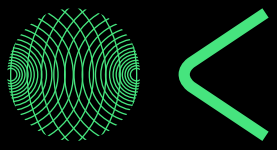

OpenKRITIS

Cyber Security Standards KRITIS-Mapping

April 2024 · Version 1.5 · OpenKRITIS

KRITIS	Thema	C5:2020	NIST	NIS2[1]	ISO 27001[2]	OH SzA
BSI-1	Managementsystem für Informationssicherheit	OIS-01	ID.BE-2 PR.IP-7	30.2.1b	4.1-10.2	P4
BSI-2	Strategische Vorgaben zur Informationssicherheit und Verantwortung der Unternehmensleitung	OIS-02	ID.GV-1 ID.BE-3 PR.AT-4 DE.DP-1	30.2.1b	6.2 A.5.1 A.5.2 A.5.4	A1 G1 G2 G3
BSI-3	Zuständigkeiten und Verantwortungen im Rahmen der Informationssicherheit	OIS-03	ID.GV-2 ID.AM-6	30.1.1	4.3 A.5.3 A.5.4	
BSI-4	Funktionstrennung	OIS-04	PR.AC-4		A.5.3	
BSI-5	Asset Inventar	AM-01	ID.AM-1 ID.AM-2	30.2.9c	A.5.9	
BSI-6	Zuweisung von Asset Verantwortlichen	AM-02	ID.AM-6	30.2.9c	A.5.4 A.5.10	
BSI-7	Nutzungsanweisungen für Assets	AM-03	PR.DS-3	30.2.9c	A.5.10 A.7.10	D13
BSI-8	Ab- und Rückgabe von Assets	AM-04	PR.DS-3 PR.IP-6	30.2.9c	A.5.11 A.7.10 A.8.10	
BSI-9	Klassifikation von Informationen	AM-05	ID.AM-5	30.2.9c	A.5.12	
BSI-10	Kennzeichnung von Informationen und Handhabung von Assets	AM-06	PR.DS-3 PR.DS-5	30.2.9c	A.5.10 A.5.13	
BSI-11	Verwaltung von Datenträgern	AM-02 AM-05	PR.PT-2		A.7.10 A.7.14 A.8.10	
BSI-12	Überführung und Entfernung von Assets	AM.02	PR.DS-3	30.2.9c	A.5.10 A.7.9 A.8.10	
BSI-13	Richtlinie für die Organisation des Risikomanagements	OIS-06	ID.GV-4 ID.RM-1	30.2.0 30.2.1a	6.1 8.2 8.3	

[1] Das NIS2-Mapping ist sehr vorläufig zu verstehen. Grundlage ist der Dezember-Entwurf des NIS2UmsuCG.
[2] Revidierte Version von 2022.

KRITIS	Thema	C5:2020	NIST	NIS2[1]	ISO 27001[2]	OH SzA
BSI-14	Identifikation, Analyse, Beurteilung und Folgeabschätzung von IT-Risiken	OIS-07 SSO-02	ID.GV-4 ID.RM-2 ID.SC-2	30.2.1a	6.1 8.2 8.3	D1
BSI-15	Richtlinien zur Folgeabschätzung	BCM-02	ID.BE-1 ID.RA-5 ID.RA-6 PR.IP-9	30.1.1 30.2.0	A.5.29 A.5.30	
BSI-16	Maßnahmenableitung	OIS-01	ID.RM-3	30.1.2 31.1	6.1.3 8.3 A.5.31	G14
BSI-17	Verantwortung der gesetzlichen Vertreter des Betreibers der Kritischen Infrastruktur	BCM-01	ID.RA-4	30.2.3a 31.1 38.1	A.5.29 A.5.31	A1 G7
BSI-18	Planung der Betriebskontinuität	BCM-03	ID.BE-4 PR.IP-9	30.2.3a	A.5.30	R3
BSI-19	Verifizierung, Aktualisierung und Test der Betriebskontinuität	BCM-04	ID.SC-4 PR.IP-9 RC.IM-1 RC.IM-2	30.2.3c	A.5.29	
BSI-20	Notwendige/ausreichende Personal- und IT-Ressourcen (Betrieb und IT-Sicherheit	OPS-01 OPS-02 OPS-03	PR.DS-4		A.8.6	G5 G6 P2
BSI-21	Schutz vor Schadprogrammen	OPS-04 OPS-05	PR.DS-6 DE.CM-4		A.8.7	A2 A4 D4 D6
BSI-22	Datensicherung und Wiederherstellung	OPS-06 OPS-09	PR.IP-4	30.2.3b	A.8.13 A.8.14	
BSI-23	Datensicherung und Wiederherstellung: Überwachung	OPS-07		30.2.3b	A.8.13 A.8.16	
BSI-24	Datensicherung und Wiederherstellung: Regelmäßige Tests	OPS-08	PR.IP-4	30.2.3b	A.8.13	
BSI-25	Umgang mit Schwachstellen, Störungen und Fehlern: System-Härtung	OPS-23	PR.IP-1	30.2.5d	A.8.19	A3
BSI-26	Geheimhaltung von Authentifizierungsinformationen	IDM-07		30.2.10a	A.5.17	

