



NIS-2, BSIG, KRITIS – Kriterienkatalog, Prüfgrundlage sowie Vorgehensweise zur Prüfung und Nachweisführung

datenschutz cert GmbH
Version 2.2

Inhaltsverzeichnis

1. Einleitung.....	4
2. Kriterienkatalog.....	5
3. Prüfgrundlage	7
4. Geltungsbereich (#Scope).....	7
5. Führung (#Führung).....	7
6. Risikoanalyse, SOA (#RA).....	7
7. Dokumentenlenkung (#Dokumentenlenkung)	8
8. KPI, Internes ISMS-Audit, Management-Bewertung (#Check)	8
9. Kontinuierlicher Verbesserungsprozess (#KVP).....	8
10. Organisation (#Organisation).....	9
11. Physische Sicherheit (#Site).....	9
12. IT (#IT).....	10
13. Personal (#HR).....	12
14. Lieferanten-/Produktsteuerung (#Einkauf).....	13
15. Threat Intelligence (#Threat-Intelligence)	13
16. Incidents, Notfälle, Krisen, BCM (#BCM).....	13
17. Compliance, Datenschutz (#Compliance).....	14
18. Systeme zur Angriffserkennung (SzA).....	14
19. Vorgehensweise zur Prüfung und Nachweisführung.....	18
20. datenschutz cert GmbH	23
21. Referenzen.....	24

Historie

Version	Datum	Geänderte Kapitel	Grund der Änderung	Geändert durch
1.0			Erstellung	Manfred Bauer Dr. Sönke Maseberg
2.0	20.01.2026	div.	Überarbeitung in Bezug auf NIS-2/BSIG	Manfred Bauer Dr. Sönke Maseberg
2.1	03.03.2026	div.	Anforderungsschärfung, Formatierung	Manfred Bauer
2.2	20.04.2026	div.	Redaktionelle Anpassungen	Manfred Bauer

1. Einleitung

- 1 Der Gesetzgeber verpflichtet im BSI-Gesetz (BSIG) „besonders wichtige Einrichtungen“ (bwE) und „wichtige Einrichtungen“ (wE) zur Einhaltung von Maßnahmen zur Informationssicherheit, was auch die Implementierung von Systemen zur Angriffserkennung (SzA) umfasst.
- 2 Zu „besonders wichtigen Einrichtungen“ zählen auch Betreiber kritischer Anlagen, die sogenannten KRITIS-Betreiber; diese müssen die Umsetzung der gesetzlichen Vorgaben in Form eines Nachweises gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) übermitteln.
- 3 Diese gesetzliche Verpflichtung betrifft zunächst Betreiber kritischer Anlagen gemäß §28 BSIG, **sofern sie die festgelegten Schwellenwerte überschreiten**, die durch die **BSI-Kritisverordnung [BSI-KritisV]** definiert sind. Diese Schwellenwerte richten sich nach **Sektor, Branche und Versorgungskapazität** der jeweiligen Anlage.
- 4 Was Betreiber kritischer Anlagen erfüllen müssen, ergibt sich direkt aus §39 Abs. 1 BSIG: Die KRITIS-Betreiber müssen
 - „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen“ ergreifen,
 - um „Störungen der
 - Verfügbarkeit,
 - Integrität,
 - Vertraulichkeit und
 - der informationstechnischen Systeme, Komponenten und Prozesse“,
 - „die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind“zu vermeiden und dem „Stand der Technik“ entsprechen.
- 5 Zudem sind Betreiber kritischer Anlagen verpflichtet, für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, Systeme zur Angriffserkennung einzusetzen (§31 Abs. 2 BSIG).
- 6 Die datenschutz cert GmbH ist bei der Deutschen Akkreditierungsstelle (DAkKS) als Zertifizierungsstelle akkreditiert und beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als IT-Sicherheitsdienstleister zertifiziert, und verfügt über Prüfer mit KRITIS-Prüfverfahrenskompetenz; damit kann die datenschutz cert GmbH die KRITIS-Prüfungen sowie die Prüfungen zu Systemen zur Angriffserkennung durchführen und Nachweise gegenüber dem BSI erbringen.
- 7 Das vorliegende Dokument enthält die Anforderungen (Kriterienkatalog) an den Betreiber kritischer Anlagen sowie Informationen zur Prüfung und Nachweisführung – inkl. der Prüfgrundlage.

2. Kriterienkatalog

- 8 Aufbauend auf §39 Abs. 1 BSIG erwartet die datenschutz cert GmbH für Betreiber kritischer Anlagen (KRITIS-Betreiber)
- ein etabliertes Informationssicherheits-Managementsystem (ISMS) gem. ISO/IEC 27001 [27001] oder ISO 27001 auf der Basis von IT-Grundschutz [IT-GS], in welches die Besonderheiten aus §31/39 BSIG berücksichtigt sind:
- Scoping
 - KRITIS-Schutzziele
 - Umgang mit Risiken
 - Maßnahmenumsetzung

Scoping

- 9 Der Geltungsbereich umfasst die betriebenen Anlagen nach BSI-KRITIS-Verordnung. Schnittstellen des Geltungsbereiches sind festgelegt.

KRITIS-Schutzziele

- 10 Im Rahmen des ISMS wurde eine Risikoanalyse erstellt. In der Risikoanalyse wird für die betriebsrelevanten Teile der jeweiligen Anlagen dem Schutzbedarf entsprechende angemessene Maßnahmen festgelegt. Schwerpunkt bei der Risikoanalyse ist das Aufrechterhalten der Versorgungssicherheit der Bevölkerung.
- 11 Im Rahmen des Risikomanagements wurden die Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität in Bezug auf die Aufrechterhaltung der kritischen Dienstleistung betrachtet.

