OPENKRITIS

Mapping KRITIS-Anforderungen auf Cyber Security Standards

April 2022

KRITIS	Thema	C5:2016	C5:2020	NIST	ISO 27001	TKG 2.0
BSI-1	Managementsystem für Informationssicherheit	OIS-01	OIS-01	ID.BE-2 PR.IP-7	4.1-10.2	3.1.1
BSI-2	Strategische Vorgaben zur Informationssicherheit und Verantwortung der Unternehmensleitung	OIS-02	OIS-02	ID.GV-1 ID.BE-3 PR.AT-4 DE.DP-1	6.2 A.5.1.1 A.6.1.1	3.9
BSI-3	Zuständigkeiten und Verantwortungen im Rahmen der Informationssicherheit	OIS-03	OIS-03	ID.GV-2 ID.AM-6	4.3 A.6.1.1 A.6.1.2	3.1.2
BSI-4	Funktionstrennung	OIS-04	OIS-04	PR.AC-4	A.6.1.2	
BSI-5	Asset Inventar	AM-01	AM-01	ID.AM-1 ID.AM-2	A.8.1.1	3.4.3
BSI-6	Zuweisung von Asset Verantwortlichen	AM-02	AM-02	ID.AM-6	A.8.1.3	3.4.3
BSI-7	Nutzungsanweisungen für Assets	AM-03	AM-03	PR.DS-3	A.8.3.1	
BSI-8	Ab- und Rückgabe von Assets	AM-04	AM-04	PR.DS-3 PR.IP-6	A.8.3.2	
BSI-9	Klassifikation von Informationen	AM-05	AM-05	ID.AM-5	A.8.1.4 A.8.2.1	
BSI-10	Kennzeichnung von Informationen und Handhabung von Assets	AM-06	AM-06	PR.DS-3 PR.DS-5	A.8.2.2 A.8.2.3	3.4.3
BSI-11	Verwaltung von Datenträgern	AM-07	AM-02 AM-05	PR.PT-2	A.8.2.1 A.8.2.2 A.8.2.3 A.8.3.1 A.8.3.3 A.11.2.9	3.3.1
BSI-12	Überführung und Entfernung von Assets	AM-08	AM.02	PR.DS-3	A.8.1.3	
BSI-13	Richtlinie für die Organisation des Risikomanagements	OIS-06	OIS-06	ID.GV-4 ID.RM-1	6.1 8.2 8.3	3.1.1

KRITIS	Thema	C5:2016	C5:2020	NIST	ISO 27001	TKG 2.0
BSI-14	Identifikation, Analyse, Beurteilung und Folgeabschätzung von IT-Risiken	OIS-07	OIS-07 SSO-02	ID.GV-4 ID.RM-2 ID.SC-2	6.1 8.2 8.3 A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.2	3.1.1
BSI-15	Richtlinien zur Folgeabschätzung	BCM-02	BCM-02	ID.BE-1 ID.RA-5 ID.RA-6 PR.IP-9	A.17.1.1	3.1.1
BSI-16	Maßnahmenableitung	B3S	B3S	ID.RM-3	6.1.3 8.3	3.1.1
BSI-17	Verantwortung der gesetzlichen Vertreter des Betreibers der Kritischen Infrastruktur	BCM-01	BCM-01	ID.RA-4	A.17.1.1	3.6.1
BSI-18	Planung der Betriebskontinuität	BCM-03	BCM-03	ID.BE-4 PR.IP-9	A.17.1.2	3.6.2
BSI-19	Verifizierung, Aktualisierung und Test der Betriebskontinuität	BCM-04	BCM-04	ID.SC-4 PR.IP-9 RC.IM-1 RC.IM-2	A.17.1.3	3.7.2
BSI-20	Notwendige/ausreichende Personal- und IT-Ressourcen (Betrieb und IT-Sicherheit	RB-01 RB-02	OPS-01 OPS-02 OPS-03	PR.DS-4	A.12.1.3	3.4.1
BSI-21	Schutz vor Schadprogrammen	RB-05	OPS-05	PR.DS-6 DE.CM-4	A.12.2.1	3.3.5
BSI-22	Datensicherung und Wiederherstellung	RB-06 RB-09	OPS-06 OPS-09	PR.IP-4	A.12.3.1 A.17.2.1	3.6.1
BSI-23	Datensicherung und Wiederherstellung: Überwachung	RB-07	OPS-07			

