NIS2-Checkliste zu § 30 und § 32 BSIG

Hinweis
Eine Zeile je Anforderung. Tragen Sie den Status (offen / teilweise / erfüllt / nicht anwendbar), Ihren Nachweis, die verantwortliche Person und einen Termin ein. Ob und in welcher Stufe Ihr Unternehmen unter NIS2 fällt, klären Sie vorab, etwa mit dem kostenlosen Betroffenheitscheck auf complass.eu.

§ 30 Abs. 2 BSIG: Mindestmaßnahmen des Risikomanagements

lit. a / Nr. 1 – Risikoanalyse und Sicherheitskonzepte

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
1	Informationssicherheitsleitlinie gebilligt Art. 21 Abs. 2 lit. a NIS2; § 30 Abs. 2 Nr. 1 BSIG	Von der Geschäftsleitung unterzeichnete Leitlinie mit Zielen, Geltungsbereich und Verantwortung; allen Beschäftigten bekannt gemacht.		
2	Asset-Inventar IT und OT Art. 21 Abs. 2 lit. a NIS2; § 30 Abs. 2 Nr. 1 BSIG	Prozesse, Systeme, OT-Komponenten, Cloud-Dienste und Dienstleister mit Verantwortlichen erfasst; Pflegeprozess definiert.		
3	Risikomethode und Risikoanalyse Art. 21 Abs. 2 lit. a NIS2; § 30 Abs. 2 Nr. 1 BSIG	Dokumentierte Methode mit Kriterien und Akzeptanzschwelle; gefahrenübergreifende Szenarien einschließlich physischer Gefahren; mindestens jährliche Aktualisierung.		
4	Risikobehandlung und Risikoakzeptanz Art. 21 Abs. 2 lit. a NIS2; § 30 Abs. 2 Nr. 1 BSIG	Jedes Risiko hat eine Behandlungsentscheidung; Restrisiken über der Schwelle sind durch die Geschäftsleitung befristet akzeptiert.		
5	Richtlinienwerk mit Dokumentenlenkung Art. 21 Abs. 2 lit. a NIS2; § 30 Abs. 2 Nr. 1 BSIG	Themenrichtlinien für alle Mindestmaßnahmen mit Version, Freigabe und Prüfintervall.		
6	Netzsegmentierung und Zonenkonzept Art. 21 Abs. 2 lit. a NIS2; § 30 Abs. 2 Nr. 1 BSIG	Trennung von IT, OT, DMZ und Gastnetzen; Übergänge über kontrollierte Firewalls; für OT z. B. Zonen und Conduits nach IEC 62443-3-2.		
7	Netzplan und Firewall-Regelwerk Art. 21 Abs. 2 lit. a und e NIS2; § 30 Abs. 2 Nr. 1 und 5 BSIG; DVO (EU) 2024/2690 Anhang Nr. 6.7	Aktueller Netzplan für IT, OT und Cloud; nur begründete Verbindungen zwischen Zonen, nicht benötigte Dienste gesperrt; Firewall-Regeln regelmäßig und nach Vorfällen überprüft; getrenntes Management-Netz.		
8	Fern- und Dienstleisterzugänge kontrolliert und befristet Art. 21 Abs. 2 lit. a und e NIS2; § 30 Abs. 2 Nr. 1 und 5 BSIG; DVO (EU) 2024/2690 Anhang Nr. 6.7.2 d, g, h	Alle Wege von außen erfasst (auch Fernwartungsboxen an Maschinen); Freigabe nur auf Antrag und befristet; zentraler Zugang mit MFA und Sitzungsprotokollierung; nur genehmigte Geräte.		