Umgang mit Risiken

- 12 In der Risikoanalyse für das ISMS wurde als Risikobehandlungsoption nur die Risikoreduktion gewählt. Risikoakzeptanz, -transfer (Versicherung) und -ausschluss sind keine validen Risikobehandlungsoptionen, so dass alle Risiken durch entsprechende Maßnahmen auf ein angemessenes Maß reduziert werden.
- 13 Es gilt die BSI-Vorgabe: „Eine rein betriebswirtschaftliche Betrachtung der Risiken und des Schutzbedarfs ist in der Regel nicht ausreichend. Es muss insbesondere das Ausmaß eines Risikos für die Allgemeinheit, d. h. die Auswirkungen auf die Funktionsfähigkeit der Kritischen Infrastruktur und der kritischen Dienstleistung berücksichtigt werden. Bei der Maßnahmenauswahl muss auf Angemessenheit geachtet werden, also die möglichen Folgen eines Ausfalls oder einer Beeinträchtigung für die Versorgung der Allgemeinheit im Verhältnis zum Aufwand der Sicherheitsvorkehrungen betrachtet werden.“

Maßnahmenumsetzung

- 14 Alle für die Aufrechterhaltung der kritischen Dienstleistung erforderlichen Maßnahmen im Rahmen der Risikobehandlung sind umgesetzt worden.

- 15 Es gilt die BSI-Vorgabe: „die von diesen Einrichtungen nach §30 zu ergreifenden Risikomanagementmaßnahmen“ sind „umzusetzen und ihre Umsetzung zu überwachen“ (§28 Abs. 1 BSIg), und „Betreiber kritischer Anlagen haben die Umsetzung der Maßnahmen [...] frühestens drei Jahre nachdem sie erstmals oder spätestens drei Jahre nachdem sie erneut als ein Betreiber einer kritischen Anlage gelten, und anschließend alle drei Jahre [...] nachzuweisen. Die Betreiber übermitteln dem BSI die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich Angaben über die dabei aufgedeckten Sicherheitsmängel [...]“ (§39 Abs. 1 BSIg).

3. Prüfgrundlage

- 16 Nachfolgend ist die Prüfgrundlage für Prüfungen von kritischen Anlagen bei KRITIS-Betreibern beschrieben.
- 17 Die Prüfgrundlage berücksichtigt ISO/IEC 27001 [27001], den SzA-Kriterienkatalog der datenschutz cert GmbH [dsc_SzA], Grundsätzliche Anforderungen im Nachweisverfahren [GAiN], Reife- und Umsetzungsgradbewertung im Rahmen der Nachweisprüfung [RUN] sowie die aus [BSIG] abgeleiteten Anforderungen an KRITIS-Betreiber im BSIG-Kontext der besonders wichtigen Einrichtungen (bWE).

4. Geltungsbereich (#Scope)

Relevante Normanforderungen

[27001, 4.1]	Verstehen der Organisation und ihres Kontextes
[27001, 4.2]	Verstehen der Erfordernisse und Erwartungen interessierter Parteien
[27001, 4.3]	Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems
[BSI_GAIN]	Kap. 3.4 Dokumentation des Geltungsbereichs

5. Führung (#Führung)

Relevante Normanforderungen

[27001, 4.4]	Informationssicherheitsmanagementsystem
[27001, 5.1]	Führung und Verpflichtung
[27001, 5.2]	Politik
[27001, 5.3]	Rollen, Verantwortlichkeiten und Befugnisse in der Organisation
[27001, 7.1]	Ressourcen
[27001, Annex A, 5.4]	Verantwortlichkeiten der Leitung
[BSIG, § 30 Abs. 1]	Verantwortung der Einrichtung für angemessene Sicherheitsmaßnahmen

6. Risikoanalyse, SOA (#RA)

Relevante Normanforderungen

[27001, 6.1/6.1.1]	Maßnahmen zum Umgang mit Risiken und Chancen/ Allgemeines
[27001, 6.1/6.1.2]	Maßnahmen zum Umgang mit Risiken und Chancen/ Informationssicherheitsrisikobeurteilung

[27001, 6.1/6.1.3]	Maßnahmen zum Umgang mit Risiken und Chancen/ Informationssicherheitsrisikobehandlung
[27001, 6.2]	Informationssicherheitsziele und Planung zu deren Erreichung
[27001, 6.3]	Planung von Änderungen
[27001, 8.1]	Betriebliche Planung und Steuerung
[27001, 8.2]	Informationssicherheitsrisikobeurteilung
[27001, 8.3]	Informationssicherheitsrisikobehandlung
[BSIG, §30 Abs. 2 Nr. 1]	Konzepte zur Risikoanalyse und zur Sicherheit in der IT

7. Dokumentenlenkung (#Dokumentenlenkung)

Relevante Normanforderungen

[27001, 7.5/7.5.1]	Dokumentierte Information/ Allgemein
[27001, 7.5/7.5.2]	Dokumentierte Information/ Erstellen und Aktualisieren
[27001, 7.5/7.5.3]	Dokumentierte Information/ Steuerung dokumentierter Information
[BSIG, §30 Abs. 1 S. 3]	Dokumentation