KRITIS	Thema	C5:2016	C5:2020	NIST	ISO 27001	TKG 2.0
BSI-24	Datensicherung und Wiederherstellung: Regelmäßige Tests	RB-08	OPS-08	PR.IP-4	A.12.3.1	-
BSI-25	Umgang mit Schwachstellen, Störungen und Fehlern: System-Härtung	RB-22	OPS-23	PR.IP-1		
BSI-26	Geheimhaltung von Authentifizierungsinformationen	IDM-07	IDM-07			3.3.6
BSI-27	Sichere Anmeldeverfahren	IDM-08	PSS-05 PSS-06 IDM-08	PR.AC-1	A.9.3.1 A.10.1.1 A.18.1.5 A.9.2.4 A.9.3.1	3.3.6
BSI-28	Systemseitige Zugriffskontrolle	IDM-10				3.3.4
BSI-29	Passwortanforderungen und Validierungsparameter	IDM-11	PSS-07	PR.AC-7	A.9.2.4 A.9.3.1	3.3.4
BSI-30	Einschränkung und Kontrolle administrativer Software	IDM-12				3.3.4
BSI-31	Zugriffskontrolle zu Quellcode	IDM-13			A.9.4.5	
BSI-32	Richtlinie zur Nutzung von Verschlüsselungsverfahren und Schlüsselverwaltung	KRY-01	CRY-01	PR.DS-5	A.10.1.1 A.10.1.2 A.13.2.1 A.13.2.2 A.18.1.5	
BSI-33	Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung)	KRY-02	CRY-02	CRY-04	A.10.1.1 A.13.1.1 A.13.2.3 A.14.1.2 A.14.1.3 A.18.1.5	
BSI-34	Verschlüsselung von sensiblen Daten bei der Speicherung	KRY-03	CRY-03	CRY-03	A.10.1.1 A.10.1.2 A.18.1.4	3.3.6

KRITIS	Thema	C5:2016	C5:2020	NIST	ISO 27001	TKG 2.0
BSI-35	Sichere Schlüsselverwaltung	KRY-04	CRY-04	PR.DS-5	A.10.1.2	3.3.6
BSI-36	Technische Schutzmaßnahmen	KOS-01	COS-01 COS-02	PR.AC-3 PR.AC-5 PR.PT-4 DE.AE-1	A.13.1.1 A.13.1.2 A.13.1.3 A.13.2.1	3.3.6
BSI-37	Überwachen von Verbindungen	KOS-02	COS-03	PR.PT-4 DE.CM-1	A.13.1.1 A.13.1.2 A.13.2.1	3.3.6
BSI-38	Netzwerkübergreifende Zugriffe	KOS-03	COS-04	DE.CM-1	A.13.1.2 A.13.1.3	
BSI-39	Netzwerke zur Administration	KOS-04	COS-05	PR.AC-5	A.13.1.3	
BSI-40	Dokumentation der Netztopologie	KOS-06	COS-06	PR.AC-5	A.13.1.3	
BSI-41	Richtlinien zur Datenübertragung	KOS-07	COS-07	PR.AC-5	-	
BSI-42	Vertraulichkeitserklärung	KOS-08	COS-08	ID.AM-3	A.13.2.1 A.13.2.2 A.13.2.3 A.14.1.1	
BSI-43	Richtlinien zur Entwicklung, Beschaffung von Informationssystemen	BEI-01	DEV-01	PR.IP-2	A.14.1.1 A.14.1.2 A.14.2.1 A.14.2.5 A.12.1.4	
BSI-44	Auslagerung der Entwicklung	BEI-02	DEV-02	DE.CM-6	A.14.2.7 A.14.2.8 A.14.2.9	
BSI-45	Richtlinien zur Änderung von Informationssystemen	BEI-03	DEV-03	PR.IP-3	8.1 A.14.2.2 A.14.2.3 A.14.2.4	3.3.5 3.4.2
BSI-46	Risikobewertung der Änderungen	BEI-04	DEV-05	PR.IP-3	8.1 A.14.2.2	3.4.2
BSI-47	Kategorisierung der Änderungen	BEI-05	DEV-05	PR.IP-3	8.1 A.14.2.2	3.4.2