KRITIS	Thema	C5:2020	NIST	NIS2[1]	ISO 27001[2]	OH SzA
BSI-27	Sichere Anmeldeverfahren	PSS-05 PSS-06 IDM-08	PR.AC-1	30.2.9b 30.2.10a	A.5.15 A.5.17 A.8.5 A.8.24	
BSI-28	Systemseitige Zugriffskontrolle			30.2.9b	A.5.15	
BSI-29	Passwortanforderungen und Validierungsparameter	PSS-07	PR.AC-7		A.5.17	
BSI-30	Einschränkung und Kontrolle administrativer Software				A.8.18 A.8.19	
BSI-31	Zugriffskontrolle zu Quellcode				A.8.4	
BSI-32	Richtlinie zur Nutzung von Verschlüsselungsverfahren und Schlüsselverwaltung	CRY-01	PR.DS-5	30.2.8	A.5.14 A.5.31 A.8.24	
BSI-33	Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung)	CRY-02		30.2.8 30.2.10b	A.8.20 A.8.21 A.8.24 A.8.33	
BSI-34	Verschlüsselung von sensiblen Daten bei der Speicherung	CRY-03		30.2.8	A.5.34 A.8.24	
BSI-35	Sichere Schlüsselverwaltung	CRY-04	PR.DS-5	30.2.8	A.8.24	
BSI-36	Technische Schutzmaßnahmen	COS-01 COS-02	PR.AC-3 PR.AC-5 PR.PT-4 DE.AE-1	- 30.2.10b	A.8.20 A.8.21 A.8.22 A.8.23 A.8.26 A.8.27	P1 D3 D5 R4
BSI-37	Überwachen von Verbindungen	COS-03	PR.PT-4 DE.CM-1		A.8.16 A.8.20 A.8.23	P1 D5
BSI-38	Netzwerkübergreifende Zugriffe	COS-04	DE.CM-1		A.8.20 A.8.21 A.8.22	
BSI-39	Netzwerke zur Administration	COS-05	PR.AC-5		A.8.22	
BSI-40	Dokumentation der Netztopologie	COS-07	PR.AC-5		A.8.22	