8. KPI, Internes ISMS-Audit, Management-Bewertung (#Check)

Relevante Normanforderungen

[27001, 9.1]	Überwachung, Messung, Analyse und Bewertung
[27001, 9.2/9.2.1]	Internes Audit/ Allgemeines
[27001, 9.2/9.2.2]	Internes Audit/ Internes Auditprogramm
[27001, 9.3/9.3.1]	Managementbewertung/ Allgemein
[27001, 9.3/9.3.2]	Managementbewertung/ Eingaben für die Managementbewertung
[27001, 9.3/9.3.3]	Managementbewertung/ Ergebnisse der Managementbewertung
[BSIG, §30 Abs. 2 Nr. 6]	Wirksamkeitsbewertung der Maßnahmen

9. Kontinuierlicher Verbesserungsprozess (#KVP)

Relevante Normanforderungen

[27001, 10.1]	Fortlaufende Verbesserung
[27001, 10.2]	Nichtkonformität und Korrekturmaßnahmen

[BSIG, §30 Abs. 2 Nr. 6] Verbesserung der Sicherheit in der Informationstechnik

10. Organisation (#Organisation)

Relevante Normanforderungen

[27001, 7.4]	Kommunikation
[27001, Annex A, 5.1]	Informationssicherheitspolitik und -richtlinien
[27001, Annex A, 5.4]	Verantwortlichkeiten der Leitung
[27001, Annex A, 5.5]	Kontakt mit Behörden
[27001, Annex A, 5.6]	Kontakt mit speziellen Interessensgruppen
[27001, Annex A, 5.8]	Informationssicherheit im Projektmanagement
[27001, Annex A, 5.9]	Inventar der Informationen und anderen damit verbundenen Werte
[27001, Annex A, 5.10]	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten
[27001, Annex A, 5.12]	Klassifizierung von Informationen
[27001, Annex A, 5.13]	Kennzeichnung von Informationen
[27001, Annex A, 5.14]	Informationsübermittlung
[27001, Annex A, 5.35]	Unabhängige Überprüfung der Informationssicherheit
[27001, Annex A, 5.37]	Dokumentierte Betriebsabläufe
[27001, Annex A, 6.8]	Meldung von Informationssicherheitsereignissen
[BSIG, §30 Abs. 1, 2 Nr. 1/12.1]	Organisatorische Maßnahmen, Werteklassifizierung

11. Physische Sicherheit (#Site)

Relevante Normanforderungen

[27001, Annex A, 5.13]	Kennzeichnung von Informationen
[27001, Annex A, 5.15]	Zugangssteuerung
[27001, Annex A, 7.1]	Physische Sicherheitsperimeter
[27001, Annex A, 7.2]	Physischer Zutritt
[27001, Annex A, 7.3]	Sichern von Büros, Räumen und Einrichtungen
[27001, Annex A, 7.4]	Physische Sicherheitsüberwachung
[27001, Annex A, 7.5]	Schutz vor physischen und umweltbedingten Bedrohungen
[27001, Annex A, 7.6]	Arbeiten in Sicherheitsbereichen

[27001, Annex A, 7.7]	Aufgeräumte Arbeitsumgebung und Bildschirmsperren
[27001, Annex A, 7.8]	Platzierung und Schutz von Geräten und Betriebsmitteln
[27001, Annex A, 7.9]	Sicherheit von Werten außerhalb der Räumlichkeiten
[27001, Annex A, 7.10]	Speichermedien
[27001, Annex A, 7.11]	Versorgungseinrichtungen
[27001, Annex A, 7.12]	Sicherheit der Verkabelung
[27001, Annex A, 7.13]	Instandhaltung von Geräten und Betriebsmitteln
[27001, Annex A, 7.14]	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln
[BSIG, §30 Abs. 2 Nr. 3]	Betriebskontinuität, inkl. Physischer Schutz von IT-/OT-Infrastruktur

12. IT (#IT)

Relevante Normanforderungen

12.1.1. Rollen und Rechte

[27001, Annex A, 5.3]	Aufgabentrennung
[27001, Annex A, 5.14]	Informationsübermittlung
[27001, Annex A, 5.15]	Zugangssteuerung
[27001, Annex A, 5.16]	Identitätsmanagement
[27001, Annex A, 5.17]	Authentisierungsinformationen
[27001, Annex A, 5.18]	Zugangsrechte
[27001, Annex A, 5.33]	Schutz von Aufzeichnungen
[27001, Annex A, 8.1]	Endpunktgeräte des Benutzers
[27001, Annex A, 8.2]	Privilegierte Zugangsrechte
[27001, Annex A, 8.3]	Informationszugangsbeschränkung
[27001, Annex A, 8.4]	Zugriff auf den Quellcode
[27001, Annex A, 8.5]	Sichere Authentisierung
[BSIG, §30 Abs. 2 Nr. 9 f.]	Zugriffskontrollen, MFA, sichere Kommunikation

12.1.2. IT-Betrieb

[27001, Annex A, 8.6]	Kapazitätssteuerung
[27001, Annex A, 8.7]	Schutz gegen Schadsoftware
[27001, Annex A, 8.8]	Handhabung von technischen Schwachstellen

[27001, Annex A, 8.9]	Konfigurationsmanagement
[27001, Annex A, 8.10]	Löschung von Informationen
[27001, Annex A, 8.11]	Datenmaskierung
[27001, Annex A, 8.12]	Verhinderung von Datenlecks
[27001, Annex A, 8.13]	Sicherung von Informationen
[27001, Annex A, 8.14]	Redundanz von informationsverarbeitenden Einrichtungen
[27001, Annex A, 8.15]	Protokollierung
[27001, Annex A, 8.16]	Überwachung von Aktivitäten
[27001, Annex A, 8.17]	Uhrensynchronisation
[27001, Annex A, 8.18]	Gebrauch von Hilfsprogrammen mit privilegierten Rechten
[27001, Annex A, 8.19]	Installation von Software auf Systemen im Betrieb
[BSIG, §30 Abs. 2 Nr. 2]	Bewältigung von Sicherheitsvorfällen (Monitoring, Logging, Reaktion)
[BSIG, §30 Abs. 2 Nr. 3]	Betriebskontinuität / Backup
[BSIG, §30 Abs. 2 Nr. 5/6]	Schwachstellen-, Patchmanagement