KRITIS	Thema	C5:2016	C5:2020	NIST	ISO 27001	TKG 2.0
BSI-48	Priorisierung der Änderungen	BEI-06	DEV-05	PR.IP-3	8.1 A.14.2.2	3.4.2
BSI-49	Testen der Änderungen	BEI-07	DEV-07	PR.IP-3	A.9.4.5 A.12.1.2 A.14.2.2 A.14.2.8 A.14.2.9	3.4.2 3.7.3
BSI-50	Zurückrollen der Änderungen	BEI-08	DEV-08	PR.IP-3	7.5.3 A.12.1.2	3.4.2
BSI-51	Überprüfen von ordnungsgemäßer Testdurchführung und Genehmigung	BEI-09	DEV-09	PR.IP-3	A.12.1.2 A.14.2.2	3.4.2
BSI-52	Notfalländerungen	BEI-10	DEV-03	PR.IP-3	8.1 A.14.2.2 A.14.2.3 A.14.2.4	3.4.2 3.7.3
BSI-53	Systemlandschaft	BEI-11	DEV-10	PR.DS-7	A.12.1.4	3.7.3 3.8
BSI-54	Funktionstrennung	BEI-12	DEV-10	PR.DS-7	A.12.1.4	-
BSI-55	Richtlinien und Verfahren zur Risikominimierung des Zugriffs über mobile Endgeräte des KRITIS-Betreibers	MDM-01			A.6.2.1	3.3.1
BSI-56	Einstellung und Sicherheitsüberprüfung	HR-01	HR-01	PR.AC-6	A.7.1.1	3.2.1
BSI-57	Einstellung und Beschäftigungsvereinbarungen	HR-02	HR-02	PR.IP-11	A.7.1.2	
BSI-58	Rollenzuweisung und Vieraugenprinzip oder Funktionstrennung	IDM-01	IDM-01 PSS-08	PR.AC-4	A.9.1.1 A.9.4.1 A.9.4.2	3.3.4 3.4.2
BSI-59	Identitäts- und Berechtigungsmanagement: Benutzerregistrierung	IDM-02	IDM-02	PR.AC-2	A.9.2.2 A.9.2.3 A.9.2.6	3.3.4

KRITIS	Thema	C5:2016	C5:2020	NIST	ISO 27001	TKG 2.0
BSI-60	Identitäts- und Berechtigungsmanagement: Zugriffsberechtigung	IDM-03	IDM-03	PR.AC-1	A.9.2.2 A.9.2.6	3.3.4
BSI-61	Vergabe und Änderung (Provisionierung) von Zugriffsberechtigungen	IDM-04	IDM-04	PR.AC-1	A.9.2.3 A.9.2.6	3.3.4
BSI-62	Identitäts- und Berechtigungsmanagement: Überprüfungen	IDM-05	IDM-05	PR.AC-1	A.9.2.5	3.3.4
BSI-63	Identitäts- und Berechtigungsmanagement: Administratoren	IDM-06	IDM-06	PR.AC-4	A.6.1.2 A.9.2.3 A.12.4.3	3.3.4
BSI-64	Identitäts- und Berechtigungsmanagement: Notfallbenutzer	IDM-09	IDM-09	PR.AC-1	A.9.4.3	3.3.4
BSI-65	Festlegung notwendiger Kompetenzen (Betrieb und IT-Sicherheit)	SA-01	SP-01	ID.GV-3	A.5.1.1	
BSI-66	Überprüfung und Freigabe von Richtlinien und Anweisungen	SA-02	SP-02		A.5.1.2	
BSI-67	Abweichungen von bestehenden Richtlinien und Anweisungen	SA-03	SP-03		A.5.1.1	
BSI-68	Schulungen und Awareness	HR-03	HR-03	PR.AT-1 PR.AT-2 PR.AT-5	A.7.2.2	3.2.2 3.3.5
BSI-69	Disziplinarverfahren	HR-04	HR-04	PR.IP-11	A.7.2.3	-
BSI-70	Beendigung des Beschäftigungsverhältnisses	HR-05	HR-05	PR.IP-11	A.7.3.1	3.2.3
BSI-71	Rechenzentrumsversorgung	BCM-05	PS-02	PR.PT-5	A.17.2.1	3.3.3
BSI-72	Perimeterschutz	PS-01	PS-01	PR.IP-5	-	3.3.2

