NNIS2-Umsetzungsgesetz - NIS2UmsuCG - Infos zu Pflichten

NIS2UmsuCG	Anforderungen	KRITIS	ISO 27001	TISAX-Richtlinien
§30 (1) Satz 1	Die Maßnahmen sollen dem Stand der Technik entsprechen, relevante europäische und internationale Normen berücksichtigen und auf einem gefahrenübergreifenden Ansatz basieren. Sie müssen mindestens folgende Punkte umfassen:	BSI-3, BSI-15	4.3, A.5.4, A.5.29, A.5.30	RL-ISMS-01, RL-ISMS-01.3, RL-ISMS-02.0
§30 (1) Satz 3	Konzepte zur Risikoanalyse und IT-Sicherheit: Entwicklung und Implementierung von Konzepten zur Analyse und Bewertung von Risiken sowie zur Sicherstellung der IT-Sicherheit	BSI-16	6.1.3, 8.3, A.5.31	RL-ISMS-01.2, RL-ISMS-06.0, RL-ISMS-07.0
§30 (2) Satz 1	Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlä- gigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen	BSI-13, BSI-15	6.1, 8.2, 8.3, A.5.29, A.5.30	RL-ISMS-01, RL-ISMS-01.2, RL-ISMS-01.3
§30 (2) Nr. 1	Konzepte zur Risikoanalyse und IT-Sicherheit: Entwicklung und Implementierung von Konzepten zur Analyse und Bewertung von Risiken sowie zur Sicherstellung der IT-Sicherheit	BSI-13, BSI-14	6.1, 8.2, 8.3	RL-ISMS-01.2, RL-ISMS-06.0, RL-ISMS-07.0
§30 (2) Nr. 1	Konzepte für IT-Sicherheit (ISMS)	BSI-1, BSI-2	4.1-10.2, A.5.1, A.5.2, A.5.4	RL-ISMS-01, RL-ISMS-01.3
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen: Maßnahmen und Verfahren zur effektiven Reaktion auf und Bewältigung von Sicherheitsvorfällen.	BSI-77, BSI-78, BSI-79, BSI-80	A.5.24, A.5.25, A.5.26, A.5.28, A.6.8	RL-ISMS-50.0, RL-ISMS-40.2
§30 (2) Nr. 3	Aufrechterhaltung des Betriebs: Implementierung von Backup-Management, Wiederherstellung nach Notfällen und Krisenmanagement, um den kontinuierlichen Betrieb sicherzustellen	BSI-17, BSI-18	A.5.29, A.5.30, A.5.31, A.8.14	RL-ISMS-46.0, RL-ISMS-46.1, RL-ISMS-46.2, RL-ISMS-46.3
§30 (2) Nr. 3	Aufrechterhaltung des Betriebs: Implementierung von Backup-Management, Wiederherstellung nach Notfällen und Krisenmanagement, um den kontinuierlichen Betrieb sicherzustellen	BSI-22, BSI-23, BSI-24	A.8.13, A.8.14, A.8.16	RL-ISMS-30.0
§30 (2) Nr. 3	Wiederherstellung nach Notfällen (DR und IT-SCM)	BSI-19	A.5.29, A.5.30	RL-ISMS-46.1, RL-ISMS-46.3
§30 (2) Nr. 3	Krisenmanagement	–	–	RL-ISMS-46.0, RL-ISMS-46.2, RL-ISMS-46.3
§30 (2) Nr. 4	Sicherheit der Lieferkette: Sicherstellung der Sicherheit in der Lieferkette, einschließlich der Berücksichtigung sicherheitsbezogener Aspekte in den Beziehungen zu Anbietern und Dienstleistern.	–	A.5.21	RL-ISMS-52.0
§30 (2) Nr. 4		BSI-42, BSI-98, BSI-99	A.5.19, A.5.20, A.5.21, A.5.22,	RL-ISMS-52.0, RL-ISMS-53.0