12.1.3. Netzwerk

[27001, Annex A, 8.20]	Netzwerksicherheit
[27001, Annex A, 8.21]	Sicherheit von Netzwerkdiensten
[27001, Annex A, 8.22]	Trennung von Netzwerken
[27001, Annex A, 8.23]	Webfilterung
[BSIG, §30 Abs. 2 Nr. 2,3, 7, 9-10]	Netz- und Kommunikationssicherheit

12.1.4. Kryptographie

[27001, Annex A, 8.24]	Verwendung von Kryptographie
[BSIG, §30 Abs. 2 Nr. 8]	Kryptografie

12.1.5. Entwicklung, Wartung, Konfiguration

[27001, Annex A, 8.25]	Lebenszyklus einer sicheren Entwicklung
[27001, Annex A, 8.26]	Anforderungen an die Anwendungssicherheit
[27001, Annex A, 8.27]	Sichere Systemarchitektur und Entwicklungsgrundsätze
[27001, Annex A, 8.28]	Sichere Codierung
[27001, Annex A, 8.29]	Sicherheitsprüfung bei Entwicklung und Abnahme

[27001, Annex A, 8.30]	Ausgegliederte Entwicklung
[27001, Annex A, 8.31]	Trennung von Entwicklungs-, Test- und Produktionsumgebungen
[BSIG, §30 Abs. 2 Nr. 4/5]	Lieferkette, Erwerb/Entwicklung/Wartung von IKT-Systemen

12.1.6. Change Management

[27001, Annex A, 8.32]	Änderungssteuerung
[27001, Annex A, 8.33]	Testdaten
[27001, Annex A, 8.34]	Schutz der Informationssysteme während Tests im Rahmen von Audits
[BSIG, §30 Abs. 2 Nr. 2-3, 5]	Änderungen, Betriebskontinuität/Wiederanlauf, Wartung

13. Personal (#HR)

Relevante Normanforderungen

[27001, 7.2]	Kompetenz
[27001, 7.3]	Bewusstsein
[27001, Annex A, 5.2]	Informationssicherheitsrollen und -verantwortlichkeiten
[27001, Annex A, 5.3]	Aufgabentrennung
[27001, Annex A, 5.4]	Verantwortlichkeiten der Leitung
[27001, Annex A, 5.11]	Rückgabe von Werten
[27001, Annex A, 5.15]	Zugangssteuerung
[27001, Annex A, 5.16]	Identitätsmanagement
[27001, Annex A, 5.17]	Authentisierungsinformationen
[27001, Annex A, 5.18]	Zugangsrechte
[27001, Annex A, 6.1]	Sicherheitsüberprüfung
[27001, Annex A, 6.2]	Beschäftigungs- und Vertragsbedingungen
[27001, Annex A, 6.3]	Informationssicherheits-, bewusstsein, -ausbildung und -schulung
[27001, Annex A, 6.4]	Maßregelungsprozess
[27001, Annex A, 6.5]	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung
[27001, Annex A, 6.6]	Vertraulichkeits- oder Geheimhaltungsvereinbarungen

[27001, Annex A, 6.7]	Remote-Arbeit
[BSIG, §30 Abs. 2 Nr. 7]	Cyberhygiene, Schulung, Sensibilisierung

14. Lieferanten-/Produktsteuerung (#Einkauf)

Relevante Normanforderungen

[27001, Annex A, 5.19]	Informationssicherheit in Lieferantenbeziehungen
[27001, Annex A, 5.20]	Behandlung von Informationssicherheit in Lieferantenvereinbarungen
[27001, Annex A, 5.21]	Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)
[27001, Annex A, 5.22]	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
[27001, Annex A, 5.23]	Informationssicherheit für die Nutzung von Cloud-Diensten
[BSIG, §30 Abs. 2 Nr. 4]	Sicherheit der Lieferkette
[BSIG, §30 Abs. 2 Nr. 5, Abs. 6]	Sicherheitsanforderungen beim Erwerb/Entwicklung/Wartung, mögliche Pflicht zur Nutzung EU-zertifizierter IKT

15. Threat Intelligence (#Threat-Intelligence)

Relevante Normanforderungen

[27001, Annex A, 5.7]	Informationen über die Bedrohungslage
[BSIG, §30 Abs. 2 Nr. 7]	Cyberhygiene und Awareness, inkl. Nutzung von Informationen zur Bedrohungslage

16. Incidents, Notfälle, Krisen, BCM (#BCM)

Relevante Normanforderungen

[27001, Annex A, 5.24]	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
[27001, Annex A, 5.25]	Beurteilung und Entscheidung über Informationssicherheitsereignisse
[27001, Annex A, 5.26]	Reaktion auf Informationssicherheitsvorfälle
[27001, Annex A, 5.27]	Erkenntnisse aus Informationssicherheitsvorfällen
[27001, Annex A, 5.28]	Sammeln von Beweismaterial
[27001, Annex A, 5.29]	Informationssicherheit bei Störungen
[27001, Annex A, 5.30]	IKT-Bereitschaft für Business-Continuity

