	Regelmäßiges Testen von Backups und Redundanzen mit Dokumentation und Korrekturmaßnahmen	A.8.13	A.8.13 Sicherung von Information
		4.3	**Krisenmanagement**	**Title**	
§30 (2) Nr. 3	Krisenmanagement	4.3.1	Prozesse für das Krisenmanagement mit Rollen, Verantwortlichkeiten, Kommunikation und unterstützenden Ressourcen	-	
§30 (2) Nr. 3	Krisenmanagement	4.3.2	Die relevanten Stellen stellen sicher, dass die Krisenmanagementprozesse mindestens die folgenden Elemente abdecken: a) Rollen und Zuständigkeiten des Personals, wobei sicherzustellen ist, dass alle Mitarbeiter ihre Rollen in Krisensituationen kennen, einschließlich der zu befolgenden konkreten Schritte; b) geeignete Kommunikationsmittel zwischen den relevanten Stellen und den jeweils zuständigen Behörden; c) Anwendung geeigneter Kontrollen wie unterstützende Systeme, Prozesse und zusätzliche Kapazitäten. Für die Zwecke von Buchstabe b umfasst der Informationsfluss zwischen den relevanten Stellen und den jeweils zuständigen Behörden sowohl obligatorische Mitteilungen, wie Vorfallberichte und zugehörige Zeitpläne, als auch nicht obligatorische Mitteilungen.		
§30 (2) Nr. 3	Krisenmanagement	4.3.3	Verfahren zum Empfangen und Verwenden von Informationen von CSIRTs und Behörden sowie zu Vorfällen, Bedrohungen und Schwachstellen	A.5.5	A.5.5 Kontakt mit Behörden
				A.5.6	A.5.6 Kontakt mit speziellen Interessensgruppen
§30 (2) Nr. 3	Krisenmanagement	4.3.4	Regelmäßige Prüfung und Überprüfung des Krisenmanagementplans	-	
§30 (2) Nr. 4	**Sicherheit der Lieferkette**	**5**	**Sicherheit der Lieferkette**	**Title**	
		5.1	**Richtlinie zur Lieferkettensicherheit**	**Title**	
§30 (2) Nr. 4	Sicherheit der Lieferkette	5.1.1	Sicherheitsrichtlinien für die Lieferkette zur Steuerung von Lieferanten und	A.5.19	A.5.19 Informationssicherheit in Lieferantenbeziehungen

			Dienstleistern und zur Minderung von Risiken für NIS	A.5.21	A.5.21 Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie(IKT)
§30 (2) Nr. 4	Sicherheit der Lieferkette	5.1.2	Festlegung von Kriterien für die Auswahl und Beauftragung von Lieferanten auf Grundlage von Cybersicherheitspraktiken, Fähigkeiten, Belastbarkeit und Lieferantenbindung der Lieferanten	A.5.19	A.5.19 Informationssicherheit in Lieferantenbeziehungen
§30 (2) Nr. 4	Sicherheit der Lieferkette	5.1.3	Berücksichtigung koordinierter Sicherheitsrisikobewertungen kritischer Lieferketten (NIS2)	A.5.21	A.5.21 Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie(IKT)
§30 (2) Nr. 4	Sicherheit der Lieferkette	5.1.4	Auf der Grundlage der Sicherheitspolitik für die Lieferkette und unter Berücksichtigung der Ergebnisse der gemäß Nummer 2.1 dieses Anhangs durchgeführten Risikobewertung stellen die relevanten Stellen sicher, dass in ihren Verträgen mit den Lieferanten und Dienstleistern – gegebenenfalls in Dienstgütevereinbarungen – Folgendes festgelegt ist: a) Cybersicherheitsanforderungen an die Lieferanten oder Dienstleister, einschließlich Anforderungen in Bezug auf die Sicherheit beim Erwerb von IKT-Diensten oder IKT-Produkten gemäß Nummer 6.1; b) Anforderungen in Bezug auf Fähigkeiten und Schulungen sowie gegebenenfalls Zertifizierungen, die von den Mitarbeitern der Lieferanten oder Dienstleister verlangt werden; c) Anforderungen in Bezug auf Hintergrundüberprüfungen der Mitarbeiter der Lieferanten und Dienstleister gemäß Nummer 10.2; d) eine Verpflichtung der Lieferanten und Dienstleister, die relevanten Stellen unverzüglich über Vorfälle zu informieren, die ein Risiko für die Sicherheit der Netz- und Informationssysteme dieser Stellen darstellen; e) Bestimmungen zu Reparaturzeiten; f) das Recht auf Prüfungen oder das Recht auf Erhalt von Prüfberichten; DE 10 DE g) eine Verpflichtung der Lieferanten und Dienstleister, Schwachstellen zu beheben, die ein Risiko für die Sicherheit der Netz- und Informationssysteme der betreffenden Stellen darstellen; h) Anforderungen an die Untervergabe von Unteraufträgen und – sofern die betreffenden Stellen die Untervergabe von Unteraufträgen zulassen – Cybersicherheitsanforderungen für Unterauftragnehmer im Einklang mit den unter Buchstabe a genannten Cybersicherheitsanforderungen; i) Verpflichtungen der Lieferanten und Dienstleister bei Beendigung des Vertrags, beispielsweise in Bezug auf den Abruf und die Vernichtung der von	A.5.19 A.5.20 A.5.21 A.5.22 A.5.23	A.5.19 Informationssicherheit in Lieferantenbeziehungen A.5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen A.5.21 Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie(IKT) A.5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A.5.23 Informationssicherheit für die Nutzung von Cloud-Diensten
§30 (2) Nr. 4	Sicherheit der Lieferkette	5.1.5	Auswahl neuer Anbieter anhand von Kriterien (5.1.2) und Risikobewertungen (5.1.3)	A.5.20 A.5.19	A.5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen A.5.19 Informationssicherheit in Lieferantenbeziehungen
§30 (2) Nr. 4	Sicherheit der Lieferkette	5.1.6	Überprüfen Sie die Lieferkettenrichtlinien und überwachen und bewerten Sie Lieferanten und deren Einhaltung	A.5.1 A.5.22	A.5.1 Informationssicherheitsrichtlinien A.5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
§30 (2) Nr. 4	Sicherheit der Lieferkette	5.1.7	Zur Anbieterauswahl überwachen Sie SLA-Berichte, überprüfen Vorfälle, planen und bewerten Audits und analysieren Änderungsrisiken	A.5.22	A.5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