NIS2UmsuCG	Anforderungen	KRITIS	ISO 27001	TISAX-Richtlinien
			A.5.23	
§30 (2) Nr. 5	Sicherheitsmaßnahmen bei IT-Erwerb, -Entwicklung und -Wartung: Sicherheitsmaßnahmen für den Erwerb, die Entwicklung und die Wartung von IT-Systemen, Komponenten und Prozessen, einschließlich des Managements und der Offenlegung von Schwachstellen	BSI-43	A.5.19, A.5.20, A.5.22, A.5.23, A.8.26	RL-ISMS-09.0
§30 (2) Nr. 5	Sicherheit bei der Entwicklung von IT	BSI-43, BSI-44	A.8.25, A.8.26, A.8.27, A.8.28, A.8.29, A.8.30	RL-ISMS-32.1
§30 (2) Nr. 5	Sicherheit bei der Wartung von IT	BSI-45, BSI-76	A.5.37, A.7.13, A.8.9, A.8.31	RL-ISMS-32.0
§30 (2) Nr. 5	Management und Offenlegung von Schwachstellen	BSI-25, BSI-84, BSI-83, BSI-96	A.5.7, A.8.8, A.8.19	RL-ISMS-06.0, RL-ISMS-27.0
§30 (2) Nr. 6	Bewertung der Wirksamkeit von Risikomanagementmaßnahmen: Konzepte und Verfahren zur regelmäßigen Bewertung der Wirksamkeit von Sicherheits- und Risikomanagementmaßnahmen.	BSI-85, BSI-86, BSI-87, BSI-88, BSI-89	9.1, 9.3, 10.1, 10.2, A.5.35, A.5.36	RL-ISMS-06.0
§30 (2) Nr. 7	Cyberhygiene und Schulungen: Einführung grundlegender Cyberhygiene-Verfahren und regelmäßige Schulungen im Bereich der IT-Sicherheit.	BSI-68	7.3, A.6.3	RL-ISMS-07.0, RL-ISMS-57.0
§30 (2) Nr. 7	Schulungen: Regelmäßige Schulungen im Bereich der IT-Sicherheit	BSI-68	7.2, A.6.3	RL-ISMS-07.0, RL-ISMS-57.0
§30 (2) Nr. 8	Kryptografie und Verschlüsselung: Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung zur Sicherung von Daten.	BSI-32, BSI-33, BSI-34, BSI-35	A8.24	RL-ISMS-39.0
§30 (2) Nr. 9	Personalsicherheit und Zugriffskontrolle: Maßnahmen zur Sicherung des Personals, Konzepte zur Zugriffskontrolle und Verwaltung von IT-Anlagen	BSI-42, BSI-56, BSI-57, BSI-69, BSI-70	A.6.1, A.6.2, A.6.4, A.6.5, A.6.6	RL-ISMS-59.0, RL-ISMS-60.0
§30 (2) Nr. 9	Zugriffskontrolle: Konzepte zur Zugriffskontrolle und Verwaltung von IT-Anlagen.	BSI-27, BSI-28, BSI-58, BSI-59, BSI-60, BSI-61	A.5.15, A.5.18	RL-ISMS-27.0
§30 (2) Nr. 9	Management von Anlagen: Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen	BSI-5, BSI-6, BSI-7, BSI-8, BSI-9,	A.5.9, A.5.10, A.5.11, A.5.12, A.5.13,	RL-ISMS-02.0, RL-ISMS-14.0, RL-ISMS-17.0, RL-ISMS-33.0