[BSIG, §30 Abs. 2 Nr. 2]	Bewältigung von Sicherheitsvorfällen
[BSIG, §30 Abs. 2 Nr. 3]	Aufrechterhaltung des Betriebs

17. Compliance, Datenschutz (#Compliance)

Relevante Normanforderungen

[27001, Annex A, 5.31]	Juristische, gesetzliche, regulatorische und vertragliche Anforderungen
[27001, Annex A, 5.32]	Geistige Eigentumsrechte
[27001, Annex A, 5.34]	Datenschutz und Schutz von personenbezogenen Daten (PbD)
[27001, Annex A, 5.36]	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
[27001, Annex A, 8.10]	Löschung von Informationen
[27001, Annex A, 8.11]	Datenmaskierung
[27001, Annex A, 8.12]	Verhinderung von Datenlecks
[BSIG, §30 Abs. 1]	Einhaltung angemessener Sicherheitsmaßnahmen („Stand der Technik“)

18. Systeme zur Angriffserkennung (SzA)

18.1. Protokollierung

Planung der Protokollierung

[dsc_SzA, SzA-01]	Risikoanalyse
[dsc_SzA, SzA-02]	Protokoll- und Protokollierungsdaten
[dsc_SzA, SzA-03]	Relevante Systeme
[dsc_SzA, SzA-04]	Modernisierungsaufforderung
[dsc_SzA, SzA-05]	Kapazitätsabschätzung
[dsc_SzA, SzA-06]	Dokumentation der Planung
[dsc_SzA, SzA-07]	Change Prozess

Umsetzung der Protokollierung

[dsc_SzA, SzA-08]	OPS.1.1.5.A1 Erstellung einer Sicherheitsrichtlinie für die Protokollierung
[dsc_SzA, SzA-09]	OPS.1.1.5.A3 Konfiguration der Protokollierung auf System- und Netzebene
[dsc_SzA, SzA-10]	OPS.1.1.5.A4 Zeitsynchronisation der IT-Systeme

[dsc_SzA, SzA-11]	OPS.1.1.5.A5 Einhaltung rechtlicher Rahmenbedingungen
[dsc_SzA, SzA-12]	Aufbau einer zentralen Protokollierungsinfrastruktur
[dsc_SzA, SzA-13]	Bereitstellung von Protokollierungsdaten für die Auswertung
[dsc_SzA, SzA-14]	Priorisierung der Protokollierungsdatenquellen
[dsc_SzA, SzA-15]	(gelöscht)
[dsc_SzA, SzA-16]	Check Umsetzung vs. Planung
[dsc_SzA, SzA-17]	Branchenspezifische Anforderungen

18.2. Detektion

Planung der Detektion

[dsc_SzA, SzA-18]	Abdeckung der Bedrohungslandschaft
-------------------	------------------------------------

Umsetzung der Detektion

[dsc_SzA, SzA-19]	DER.1.A1 Erstellung einer Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen
[dsc_SzA, SzA-20]	DER.1.A2 Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokollierungsdaten
[dsc_SzA, SzA-21]	DER.1.A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse
[dsc_SzA, SzA-22]	DER.1.A4 Sensibilisierung der Mitarbeiter
[dsc_SzA, SzA-23]	DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion
[dsc_SzA, SzA-24]	Kontinuierliche Überwachung und Auswertung von Protokoll- und Protokollierungsdaten
[dsc_SzA, SzA-25]	Einsatz zusätzlicher Detektionssysteme
[dsc_SzA, SzA-26]	Infrastruktur zur Auswertung von Protokoll- und Protokollierungsdaten und Prüfung sicherheitsrelevanter Ereignisse
[dsc_SzA, SzA-27]	Auswertung von Informationen aus externen Quellen
[dsc_SzA, SzA-28]	Auswertung der Protokoll- und Protokollierungsdaten durch spezialisiertes Personal
[dsc_SzA, SzA-29]	Zentrale Detektion und Echtzeitüberprüfungen von Ereignismeldungen
[dsc_SzA, SzA-30]	Stand der Technik

[dsc_SzA, SzA-31]	Kalibrierung
[dsc_SzA, SzA-32]	Bewertung
[dsc_SzA, SzA-33]	Branchenspezifische Anforderungen

18.3. Reaktion

[dsc_SzA, SzA-34]	DER.2.1.A1 Definition eines Sicherheitsvorfalls
[dsc_SzA, SzA-35]	DER.2.1.A2 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen
[dsc_SzA, SzA-36]	DER.2.1.A3 Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen
[dsc_SzA, SzA-37]	DER.2.1.A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen
[dsc_SzA, SzA-38]	DER.2.1.A5 Behebung von Sicherheitsvorfällen
[dsc_SzA, SzA-39]	DER.2.1.A6 Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen
[dsc_SzA, SzA-40]	DER.2.1.A7 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen
[dsc_SzA, SzA-41]	DER.2.1.A8 Aufbau von Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen
[dsc_SzA, SzA-42]	DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle
[dsc_SzA, SzA-43]	DER.2.1.A10 Eindämmen der Auswirkung von Sicherheitsvorfällen
[dsc_SzA, SzA-44]	DER.2.1.A11 Einstufung von Sicherheitsvorfällen
[dsc_SzA, SzA-45]	DER.2.1.A12 Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung
[dsc_SzA, SzA-46]	DER.2.1.A13 Einbindung in das Sicherheits- und Notfallmanagement
[dsc_SzA, SzA-47]	DER.2.1.A14 Eskalationsstrategie für Sicherheitsvorfälle
[dsc_SzA, SzA-48]	DER.2.1.A15 Schulung der Mitarbeiter des Service Desk
[dsc_SzA, SzA-49]	DER.2.1.A16 Dokumentation der Behebung von Sicherheitsvorfällen
[dsc_SzA, SzA-50]	DER.2.1.A17 Nachbereitung von Sicherheitsvorfällen
[dsc_SzA, SzA-51]	DER.2.1.A18 Weiterentwicklung der Prozesse durch Erkenntnisse aus Sicherheitsvorfällen und Branchenentwicklungen