KRITIS	Thema	C5:2016	C5:2020	NIST	ISO 27001	TKG 2.0
BSI-73	Physischer Zutrittsschutz	PS-02	PS-04	PR.AC-2	A.9.2.1 A.9.2.2 A.9.2.3 A.11.1.2 A.11.1.3 A.11.1.6	3.3.2
BSI-74	Schutz vor Bedrohungen von außen	PS-03	PS-03 PS-05	DE.CM-2 ID.BE-5	A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.4	3.3.2
BSI-75	Schutz vor Unterbrechungen durch Stromausfälle und andere derartige Risiken	PS-04	PS-06	PR.DS-8 PR.IP-5	A.11.2.1 A.11.2.2 A.11.2.3 A.11.2.4 A.17.2.1	3.3.3
BSI-76	Wartung der Infrastruktur	PS-05	PS-07	PR.MA-1	A.11.1.2 A.11.2.4 A.11.2.5 A.11.2.6	3.3.2
BSI-77	Verantwortlichkeiten und Vorgehensmodell	SIM-01	SIM-01	PR.IP-8 DE.AE-4 RS.RP-1 RS.AN-2 RS.AN-4 RS.AN-5 RC.RP-1	A.16.1.1 A.16.1.2 A.16.1.4 A.16.1.5 A.16.1.6	3.5.2
BSI-78	Bearbeitung von Sicherheitsvorfällen	SIM-03	SIM-02	DE.AE-2 DE.AE-4 RS.CO-1 RS.MI-1 RS.MI-2	A.16.1.1 A.16.1.4 A.6.1.3 A.6.1.4	3.5.2
BSI-79	Dokumentation und Berichterstattung über Sicherheitsvorfälle	SIM-04	SIM-03	DE.DP-4 RS.CO-2	A.16.1.1 A.16.1.2 A.16.1.7	3.5.2 3.2.4

KRITIS	Thema	C5:2016	C5:2020	NIST	ISO 27001	TKG 2.0
BSI-80	Security Incident Event Management	SIM-05	SIM-05	DE.AE-3 RS.AN-1	A.12.4.1, A.16.1.7	3.5.1
BSI-81	Verpflichtung der Nutzer zur Meldung von Sicherheitsvorfällen an eine zentrale Stelle	SIM-06	SIM-04	RS.CO-3 RS.CO-4	A.16.1.2 A.16.1.3	3.5.3
BSI-82	Auswertung und Lernprozess	SIM-07	SIM-05	PR.IP-7 DE.DP-5 RS.IM-1 RS.IM-2 RC.IM-1 RC.IM-2	A.16.1.3 A.16.1.4 A.16.1.5 A.16.1.6	3.5.2
BSI-83	Anlassbezogene Prüfungen: Konzept	RB-17	OPS-17 OPS-20 OPS-22	PR.PT-5 ID.RA-1 PR.IP-12 ID.RA-3 DE.CM-8	A.12.1.2 A.12.6.1 A.14.2.2 A.17.2.1	
BSI-84	Umgang mit Schwachstellen, Störungen und Fehlern: Prüfung offener Schwachstellen	RB-21	OPS-21	DE.CM-8	A.12.6.1	3.7.3
BSI-85	Informieren der Unternehmensleitung	SPN-01	COM-01	DE.DP-2	A.18.1.1	
BSI-86	Interne Überprüfungen der Compliance von IT-Prozessen mit internen Informationssicherheitsrichtlinien und Standards	SPN-02	COM-02	PR.IP-7	9.2 A.12.7.1	3.7.3 3.9
BSI-87	Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen: interne IT- Prüfungen	SPN-03	COM-03 COM-04 PSS-02	PR.IP-7 ID.RA-1 DE.CM-8 RS.MI-3	9.2 9.3 A.12.7.1 A.18.2.2	3.7.3
BSI-88	Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen: Planung externer Audits	COM-02	COM-02	PR.IP-7	9.2 A.12.7.1	