§30 (2) Nr. 4	Sicherheitsaspekte zu Anbietern und Dienstleistern	5.2	Lieferanten- und Dienstleisterverzeichnis mit Anlaufstellen und Auflistung der ICT-Produkte, -Dienste etc.	A.5.21	A.5.21 Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie(IKT)
§30 (2) Nr. 5	**Sicherheit beim Einkauf von IT**	**6**	**Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netzwerk- und**	**Title**	
		6.1	**Sicherheit beim Erwerb von IKT-Dienstleistungen oder IKT-Produkten**	**Title**	
§30 (2) Nr. 5	Sicherheit beim Einkauf von IT	6.1.1	Prozesse zur Verwaltung von Risiken bei der Beschaffung von IKT-Diensten und -Produkten, die kritisch sind	A.5.19 A.5.20 A.5.22 A.5.23 A.8.30	A.5.19 Informationssicherheit in Lieferantenbeziehungen A.5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen A.5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A.5.23 Informationssicherheit für die Nutzung von Cloud-Diensten A.8.30 Ausgegliederte Entwicklung
§30 (2) Nr. 5	Sicherheit beim Einkauf von IT	6.1.2	Sicherheitsanforderungen, Updates, Informationen zu Cybersicherheitsfunktionen, Compliance und Validierung	A.5.19 A.5.20 A.5.22 A.5.23 A.8.30	A.5.19 Informationssicherheit in Lieferantenbeziehungen A.5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen A.5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A.5.23 Informationssicherheit für die Nutzung von Cloud-Diensten A.8.30 Ausgegliederte Entwicklung
§30 (2) Nr. 5	Sicherheit beim Einkauf von IT	6.1.3	Überprüfen und aktualisieren Sie die Prozesse für die Akquisition regelmäßig	A.5.19 A.5.20 A.5.22 A.5.23 A.8.30 A.5.1	A.5.19 Informationssicherheit in Lieferantenbeziehungen A.5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen A.5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen A.5.23 Informationssicherheit für die Nutzung von Cloud-Diensten A.8.30 Ausgegliederte Entwicklung A.5.1 Informationssicherheitsrichtlinien
		6.2	**Sicherer Entwicklungslebenszyklus (SDLC)**	**Title**	
§30 (2) Nr. 5	Sicherheit bei der Entwicklung von IT	6.2.1	Regeln zur sicheren Entwicklung von Netzwerk- und Informationssystemen für alle Entwicklungsphasen	A.5.8 A.8.25 A.8.26 A.8.27 A.8.28	A.5.8 Informationssicherheit im Projektmanagement A.8.25 Lebenszyklus einer sicheren Entwicklung A.8.26 Anforderungen an die Anwendungssicherheit A.8.27 Sichere Systemarchitektur und technische Grundsätze A.8.28 Sichere Kodierung
§30 (2) Nr. 5	Sicherheit bei der Entwicklung von IT	6.2.2	Analyse von Sicherheitsanforderungen, Grundsätze für sicheres Engineering, sichere Entwicklungsumgebungen, Sicherheitstests, Daten	A.8.25 A.5.8 A.8.33	A.8.25 Lebenszyklus einer sicheren Entwicklung A.5.8 Informationssicherheit im Projektmanagement A.8.33 Informationen zur Prüfung
§30 (2) Nr. 5	Sicherheit bei der Entwicklung von IT	6.2.3	Berücksichtigen Sie Sicherheitsaspekte und Lieferkettensicherheit bei der ausgelagerten Entwicklung	A.5.8 A.8.29 A.8.30	A.5.8 Informationssicherheit im Projektmanagement A.8.29 Sicherheitsprüfung in Entwicklung und Abnahme A.8.30 Ausgegliederte Entwicklung
§30 (2) Nr. 5	Sicherheit bei der Entwicklung von IT	6.2.4	Überprüfen und aktualisieren Sie die Prozesse für eine sichere Entwicklung regelmäßig	A.8.29 A.8.30 A.5.1	A.8.29 Sicherheitsprüfung in Entwicklung und Abnahme A.8.30 Ausgegliederte Entwicklung A.5.1 Informationssicherheitsrichtlinien
		6.3	**Konfigurationsverwaltung**	**Title**	
§30 (2) Nr. 5	Sicherheit bei der Wartung von IT	6.3.1	Dokumentieren, implementieren und überwachen Sie Konfigurationen, einschließlich sicherer Konfigurationen	A.7.13 A.8.9	A.7.13 Instandhalten von Geräten und Betriebsmitteln A.8.9 Konfigurationsmanagement
§30 (2) Nr. 5	Sicherheit bei der Wartung von IT	6.3.2	Definieren Sie Sicherheitskonfigurationen und -prozesse, um sichere Konfigurationen für neue Systeme und während des Betriebs durchzusetzen	8.1 A.8.9 A.8.19 A.8.31 A.8.32	8.1 Betriebliche Planung und Steuerung A.8.9 Konfigurationsmanagement A.8.19 Installation von Software auf Systemen im Betrieb A.8.31 Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen A.8.32 Änderungssteuerung
§30 (2) Nr. 5	Sicherheit bei der Wartung von IT	6.3.3	Überprüfen und aktualisieren Sie Konfigurationen regelmäßig und nach bedeutenden Vorfällen oder Änderungen	A.8.9	A.8.9 Konfigurationsmanagement
		6.4	**Änderungsmanagement, Reparaturen und Wartung**	**Title**	
§30 (2) Nr. 5	Sicherheit bei der Wartung von IT	6.4.1	Managementverfahren für Änderungen, Wartung von Netzwerk- und Informationssystemen	8.1 A.8.31 A.8.32 A.7.13	8.1 Betriebliche Planung und Steuerung A.8.31 Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen A.8.32 Änderungssteuerung A.7.13 Instandhalten von Geräten und Betriebsmitteln
§30 (2) Nr. 5	Sicherheit bei der Wartung von IT	6.4.2	Anwendung von Verfahren auf Releases, Modifikationen und Notfalländerungen von Software, Hardware und Konfiguration	8.1 A.8.9 A.8.32 A.8.33 A.8.32 A.8.32	8.1 Betriebliche Planung und Steuerung A.8.9 Konfigurationsmanagement A.8.32 Änderungssteuerung A.8.33 Informationen zur Prüfung A.8.32 Änderungssteuerung A.8.32 Änderungssteuerung
§30 (2) Nr. 5	Sicherheit bei der Wartung von IT	6.4.3	Dringende Änderungen mit Erklärungen dokumentiert	A.8.32	A.8.32 Änderungssteuerung