[dsc_SzA, SzA-52]	Automatische Reaktion auf sicherheitsrelevante Ereignisse
[dsc_SzA, SzA-53]	Behandlung
[dsc_SzA, SzA-54]	Meldepflichten
[dsc_SzA, SzA-55]	Automatisierte Maßnahmen
[dsc_SzA, SzA-56]	Manuelle Maßnahmen

19. Vorgehensweise zur Prüfung und Nachweisführung

- 18 Die Prüfung wird in Form eines Audits sowie einer technischen Prüfung durchgeführt. Die Prüfung spaltet sich auf in
- Vorbereitung
 - Dokumentenprüfung
 - Site Visit
 - Nachbereitung inkl. BSI-Nachweis

19.1. Vorbereitung

- 19 Im Rahmen der Vorbereitung stellt der KRITIS-Betreiber dem Prüfteam die benötigten Referenzdokumente zur Verfügung – dies umfasst
- eine Darstellung des Geltungsbereiches mit Detailinformationen zu Netzstruktur und IT-Systemen, insb. Netzstrukturplan
 - die Umsetzungsdokumentation zu allen Anforderungselementen des Kriterienkatalogs
 - alle relevanten Richtlinien und Prozessbeschreibungen

19.2. Dokumentenprüfung

- 20 Die Dokumentenprüfung besteht aus einer Sichtung der Referenzdokumente.
- 21 Ziel ist es, den Geltungsbereich und den Umfang der IT-Infrastruktur kennenzulernen und Ihre Umsetzung der normativen Vorgaben einzuschätzen. Dazu werden stichpunktartig Aspekte des Kriterienkatalogs geprüft.

19.3. Site Visit

- 22 Das Ziel des Site Visits ist es, die Umsetzung einschließlich der Wirksamkeit Ihrer Systeme zur Angriffserkennung hinsichtlich der Vorgaben zu beurteilen.
- 23 Dazu prüft das Prüfteam zu jedem Anforderungselement des Kriterienkatalogs
- Ihre Umsetzungsbeschreibung sowie
 - die Wirksamkeit der beschriebenen Maßnahmen in der Realität,
- und dokumentiert die Ergebnisse der Prüfung in einem Report.

19.4. Bewertung

- 24 Die Bewertung der Prüfung durch den Prüfer erfolgt konform zur Orientierungshilfe zu Systemen zur Angriffserkennung [BSI_SzA] sowie der Orientierungshilfe zu Nachweisen gemäß §8a BSIg [BSI_8a] sowie:
- 1: Anforderungen der Prüfgrundlage sind erfüllt;
 - 2: Empfehlung: Eine „Empfehlung“ stellt einen Verbesserungshinweis dar. Durch die Umsetzung der Empfehlung kann die Sicherheit erhöht werden.

- 3: Geringfügige/r Abweichung/Sicherheitsmangel: Eine „geringfügige Abweichung“ stellt eine Gefährdung bzw. ein Risiko dar. Es besteht kein akuter Handlungsbedarf.
 - 4: Schwerwiegende/r oder erhebliche/r Abweichung/Sicherheitsmangel: Eine „schwerwiegende Abweichung“ stellt eine gravierende Gefährdung bzw. ein gravierendes Risiko dar. Eine „erhebliche Abweichung“ stellt eine große Gefährdung bzw. ein großes Risiko dar.
- 25 Zusätzlich erfolgt die Bewertung des Reife-/Umsetzungsgrads; die [BSI_SzA] und [BSI_RUN] sieht die Bewertung nach dem folgenden Reife-/Umsetzungsgradmodellen vor.
- 26 RUN definiert jeweils fünf Reifegrade und fünf Umsetzungsgrade, um die Reife von Managementsystemen und den Umsetzungsstand von Maßnahmen durch Prüfer bewerten zu lassen:

Grad	Reifegrad ISMS, BCMS	Umsetzungsgrad Annex-Maßnahmen	Umsetzungsgrad SzA
1	Geplant	Ohne Maßnahmenumsetzung	Geplant, ohne Maßnahmenumsetzung
2	Gesteuert	Einzelmaßnahmen, Teildurchführung	Einzelmaßnahmen, Teildurchführung MUSS
3	Etabliert	Maßnahmen umgesetzt, Prozessdurchführung	MUSS-Maßnahmen umgesetzt, SOLLTE teilweise geprüft, KVP in Planung/etabliert
4	Messbar	3, plus Messbarkeit	3, plus SOLLTE erfüllt/ausgeschlossen, KVP etabliert
5	Kontinuierlich verbessert	4, plus Verbesserung	4, plus KANN erfüllt/ausgeschlossen, zusätzliche Maßnahmen

- 27 Reifegrade – Informationssicherheit (ISMS)
- o. ISMS ist geplant, Grundlagen fehlen oder sind nur teilweise vorhanden (Geltungsbereich, Risikomanagement, Dokumentensteuerung, Audits)
 1. ISMS ist gesteuert, teilweise etablierter Prozess (Geltungsbereich, Strategie und Vorgaben, Risikoanalysen, Steuerung)
 2. ISMS ist etabliert, vollständige Prozesse (integrierter Prozess mit Schnittstellen, Organisation, Abhängigkeiten)