lit. b / Nr. 2 – Bewältigung von Sicherheitsvorfällen

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
9	Incident-Response-Prozess dokumentiert Art. 21 Abs. 2 lit. b NIS2; § 30 Abs. 2 Nr. 2 BSIG	Phasen, Rollen, Schweregrade, Eskalation zur Geschäftsleitung; 24/7-Erreichbarkeit geregelt.		
10	Protokollierung und Erkennung Art. 21 Abs. 2 lit. b NIS2; § 30 Abs. 2 Nr. 2 BSIG	Zentrale Log-Sammlung, Überwachung (SIEM/MDR), EDR auf Endpunkten; OT-Netzwerküberwachung. KRITIS-Betreiber: Angriffserkennung nach § 31 Abs. 2 BSIG.		
11	Playbooks für Kernszenarien Art. 21 Abs. 2 lit. b NIS2; § 30 Abs. 2 Nr. 2 BSIG	Ransomware, kompromittiertes Konto, Phishing, Angriff über Fernwartung/OT, Datenabfluss – mit OT-spezifischen Entscheidungen zum Abfahren von Anlagen.		
12	Externe Unterstützung vereinbart Art. 21 Abs. 2 lit. b NIS2; § 30 Abs. 2 Nr. 2 BSIG	Rahmenvertrag mit IR-Dienstleister, Kontaktdaten Cyberversicherung, ggf. Forensik; Abrufweg dokumentiert.		
13	Meldeprozess nach § 32 BSIG Art. 21 Abs. 2 lit. b NIS2; § 30 Abs. 2 Nr. 2 BSIG	Kriterien für Erheblichkeit, Fristen 24 h/72 h/1 Monat, Vorlagen, Zugang zum BSI-Portal auch bei IT-Ausfall.		
14	Nachbereitung und Lessons Learned Art. 21 Abs. 2 lit. b NIS2; § 30 Abs. 2 Nr. 2 BSIG	Ursachenanalyse nach jedem relevanten Vorfall; Maßnahmen fließen in den Maßnahmenplan.		
15	Protokollierungskonzept: Quellen, Aufbewahrung, Zeit und Alarme Art. 21 Abs. 2 lit. b NIS2; § 30 Abs. 2 Nr. 2 BSIG; DVO (EU) 2024/2690 Anhang Nr. 3.2	Protokollierungskonzept mit Liste der Protokollquellen (IT, OT, Cloud), Ereignisarten nach DVO-Anhang Nr. 3.2.3, Aufbewahrung und Integritätsschutz, Zeitsynchronisation, Alarmregeln mit Reaktionszeiten; für Betreiber kritischer Anlagen Systeme zur Angriffserkennung (§ 31 Abs. 2 BSIG).		
16	Systeme zur Angriffserkennung betreiben (Betreiber kritischer Anlagen) § 31 Abs. 2 BSIG; § 39 Abs. 1 BSIG	Pflichtpunkt nur für Betreiber kritischer Anlagen: Die Systeme erfassen und werten Parameter aus dem laufenden Betrieb kontinuierlich und automatisch aus. Umsetzungsgrad nach der Orientierungshilfe des BSI bewerten und für den Nachweis nach § 39 BSIG festhalten. Für besonders wichtige Einrichtungen ohne kritische Anlage empfohlen, für wichtige Einrichtungen nicht erforderlich.		

lit. c / Nr. 3 – Aufrechterhaltung des Betriebs, Backup und Krisenmanagement

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
17	Business-Impact-Analyse Art. 21 Abs. 2 lit. c NIS2; § 30 Abs. 2 Nr. 3 BSIG	RTO/RPO für kritische Prozesse bestimmt und mit Prozessverantwortlichen abgestimmt.		
18	Notfall- und Wiederanlaufpläne Art. 21 Abs. 2 lit. c NIS2; § 30 Abs. 2 Nr. 3 BSIG	Notbetrieb und Wiederanlaufreihenfolge je kritischem Prozess, einschließlich Produktionsanlagen.		
19	Backup mit offline/unveränderlicher Kopie Art. 21 Abs. 2 lit. c NIS2; § 30 Abs. 2 Nr. 3 BSIG	3-2-1-Regel, getrennte Administration mit MFA, Sicherung von OT-Projekten und Konfigurationen.		

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
20	Regelmäßige Wiederherstellungstests Art. 21 Abs. 2 lit. c NIS2; § 30 Abs. 2 Nr. 3 BSIG	Protokollierte Restore-Tests mit gemessener Dauer im Vergleich zum RTO.		
21	Krisenstab und Krisenkommunikation Art. 21 Abs. 2 lit. c NIS2; § 30 Abs. 2 Nr. 3 BSIG	Zusammensetzung, Alarmierung, Krisenraum ohne IT-Abhängigkeit, Kommunikationsvorlagen.		
22	Krisen- und Notfallübungen Art. 21 Abs. 2 lit. c NIS2; § 30 Abs. 2 Nr. 3 BSIG	Mindestens jährlich, unter Beteiligung der Geschäftsleitung; Auswertung dokumentiert.		
23	Redundanz und geprüfte Integrität der Sicherungen (auch OT) Art. 21 Abs. 2 lit. c NIS2; § 30 Abs. 2 Nr. 3 BSIG; DVO (EU) 2024/2690 Anhang Nr. 4.2	Mindestens teilweise Redundanz von Systemen, Standorten, Personal und Kommunikation nach BIA; vollständige Sicherungen einschließlich Konfiguration und Cloud-Daten mit regelmäßiger Integritätsprüfung; Sicherung und Abgleich der OT-Projektstände und Images.		
24	Versorgung und Schutz vor Umgebungsgefahren (USV, Klima, Brand, Wasser) Art. 21 Abs. 2 lit. c NIS2; § 30 Abs. 2 Nr. 3 BSIG; DVO (EU) 2024/2690 Anhang Nr. 13.1 und 13.2	Schutz von Serverräumen, Netzverteilern und Leitwarten gegen Ausfall von Strom, Klima und Telekommunikation, gegen Brand und Wasser; Grenzwerte, Überwachung mit Alarm, Notversorgungsverträge, regelmäßige Tests.		

lit. d / Nr. 4 – Sicherheit der Lieferkette

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
25	Lieferanteninventar Art. 21 Abs. 2 lit. d NIS2; § 30 Abs. 2 Nr. 4 BSIG	Alle Anbieter und Diensteanbieter mit Zugriff auf Systeme/Daten oder kritischen Lieferungen erfasst.		
26	Kritikalitätseinstufung Art. 21 Abs. 2 lit. d NIS2; § 30 Abs. 2 Nr. 4 BSIG	Einstufung nach Zugriff, Abhängigkeit und Ersetzbarkeit; Berücksichtigung spezifischer Schwachstellen und der Sicherheitspraxis der Anbieter (Art. 21 Abs. 3 NIS2).		
27	Sicherheitsanforderungen und Vertragsklauseln Art. 21 Abs. 2 lit. d NIS2; § 30 Abs. 2 Nr. 4 BSIG	Abgestufte Mindestanforderungen, Meldepflicht bei Vorfällen, Auditrecht, Regelungen zu Unterauftragnehmern und Patchversorgung.		
28	Kontrollierte Dienstleisterzugänge Art. 21 Abs. 2 lit. d NIS2; § 30 Abs. 2 Nr. 4 BSIG	Fernwartung nur über zentrales Gateway mit persönlichem Konto, MFA, Freigabe und Protokollierung.		
29	Laufende Lieferantenüberwachung Art. 21 Abs. 2 lit. d NIS2; § 30 Abs. 2 Nr. 4 BSIG	Regelmäßige Neubewertung kritischer Lieferanten, Überwachung von Zertifikatsabläufen und Vorfällen, Exit-Strategie.		

lit. e / Nr. 5 – Sicherheit bei Erwerb, Entwicklung und Wartung; Schwachstellenmanagement

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
30	Sicherheitsanforderungen in der Beschaffung Art. 21 Abs. 2 lit. e NIS2; § 30 Abs. 2 Nr. 5 BSIG	Anforderungskatalog für IT- und OT-Beschaffungen (z. B. MFA-Fähigkeit, Logging, Supportzeitraum, Härtung, IEC 62443-4-2 für Komponenten).		
31	Sichere Entwicklung Art. 21 Abs. 2 lit. e NIS2; § 30 Abs. 2 Nr. 5 BSIG	Richtlinie für eigene Software und Steuerungsprogramme: Reviews, Umgebungstrennung, Abhängigkeitsprüfung, Geheimnisverwaltung.		
32	Change- und Konfigurationsmanagement Art. 21 Abs. 2 lit. e NIS2; § 30 Abs. 2 Nr. 5 BSIG	Änderungen mit Risikobewertung, Test, Freigabe und Rückfallplan; Härtungsstandards für Systeme.		
33	Schwachstellenmanagement mit Fristen Art. 21 Abs. 2 lit. e NIS2; § 30 Abs. 2 Nr. 5 BSIG	Quellen (Hersteller, CERT-Bund, ICS-Advisories), Bewertung nach Kritikalität und Exposition, definierte Behebungsfristen.		
34	Kompensation nicht patchbarer Systeme Art. 21 Abs. 2 lit. e NIS2; § 30 Abs. 2 Nr. 5 BSIG	Liste von EoL- und nicht patchbaren OT-Systemen mit dokumentierten kompensierenden Maßnahmen.		
35	Offenlegung von Schwachstellen Art. 21 Abs. 2 lit. e NIS2; § 30 Abs. 2 Nr. 5 BSIG	Veröffentlichter Kontaktweg (z. B. security.txt) und Verfahren für Coordinated Vulnerability Disclosure.		
36	Härtung, sichere Konfiguration und Schutz vor Schadsoftware Art. 21 Abs. 2 lit. e NIS2; § 30 Abs. 2 Nr. 5 BSIG; DVO (EU) 2024/2690 Anhang Nr. 6.3 und 6.9	Härtungs-Baselines je Systemtyp (CIS, BSI oder Hersteller, für SPS Schutzstufen), Anwendung bei Neuinstallation, regelmäßiger Soll-Ist-Abgleich; EDR oder Anwendungs-Whitelisting gegen Schadsoftware und nicht genehmigte Software.		

lit. f / Nr. 6 – Bewertung der Wirksamkeit

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
37	Messkonzept und Kennzahlen Art. 21 Abs. 2 lit. f NIS2; § 30 Abs. 2 Nr. 6 BSIG	Acht bis zwölf Kennzahlen mit Zielwerten, Verantwortlichen und Messintervall.		
38	Technische Prüfungen Art. 21 Abs. 2 lit. f NIS2; § 30 Abs. 2 Nr. 6 BSIG	Schwachstellenscans, Penetrationstests (OT abgestimmt), Konfigurationsprüfungen.		
39	Interne Audits Art. 21 Abs. 2 lit. f NIS2; § 30 Abs. 2 Nr. 6 BSIG	Jährliches risikoorientiertes Audit der Mindestmaßnahmen durch unabhängige Prüfer.		
40	Berichterstattung an die Geschäftsleitung Art. 21 Abs. 2 lit. f NIS2; § 30 Abs. 2 Nr. 6 BSIG	Regelmäßige Berichte zu Kennzahlen, Auditergebnissen und Maßnahmenfortschritt.		
41	Managementbewertung und Korrekturmaßnahmen Art. 21 Abs. 2 lit. f NIS2; § 30 Abs. 2 Nr. 6 BSIG	Jährliche Bewertung mit Beschlüssen; Abweichungen führen zu Maßnahmen im Maßnahmenplan.		

lit. g / Nr. 7 – Cyberhygiene und Schulungen

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
42	Cyberhygiene-Basisregeln umgesetzt Art. 21 Abs. 2 lit. g NIS2; § 30 Abs. 2 Nr. 7 BSIG	Patchen, Standardpasswörter ändern, keine lokalen Adminrechte, E-Mail- und Endpoint-Schutz, Wechseldatenträger-Regeln.		
43	Grundschulung aller Beschäftigten Art. 21 Abs. 2 lit. g NIS2; § 30 Abs. 2 Nr. 7 BSIG	Verpflichtend beim Onboarding und jährlich; inklusive Fremdpersonal mit Systemzugang.		
44	Zielgruppenschulungen Art. 21 Abs. 2 lit. g NIS2; § 30 Abs. 2 Nr. 7 BSIG	Admins, OT-Personal, Einkauf, Personal, Buchhaltung/Assistenz mit spezifischen Inhalten.		
45	Schulung der Geschäftsleitung Art. 21 Abs. 2 lit. g NIS2; § 30 Abs. 2 Nr. 7 BSIG	Regelmäßige Teilnahme aller Mitglieder nach § 38 Abs. 3 BSIG mit Nachweis.		
46	Sensibilisierung und Simulationen Art. 21 Abs. 2 lit. g NIS2; § 30 Abs. 2 Nr. 7 BSIG	Phishing-Simulationen und Kampagnen; Wirkung über Melde- und Klickrate messen.		

lit. h / Nr. 8 – Kryptografie und Verschlüsselung

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
47	Kryptografiekonzept Art. 21 Abs. 2 lit. h NIS2; § 30 Abs. 2 Nr. 8 BSIG	Einsatzbereiche, zulässige Verfahren (Orientierung BSI TR-02102), Verantwortlichkeiten, Ausnahmeprozess.		
48	Verschlüsselung von Daten in Übertragung Art. 21 Abs. 2 lit. h NIS2; § 30 Abs. 2 Nr. 8 BSIG	TLS 1.2+/1.3 für Webdienste und Schnittstellen, verschlüsselte VPN- und Fernwartungsverbindungen, E-Mail-Transportverschlüsselung.		
49	Verschlüsselung von Daten in Ruhe Art. 21 Abs. 2 lit. h NIS2; § 30 Abs. 2 Nr. 8 BSIG	Festplattenverschlüsselung mobiler Geräte, verschlüsselte Backups und Cloud-Speicher mit sicherer Schlüsselverwahrung.		
50	Schlüssel- und Zertifikatsmanagement Art. 21 Abs. 2 lit. h NIS2; § 30 Abs. 2 Nr. 8 BSIG	Zertifikatsinventar, Ablaufüberwachung, sichere Schlüsselspeicherung, Rotation und Sperrung.		
51	Ablösung veralteter Verfahren Art. 21 Abs. 2 lit. h NIS2; § 30 Abs. 2 Nr. 8 BSIG	SSL, TLS 1.0/1.1, SHA-1, schwache Cipher Suites identifiziert und abgelöst oder begründet kompensiert (v. a. in der OT).		

lit. i / Nr. 9 – Personalsicherheit, Zugriffskontrolle und Management von Anlagen

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
52	Sicherheit im Personalprozess Art. 21 Abs. 2 lit. i NIS2; § 30 Abs. 2 Nr. 9 BSIG	Überprüfung vor Einstellung in sensiblen Rollen, Vertraulichkeitsverpflichtung, geregelter Austritt mit Rückgabe und Zugangsentzug.		

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
53	Berechtigungskonzept und Rollenmodell Art. 21 Abs. 2 lit. i NIS2; § 30 Abs. 2 Nr. 9 BSIG	Least Privilege, rollenbasierte Rechte, Antrags- und Genehmigungsprozess.		
54	Privilegierte Konten Art. 21 Abs. 2 lit. i NIS2; § 30 Abs. 2 Nr. 9 BSIG	Getrennte Admin-Konten, Tiering/PAM, versiegelte Notfallkonten, halbjährliche Rezertifizierung.		
55	Joiner-Mover-Leaver-Prozess Art. 21 Abs. 2 lit. i NIS2; § 30 Abs. 2 Nr. 9 BSIG	Automatisierte Kopplung an das Personalsystem; Dienstleisterkonten befristet.		
56	Physische Zutrittskontrolle Art. 21 Abs. 2 lit. i NIS2; § 30 Abs. 2 Nr. 9 BSIG	Zutritt zu Serverräumen, Leitwarten, Schaltschränken und Netzwerkverteilern geregelt und protokolliert.		
57	Asset-Management als laufender Prozess Art. 21 Abs. 2 lit. i NIS2; § 30 Abs. 2 Nr. 9 BSIG	Aufnahme, Klassifizierung, Verantwortliche, Lebenszyklus und sichere Außerbetriebnahme von IKT-Systemen und -Produkten.		
58	Vollständiges Inventar mit Klassifizierung und Software-Inventar Art. 21 Abs. 2 lit. i NIS2; § 30 Abs. 2 Nr. 9 BSIG; DVO (EU) 2024/2690 Anhang Nr. 12.1 und 12.4	Dienste und tragende Systeme, Pflichtangaben je Asset (u. a. Version, Zone, Verantwortliche, Support-Ende), Klassifizierungsstufen, Software-Inventar mit SBOM für kritische Produkte, nachvollziehbare Änderungen.		
59	Sichere Löschung, Entsorgung, Wechseldatenträger und Rückgabe Art. 21 Abs. 2 lit. i NIS2; § 30 Abs. 2 Nr. 9 BSIG; DVO (EU) 2024/2690 Anhang Nr. 12.2, 12.3 und 12.5	Nachweisbare Löschung oder Vernichtung vor Entsorgung und Reparatur (auch OT-Speicherkarten), Regeln für Wechseldatenträger, Rückgabe oder Sperrung von Geräten beim Austritt.		

lit. j / Nr. 10 – MFA, gesicherte Kommunikation und Notfallkommunikation

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
60	MFA für Fernzugänge Art. 21 Abs. 2 lit. j NIS2; § 30 Abs. 2 Nr. 10 BSIG	VPN, Remote-Desktop, Fernwartungsportale – einschließlich Dienstleisterzugängen in die OT (MFA am Gateway/Jump-Server).		
61	MFA für Cloud, E-Mail und privilegierte Konten Art. 21 Abs. 2 lit. j NIS2; § 30 Abs. 2 Nr. 10 BSIG	Phishing-resistente Verfahren (FIDO2, Smartcard) bevorzugen; Legacy-Anmeldungen deaktivieren.		
62	MFA für alle Nutzer Art. 21 Abs. 2 lit. j NIS2; § 30 Abs. 2 Nr. 10 BSIG	Flächendeckende MFA bzw. kontinuierliche Authentifizierung mit dokumentierten Ausnahmen.		
63	Gesicherte Sprach-, Video- und Textkommunikation Art. 21 Abs. 2 lit. j NIS2; § 30 Abs. 2 Nr. 10 BSIG	Zugelassene Werkzeuge mit Verschlüsselung und geregelter Administration; Regeln für private Messenger.		
64	Notfallkommunikationssystem Art. 21 Abs. 2 lit. j NIS2; § 30 Abs. 2 Nr. 10 BSIG	Out-of-Band-Kanal für den Krisenstab, unabhängig von der Unternehmens-IT, regelmäßig getestet.		

§ 32 BSIG: Meldepflichten bei erheblichen Sicherheitsvorfällen

Erheblichkeit bewerten: Wann ist ein Vorfall meldepflichtig?

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
65	Unternehmensspezifische Kriterien für erhebliche Sicherheitsvorfälle sind festgelegt § 2 BSIG; Art. 23 Abs. 3 NIS2			
66	Zuständigkeit für Bewertung und Meldeentscheidung (inkl. Vertretung, 24/7) ist geregelt § 32 Abs. 1 BSIG			
67	Zeitpunkt der Kenntniserlangung wird im Vorfallprotokoll dokumentiert § 32 Abs. 1 BSIG			
68	Bewertungen „nicht meldepflichtig“ werden begründet dokumentiert § 30 Abs. 1 BSIG			
69	Stand der Konkretisierungen ist geprüft und dokumentiert: Verordnung nach § 56 Abs. 4 BSIG (bisher nicht erlassen), DVO (EU) 2024/2690 Art. 3–14 (sofern Einrichtungsart erfasst) und aktuelle BSI-Hinweise zur Meldepflicht § 2 Nr. 11 BSIG; § 56 Abs. 4 BSIG; Art. 3–14 DVO (EU) 2024/2690			

Meldefristen und Meldeinhalte umsetzen

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
70	Meldeplan mit den Stufen 24 h / 72 h / Zwischenmeldung / ein Monat ist dokumentiert § 32 Abs. 1 BSIG; Art. 23 Abs. 4 NIS2			
71	Meldevorlagen enthalten alle Pflichtinhalte je Meldestufe § 32 Abs. 1 BSIG			

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
72	Verfahren für Fortschrittsmeldung bei andauernden Vorfällen ist beschrieben § 32 Abs. 2 BSIG			
73	KRITIS-Betreiber: Zusatzangaben zur kritischen Anlage sind in der Vorlage enthalten § 32 Abs. 3 BSIG			
74	Parallele Meldepflichten (DSGVO, Versicherung, Kunden) sind im Plan verknüpft Art. 33 DSGVO; § 35 BSIG			
75	Zugang zum BSI-Portal ist auch bei Ausfall der eigenen IT möglich § 32 Abs. 1 BSIG			

Unterrichtung von Dienstempfängern und Meldeübungen

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
76	Kommunikationsvorlagen und Freigabeprozess für Dienstempfänger liegen vor § 35 BSIG; Art. 23 Abs. 1 NIS2			
77	Informationspflichten aus Kundenverträgen sind erfasst § 30 Abs. 2 Nr. 4 BSIG			
78	Meldeübung wurde durchgeführt und die Zeit bis zur Erstmeldung gemessen § 32 Abs. 1 BSIG; § 30 Abs. 2 Nr. 6 BSIG			
79	Erkenntnisse aus Übungen und Vorfällen sind in den Maßnahmenplan übernommen § 30 Abs. 2 Nr. 6 BSIG			

Über diese Vorlage

Vorlagenversion 1.0-9f0aae94
Stand der Inhalte 12.11.2026
Herausgeber Erstellt mit Complass, https://complass.eu

Rechtsgrundlage (Stand): BSIG 2025 (gesetze-im-internet.de, Stand: zuletzt geändert durch Art. 8 G v. 22.10.2026 I Nr. 318), KRITISDachG (BGBl. 2026 I Nr. 66, in Kraft seit 17.3.2026), BSI-KritisV (Stand: G v. 15.5.2026 I Nr. 148), DVO (EU) 2024/2690 (EUR-Lex), BSI-Infopaket NIS-2-Meldepflicht und BSI-FAQ zu NIS-2

Diese Vorlage ist keine Rechtsberatung. Sie ersetzt nicht die Prüfung, welche Anforderungen für Ihr Unternehmen gelten, und garantiert kein Prüfungs- oder Zertifizierungsergebnis.

Lizenz: Creative Commons Namensnennung 4.0 International (CC BY 4.0). Sie dürfen die Vorlage verwenden, ändern und weitergeben, auch kommerziell, wenn Sie die Quelle nennen. Namensnennung: „Vorlage: Complass (complass.eu), CC BY 4.0“. https://creativecommons.org/licenses/by/4.0/deed.de