KRITIS	Thema	C5:2020	NIST	NIS2[1]	ISO 27001[2]	OH SzA
BSI-41	Richtlinien zur Datenübertragung	COS-08	PR.AC-5	30.2.10b	A.5.14	
BSI-42	Vertraulichkeitserklärung	COS-08	ID.AM-3	30.2.4b 30.2.9a	A.5.8 A.5.14 A.6.6	
BSI-43	Richtlinien zur Entwicklung, Beschaffung von Informationssystemen	DEV-01	PR.IP-2	30.2.5a 30.2.9a	A.5.8 A.8.25 A.8.26 A.8.27 A.8.28	
BSI-44	Auslagerung der Entwicklung	DEV-02	DE.CM-6	30.2.5b	A.8.29 A.8.30	
BSI-45	Richtlinien zur Änderung von Informationssystemen	DEV-03	PR.IP-3	30.2.5c	8.1 A.8.31 A.8.32	P4
BSI-46	Risikobewertung der Änderungen	DEV-05	PR.IP-3		8.1 A.8.9 A.8.32	
BSI-47	Kategorisierung der Änderungen	DEV-05	PR.IP-3		8.1 A.8.32	
BSI-48	Priorisierung der Änderungen	DEV-05	PR.IP-3		8.1 A.8.32	
BSI-49	Testen der Änderungen	DEV-07	PR.IP-3		A.8.29 A.8.32 A.8.33	
BSI-50	Zurückrollen der Änderungen	DEV-08	PR.IP-3		A.8.32	
BSI-51	Überprüfen von ordnungsgemäßer Testdurchführung und Genehmigung	DEV-09	PR.IP-3		A.8.32	
BSI-52	Notfalländerungen	DEV-03	PR.IP-3		8.1 A.8.32	
BSI-53	Systemlandschaft	DEV-10	PR.DS-7		A.8.31	
BSI-54	Funktionstrennung	DEV-10	PR.DS-7		A.8.31	

KRITIS	Thema	C5:2020	NIST	NIS2[1]	ISO 27001[2]	OH SzA
BSI-55	Richtlinien und Verfahren zur Risikominimierung des Zugriffs über mobile Endgeräte des KRITIS-Betreibers				A.8.1	
BSI-56	Einstellung und Sicherheitsüberprüfung	HR-01	PR.AC-6	30.2.9a	A.6.1	
BSI-57	Einstellung und Beschäftigungsvereinbarungen	HR-02	PR.IP-11	30.2.9a	A.6.2	
BSI-58	Rollenzuweisung und Vieraugenprinzip oder Funktionstrennung	IDM-01 PSS-08	PR.AC-4	30.2.9b	A.5.3 A.5.15 A.8.3	
BSI-59	Identitäts- und Berechtigungsmanagement: Benutzerregistrierung	IDM-02	PR.AC-2	30.2.9b	A.5.16 A.5.17	
BSI-60	Identitäts- und Berechtigungsmanagement: Zugriffsberechtigung	IDM-03	PR.AC-1	30.2.9b	A.5.18	
BSI-61	Vergabe und Änderung (Provisionierung) von Zugriffsberechtigungen	IDM-04	PR.AC-1	30.2.9b	A.5.18	
BSI-62	Identitäts- und Berechtigungsmanagement: Überprüfungen	IDM-05	PR.AC-1		A.5.18	
BSI-63	Identitäts- und Berechtigungsmanagement: Administratoren	IDM-06	PR.AC-4		A.5.3 A.5.18 A.8.2	
BSI-64	Identitäts- und Berechtigungsmanagement: Notfallbenutzer	IDM-09	PR.AC-1	30.2.10a	A.5.17 A.5.18	
BSI-65	Festlegung notwendiger Kompetenzen (Betrieb und IT-Sicherheit)	SP-01	ID.GV-3		A.5.1 A.5.2	
BSI-66	Überprüfung und Freigabe von Richtlinien und Anweisungen	SP-02			A.5.1	G1 G2 G3
BSI-67	Abweichungen von bestehenden Richtlinien und Anweisungen	SP-03			A.5.1	
BSI-68	Schulungen und Awareness	HR-03	PR.AT-1 PR.AT-2 PR.AT-5	30.2.7a 30.2.7b 38.3	7.2 A.6.3	G9
BSI-69	Disziplinarverfahren	HR-04	PR.IP-11	30.2.9a	A.6.4	
BSI-70	Beendigung des Beschäftigungsverhältnisses	HR-05	PR.IP-11	30.2.9a	A.6.5	
BSI-71	Rechenzentrumsversorgung	PS-02	PR.PT-5		A.8.14	

KRITIS	Thema	C5:2020	NIST	NIS2[1]	ISO 27001[2]	OH SzA
BSI-72	Perimeterschutz	PS-01	PR.IP-5		A.7.1	
BSI-73	Physischer Zutrittsschutz	PS-04	PR.AC-2		A.5.15 A.5.18 A.7.2 A.7.3 A.7.4 A.8.2	
BSI-74	Schutz vor Bedrohungen von außen	PS-03 PS-05	DE.CM-2 ID.BE-5		A.7.3 A.7.4 A.7.5	
BSI-75	Schutz vor Unterbrechungen durch Stromausfälle und andere derartige Risiken	PS-06	PR.DS-8 PR.IP-5		A.7.5 A.7.8 A.7.11 A.7.12	
BSI-76	Wartung der Infrastruktur	PS-07	PR.MA-1	30.2.5c	A.7.2 A.7.3 A.7.13	
BSI-77	Verantwortlichkeiten und Vorgehensmodell	SIM-01	PR.IP-8 DE.AE-4 RS.RP-1 RS.AN-2 RS.AN-4 RS.AN-5 RC.RP-1	30.2.2	A.5.24 A.6.8	G2 G3 G4 G7 D9 R1 R2
BSI-78	Bearbeitung von Sicherheitsvorfällen	SIM-02	DE.AE-2 DE.AE-4 RS.CO-1 RS.MI-1 RS.MI-2	30.2.2	A.5.25 A.5.26	G6 D14 R2 R5
BSI-79	Dokumentation und Berichterstattung über Sicherheitsvorfälle	SIM-03	DE.DP-4 RS.CO-2	30.2.2	A.5.25 A.5.26	
BSI-80	Security Incident Event Management (SIEM)	SIM-05 COS-01	DE.AE-3 RS.AN-1	30.2.2	A.5.28 A.6.8 A.8.15	P5 D6 D7 D10

KRITIS	Thema	C5:2020	NIST	NIS2[1]	ISO 27001[2]	OH SzA
BSI-81	Verpflichtung der Nutzer zur Meldung von Sicherheitsvorfällen an eine zentrale Stelle	SIM-04	RS.CO-3 RS.CO-4		A.5.2 A.5.24 A.6.8	G8
BSI-82	Auswertung und Lernprozess	SIM-05	PR.IP-7 DE.DP-5 RS.IM-1 RS.IM-2 RC.IM-1 RC.IM-2		A.5.27	G9 D14
BSI-83	Anlassbezogene Prüfungen: Konzept	OPS-17 OPS-20 OPS-22	PR.PT-5 ID.RA-1 PR.IP-12 ID.RA-3 DE.CM-8	30.2.5d	A.8.8 A.8.34	
BSI-84	Umgang mit Schwachstellen, Störungen und Fehlern: Prüfung offener Schwachstellen	OPS-21	DE.CM-8	30.2.5d	A.8.8	
BSI-85	Compliance und Informieren der Unternehmensleitung	COM-01	DE.DP-2	30.2.6	A.5.31 A.5.36	G12 G13
BSI-86	Interne Überprüfungen der Compliance von IT-Prozessen mit internen Informationssicherheitsrichtlinien und Standards	COM-02	PR.IP-7	30.2.6	9.2 A.5.36 A.8.34	
BSI-87	Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen: interne IT- Prüfungen	COM-03 COM-04 PSS-02	PR.IP-7 ID.RA-1 DE.CM-8 RS.MI-3	30.2.6	9.2 9.3 A.5.36 A.8.34	G1 G2 G3 P3
BSI-88	Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen: Planung externer Audits	COM-02	PR.IP-7	30.2.6	9.2 A.5.35 A.5.36 A.8.34	P3
BSI-89	Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen: Durchführung externer Audits	COM-03	PR.IP-7	30.2.6	9.2 9.3 A.5.35 A.5.36 A.8.34	

KRITIS	Thema	C5:2020	NIST	NIS2[1]	ISO 27001[2]	OH SzA
BSI-90	Systematische Log-Auswertung: Konzept	OPS-10 OPS-14	PR.PT-1	31.2	A.8.15	P2 D2 D9
BSI-91	Systematische Log-Auswertung: kritische Assets	OPS-13	PR.PT-1	31.2	A.8.15	A5 P4 D3 D8 D10 D11
BSI-92	Systematische Log-Auswertung: Aufbewahrung	OPS-14	DE.CM-7	31.2	A.8.15	
BSI-93	Systematische Log-Auswertung: Konfiguration	OPS-16	RS.AN-3	31.2	A.8.9 A.8.15	A5
BSI-94	Systematische Log-Auswertung: Verfügbarkeit	OPS-17	PR.PT-1	31.2	A.8.15	
BSI-95	Penetrationstest	OPS-19	PR.IP-12 RS.MI-3		A.8.8 A.8.34	
BSI-96	Umgang mit Schwachstellen, Störungen und Fehlern: Integration mit Änderungs- und Incident-Management	OPS-20	ID.RA-1	30.2.5d	A.5.7 A.8.8 A.8.32	A2 D13
BSI-97	Kontakt zu relevanten Behörden und Interessenverbänden	OIS-05	ID.RA-2 RS.CO-5 RC.CO-1	30.7	A.5.5 A.5.6	A2 D12
BSI-98	Richtlinie zum Umgang mit und Sicherheitsanforderungen an Dienstleister des KRITIS-Betreibers	SSO-01	ID.SC-1 ID.SC-3 PR.AT-3 PR.MA-2	30.2.4b	A.5.19 A.5.20 A.5.21 A.5.23	
BSI-99	Kontrolle der Leistungserbringung und der Sicherheitsanforderungen an Dienstleister und Lieferanten des KRITIS-Betreibers	SSO-04	ID.SC-4 PR.MA-2 DE.CM-6	30.2.4b	A.5.22	
BSI-100	Einrichtung einer Kontaktstelle	OIS-05		32.1 33.2	A.5.5 A.5.31	G10 G11

Quelle: Eigene Zusammenstellung teilweise nach BSI und NIST, April 2024

Das OpenKRITIS-Mapping legt folgende Cyber Security Standards zu Grunde:

BSI-Konkretisierung: Die 100 KRITIS-Anforderungen als Index für Betreiber (Mapping).

C5:2020: Aktualisierter BSI Cloud Security Standard mit einigen Veränderungen.

NIST CSF: Subkategorien der Security-Funktionen aus dem Cybersecurity-Framework.

NIS2: Aufgeschlüsselte Einzelanforderungen aus BSIG-E (NIS2UmsuCG) von Dezember 2023 (Mapping)

ISO/IEC 27001:2022: Annex A-Kontrollen und Management-Kapitel der jeweiligen Standard-Version.

OH SzA: Anforderungen der Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung, V 1.0.

Das Mapping basiert auf der Grundlagenarbeit der BSI C5 und NIST CSF Kreuztabellen, die andere Security-Standards referenzieren: Referenzierung Cloud Computing C5:2020 auf internationale Standards (BSI) und NIST Cybersecurity Framework Core (NIST 1.1)

OpenKRITIS

Das freie Informationsportal für Kritische Infrastrukturen

Mapping BSI KRITIS-Anforderungen und Cyber Security

Abgleich der KRITIS Cyber Security Anforderungen aus der §8a BSIG-Konkretisierung mit aktuellen Cyber Security Standards.
Ohne Gewähr und ohne Anspruch auf Vollständigkeit.

Stand: 9. April 2024
Version: 1.5
© Copyright Paul Weissmann 2024

Impressum

Paul Weissmann c/o Insignals GmbH
Rheinwerkallee 6
53227 Bonn

https://www.openkritis.de · ISSN 2748-565X
info@openkritis.de · +49 176 58952135