3. ISMS ist messbar, Standardprozesse mit Kennzahlen (vollständig etabliert, Wirksamkeitsmessung, KPIs und Überwachung)
 4. ISMS wird verbessert, Prozesse mit umgesetzten Verbesserungen (kontinuierliche Weiterentwicklung mit Zielen, Verbesserungen, Revisionen)
- 28 Reifegrade – Business Continuity (BCMS)
1. BCMS ist geplant, unvollständige Abdeckung und Prozesse (Aufbau des Themenbereichs ist geplant, wenig bis keine Festlegungen)
 2. BCMS ist gesteuert, teilweise etablierter Prozess (Schnittstellen ISMS, Aufrechterhaltung, Krisenmanagement, Pläne)
 3. BCMS ist etabliert, vollständige Prozesse (integrierter Standardprozess, Nachweise, BC-Risiken, Notfallpläne)
 4. BCMS ist messbar, Standardprozesse mit Kennzahlen (vollständig etabliert, Wirksamkeit Pläne, Tests und Überwachung)
 5. BCMS wird verbessert, Prozesse mit umgesetzten Verbesserungen (kontinuierliche Weiterentwicklung, verbesserte Aufrechterhaltung, Revisionen)

Annex-Controls

- 29 Bei technischen und organisatorischen Maßnahmen müssen Umsetzungsgrade (vgl. Kap. 5.2 von [BSI_RUN]) bewertet werden, die sich an die Umsetzungsgrade der Angriffserkennung (SzA) anlehnen. RUN legt dafür fachliche Themenbereiche fest, die sich auf die Konkretisierung der Anforderungen beziehen.
- 30 Grundlage der Prüfung sind
- Organisatorische Maßnahmen (OrgM)
 - Personenbezogene Maßnahmen (PersM)
 - Physische Maßnahmen (PhyM)
 - Technische Maßnahmen (TecM)
- 31 Umsetzungsgrade – Annex-Controls:
1. Dieser Umsetzungsgrad besteht bei einem Zustand ohne bisher erfolgte Maßnahmenumsetzung. Es ist lediglich die Planung einer Maßnahme oder eines Prozesses vorhanden.
 2. Dieser Umsetzungsgrad besteht, wenn solche Maßnahmen umgesetzt worden sind, die gemeinsam nur einen Teil eines Prozesses oder eines Managementsystems darstellen. Es handelt sich um Einzelmaßnahmen, die zu einem Verbund von Maßnahmen gehören oder die nur einen Teil der Durchführung eines Prozesses darstellen. Typischerweise gehören hierzu Regelungen, Leitlinien, Strategien, aber auch einzelne technische Maßnahmen.
 3. Dieser Umsetzungsgrad besteht, wenn solche Maßnahmen umgesetzt worden sind, welche die Durchführung eines gesamten Prozesses oder eines Managementsystems (Asset Management, Incident Management, Continuity Management, etc.) betreffen. Maßnahmen des Umsetzungsgrades 2 stellen in der Regel einen Teilaspekt dar und müssen daher notwendigerweise erfüllt sein, damit der Umsetzungsgrad 3 erreicht werden kann.

4. Dieser Umsetzungsgrad besteht, wenn weiterhin solche Maßnahmen umgesetzt worden sind, die sich primär auf die Überprüfung und die Messbarkeit der Durchführung von Standardprozessen und Managementsystemen beziehen. Umsetzungsgrad 3 muss notwendigerweise zuerst erfüllt sein, damit eine Durchführung gemessen und bewertet werden kann.
 5. Dieser Umsetzungsgrad besteht, wenn weiterhin solche Maßnahmen umgesetzt worden sind, die sich primär auf die Verbesserung der Durchführung von Maßnahmen, Prozessen und Managementsystemen beziehen. Die Verbesserungen ergeben sich i. d. R. erst aus den gemessenen Ergebnissen oder Überprüfungen der Maßnahmen des Umsetzungsgrades 4. Damit ist Umsetzungsgrad 4 eine notwendige Voraussetzung zur Erreichung des Umsetzungsgrades 5.
- 32 Umsetzungsgrad – Systeme zur Angriffserkennung:
0. Es sind bisher keine Anforderungen umgesetzt und es bestehen auch keine Planungen zur Umsetzung von Anforderungen.
 1. Es bestehen Planungen zur Umsetzung von Anforderungen, jedoch für mindestens einen Bereich noch keine konkreten Umsetzungen.
 2. In allen Bereichen wurde mit der Umsetzung von Anforderungen begonnen. Es sind noch nicht alle MUSS-Anforderungen umgesetzt worden.
 3. Alle MUSS-Anforderungen wurden für alle Bereiche umgesetzt. Idealerweise wurden SOLLTE-Anforderungen hinsichtlich ihrer Notwendigkeit und Umsetzbarkeit geprüft. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.
 4. Alle MUSS-Anforderungen wurden für alle Bereiche umgesetzt. Alle SOLLTE-Anforderungen wurden umgesetzt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.
 5. Alle MUSS-Anforderungen wurden für alle Bereiche umgesetzt. Alle SOLLTE-Anforderungen und KANN-Anforderungen wurden für alle Bereiche umgesetzt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Für alle Bereiche wurden sinnvolle zusätzliche Maßnahmen entsprechend der Risikoanalyse / Schutzbedarfsfeststellung identifiziert und umgesetzt. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.