§30 (2) Nr. 5	Sicherheit bei der Wartung von IT	6.4.4	Überprüfen und aktualisieren Sie Änderungsverfahren regelmäßig und nach bedeutenden Vorfällen oder Änderungen.	8.1 A.8.31 A.8.32 A.5.1	8.1 Betriebliche Planung und Steuerung A.8.31 Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen A.8.32 Änderungssteuerung A.5.1 Informationssicherheitsrichtlinien
		6.5	**Sicherheitstests**	**Title**	
§30 (2) Nr. 5	Management und Offenlegung von Schwachstellen	6.5.1	Richtlinien und Prozesse für Sicherheitstests	A.8.8	A.8.8 Handhabung von technischen Schwachstellen

				A.8.34	A.8.34 Schutz der Informationssysteme während der Überwachungsprüfung
§30 (2) Nr. 5	Management und Offenlegung von Schwachstellen	6.5.2	Risikobasierte Anforderungen für Sicherheitstests, die nach etablierter Methodik durchgeführt werden, mit Dokumentation der Ergebnisse und Minderungsmaßnahmen	A.8.29	A.8.29 Sicherheitsprüfung in Entwicklung und Abnahme
				A.8.33	A.8.33 Informationen zur Prüfung
				A.8.34	A.8.34 Schutz der Informationssysteme während der Überwachungsprüfung
§30 (2) Nr. 5	Management und Offenlegung von Schwachstellen	6.5.3	Überprüfen und aktualisieren Sie regelmäßig die Richtlinien und Prozesse für Sicherheitstests	9.1	9.1 Überwachung, Messung, Analyse und Bewertung
				A.8.8	A.8.8 Handhabung von technischen Schwachstellen
				A.8.34	A.8.34 Schutz der Informationssysteme während der Überwachungsprüfung
		6.6	**Sicherheitspatch-Verwaltung**	**Title**	
§30 (2) Nr. 5	Management und Offenlegung von Schwachstellen	6.6.1	Prozesse zur Verwaltung von Sicherheitspatches mit Zeitrahmen, Tests, vertrauenswürdigen Quellen und Ausnahmebehandlung	A.8.19	A.8.19 Installation von Software auf Systemen im Betrieb
				A.8.8	A.8.8 Handhabung von technischen Schwachstellen
				A.5.7	A.5.7 Erkenntnisse über Bedrohungen
				A.8.32	A.8.32 Änderungssteuerung
§30 (2) Nr. 5	Management und Offenlegung von Schwachstellen	6.6.2	Ausnahmen von Sicherheitspatches sind zulässig, wenn die Nachteile die Vorteile überwiegen und die Gründe dafür begründet und dokumentiert sind.	A.8.8	A.8.8 Handhabung von technischen Schwachstellen
		6.7	**Netzwerksicherheit**	**Title**	
		6.7.1	Maßnahmen zum Schutz von Netzwerken und Informationssystemen vor Cyberbedrohungen	A.8.20	A.8.20 Netzwerksicherheit
				A.8.21	A.8.21 Sicherheit von Netzwerkdiensten
				A.8.23	A.8.23 Webfilterung
				A.8.26	A.8.26 Anforderungen an die Anwendungssicherheit
		6.7.2	Dokumentation der Netzwerkarchitektur, Netzwerkzugriffskontrollen, sichere Konfiguration und Fernzugriff, sichere Verbindungen, vertrauenswürdige Kanäle und moderne (neueste) und sichere Technologien	A.8.20	A.8.20 Netzwerksicherheit
				A.8.20	A.8.20 Netzwerksicherheit
				A.8.21	A.8.21 Sicherheit von Netzwerkdiensten
				A.8.22	A.8.22 Trennung von Netzwerken
		6.7.3	Überprüfen und aktualisieren Sie Sicherheitsmaßnahmen regelmäßig und nach bedeutenden Vorfällen oder Änderungen	6.1.3	6.1.3 Informationssicherheitsrisikobehandlung
				8.3	8.3 Informationssicherheitsrisikobehandlung
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
		6.8	**Netzwerksegmentierung**	**Title**	
		6.8.1	Segmentierung der Systeme in Netzwerke oder Zonen auf Basis des Risikos, getrennt von Systemen von Drittanbietern	A.8.22	A.8.22 Trennung von Netzwerken
				A.8.26	A.8.26 Anforderungen an die Anwendungssicherheit
				A.8.20	A.8.20 Netzwerksicherheit
		6.8.2	Sicherheitsanforderungen für Netzwerksegmentierungen, einschließlich Beziehungen, Maßnahmen, Zugriffsanforderungen und -kontrolle, Verwaltung und Entwicklung usw.	A.8.22	A.8.22 Trennung von Netzwerken
				A.8.26	A.8.26 Anforderungen an die Anwendungssicherheit
				A.8.27	A.8.27 Sichere Systemarchitektur und technische Grundsätze
				A.8.31	A.8.31 Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen
				A.8.20	A.8.20 Netzwerksicherheit
		6.8.3	Überprüfen und aktualisieren Sie die Netzwerksegmentierung regelmäßig und nach bedeutenden Vorfällen oder Änderungen.	A.8.22	A.8.22 Trennung von Netzwerken
				9.1	9.1 Überwachung, Messung, Analyse und Bewertung
				10.1	10.1 Fortlaufende Verbesserung
		6.9	**Schutz vor Schadsoftware und nicht autorisierter Software**	**Title**	
		6.9.1	Schutz von Netzwerk- und Informationssystemen vor bösartiger und nicht autorisierter Software	A.8.7	A.8.7 Schutz gegen Schadsoftware
				A.8.23	A.8.23 Webfilterung
		6.9.2	Regelmäßig aktualisierte Software zur Malware-Erkennung und -Reparatur	A.8.7	A.8.7 Schutz gegen Schadsoftware
		6.10	**Umgang mit Schwachstellen und Offenlegung**	**Title**	
§30 (2) Nr. 5	Management und Offenlegung von Schwachstellen	6.10.1	Sammlung und Analyse von Informationen zu Schwachstellen und zur eigenen Gefährdung	A.8.8	A.8.8 Handhabung von technischen Schwachstellen
				A.5.7	A.5.7 Erkenntnisse über Bedrohungen
§30 (2) Nr. 5	Management und Offenlegung von Schwachstellen	6.10.2	Ankündigungen von CSIRTs und Behörden überwachen, Scans durchführen, Schwachstellen beheben, Verfahren definieren und Umsetzung sicherstellen	A.8.8	A.8.8 Handhabung von technischen Schwachstellen
				A.5.5	A.5.5 Kontakt mit Behörden
				A.5.6	A.5.6 Kontakt mit speziellen Interessensgruppen
				A.5.7	A.5.7 Erkenntnisse über Bedrohungen