NIS2UmsuCG	Anforderungen	KRITIS	ISO 27001	TISAX-Richtlinien
		BSI-10, BSI-12	A.7.9, A.8.3	
§30 (2) Nr. 10	Multi-Faktor-Authentifizierung und gesicherte Kommunikation: Einsatz von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung sowie gesicherte Kommunikationssysteme (Sprach-, Video- und Textkommunikation) und gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung	BSI-26, BSI-27, BSI-64	A.5.16, A.5.17, A.8.5	RL-ISMS-24.0
§30 (2) Nr. 10	Gesicherte Kommunikationssysteme (Sprach-, Video- und Textkommunikation)	BSI-33, BSI-36, BSI-41	A.8.20, A.8.21, A.8.12	RL-ISMS-29.0
§30 (2) Nr. 10	Gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung	–	A.8.14	RL-ISMS-46.0, RL-ISMS-46.3
§30 (7)	Informationsaustausch	BSI-97	A.5.5	RL-ISMS-43.0
§31 (1)	Für Betreiber kritischer Anlagen gelten besonders aufwändige Maßnahmen für ihre informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit ihrer kritischen Anlagen entscheidend sind	BSI-16, BSI-17	6.1.3, 8.3, A.5.31	RL-ISMS-01, RL-ISMS-02.0
§31 (2)	Betreiber kritischer Anlagen sind verpflichtet, Systeme zur Angriffserkennung einzusetzen. Diese Systeme müssen in der Lage sein, kontinuierlich und automatisch geeignete Parameter und Merkmale aus dem laufenden Betrieb zu erfassen und auszuwerten.	OH SzA, BSI-90, BSI-91, BSI-92, BSI-93, BSI-94	viele	RL-ISMS-35.0, RL-ISMS-37.0, RL-ISMS-54.0
§32 (1)	Meldeverpflichtungen bei erheblichen Sicherheitsvorfällen zum Zeitpunkt: Unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung eines erheblichen Sicherheitsvorfalls. Inhalt: Bestätigung oder Aktualisierung der Informationen aus der frühen Erstmeldung. Einschließlich einer ersten Bewertung des Schweregrads und der Auswirkungen des Sicherheitsvorfalls sowie gegebenenfalls die Angabe von Kompromittierungsindikatoren.	BSI-100	A.5.24, A.5.31	RL-ISMS-01.2, RL-ISMS-06.0, RL-ISMS-07.0
§33 (1)	Besonders wichtige Einrichtungen, wichtige Einrichtungen sowie Domain-Name-Registry-Diensteanbieter sind verpflichtet, sich beim Bundesamt zu registrieren. Diese Registrierung muss spätestens drei Monate nach der erstmaligen oder erneuten Anerkennung als eine der genannten Einrichtungen oder nach dem Beginn der Domain-Name-Registry-Dienstleistungen erfolgen	–	A.5.5	RL-ISMS-01.2
§33 (2)	Besondere Registrierungspflicht für bestimmte Einrichtungsarten	BSI-100	A.5.5	RL-ISMS-01.2, RL-ISMS-40.0
§34 (1)	Gilt für einschlägiger Sektor, Branche und Einrichtungsart wie in Anlage 1 bestimmt	–	A.5.5	RL-ISMS-01.2
§35 (1)	Unterrichtung der Kunden: Im Fall eines erheblichen	–	A.5.26,	RL-ISMS-31.0

NIS2UmsuCG	Anforderungen	KRITIS	ISO 27001	TISAX-Richtlinien
	Sicherheitsvorfalls kann das Bundesamt besonders wichtige Einrichtungen und wichtige Einrichtungen anweisen, die Empfänger ihrer Dienste unverzüglich über den Vorfall zu unterrichten, wenn dieser die Erbringung des jeweiligen Dienstes beeinträchtigen könnte		A.5.31	
§35 (2)	Einrichtungen aus den Sektoren Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten und digitale Dienste müssen bei einer erheblichen Cyberbedrohung unverzüglich alle Maßnahmen oder Abhilfemaßnahmen an die potenziell betroffenen Empfänger ihrer Dienste und das Bundesamt mitteilen	–	A.5.31	RL-ISMS-31.0
§38 (1)	Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen beson- ders wichtiger Einrichtungen und wichtiger Einrichtungen	BSI-17	5.1, A.5.31	RL-ISMS-40.0
§38 (3)	Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, regelmäßig an Schulungen teilzunehmen. Diese Schulungen sollen sicherstellen, dass die Geschäftsleitungen über ausreichende Kenntnisse und Fähigkeiten verfügen	BSI-68	7.2, A.5.31	RL-ISMS-07.0, RL-ISMS-57.0

Bearbeiten