SKAFFON

Wir schaffen. Damit Sie mehr schaffen.

NIS2-Checkliste

Technische Maßnahmen nach § 30 Abs. 2 BSIG: Controls, Nachweise, Zuständigkeiten

Stand	November 2026 (Version 1.0)
Herausgeber	SKAFFON GmbH, Grünwald bei München
Rechtsquelle	BGBl. 2025 I Nr. 301 vom 5. Dezember 2025 (NIS2UmsuCG), Artikel 1: BSIG, § 30
Gesetzestext	https://www.recht.bund.de/bgbl/1/2025/301/VO.html
Gesetzestext (PDF)	https://www.recht.bund.de/bgbl/1/2025/301/regelungstext.pdf
Geprüft	Wortlaut abgeglichen am 13. November 2026
Zielgruppe	IT-Leitung, CISO, CTO

Technische Checkliste, keine Rechtsberatung. Dieses Dokument ordnet die Bereiche des § 30 Abs. 2 BSIG technischen Maßnahmen zu. Es ist unsere fachliche Übersetzung in Arbeitspakete und keine amtliche Auslegung; verbindlich ist allein der Gesetzestext. Es stellt weder fest, ob Ihr Unternehmen unter das Gesetz fällt, noch bestätigt es Konformität, noch ersetzt es eine Zertifizierung oder Prüfung.

SKAFFON NIS2-Checkliste: technische Maßnahmen nach § 30 Abs. 2 BSIG

1. Zweck und Nutzung

Die Checkliste richtet sich an IT-Leitung, CISO und CTO, die aus den zehn Mindestbereichen des § 30 Abs. 2 BSIG konkrete Konfiguration und belegbare Nachweise machen müssen. Zu jedem Bereich finden Sie (1) den Gesetzeswortlaut, (2) die technischen Controls, die wir umsetzen oder prüfen, (3) das Nachweis-Artefakt, das dabei entstehen sollte, und (4) was ausdrücklich bei Ihnen und Ihrer Geschäftsleitung bleibt.

Zur Nutzung: Gehen Sie die Controls je Bereich durch und tragen Sie den Stand ein (umgesetzt, teilweise, offen, nicht zutreffend) sowie den Fundort des Nachweises. Die Eintragungsfelder sind im PDF zum Ausfüllen von Hand vorgesehen; in der Markdown-Fassung stehen Checkboxen. Ob eine Maßnahme im Einzelfall „geeignet, verhältnismäßig und wirksam“ ist, hängt von Ihrer Risikoanalyse und der Verhältnismäßigkeit nach § 30 Abs. 1 BSIG ab und kann diese Checkliste nicht beantworten.

2. Rechtsstand und Quellen

Das NIS2-Umsetzungsgesetz wurde am 5. Dezember 2025 im Bundesgesetzblatt verkündet (BGBl. 2025 I Nr. 301). Nach Artikel 30 des Gesetzes („Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.“) ist es am 6. Dezember 2025 in Kraft getreten. Artikel 1 enthält das neu gefasste BSI-Gesetz (BSIG). Der Gesetzestext wurde am 13. November 2026 im Bundesgesetzblatt gelesen und gegen diese Checkliste abgeglichen; spätere Änderungen sind nicht berücksichtigt.

- Gesetzestext (Regelungstext, PDF): https://www.recht.bund.de/bgbl/1/2025/301/regelungstext.pdf
- Bekanntmachung im Bundesgesetzblatt (HTML): https://www.recht.bund.de/bgbl/1/2025/301/VO.html
- Kanonischer Identifikator (ELI): https://www.recht.bund.de/eli/bund/bgbl-1/2025/301
- Europäische Grundlage: Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie), https://eur-lex.europa.eu/eli/dir/2022/2555/oj

§ 30 Abs. 1 BSIG verpflichtet besonders wichtige und wichtige Einrichtungen, „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen“ zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der genutzten informationstechnischen Systeme, Komponenten und Prozesse zu vermeiden und die Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Bei der Verhältnismäßigkeit sind nach Satz 2 „das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen“ zu berücksichtigen. Nach Satz 3 ist die Einhaltung „durch die Einrichtungen zu dokumentieren“.

§ 30 Abs. 2 BSIG konkretisiert dies: Die Maßnahmen „sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen“ und „müssen zumindest Folgendes umfassen“ (Nummern 1 bis 10, siehe Abschnitt 3).

Weitere Vorschriften, die diese Checkliste berührt, aber nicht erfüllt: **§ 28 BSIG** (welche Einrichtungen besonders wichtig oder wichtig sind), **§ 32 BSIG** (Meldepflichten bei erheblichen Sicherheitsvorfällen), **§ 33 BSIG** (Registrierungspflicht) und **§ 38 BSIG** (Umsetzungs-, Überwachungs- und Schulungspflicht der Geschäftsleitung; Abs. 3: regelmäßige Teilnahme an Schulungen). Diese Pflichten liegen bei Ihrem Unternehmen und seiner Geschäftsleitung.

3. Die zehn Bereiche des § 30 Abs. 2 BSIG

Die Überschriften entsprechen der Kurzfassung der Zuordnung auf skaffon.de; der Gesetzeswortlaut steht jeweils darunter. Bereiche, deren Schwerpunkt bei Organisation, Recht oder Geschäftsleitung liegt (zum Beispiel Nr. 7), sind nur zu einem Teil technisch abbildbar; der verbleibende Teil steht unter „Bleibt bei Ihnen“.

Nr. 1: Konzepte zu Risikoanalyse und IT-Sicherheit

Wortlaut § 30 Abs. 2 Satz 2 Nr. 1 BSIG: „Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik“

Technische Controls

[ ] Technische Systeminventur aus IaC-Zustand und Konfigurationsexporten
[ ] Schwachstellen- und Fehlkonfigurationsprüfung
[ ] Sicherheits-Baseline für Plattformen

Nachweis-Artefakt: Systeminventar, Gap-Bericht mit Einstufung

Bleibt bei Ihnen: Risikomethodik, Risikoakzeptanz, Sicherheitsleitlinie

Stand: [ ] umgesetzt [ ] teilweise [ ] offen [ ] nicht zutreffend
Fundort des Nachweises / Bemerkung:

Nr. 2: Bewältigung von Sicherheitsvorfällen

Wortlaut § 30 Abs. 2 Satz 2 Nr. 2 BSIG: „Bewältigung von Sicherheitsvorfällen“

Technische Controls

[ ] Zentrale Log-Erfassung, Anbindung an Ihr SIEM, Alarmierungswege
[ ] unveränderliche Audit-Logs
[ ] technische Eindämmung als Runbook (Zugangsdaten sperren, Workload isolieren, Snapshot sichern)

Nachweis-Artefakt: Log-Architekturdiagramm, Runbooks, Alarm-Testprotokoll

Bleibt bei Ihnen: Einstufung von Vorfällen, Meldungen nach § 32 BSIG, Krisenstab

Stand: [ ] umgesetzt [ ] teilweise [ ] offen [ ] nicht zutreffend
Fundort des Nachweises / Bemerkung:

Nr. 3: Aufrechterhaltung des Betriebs, Backup, Wiederherstellung

Wortlaut § 30 Abs. 2 Satz 2 Nr. 3 BSIG: „Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement“

Technische Controls

[ ] Backup-Architektur mit Offsite- und unveränderlicher Kopie, getrennte Zugangsdaten, dokumentierte Wiederanlaufreihenfolge, regelmäßiger Restore-Test

Nachweis-Artefakt: Backup-Konzept, Restore-Testprotokoll, Wiederanlauf-Runbook

Bleibt bei Ihnen: Festlegung der Wiederanlaufziele (RPO/RTO) aus Geschäftssicht, Notfall- und Krisenmanagement

Stand: [ ] umgesetzt [ ] teilweise [ ] offen [ ] nicht zutreffend
Fundort des Nachweises / Bemerkung:

Nr. 4: Sicherheit der Lieferkette

Wortlaut § 30 Abs. 2 Satz 2 Nr. 4 BSIG: „Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern“

Technische Controls

[ ] Technisches Inventar externer Dienste und deren Zugriffsrechte

[ ] Beschränkung und Protokollierung von Dienstleisterzugängen

[ ] Software-Lieferkette mit SBOM, signierten Artefakten und Registry-Richtlinien (siehe DevSecOps und Lieferketten)

Nachweis-Artefakt: Lieferantenzugriffs-Matrix, SBOM-Pipeline

Bleibt bei Ihnen: Vertragliche und organisatorische Lieferantenbewertung

Stand: [ ] umgesetzt [ ] teilweise [ ] offen [ ] nicht zutreffend
Fundort des Nachweises / Bemerkung:

Nr. 5: Sicherheit bei Erwerb, Entwicklung, Wartung, Schwachstellenmanagement

Wortlaut § 30 Abs. 2 Satz 2 Nr. 5 BSIG: „Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen“

Technische Controls

[ ] Image- und Abhängigkeits-Scanning in der Pipeline, IaC-Prüfung, Patch- und Update-Prozess, Härtungs-Baselines, Richtlinien als Code (z. B. Kyverno für Kubernetes)

Nachweis-Artefakt: Pipeline-Konfiguration, Scan-Berichte, Patch-Runbook

Bleibt bei Ihnen: Beschaffungsvorgaben, Prozess der Schwachstellenoffenlegung

Stand: [ ] umgesetzt [ ] teilweise [ ] offen [ ] nicht zutreffend
Fundort des Nachweises / Bemerkung:

Nr. 6: Verfahren zur Wirksamkeitsbewertung

Wortlaut § 30 Abs. 2 Satz 2 Nr. 6 BSIG: „Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik“

Technische Controls

[ ] Laufende Konformitätsprüfung der Konfiguration (Policy-Audit, Cloud-Posture-Prüfung), Drift-Erkennung, wiederholbare Restore- und Alarmtests

Nachweis-Artefakt: Prüfberichte mit Datum, Testkalender

Bleibt bei Ihnen: Interne Revision, unabhängige Audits und Penetrationstests (nicht Teil dieser Leistung)

Stand: [ ] umgesetzt [ ] teilweise [ ] offen [ ] nicht zutreffend
Fundort des Nachweises / Bemerkung:

Nr. 7: Schulung und Sensibilisierung

Wortlaut § 30 Abs. 2 Satz 2 Nr. 7 BSIG: „grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik“

Technische Controls

[ ] Technische Einweisung Ihrer Administratoren anhand der Runbooks

Nachweis-Artefakt: Übergabedokumentation

Bleibt bei Ihnen: Inhalte und Durchführung von Schulungen für Beschäftigte und Geschäftsleitung (§ 38 Abs. 3 BSIG)

Stand: [ ] umgesetzt [ ] teilweise [ ] offen [ ] nicht zutreffend
Fundort des Nachweises / Bemerkung:

Nr. 8: Kryptographie

Wortlaut § 30 Abs. 2 Satz 2 Nr. 8 BSIG: „Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren“

Technische Controls

[ ] Schlüsselverwaltung (KMS, Secrets-Management z. B. mit OpenBao), Verschlüsselung ruhender Daten, TLS-Konfiguration, Zertifikats- und Schlüsselrotation

Nachweis-Artefakt: Kryptographie-Parameterliste je System, Rotationsnachweis

Bleibt bei Ihnen: Kryptokonzept und Freigabe von Verfahren

Stand: [ ] umgesetzt [ ] teilweise [ ] offen [ ] nicht zutreffend
Fundort des Nachweises / Bemerkung:

Nr. 9: Personal, Zugriffskontrolle, Verwaltung von IKT-Systemen

Wortlaut § 30 Abs. 2 Satz 2 Nr. 9 BSIG: „Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen“

Technische Controls

[ ] Rollenmodell nach Least Privilege, zentrale Identitäten, privilegierter Zugriff mit Protokollierung, Break-Glass-Konten, Trennung von Umgebungen

Nachweis-Artefakt: Rollen- und Rechtematrix, Berechtigungsreview

Bleibt bei Ihnen: Personalsicherheit, Ein-/Austrittsprozess, Rollenfreigabe

Stand: [ ] umgesetzt [ ] teilweise [ ] offen [ ] nicht zutreffend
Fundort des Nachweises / Bemerkung:

Nr. 10: MFA, gesicherte Kommunikation, Notfallkommunikation

Wortlaut § 30 Abs. 2 Satz 2 Nr. 10 BSIG: „Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung“

Technische Controls

[ ] Mehrfaktor-Authentifizierung für Administratorzugänge und Fernzugriff, möglichst phishing-resistent

[ ] Zugangspfade, die bei Ausfall der Primärumgebung weiter funktionieren

Nachweis-Artefakt: MFA-Abdeckungsbericht, Zugangspfad-Dokumentation

Bleibt bei Ihnen: Auswahl der Kommunikationsmittel, Notfallkommunikationskonzept

Stand: [ ] umgesetzt [ ] teilweise [ ] offen [ ] nicht zutreffend
Fundort des Nachweises / Bemerkung:

4. Übersicht zum Eintragen

Nr.	Bereich nach § 30 Abs. 2 BSIG	umgesetzt	teil-weise	offen	n. z.	Verantwortlich / Datum
1	Konzepte zu Risikoanalyse und IT-Sicherheit					
2	Bewältigung von Sicherheitsvorfällen					
3	Aufrechterhaltung des Betriebs, Backup, Wiederherstellung					
4	Sicherheit der Lieferkette					
5	Sicherheit bei Erwerb, Entwicklung, Wartung, Schwachstellenmanagement					
6	Verfahren zur Wirksamkeitsbewertung					
7	Schulung und Sensibilisierung					
8	Kryptographie					
9	Personal, Zugriffskontrolle, Verwaltung von IKT-Systemen					
10	MFA, gesicherte Kommunikation, Notfallkommunikation					

5. Abgrenzung und Haftungsausschluss

- **Keine Rechtsberatung.** Ob Ihr Unternehmen eine besonders wichtige oder wichtige Einrichtung nach § 28 BSIG ist, klären Sie mit Ihrer Rechtsberatung.
- **Keine Konformitätsaussage.** Das Abhaken dieser Liste belegt keine Erfüllung des § 30 BSIG. Die Bewertung liegt bei Ihnen, Ihren Prüfern und der Aufsicht.
- **Keine Zertifizierung.** SKAFFON stellt kein Zertifikat aus und führt keine ISO-27001- oder sonstige Zertifizierung durch.
- **Keine amtliche Auslegung.** Die Zuordnung der Controls ist unsere fachliche Übersetzung. Maßgeblich ist der Gesetzestext einschließlich später ergangener Durchführungsrechtsakte und Rechtsverordnungen (§ 30 Abs. 3 bis 5 BSIG).
- **Nicht abschließend.** Der Umfang geeigneter Maßnahmen folgt aus Ihrer Risikoanalyse und der Verhältnismäßigkeit nach § 30 Abs. 1 BSIG. Branchen- und anlagenspezifische Anforderungen (zum Beispiel § 31 BSIG für Betreiber kritischer Anlagen) sind nicht Gegenstand.