§30 (2) Nr. 5	Management und Offenlegung von Schwachstellen	6.10.3	Implementieren Sie einen Plan zum Umgang mit Schwachstellen basierend auf deren Auswirkung und dokumentieren Sie Ausnahmen und Gründe.	A.8.8	A.8.8 Handhabung von technischen Schwachstellen
				A.8.19	A.8.19 Installation von Software auf Systemen im Betrieb
§30 (2) Nr. 5	Management und Offenlegung von Schwachstellen	6.10.4	Überprüfen und aktualisieren Sie regelmäßig die Informationskanäle zu Sicherheitslücken	9.1	9.1 Überwachung, Messung, Analyse und Bewertung
				10.1	10.1 Fortlaufende Verbesserung
				A.8.8	A.8.8 Handhabung von technischen Schwachstellen
		7	**Richtlinien und Verfahren zur Bewertung der Wirksamkeit von Maßnahmen zum Risikomanagement im Bereich Cybersicherheit**	**Title**	
				Title	
§30 (2) Nr. 6	Bewertung der Wirksamkeit von Maßnahmen	7.1.1	Implementieren Sie Richtlinien und Prozesse, um die Umsetzung und Wirksamkeit von Richtlinien zu bewerten	9.1	9.1 Überwachung, Messung, Analyse und Bewertung
				9.2	9.2 Internes Audit
				A.5.36	A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
				A.8.34	A.8.34 Schutz der Informationssysteme während der Überwachungsprüfung
§30 (2) Nr. 6	Bewertung der Wirksamkeit von Maßnahmen	7.1.2	Prozess, Sicherheitsbewertungen und Sicherheitstests von Cybersicherheitsmaßnahmen mit Methoden, Definitionen und Verantwortlichkeiten	9.2	9.2 Internes Audit
				A.5.36	A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
				A.8.34	A.8.34 Schutz der Informationssysteme während der Überwachungsprüfung
§30 (2) Nr. 6	Bewertung der Wirksamkeit von Maßnahmen	7.1.3	Überprüfen und aktualisieren Sie Bewertungsrichtlinien und -prozesse regelmäßig oder nach bedeutenden Vorfällen und Änderungen.	9.3	9.3 Managementbewertung
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
				A.5.36	A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
§30 (2) Nr. 7	**Cyberhygiene und Awareness**	**8.**	**Grundlegende Cyberhygienepraktiken und Sicherheitsschulungen**	**Title**	
				Title	
		8.1	**Sensibilisierung und grundlegende Praktiken der Cyberhygiene**	**Title**	
§30 (2) Nr. 7	Cyberhygiene und Awareness	8.1.1	Bewusstsein der Mitarbeiter für Risiken, Bedeutung der Cybersicherheit und Cyberhygiene	7.3	7.3 Bewusstsein
				A.6.3	A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung
				A.7.7	A.7.7 Aufgeräumte Arbeitsumgebung und Bildschirmsperren
§30 (2) Nr. 7	Cyberhygiene und Awareness	8.1.2	Programm zur Sensibilisierung der Mitarbeiter und des Managements für Sicherheit, wiederkehrende Termine, im Einklang mit Richtlinien, die	7.3	7.3 Bewusstsein
				A.6.3	A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung
§30 (2) Nr. 7	Cyberhygiene und Awareness	8.1.3	Regelmäßiges Testen und Aktualisieren des Sensibilisierungsprogramms unter Berücksichtigung von Änderungen der Bedrohungslandschaft, der Risiken und	7.3	7.3 Bewusstsein
				A.6.3	A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung
		8.2	**Sicherheitstraining**	**Title**	
§30 (2) Nr. 7	Schulungen Informationssicherheit	8.2.1	Schulung zur Netzwerk- und Informationssystemsicherheit für Mitarbeiter	7.2	7.2 Kompetenz
				A.6.3	A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung
§30 (2) Nr. 7	Schulungen Informationssicherheit	8.2.2	Schulungsprogramm basierend auf Richtlinien, spezifischen Sicherheitsthemen und -verfahren, basierend auf Rollen- und	7.2	7.2 Kompetenz
				A.6.3	A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung
§30 (2) Nr. 7	Schulungen Informationssicherheit	8.2.3	Bewertung der Wirksamkeit von Schulungen und ihrer Relevanz in Bezug auf sichere Konfiguration und Betrieb, Cyberbedrohungen und Verhalten	9.1	9.1 Überwachung, Messung, Analyse und Bewertung
§30 (2) Nr. 7	Schulungen Informationssicherheit	8.2.4	Schulung für Mitarbeiter, die ihren Arbeitsplatz wechseln	A.6.5	A.6.5 Verantwortlichkeiten nach Beendigung oder Änderung der Beschäftigung
§30 (2) Nr. 7	Schulungen Informationssicherheit	8.2.5	Aktualisieren Sie das Sicherheitsschulungsprogramm basierend auf Richtlinien, Regeln, Rollen, Bedrohungen und Technologien	7.2	7.2 Kompetenz
				A.6.3	A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung
				A.5.1	A.5.1 Informationssicherheitsrichtlinien
§30 (2) Nr. 8	**Kryptografie und Verschlüsselung**	**9.**	**Kryptographie**	**Title**	
				Title	
§30 (2) Nr. 8	Kryptografie und Verschlüsselung	9.1.1	Richtlinien und Verfahren für Kryptographie zum Schutz von Informationen (C/I/A)	A.5.1	A.5.1 Informationssicherheitsrichtlinien
				A.8.24	A.8.24 Verwendung von Kryptographie
§30 (2) Nr. 8	Kryptografie und Verschlüsselung	9.1.2	Die Richtlinie definiert kryptografische Maßnahmen basierend auf Klassifizierung, Kryptoprotokollen, Algorithmen, Chiffren, Schlüssellängen, Schlüsselverwaltung usw.	A.5.14	A.5.14 Informationsübertragung
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
				A.8.20	A.8.20 Netzwerksicherheit
				A.8.21	A.8.21 Sicherheit von Netzwerkdiensten
				A.8.24	A.8.24 Verwendung von Kryptographie
				A.8.33	A.8.33 Informationen zur Prüfung
§30 (2) Nr. 8	Kryptografie und Verschlüsselung	9.1.3	Überprüfen und aktualisieren Sie regelmäßig die Kryptographierichtlinien und -prozesse und überwachen Sie den neuesten Stand der Kryptotechnik.	A.5.1	A.5.1 Informationssicherheitsrichtlinien
				A.8.24	A.8.24 Verwendung von Kryptographie
§30 (2) Nr. 9	**Personalsicherheit (HR-Security)**	**10**	**Personalsicherheit**	**Title**	
