

KRITIS-Dachgesetz & BSI-Begleitdokument

Pflichtdokumente und Nachweise — Übersicht aller gesetzlichen Anforderungen

8 Risikobereiche	20 Pflichtdokumente	2 Rechtsquellen
---------------------	------------------------	--------------------

§ 11 Abs. 1 — Resilienzmaßnahmen — Allgemeine Pflicht

Betreiber kritischer Anlagen müssen geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen ergreifen, um die Resilienz zu gewährleisten.

Erforderliche Dokumente & Nachweise:

ID	Dokument	Klasse	Frist
RA-ORG-01	Schutzkonzept / Leitlinie	Richtlinie	—
RA-ORG-02	GF-Beauftragungsschreiben	Nachweis	—
RA-ORG-03	Risikobewertungsmethodik & Matrix	Richtlinie	—

§ 11 Abs. 1 Nr. 2 — Technische Sicherheit (IT/OT)

Maßnahmen zur Bewältigung der Risiken für die Sicherheit der Netz- und Informationssysteme, die für die Erbringung der kritischen Dienstleistung genutzt werden.

Erforderliche Dokumente & Nachweise:

ID	Dokument	Klasse	Frist
RA-TECH-01	Asset-Register mit Kritikalitätsstufen	Analyse	—
RA-TECH-02	Schwachstellenregister (max. 90 Tage)	Analyse	Aktualisierung alle 90 Tage
RA-TECH-03	Patch-Management-Verfahren	Prozess	—

§ 11 Abs. 1 Nr. 3 — Physische Sicherheit

Physische Schutzmaßnahmen einschließlich Perimeterschutz, Zutrittskontrollsysteme und Videoüberwachung.

Erforderliche Dokumente & Nachweise:

ID	Dokument	Klasse	Frist
RA-PHY-01	Physisches Schutzkonzept	Richtlinie	—
RA-PHY-02	Zutrittsprotokoll	Nachweis	—

§ 11 Abs. 1 Nr. 4 — Lieferkette & Dritte

Sicherstellung der Resilienz in der Lieferkette, einschließlich vertraglicher Sicherheitsanforderungen an Dienstleister und Zulieferer.

Erforderliche Dokumente & Nachweise:

ID	Dokument	Klasse	Frist
RA-SUP-01	Lieferanten-Risikobewertung	Analyse	—
RA-SUP-02	Dienstleistersteuerungskonzept	Richtlinie	—

§ 11 Abs. 1 Nr. 5 — Personal & Awareness

Personalüberprüfung, Sicherheitsüberprüfungen und Schulungsprogramme für Mitarbeitende in sicherheitsrelevanten Bereichen.

Erforderliche Dokumente & Nachweise:

ID	Dokument	Klasse	Frist
RA-PER-01	Personalüberprüfungskonzept	Richtlinie	—
RA-PER-02	Schulungsbelege	Nachweis	Jährlich

§ 13 — Business Continuity

Erstellung eines Resilienzplans mit Business Impact Analyse und Notfall- & Wiederanlaufplanung.

Erforderliche Dokumente & Nachweise:

ID	Dokument	Klasse	Frist
RA-BC-01	BIA-Bericht	Analyse	—
RA-BC-02	BCM-Konzept & Resilienzplan	Richtlinie	10 Monate nach Registrierung
RA-BC-03	Übungsprotokoll	Nachweis	Jährlich

§ 14 — Meldepflichten bei Sicherheitsvorfällen

Erhebliche Sicherheitsvorfälle müssen dem BSI gemeldet werden: Erstmeldung ≤ 24 Stunden, Detailmeldung ≤ 72 Stunden nach Feststellung.

Erforderliche Dokumente & Nachweise:

ID	Dokument	Klasse	Frist
RA-INC-01	Incident-Response-Verfahren	Prozess	—
RA-INC-02	BSI-Meldeprozess (§ 14)	Prozess	Erstmeldung ≤ 24h
RA-INC-03	Schwellwert-Definition	Richtlinie	—

BSI TR-02102 / CON-Bausteine — Kryptographie & Datenschutz

Anforderungen an Verschlüsselung, Schlüsselmanagement und Datensicherung gemäß BSI-Technischen Richtlinien.

Erforderliche Dokumente & Nachweise:

ID	Dokument	Klasse	Frist
RA-KRY-01	Kryptokonzept (BSI TR-02102)	Richtlinie	—
RA-KRY-02	Schlüsselmanagement-Verfahren	Prozess	—

Quellen: KRITIS-Dachgesetz (gesetze-im-internet.de/kritisg) · BSI-Begleitdokument (bsi.bund.de)
Erstellt mit KRITIS Compass · kritis-compass.de