19.5. Nachbereitung

- 33 Das Ergebnis der Prüfung wird dokumentiert.
- 34 Zudem wird der BSI-Nachweis von der Zertifizierungsstelle der datenschutz cert GmbH erzeugt, zur Vorlage beim BSI.

19.6. Kontinuität und Laufzeit

- 35 Informationssicherheit nach Stand der Technik setzt insbesondere ein Informationssicherheits-Managementsystem (ISMS) voraus.
- 36 Unser Modell zur Nachweisführung setzt auf Kontinuität und Transparenz:
 - Die Prüfung erfolgt alle zwei Jahre.

- Nach der Prüfung erhalten Sie den BSI-Nachweis gemäß der gesetzlichen Vorgaben sowie einen detaillierten Bericht, auf den Sie bei behördlichen Nachfragen referenzieren und unabhängig bestätigt die konkrete Umsetzung aller Anforderungen der Orientierungshilfe nachweisen können.

20. datenschutz cert GmbH

20.1. Was wir tun

- 37 Die datenschutz cert GmbH bietet Konformitätsbewertungen auf dem Gebiet des Datenschutzes und der Informationssicherheit an. Diese Konformitätsbewertungen schließen sowohl Prüfaktivitäten als auch Zertifizierungstätigkeiten ein – einerseits für IT-Systeme und -Produkte und andererseits für Verfahren und Managementprozesse.
- 38 Die datenschutz cert GmbH ist ein Unternehmen der DSN GROUP. Sitz der Gesellschaft ist Bremen. Geschäftsführer ist Dr. Sönke Maseberg. Die Unternehmen der DSN GROUP sind inhabergeführt.

20.2. Unsere Anerkennungen und Akkreditierungen

- 39 Die datenschutz cert GmbH ist bei der Deutschen Akkreditierungsstelle GmbH (DAkkS) zu folgenden Regelwerken akkreditiert:
- ISO/IEC 27001 für Informationssicherheits-Managementsysteme (ISMS)
 - „IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG“ für Strom- und Gasnetzbetreiber
 - „IT-Sicherheitskatalog gemäß § 11 Abs. 1b EnWG“ für Energieanlagenbetreiber
 - ISO/IEC 27701 für Datenschutz-Managementsysteme (DSMS)
 - eIDAS für Vertrauensdiensteanbieter
 - „ips-VSS-IT“ für Videosprechstunden
 - Zertifizierungsstandard ‚DSGVO – information privacy standard‘ gem. Art. 42 DSGVO
- 40 Auditoren der datenschutz cert GmbH sind beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als Auditoren für die TR-03109-6 (Smart Meter Gateway Administratoren) sowie BSI TR-03145 (Secure CA Operation) zertifiziert.
- 41 Die datenschutz cert GmbH ist als Prüfstelle für IT-Sicherheit und IT-Sicherheitsdienstleister beim Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannt.
- 42 Die datenschutz cert GmbH beschäftigt beim BSI lizenzierte IT-Grundschutz-Auditoren und IS-Revisoren. Die datenschutz cert GmbH stellt eines der beiden GS-Zertlabs, die für das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Prüfbegleitung in den IT-Grundschutz-Verfahren durchführt.
- 43 Die datenschutz cert GmbH ist bei der Bundesnetzagentur anerkannte Zertifizierungsstelle nach eIDAS gem. Vertrauensdienstegesetz (VDG).
- 44 Aufgrund der Akkreditierung bei der DAkkS und der Anerkennung beim BSI darf die datenschutz cert GmbH im Kontext von §8a BSIG/KRITIS-VO-Verfahren die Rolle der „prüfenden Stelle“ einnehmen. Ferner sind die Auditoren der datenschutz cert GmbH beim BSI als Prüfer für § 8a BSIG anerkannt; dies umfasst auch die Prüfung von Systemen zur Angriffserkennung (SzA).

21. Referenzen

- [27001] ISO/IEC 27001:2022, „Information security, cybersecurity and privacy protection – Information security management systems – Requirements“, ISO/IEC 27001, third edition 2022-10.
 DIN EN ISO/IEC 27001:2024-01, "Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2022)"; Deutsche Fassung EN ISO/IEC 27001:2023
- [BSIG] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz - BSIG), 02.12.2025.
- [BSI_KritisV] Bundesamt für Sicherheit in der Informationstechnik „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ (BSI-Kritisverordnung – BSI-KritisV) 22.04.2016 Zuletzt geändert durch Art. 2 G v. 18.12.2025 I Nr. 347.
- [BSI_Konkr] Bundesamt für Sicherheit in der Informationstechnik, „Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“, Version 1.2, 10.09.2024.
- [BSI_GAIN] Bundesamt für Sicherheit in der Informationstechnik (BSI) „Anforderungen nach § 8a Absatz 5 BSIG“, „Grundsätzliche Anforderungen im Nachweisverfahren (GAiN)“, Version 2.1, 24.03.2025.
- [BSI_RUN] Bundesamt für Sicherheit in der Informationstechnik (BSI) „Reife- und Umsetzungsgrad-bewertung im Rahmen der Nachweisprüfung (RUN)“, Version 1.0, 09.01.2025.
- [BSI_SzA] Bundesamt für Sicherheit in der Informationstechnik (BSI) „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“, Version 1.1, 18.11.2024
- [dsc_SzA] datenschutz cert GmbH, „Systeme zur Angriffserkennung – Kriterienkatalog und Vorgehensweise zur Prüfung und Nachweisführung“, Version 1.6, 10.03.2025.