		10.1	**Personalsicherheit**	**Title**	
§30 (2) Nr. 9	Personalsicherheit (HR-Security)	10.1.1	Stellen Sie sicher, dass Mitarbeiter und Dritte ihre Sicherheitsverantwortung im Einklang mit den Richtlinien wahrnehmen	A.6.2	A.6.2 Beschäftigungs- und Vertragsbedingungen
				A.6.6	A.6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

§30 (2) Nr. 9	Personalsicherheit (HR-Security)	10.1.2	Prozesse, um sicherzustellen, dass Mitarbeiter und Dritte die Cyberhygiene einhalten, Rollen und Verantwortlichkeiten, einschließlich Managementorganen usw., einhalten.	A.6.3	A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung
				7.2	7.2 Kompetenz
				7.3	7.3 Bewusstsein
§30 (2) Nr. 9	Personalsicherheit (HR-Security)	10.1.3	Überprüfen Sie die zugewiesenen Rollen und den Ressourceneinsatz regelmäßig und aktualisieren Sie diese bei Bedarf.	5.3	5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation
				7.1	7.1 Ressourcen
		10.2	**Hintergrundüberprüfungen**	**Title**	
§30 (2) Nr. 9	Personalsicherheit (HR-Security)	10.2.1	Hintergrundüberprüfungen von Mitarbeitern und Dritten, falls dies für ihre Rolle erforderlich ist, Genehmigungen	A.6.1	A.6.1 Sicherheitsüberprüfung
				A.5.20	A.5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen
§30 (2) Nr. 9	Personalsicherheit (HR-Security)	10.2.2	Kriterien für Hintergrundüberprüfungen, nur autorisierte Personen, Überprüfungen vor der Rollenzuweisung, basierend auf Gesetzen und Vorschriften	A.6.1	A.6.1 Sicherheitsüberprüfung
§30 (2) Nr. 9	Personalsicherheit (HR-Security)	10.2.3	Überprüfen und aktualisieren Sie die Richtlinien zur Hintergrundüberprüfung regelmäßig	A.5.1	A.5.1 Informationssicherheitsrichtlinien
				A.5.20	A.5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen
		10.3	**Beendigung oder Änderung des Beschäftigungsverfahrens**	**Title**	
§30 (2) Nr. 9	Personalsicherheit (HR-Security)	10.3.1	Verantwortlichkeiten und Pflichten, die nach der Kündigung oder Änderung gültig sind, werden kommuniziert und verstanden	A.6.5	A.6.5 Verantwortlichkeiten nach Beendigung oder Änderung der Beschäftigung
§30 (2) Nr. 9	Personalsicherheit (HR-Security)	10.3.2	Verantwortlichkeiten (wie Vertraulichkeit) werden in Verträgen festgelegt, Zugangskontrollrichtlinien sorgen für die Einhaltung, Änderungsprozesse	A.5.8	A.5.8 Informationssicherheit im Projektmanagement
				A.5.14	A.5.14 Informationsübertragung
				A.6.2	A.6.2 Beschäftigungs- und Vertragsbedingungen
				A.6.6	A.6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen
		10.4	**Disziplinarverfahren**	**Title**	
§30 (2) Nr. 9	Personalsicherheit (HR-Security)	10.4.1	Disziplinarverfahren zur Behandlung von Verstößen gegen Netzwerk- und Informationssysteme	A.6.4	A.6.4 Maßregelungsprozess
§30 (2) Nr. 9	Personalsicherheit (HR-Security)	10.4.2	Regelmäßige Überprüfung und Aktualisierung des Disziplinarverfahrens oder aufgrund rechtlicher oder betrieblicher Änderungen	A.6.4	A.6.4 Maßregelungsprozess
				A.5.1	A.5.1 Informationssicherheitsrichtlinien
§30 (2) Nr. 9	**Konzepte für Zugriffskontrolle**	**11.**	**Zutrittskontrolle**	**Title**	
		11.1	**Zugriffskontrollrichtlinie**	**Title**	
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.1.1	Zugriffskontrollrichtlinie für die logische und physische Zugriffskontrolle auf Netzwerk- und Informationssysteme	A.5.15	A.5.15 Zugangssteuerung
				A.8.3	A.8.3 Informationszugangsbeschränkung
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.1.2	Die Zugriffskontrollrichtlinie umfasst den Zugriff von Mitarbeitern und externen Personen (Lieferanten, Anbieter) sowie den Zugriff durch Prozesse, der nur nach Authentifizierung gewährt wird.	A.5.15	A.5.15 Zugangssteuerung
				A.5.19	A.5.19 Informationssicherheit in Lieferantenbeziehungen
				A.5.20	A.5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen
				A.5.21	A.5.21 Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie(IKT)
				A.5.23	A.5.23 Informationssicherheit für die Nutzung von Cloud-Diensten
				A.8.3	A.8.3 Informationszugangsbeschränkung
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.1.3	Überprüfen und aktualisieren Sie die Zugriffskontrollrichtlinien regelmäßig und nach bedeutenden Vorfällen oder Änderungen.	A.5.1	A.5.1 Informationssicherheitsrichtlinien
		11.2	**Verwaltung von Zugriffsrechten**	**Title**	
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.2.1	Verwalten Sie Zugriffsrechte entsprechend der Zugriffskontrollrichtlinie	A.5.18	A.5.18 Zugangsrechte
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.2.2	Zugriffsrechte basierend auf Need-to-know, geringsten Privilegien, Aufgabentrennung, ordnungsgemäßer Autorisierung, einschließlich Zugriff und Änderungen durch Dritte usw.	A.5.3	A.5.3 Aufgabentrennung
				A.5.18	A.5.18 Zugangsrechte
				A.8.3	A.8.3 Informationszugangsbeschränkung
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.2.3	Zugriffsrechte regelmäßig prüfen und bei organisatorischen Änderungen aktualisieren; Dokumentprüfung	9.1	
				A.5.18	A.5.18 Zugangsrechte
		11.3	**Privilegierte Konten und Systemadministrationskonten**	**Title**	
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.3.1	Richtlinien für die Verwaltung privilegierter und administrativer Konten	A.5.3	A.5.3 Aufgabentrennung
				A.5.18	A.5.18 Zugangsrechte
				A.8.2	A.8.2 Privilegierte Zugangsrechte