KRITIS	Thema	C5:2016	C5:2020	NIST	ISO 27001	TKG 2.0
BSI-89	Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen: Durchführung externer Audits	COM-03	COM-03	PR.IP-7	9.2 9.3 A.12.7.1 A.18.2.2	
BSI-90	Systematische Log-Auswertung: Konzept	RB-10 RB-14	OPS-10 OPS-14	PR.PT-1	A.12.4.1 A.12.4.2 A.12.4.3	3.7.1
BSI-91	Systematische Log-Auswertung: kritische Assets	RB-12	OPS-12	PR.PT-1	A.12.4.1 A.12.4.2 A.12.4.3	3.7.1
BSI-92	Systematische Log-Auswertung: Aufbewahrung	RB-13	OPS-13	DE.CM-7		3.7.1
BSI-93	Systematische Log-Auswertung: Konfiguration	RB-15	OPS-15	RS.AN-3		
BSI-94	Systematische Log-Auswertung: Verfügbarkeit	RB-16	OPS-16	PR.PT-1	A.9.4.4 A.12.4.2	
BSI-95	Penetrationstest	RB-18	OPS-18	PR.IP-12 RS.MI-3	A.12.6.1	3.7.3 3.8
BSI-96	Umgang mit Schwachstellen, Störungen und Fehlern: Integration mit Änderungs- und Incident-Management	RB-19	OPS-19	ID.RA-1	A.13.1.1 A.18.2.3	
BSI-97	Kontakt zu relevanten Behörden und Interessenverbänden	OIS-05	OIS-05	ID.RA-2 RS.CO-5 RC.CO-1	A.6.1.3 A.6.1.4	
BSI-98	Richtlinie zum Umgang mit und Sicherheitsanforderungen an Dienstleister des KRITIS-Betreibers	DLL-01	SSO-01	ID.SC-1 ID.SC-3 PR.AT-3 PR.MA-2	A.15.1.1 A.15.1.2 A.15.1.3 A.7.2.2	3.1.3

KRITIS	Thema	C5:2016	C5:2020	NIST	ISO 27001	TKG 2.0
BSI-99	Kontrolle der Leistungserbringung und der Sicherheitsanforderungen an Dienstleister und Lieferanten des KRITIS-Betreibers	DLL-02	SSO-04	ID.SC-4 PR.MA-2 DE.CM-6	A.15.2.1	3.1.3
BSI-100	Einrichtung einer Kontaktstelle					3.5.3

Quelle: *Eigene Zusammenstellung, teilweise nach BSI und NIST Kreuztabellen, April 2022*

Das OpenKRITIS-Mapping ist eine Gegenüberstellung der 100 KRITIS-Anforderungen der *Konkretisierung der §8a BSIG Maßnahmen* des BSI mit fünf aktuellen Cyber Security Standards:

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

C5:2016: BSI Cloud Security Standard von 2016, auf dem die BSI Anforderungen basieren.

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

ISO 27001: Informationssicherheit der 27001 Annex A Kontrollen.

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

TKG Sicherheitskatalog 2.0: IT-Sicherheit in den Kapiteln des neuen TK-Sicherheitskatalogs.

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, Webseite BSI

NIST Cybersecurity Framework Core (XLS), NIST Version 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: 17. April 2022
Version: Draft 1.1

Impressum

Paul Weissmann c/o Insignals GmbH
Rheinwerkallee 6
53227 Bonn

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