NIS2-Geschäftsführer-Checkliste

Umsetzungsstand der Pflichten der Leitung nach NISG 2026 · 31 Punkte

Selbsteinschätzung des Umsetzungsstands gegen die NIS2-Pflichten der Leitung. Pro Punkt ein Feld ankreuzen — Orientierung für die Geschäftsführung, ersetzt keine Rechtsberatung.

Pro Punkt ankreuzen: ☐ offen ☐ teilweise ☐ erledigt

INKRAFTTRETEN	REGISTRIERUNG	SELBSTDEKLARATION
01.10.2026	**+ 3 Mon.**	**+ 12 Mon.**

01 Registrierung & Meldekette

§ 29

Betroffene Einrichtungen registrieren sich bei der Cybersicherheitsbehörde — binnen drei Monaten ab Inkrafttreten (§ 29 Abs. 3).

Die Betroffenheit ist geklärt: wesentliche oder wichtige Einrichtung?	☐	☐	☐
Die Registrierung bei der Cybersicherheitsbehörde ist vorbereitet oder erfolgt (§ 29 Abs. 3).	☐	☐	☐
Die für die Registrierung nötigen Stammdaten sind zusammengestellt (Sektor, Kontaktdaten, Ansprechpartner).	☐	☐	☐
Eine Kontaktstelle gegenüber der Behörde ist benannt.	☐	☐	☐

02 Governance & Verantwortung der Leitung

§ 31 ABS. 1

Die Leitungsorgane müssen die Risikomanagementmaßnahmen nach § 32 sicherstellen und beaufsichtigen. Diese Verantwortung ist nicht delegierbar.

Die Leitungsorgane haben die Verantwortung für die Cybersicherheitsmaßnahmen formell übernommen.	☐	☐	☐
Die Geschäftsführung gibt die Maßnahmen frei und überwacht ihre Umsetzung (regelmäßiges Reporting).	☐	☐	☐
Eine zuständige Person oder Rolle für Informationssicherheit ist benannt (z. B. CISO).	☐	☐	☐
Cyber-Risiken sind fester Punkt auf der Agenda von Geschäftsführung bzw. Aufsichtsrat.	☐	☐	☐

03 Schulung

§ 31 ABS. 2

Die Leitungsorgane müssen an spezifischen Cybersicherheitsschulungen teilnehmen; Mitarbeitende sind regelmäßig zu schulen.

Die Leitungsorgane haben an einer spezifischen Cybersicherheitsschulung teilgenommen.	☐	☐	☐
Es gibt ein laufendes Awareness- und Schulungsprogramm für die Mitarbeitenden.	☐	☐	☐
Teilnahmen und Schulungsinhalte werden nachvollziehbar dokumentiert.	☐	☐	☐

04 Risikomanagement-Maßnahmen

§ 32 ABS. 4

Der Maßnahmenkatalog nach § 32 Abs. 4 umfasst zehn Bereiche (lit. a–j) als gefahrenübergreifenden Mindeststandard — verbindlich ab 1.10.2026.

Risikoanalyse und Sicherheitskonzepte für die Informationssysteme (lit. a).	☐	☐	☐
Verfahren zur Bewältigung von Sicherheitsvorfällen (lit. b).	☐	☐	☐
Aufrechterhaltung des Betriebs: Backup-Management, Wiederherstellung, Krisenmanagement (lit. c).	☐	☐	☐
Sicherheit der Lieferkette gegenüber unmittelbaren Anbietern (lit. d).	☐	☐	☐
Sicherheit bei Beschaffung, Entwicklung und Wartung inkl. Schwachstellen-Management (lit. e).	☐	☐	☐
Verfahren zur Bewertung der Wirksamkeit der Maßnahmen (lit. f).	☐	☐	☐
Grundlegende Cyberhygiene und Cybersicherheitsschulungen (lit. g).	☐	☐	☐
Konzepte für Kryptografie und Verschlüsselung (lit. h).	☐	☐	☐
Personalsicherheit, Zugriffskontrolle und Asset-Management (lit. i).	☐	☐	☐
Multi-Faktor-Authentifizierung und gesicherte Kommunikation (lit. j).	☐	☐	☐

05 Selbstdeklaration & Nachweis

§ 33

Binnen zwölf Monaten nach Eintritt der Registrierungspflicht ist eine Selbstdeklaration zu übermitteln (§ 33 Abs. 1); spätere Nachweise sind auch über gültige Zertifikate möglich (§ 33 Abs. 2).

- [ ] [ ] [ ] Der Umsetzungsstand der § 32-Maßnahmen ist dokumentiert und belegbar.
- [ ] [ ] [ ] Die Selbstdeklaration an die Behörde ist vorbereitet (§ 33 Abs. 1).
- [ ] [ ] [ ] Der Nachweisweg ist geklärt: interne Belege oder ein gültiges Zertifikat wie ISO 27001 (§ 33 Abs. 2).

06 Meldewesen

§ 34

Erhebliche Cybersicherheitsvorfälle sind in einer Kaskade zu melden: Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussbericht spätestens einen Monat danach (§ 34 Abs. 2).

- [ ] [ ] [ ] Es ist definiert, wer einen erheblichen Vorfall erkennt und bewertet.
- [ ] [ ] [ ] Der Meldeprozess steht: 24-Stunden-Frühwarnung, 72-Stunden-Meldung, Abschlussbericht binnen eines Monats.
- [ ] [ ] [ ] Die Meldewege zur Behörde bzw. zum CSIRT sind hinterlegt und im Team bekannt.
- [ ] [ ] [ ] Der Ablauf wurde geübt (z. B. in einer Tabletop-Übung).

07 Lieferketten-Sicherheit

§ 32 ABS. 4 LIT. D

Die Lieferkettensicherheit ist in der Praxis ein eigener Arbeitsstrang. Auch nicht direkt betroffene Unternehmen kommen über die Lieferkette ihrer Kunden in die Pflicht.

- [ ] [ ] [ ] Die kritischen Lieferanten und Dienstleister sind erfasst und nach Risiko eingestuft.
- [ ] [ ] [ ] Sicherheitsanforderungen und Prüf- bzw. Audit-Rechte sind vertraglich verankert.
- [ ] [ ] [ ] Die Sicherheitslage wesentlicher Lieferanten wird laufend beobachtet.