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.3.2	Implementierung starker Authentifizierung, MFA und Verfahren; spezifische Konten für Verwaltungen; individuelle Berechtigungen	A.5.3	A.5.3 Aufgabentrennung
				A.5.18	A.5.18 Zugangsrechte
				A.8.2	A.8.2 Privilegierte Zugangsrechte
				A.8.5	A.8.5 Sichere Authentifizierung
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.3.3	Überprüfen Sie privilegierte Konten regelmäßig und aktualisieren Sie sie auf der Grundlage organisatorischer Änderungen; überprüfen Sie die Dokumente	A.5.3	A.5.3 Aufgabentrennung
				A.5.18	A.5.18 Zugangsrechte
				A.8.2	A.8.2 Privilegierte Zugangsrechte
		11.4	**Verwaltungssysteme**	**Title**	
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.4.1	Kontrollieren Sie die Verwendung von Systemverwaltungssystemen	A.8.18	A.8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten
				A.8.19	A.8.19 Installation von Software auf Systemen im Betrieb
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.4.2	Separates und verwaltungsspezifisches System, besonders gesichert	A.8.22	A.8.22 Trennung von Netzwerken
				partial	
		11.5	**Identifikation**	**Title**	
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.5.1	Vollständiges Lebenszyklusmanagement der Identitäten von Netzwerk- und Informationssystemen sowie Benutzern	A.5.16	A.5.16 Identitätsmanagement
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.5.2	Eindeutige Identitäten für Systeme und Benutzer; mit Überwachung und Protokollierung	A.5.3	A.5.3 Aufgabentrennung
				A.5.16	A.5.16 Identitätsmanagement
				A.8.3	A.8.3 Informationszugangsbeschränkung
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.5.3	Gemeinsame Identitäten nur in Sonderfällen, wenn nötig und mit ausdrücklicher Genehmigung und Dokumentation	A.5.16	A.5.16 Identitätsmanagement
				A.5.17	A.5.17 Informationen zur Authentifizierung
				A.5.18	A.5.18 Zugangsrechte
		11.6	**Authentifizierung**	**Title**	
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.6.1	Sichere Authentifizierungsverfahren und -technologien basierend auf Zugriffskontrolle und Richtlinien	A.5.17	A.5.17 Informationen zur Authentifizierung
				A.8.5	A.8.5 Sichere Authentifizierung
				A.8.24	A.8.24 Verwendung von Kryptographie
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.6.2	Starke Authentifizierung, kontrollierter Authentifizierungsprozess, Erständerungen, Reset und Beendigung	A.5.17	A.5.17 Informationen zur Authentifizierung
				A.8.5	A.8.5 Sichere Authentifizierung
				A.8.24	A.8.24 Verwendung von Kryptographie
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.6.3	Modernste Authentifizierungsmethoden basierend auf Risiko und Klassifizierung	A.8.5	A.8.5 Sichere Authentifizierung
				A.8.24	A.8.24 Verwendung von Kryptographie
§30 (2) Nr. 9	Konzepte für Zugriffskontrolle	11.6.4	Identitäten regelmäßig prüfen und bei Nichtbedarf deaktivieren	A.5.16	A.5.16 Identitätsmanagement
		11.7	**Multi-Faktor-Authentifizierung**	**Title**	
§30 (2) Nr. 10	Multi-Faktor-Authentifizierung (MFA) und kontinuierliche Authentifizierung (SSO)	11.7.1	Mehrstufige oder kontinuierliche Authentifizierung (SSO) für den Zugriff auf Netzwerk- und Informationssysteme basierend auf der Systemklassifizierung	A.5.17	A.5.17 Informationen zur Authentifizierung
				A.8.5	A.8.5 Sichere Authentifizierung
				A.8.24	A.8.24 Verwendung von Kryptographie
§30 (2) Nr. 10	Multi-Faktor-Authentifizierung (MFA) und kontinuierliche Authentifizierung (SSO)	11.7.2	Die Authentifizierungsstärke muss für die Klassifizierung der Vermögenswerte geeignet sein	A.8.5	A.8.5 Sichere Authentifizierung
				A.8.24	A.8.24 Verwendung von Kryptographie
§30 (2) Nr. 9	**Management von Anlagen (Asset Management)**	**12**	**Vermögensverwaltung**	**Title**	
		12.1	**Klassifizierung der Vermögenswerte**	**Title**	
§30 (2) Nr. 9	Management von Anlagen (Asset Management)	12.1.1	Klassifizierung und Schutzniveau für Informationen und Vermögenswerte	A.5.12	A.5.12 Klassifizierung von Information
§30 (2) Nr. 9	Management von Anlagen (Asset Management)	12.1.2	Klassifizierungssystem für Vermögenswerte und Informationen (unter Verwendung von C/I/A/A) zur Angabe von Schutzanforderungen und -zielen	A.5.10	A.5.10 Zulässiger Gebrauch von Informationen und anderen damit
				A.5.12	A.5.12 Klassifizierung von Information
				A.5.13	A.5.13 Kennzeichnung von Information
§30 (2) Nr. 9	Management von Anlagen (Asset Management)	12.1.3	Überprüfen und aktualisieren Sie regelmäßig die Klassifizierungsstufen von Vermögenswerten und Informationen	A.5.10	A.5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten
				A.5.12	A.5.12 Klassifizierung von Information
		12.2	**Umgang mit Informationen und Vermögenswerten**	**Title**	
§30 (2) Nr. 9	Management von Anlagen (Asset Management)	12.2.1	Richtlinie für den Umgang mit Vermögenswerten und Informationen gemäß der Sicherheitsrichtlinie	A.5.10	A.5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten
				A.7.10	A.7.10 Speichermedien
				A.5.13	A.5.13 Kennzeichnung von Information
§30 (2) Nr. 9	Management von Anlagen (Asset Management)	12.2.2	Die Richtlinie muss: (a) den gesamten Lebenszyklus der Informationen und Vermögenswerte abdecken, einschließlich Erwerb, Verwendung, Speicherung, Transport und Entsorgung; (b) Anweisungen für die sichere Verwendung, sichere Speicherung, den sicheren Transport und die unwiederbringliche Löschung und Vernichtung der Informationen und Vermögenswerte enthalten; (c) vorsehen, dass Geräte, Hardware, Software und Daten nur nach Genehmigung durch von den Leitungsorganen gemäß den Richtlinien	A.5.10	A.5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten
				A.6.7	A.6.7 Telearbeit
				A.7.9	A.7.9 Sicherheit von Werten außerhalb der Räumlichkeiten
				A.7.10	A.7.10 Speichermedien
				A.7.14	A.7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln
				A.8.10	A.8.10 Löschung von Informationen
§30 (2) Nr. 9	Management von Anlagen (Asset Management)	12.2.3	Überprüfen und aktualisieren Sie die Richtlinien zur Anlagenhandhabung regelmäßig oder nach bedeutenden Vorfällen und Änderungen.	A.5.10	A.5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten

				A.5.1	A.5.1 Informationssicherheitsrichtlinien
		12.3	**Richtlinie für Wechseldatenträger**	**Title**	
§30 (2) Nr. 9	Management von Anlagen (Asset Management)	12.3.1	Wechseldatenträgerrichtlinie für die Verwaltung von Wechselspeichermedien an Standorten und in Geschäftsräumen	A.7.10	A.7.10 Speichermedien
				A.7.14	A.7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln
				A.8.10	A.8.10 Löschung von Informationen
§30 (2) Nr. 9	Management von Anlagen (Asset Management)	12.3.2	Die Richtlinie muss: (a) ein technisches Verbot des Anschlusses von Wechseldatenträgern vorsehen, sofern für deren Verwendung kein organisatorischer Grund vorliegt; (b) eine Deaktivierung der eigenständigen Ausführung von solchen Datenträgern und eine Überprüfung der Datenträger auf Schadcode vorsehen, bevor sie auf den Systemen der Unternehmen verwendet werden; (c) Maßnahmen zur Kontrolle und zum Schutz tragbarer	A.7.10	A.7.10 Speichermedien
				A.7.14	A.7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln
				A.8.10	A.8.10 Löschung von Informationen
				A.5.34	A.5.34 Privatsphäre und Schutz von personenbezogenen Daten(PbD)
				A.8.24	A.8.24 Verwendung von Kryptographie
§30 (2) Nr. 9	Management von Anlagen (Asset Management)	12.3.3	Überprüfen und aktualisieren Sie die Richtlinie für Wechseldatenträger regelmäßig oder nach bedeutenden Vorfällen und Änderungen	A.7.10	A.7.10 Speichermedien
				A.7.14	A.7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln
				A.8.10	A.8.10 Löschung von Informationen
		12.4	**Anlageninventar**	**Title**	
§30 (2) Nr. 9	Management von Anlagen (Asset Management)	12.4.1	Vollständige und genaue Bestandsaufnahme der Vermögenswerte mit aufgezeichneten Änderungen	A.5.9	A.5.9 Inventar der Informationen und anderen damit verbundenen Werten
§30 (2) Nr. 9	Management von Anlagen (Asset Management)	12.4.2	Die Inventarisierung mit der entsprechenden Granularität umfasst eine Liste der Vorgänge und Dienste sowie eine Liste der Vermögenswerte (NIS), die Vorgänge und Dienste unterstützen.	A.5.9	A.5.9 Inventar der Informationen und anderen damit verbundenen Werten
§30 (2) Nr. 9	Management von Anlagen (Asset Management)	12.4.3	Überprüfen und aktualisieren Sie regelmäßig das Inventar der Vermögenswerte und dokumentieren Sie den Verlauf	A.5.9	A.5.9 Inventar der Informationen und anderen damit verbundenen Werten
§30 (2) Nr. 9	Management von Anlagen (Asset Management)	12.5	Rückgabe oder Löschung von Vermögenswerten bei Beendigung des Arbeitsverhältnisses mit entsprechenden Prozessen	A.5.11	A.5.11 Rückgabe von Werten
				A.7.10	A.7.10 Speichermedien
				A.8.10	A.8.10 Löschung von Informationen
		13	**Umwelt- und physische Sicherheit**	**Title**	
		13.1	**Unterstützende Dienstprogramme**	**Title**	
		13.1.1	Vermeidung von Verlusten, Schäden oder Gefährdungen durch Ausfall oder Unterbrechung unterstützender Versorgungseinrichtungen	A.7.5	A.7.5 Schutz vor physischen und umweltbedingten Bedrohungen
				A.7.8	A.7.8 Platzierung und Schutz von Geräten und Betriebsmitteln
				A.7.11	A.7.11 Versorgungseinrichtungen
				A.7.12	A.7.12 Sicherheit der Verkabelung
		13.1.2	Zu diesem Zweck müssen die betreffenden Stellen: a) die Einrichtungen vor Stromausfällen und anderen Störungen schützen, die durch Ausfälle bei unterstützenden Versorgungsleistungen wie Strom, Telekommunikation, Wasserversorgung, Gas, Abwasser, Lüftung und Klimaanlagen verursacht werden; b) gegebenenfalls den Einsatz von Redundanz bei Versorgungsleistungen in Betracht ziehen; c) Versorgungsleistungen für Strom	A.7.5	A.7.5 Schutz vor physischen und umweltbedingten Bedrohungen
				A.7.8	A.7.8 Platzierung und Schutz von Geräten und Betriebsmitteln
				A.7.9	A.7.9 Sicherheit von Werten außerhalb der Räumlichkeiten
				A.7.11	A.7.11 Versorgungseinrichtungen
				A.7.12	A.7.12 Sicherheit der Verkabelung
				A.8.14	A.8.14 Redundanz von informationsverarbeitenden Einrichtungen
		13.1.3	Überprüfen, testen und aktualisieren Sie Schutzmaßnahmen regelmäßig und nach Vorfällen	9.1	
				A.7.5	A.7.5 Schutz vor physischen und umweltbedingten Bedrohungen
				A.7.11	A.7.11 Versorgungseinrichtungen
		13.2	**Schutz vor physischen und umweltbedingten Bedrohungen**	**Title**	
		13.2.1	Vorbeugung und Reduzierung der Folgen ökologischer und physischer Bedrohungen	A.7.3	A.7.3 Sichern von Büros, Räumen und Einrichtungen
				A.7.4	A.7.4 Physische Sicherheitsüberwachung
				A.7.5	A.7.5 Schutz vor physischen und umweltbedingten Bedrohungen
		13.2.2	Konzipieren Sie Schutzmaßnahmen auf der Grundlage von Risikobewertung, Kontrollschwellen und Überwachung von Umweltbedrohungen	A.7.3	A.7.3 Sichern von Büros, Räumen und Einrichtungen
				A.7.4	A.7.4 Physische Sicherheitsüberwachung
				A.7.5	A.7.5 Schutz vor physischen und umweltbedingten Bedrohungen
		13.2.3	Überprüfen, testen und aktualisieren Sie Schutzmaßnahmen regelmäßig und nach Vorfällen	9.1	
				A.7.13	A.7.13 Instandhalten von Geräten und Betriebsmitteln
		13.3	**Perimeter- und physische Zugangskontrolle**	**Title**	
		13.3.1	Verhindern und überwachen Sie unbefugten physischen Zugriff, Schäden und Störungen	A.7.1	A.7.1 Physische Sicherheitsperimeter
				A.7.2	A.7.2 Physischer Zutritt
				A.7.3	A.7.3 Sichern von Büros, Räumen und Einrichtungen
				A.7.4	A.7.4 Physische Sicherheitsüberwachung
		13.3.2	Implementierung von Sicherheitsperimetern, Zutrittskontrollen und Zugangspunkten, physischer Sicherheit für Büros und Einrichtungen, kontinuierliche Überwachung	A.5.15	A.5.15 Zugangssteuerung
				A.5.18	A.5.18 Zugangsrechte
				A.7.1	A.7.1 Physische Sicherheitsperimeter
				A.7.2	A.7.2 Physischer Zutritt
				A.7.3	A.7.3 Sichern von Büros, Räumen und Einrichtungen
				A.7.4	A.7.4 Physische Sicherheitsüberwachung
				A.8.2	A.8.2 Privilegierte Zugangsrechte
		13.3.3	Überprüfen, testen und aktualisieren Sie physische Kontrollmaßnahmen regelmäßig und nach Vorfällen	9.1	9.1 Überwachung, Messung, Analyse und Bewertung
				A.7.2	A.7.2 Physischer Zutritt
				A.7.5	A.7.5 Schutz vor physischen und umweltbedingten Bedrohungen
§30 (2) Nr. 10	Gesicherte Sprach-, Video- und Textkommunikation			A.8.20	A.8.20 Netzwerksicherheit
				A.8.21	A.8.21 Sicherheit von Netzwerkdiensten
				A.8.12	A.8.12 Verhinderung von Datenlecks
§30 (2) Nr. 10	Gesicherte Notfallkommunikationssysteme			A.8.14	A.8.14 Redundanz von informationsverarbeitenden Einrichtungen
§31	**Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer**				
§31 (1)	Besondere Maßnahmen für Betreiber kritischer Anlagen	Kritis		6.1.3	6.1.3 Informationssicherheitsrisikobehandlung
				8.3	8.3 Informationssicherheitsrisikobehandlung
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
§31 (2)	Systeme zur Angriffserkennung			viele	
§32	**Meldepflichten**				
§32 (1)	Meldepflichten		(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, fol-gende Informationen an eine vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete gemeinsame Meldestelle zu melden: 1. unverzüglich, spätestens jedoch	A.5.24	A.5.24 Planung und Vorbereitung der Handhabung von Informations-sicherheitsvorfällen
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
§33	**Registrierungspflicht**				
§33 (1)	Registrierung Einrichtung		Besonders wichtige Einrichtungen und wichtige Einrichtungen sowie Domain Name-Registry-Diensteanbieter sind verpflichtet, spätestens drei Monate, nachdem sie	A.5.5	A.5.5 Kontakt mit Behörden
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
§33 (2)	Kontaktstelle KRITIS	Kritis	(2) Betreiber kritischer Anlagen übermitteln mit den Angaben nach Absatz 1 die kriti sche Dienstleistung, die öffentlichen IP-Adressbereiche der von ihnen betriebenen Anlagen	A.5.5	A.5.5 Kontakt mit Behörden
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
§34	**Besondere Registrierungspflicht für bestimmte Einrichtungsarten**				
§34 (1)	Registrierung besondere Einrichtung		(1) Eine Einrichtung der in § 60 Absatz 1 Satz 1 genannten Einrichtungsart ist ver pflichtet, spätestens drei Monate, nachdem sie als eine der vorgenannten Einrichtungen	A.5.5	A.5.5 Kontakt mit Behörden
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
§35	**Unterrichtungspflichten**				
§35 (1)	Unterrichtung Kunden		(1) Im Fall eines erheblichen Sicherheitsvorfalls kann das Bundesamt besonders wichtigen Einrichtungen und wichtigen Einrichtungen anordnen, die Empfänger	A.5.26	A.5.26 Reaktion auf Informationssicherheitsvorfälle
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen

§35 (2)	Gegenmaßnahmen Kunden		2) Einrichtungen nach Absatz 1 Satz 1 aus den Sektoren Finanzwesen, Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende, digitale Infrastruktur, Verwaltung von IKT-Diensten und Digitale Dienste teilen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste und dem Bundesamt unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mit, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Einrichtungen informieren zugleich diese Empfänger auch über die erhebliche Cyberbedrohung selbst. Die Pflichten nach Satz 1 oder 2 gelten nur dann, wenn in Abwägung der Interessen der Einrichtung und des Empfängers die Interes sen des Empfängers überwiegen.	A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
§38	**Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen**				
§38 (1)	Verantwortung Geschäftsführung		Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtun gen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikoma nagementmaßnahmen umzusetzen und ihre	5.1	5.1 Führung und Verpflichtung
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
§38 (3)	Schulungen Geschäftsführung		3) Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von	7.2	7.2 Kompetenz
				A.5.31	A.5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
				A.6.3	A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung