

CHECKLISTE · TOMORIS TOOLBOX

NIS2-Risikomanagement: die Maßnahmen nach § 32 NISG 2026 als Checkliste

Die Mindestinhalte nach § 32 Abs. 4 NISG 2026 mit dem Anhang der DVO (EU) 2024/2690, Nachweisideen, Pflichten der Leitungsorgane und Selbstdeklaration

STAND

25.10.2026

UMFANG

PDF, 10 Seiten

ONLINE

tomoris.com/downloads/nis2-risikomanagement-checkliste

AUF EINEN BLICK

10

Mindestinhalte nach § 32 Abs. 4 lit. a bis j NISG 2026

13

Nummern im Anhang der DVO (EU) 2024/2690

jährlich

Sicherheitskonzept durch die Leitung überprüfen

2027

Selbstdeklaration bis 30. September 2027

FÜR WEN

- Informationssicherheitsbeauftragte und CISOs wesentlicher und wichtiger Einrichtungen nach dem NISG 2026
- Geschäftsführung, Vorstand und andere Leitungsorgane, die die Umsetzung sicherstellen und beaufsichtigen müssen
- IT-Leitung, Compliance und Revision, die Nachweise sammeln und die Selbstdeklaration vorbereiten

WURUM ES GEHT

Seit 1. Oktober 2026 müssen wesentliche und wichtige Einrichtungen Risikomanagementmaßnahmen nach § 32 NISG 2026 umsetzen. Was die zehn Mindestinhalte im Einzelnen verlangen, regelt der Anhang der Durchführungsverordnung (EU) 2024/2690; § 2 NISV 2026 erstreckt ihn auf alle wesentlichen und wichtigen Einrichtungen, für die er nicht ohnehin gilt. Diese Checkliste ordnet jedem Buchstaben des § 32 Abs. 4 die Nummern des Anhangs zu, fasst den Kern jeder Anforderung zusammen und nennt Nachweise, die Sie vorhalten sollten. Dazu kommen die Pflichten der Leitungsorgane nach § 31, Verhältnismäßigkeit und kompensierende Maßnahmen sowie Selbstdeklaration, Prüfung und Fristen nach § 33.

Die Checklisten sind eine Empfehlung von TOMORIS und ersetzen keine Rechtsberatung. Maßgeblich sind NISG 2026 und NISV 2026 in der geltenden Fassung, der Anhang der DVO (EU) 2024/2690 (über § 2 NISV 2026 in der Fassung bei deren Inkrafttreten) sowie die Vorgaben der Cybersicherheitsbehörde zur Selbstdeklaration. Die Nachweisideen sind Beispiele; die ENISA-Leitlinie ist nicht verbindlich.

INHALT

01	Worum es geht und was verbindlich ist	3
02	Zuordnung: § 32 Abs. 4 NISG 2026 und DVO-Anhang	3
03	Checkliste 1: Konzepte, Risiko, Vorfälle, Betrieb	4
04	Checkliste 2: Lieferkette, Beschaffung, Betrieb	5
05	Checkliste 3: Schulung, Zugriff, Anlagen, Umfeld	5
06	Pflichten der Leitungsorgane (§ 31 NISG 2026)	6
07	Verhältnismäßigkeit und kompensierende Maßnahmen	7
08	Selbstdeklaration, Prüfung und Fristen (§ 33 NISG 2026)	8
09	Häufige Fehler	9
10	Quellen	10

01 —

Worum es geht und was verbindlich ist

Zehn Mindestinhalte im NISG 2026, Einzelheiten im DVO-Anhang, Nachweisideen als Empfehlung.

Seit 1. Oktober 2026 müssen wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Risikomanagementmaßnahmen umsetzen (§ 32 Abs. 1 und 2 NISG 2026). Sie beruhen auf einem gefahrenübergreifenden Ansatz und umfassen zumindest die zehn Inhalte des § 32 Abs. 4 lit. a bis j, die Art. 21 Abs. 2 der NIS-2-Richtlinie umsetzen.

- Verbindlich: §§ 31 bis 33 NISG 2026 mit Leitungspflichten, Mindestinhalten und Nachweis.
- Verbindlich: der Anhang der DVO (EU) 2024/2690 mit dreizehn Nummern, für digitale Anbieter wie Cloud- und verwaltete Dienste unmittelbar, für alle übrigen Einrichtungen über § 2 NISV 2026.
- Nicht verbindlich: die ENISA-Leitlinie (Juni 2025) und die FAQ des Bundesamts für Cybersicherheit (BCS).
- Ausnahme: Gleichwertiges EU-Sektorrecht wie DORA verdrängt § 32 insoweit (§ 27 NISG 2026).

So lesen Sie die Tabellen: Der „Kern der Anforderung“ ist verbindlich; wo der Anhang „soweit angemessen, anwendbar oder durchführbar“ sagt, dürfen Sie nur mit dokumentierter Begründung abweichen (Art. 2 Abs. 2 DVO).

02 —

Zuordnung: § 32 Abs. 4 NISG 2026 und DVO-Anhang

Welche Nummern des DVO-Anhangs die zehn Buchstaben des § 32 Abs. 4 NISG 2026 konkretisieren.

§ 32 Abs. 4 NISG 2026 (Art. 21 Abs. 2 NIS-2-Richtlinie) und Anhang Nr. nach Überschriften und Einleitungssätzen

LIT.	MINDESTINHALT NACH § 32 ABS. 4 NISG 2026	ANHANG NR.
a	Konzepte für Risikoanalyse und Sicherheit der Informationssysteme	1, 2
b	Bewältigung von Cybersicherheitsvorfällen	3
c	Aufrechterhaltung des Betriebs: Backup, Wiederherstellung, Krisenmanagement	4, 13.1
d	Sicherheit der Lieferkette, auch zu unmittelbaren Anbietern	5
e	Erwerb, Entwicklung, Wartung; Umgang mit und Offenlegung von Schwachstellen	6, 13.2
f	Bewertung der Wirksamkeit der Risikomanagementmaßnahmen	7
g	Grundlegende Cyberhygiene und Schulungen	8
h	Kryptografie und gegebenenfalls Verschlüsselung	9
i	Sicherheit des Personals, Zugriffskontrolle, Management von Anlagen	10 bis 12, 13.3
j	MFA oder kontinuierliche Authentifizierung; gesicherte Kommunikation	11 (11.7)

03

Checkliste 1: Konzepte, Risiko, Vorfälle, Betrieb

lit. a bis c, Anhang Nr. 1 bis 4: Konzept, Rollen, Risiken, Vorfälle, Notfall, Backup und Krise.

lit. a bis c: Anhang Nr. 1 bis 4 DVO (EU) 2024/2690; Nachweisisdeen nach ENISA

ANHANG NR.	KERN DER ANFORDERUNG (VERBINDLICH)	NACHWEISIDEEN (EMPFEHLUNG)
1.1 Konzept	Konzept für die Sicherheit der Netz- und Informationssysteme mit Zielen, Ressourcen, Rollen und Kennzahlen, von den Leitungsorganen förmlich genehmigt und mindestens jährlich überprüft (1.1).	Konzept mit Genehmigungsdatum; Kenntnisnahme durch Mitarbeitende; Protokoll der Überprüfung.
1.2 Rollen	Verantwortlichkeiten festgelegt und der Leitung mitgeteilt; mindestens eine Person ist den Leitungsorganen direkt verantwortlich (1.2).	Datiertes Organigramm mit Berichtslinie; formelle Bestellung der Rollen.
2.1 Risiken	Methodik und Kriterien; Risiken gefahrenübergreifend ermitteln und bewerten; Behandlungsplan; Restrisiken akzeptiert; mindestens jährlich überprüft (2.1); Kategorien nach § 3 NISV 2026.	Methodik; Risikoregister; Behandlungsplan; Freigabe der Restrisiken.
2.2, 2.3 Prüfung	Einhaltung regelmäßig prüfen und der Leitung berichten; unabhängige Überprüfung in geplanten Abständen, intern nur durch Personen, die dem geprüften Bereich nicht unterstellt sind, sonst alternative Maßnahmen für die Unparteilichkeit (2.2, 2.3).	Prüfplan und Prüfberichte; Liste genehmigter Ausnahmen.
3.1, 3.2 Vorfälle	Konzept für Erkennung, Eindämmung, Wiederherstellung und Meldung, abgestimmt mit dem Notfallplan; Überwachung und geschützte Protokolle (3.1, 3.2).	Kategorien für Vorfälle; Eskalationsplan; Einstellungen der Protokollierung.
3.3 bis 3.6 Reaktion	Einfacher Meldeweg für Mitarbeitende, Anbieter und Kunden; Bewertung nach vorab festgelegten Kriterien; vierteljährlich auf wiederholte Vorfälle prüfen (3.4.2 lit. b, sonst § 7 NISV 2026 analog); Reaktion nach dokumentierten Verfahren; Tests; Lehren dokumentieren (3.3 bis 3.6).	Meldekanäle; Playbooks; Liste der Meldepflichten und Fristen; Testprotokolle.
4.1 Notfall	Notfallplan auf Basis der Risikobewertung; Analyse der betrieblichen Auswirkungen; Plan in geplanten Abständen getestet (4.1).	Notfallplan; Analyse mit Wiederherstellungszielen; Testberichte.
4.2 Backup, Redundanz	Sicherungspläne mit Wiederherstellungszeiten; Kopien nicht im selben Netz und ausreichend entfernt; regelmäßige Integritätsprüfungen; zumindest teilweise Redundanz von Systemen, Anlagen, Personal und Kommunikationskanälen; Wiederherstellungstests mit dokumentierten Ergebnissen (4.2).	Sicherungsplan; Protokolle der Sicherungen; Testberichte mit erreichten Zeiten.
4.3 Krise	Krisenmanagement mit Rollen, Kommunikationsmitteln zu den Behörden und Maßnahmen für die Sicherheit; Plan getestet (4.3).	Krisenstab mit Vertretungen; Krisenkommunikationsplan; Übungsberichte.

04

Checkliste 2: Lieferkette, Beschaffung, Betrieb

lit. d bis f, Anhang Nr. 5 bis 7: Lieferkette, Erwerb, Änderungen, Patches, Netz und Wirksamkeit.

lit. d bis f: Anhang Nr. 5 bis 7 DVO (EU) 2024/2690; Nachweisideen nach ENISA

ANHANG NR.	KERN DER ANFORDERUNG (VERBINDLICH)	NACHWEISIDEEN (EMPFEHLUNG)
5.1 Lieferkette	Konzept mit Auswahlkriterien für direkte Anbieter; Verträge soweit angemessen mit Sicherheitsanforderungen, Meldung von Vorfällen, Prüfrecht und Pflichten bei Vertragsende (5.1).	Konzept; Verträge mit den Klauseln aus 5.1.4; Liste der Vorfälle bei Anbietern.
5.2 Anbieter	Aktuelles Verzeichnis der direkten Anbieter mit Kontaktstelle und gelieferten IKT-Produkten, -Dienstleistungen und -Prozessen (5.2).	Verzeichnis mit Änderungsverlauf; Einstufung nach Kritikalität.
6.1, 6.2 Erwerb	Sicherheitsanforderungen beim Erwerb von IKT-Produkten und -Dienstleistungen, auch Updates über die Lebensdauer; Regeln für sichere Entwicklung, auch ausgelagert (6.1, 6.2).	Ausschreibungsvorlagen; Entwicklungsregeln; getrennte Testumgebung.
6.3, 6.4 Änderungen	Sichere Konfigurationen festlegen und durchsetzen; Änderungen dokumentieren und vorher testen; Notfalländerungen nachträglich begründen (6.3, 6.4).	Basiskonfiguration mit Ausnahmen; Änderungsprotokolle; Rückfallpläne.
6.5, 6.6 Patches	Sicherheitsprüfungen risikobasiert planen; Patches in angemessener Frist, getestet, aus vertrauenswürdiger Quelle; Verzicht dokumentiert und begründet (6.5, 6.6).	Berichte von Penetrationstests; Patch-Verlauf; Begründung bei Verzicht.
6.7, 6.8 Netz	Netzarchitektur dokumentiert; unnötige Dienste deaktiviert; Fernzugriff kontrolliert; Pläne für neue Netzwerkprotokolle und E-Mail-Normen; Zonen nach Risiko (6.7, 6.8).	Netzpläne; Firewall-Regelwerke; Zonenmodell.
6.9, 6.10 Schadcode, Schwachstellen	Schutz vor Schadsoftware und nicht genehmigter Software; kritische Schwachstellen unverzüglich beheben; Verfahren zur koordinierten Offenlegung (6.9, 6.10).	Einstellungen von EDR; Scan-Protokolle; Behebungsnachweise.
7 Wirksamkeit	Festlegen, was wie, wann und von wem gemessen und ausgewertet wird; in geplanten Abständen überprüfen (7).	Kennzahlen; Berichte an die Leitungsorgane.

05

Checkliste 3: Schulung, Zugriff, Anlagen, Umfeld

lit. g bis j, Anhang Nr. 8 bis 13: Schulung, Kryptografie, Personal, Zugriff, MFA, Anlagen, Umfeld.

lit. g bis j und Nr. 13 (lit. c, e, i): Anhang Nr. 8 bis 13 DVO (EU) 2024/2690; Nachweisideen nach ENISA

ANHANG NR.	KERN DER ANFORDERUNG (VERBINDLICH)	NACHWEISIDEEN (EMPFEHLUNG)
8.1 Hygiene	Sensibilisierung aller Mitarbeitenden einschließlich der Leitungsorgane, wiederkehrend und für neue Mitarbeitende, zu Bedrohungen und Cyberhygiene (8.1).	Programm mit Terminen; Teilnahmelisten; Testergebnisse.

8.2 Schulung	Rollen mit Sicherheitsaufgaben ermitteln und regelmäßig schulen; Wirksamkeit bewerten (8.2).	Schulungsplan je Rolle; Teilnahmehachweise.
9 Kryptografie	Konzept zu Art und Stärke der Kryptografie nach Klassifizierung, zugelassenen Algorithmen und Schlüsselmanagement; nach dem Stand der Technik überprüft (9).	Richtlinie mit Algorithmen und Schlüssellängen.
10 Personal	Pflichten bekannt und verbindlich; Rollen mindestens jährlich prüfen; Zuverlässigkeitsprüfung soweit durchführbar; Pflichten nach dem Austritt; Disziplinarverfahren (10).	Rollenliste; Vertraulichkeitsklauseln; Prüfverfahren.
11.1 bis 11.4 Zugriff	Zugriffskonzept; Rechte nach Need-to-know und Aufgabentrennung, im Register, regelmäßig überprüft; eigene Verwaltungskonten mit starker Authentifizierung (11.1 bis 11.4).	Berechtigungsregister; Protokolle der Überprüfung; Liste privilegierter Konten.
11.5 bis 11.7 MFA	Eindeutige Kennungen je Person; Sperre nach Fehlversuchen; soweit angemessen mehrere Faktoren oder kontinuierliche Authentifizierung nach Klassifizierung (11.5 bis 11.7).	Anmeldeprotokolle; MFA-Konfiguration; genehmigte Ausnahmen.
12 Anlagen	Klassifizierung nach Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit; Regeln bis zur Löschung; Wechseldatenträger; aktuelles Inventar (12).	Klassifizierungsschema; Inventar mit Änderungsverlauf.
13 Umfeld	Schutz vor Ausfall von Versorgungsleistungen wie Strom und Telekommunikation und vor physischen Bedrohungen; Zutrittskontrolle; Tests (13).	Umgebungsüberwachung; Liste der Zutrittsberechtigten.
lit. j Kommunikation	Gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung (§ 32 Abs. 4 lit. j). Keine eigene Nummer im Anhang; verwandt sind Kommunikationskanäle im Notfallplan (4.1.2 lit. c), redundante Kanäle (4.2.4 lit. d), Kommunikationsmittel zu den Behörden (4.3.2 lit. b) und die Verschlüsselung übermittelter Daten (9.2 lit. a).	Empfehlung von TOMORIS: verschlüsselte Dienste festlegen; Ersatzkanal für den Notfall festlegen und testen, denn laut ENISA sind gewohnte Kanäle in der Krise womöglich nicht sicher.

06

Pflichten der Leitungsorgane (§ 31 NISG 2026)

Sicherstellen, beaufsichtigen, billigen, sich schulen lassen: was die Geschäftsführung selbst tun muss.

Leitungsorgan ist, wer nach Gesetz, Satzung oder Vertrag zur Führung der Geschäfte berufen ist (§ 3 Z 11 NISG 2026), laut BCS etwa Geschäftsführung oder Vorstand, nicht schon die IT-Leitung oder der CISO. Die Leitungsorgane haben die Einhaltung der Risikomanagementmaßnahmen sicherzustellen und zu beaufsichtigen (§ 31 Abs. 1), laut den Erläuterungen zur Regierungsvorlage einschließlich der Billigung der Vorgaben (vgl. Art. 20 Abs. 1 NIS-2-Richtlinie), und an für sie gestalteten Cybersicherheitsschulungen teilzunehmen (§ 31 Abs. 2).

- ☐ Sicherheitskonzept genehmigt und jährlich überprüft (Anhang Nr. 1.1.1 lit. k, 1.1.2 DVO).
- ☐ Ressourcen zugesagt: Personal, Finanzmittel, Verfahren und Technologien (Nr. 1.1.1 lit. e).
- ☐ Mindestens eine Person ist der Leitung direkt für die Sicherheit verantwortlich (Nr. 1.2.3).

- ☐ Risikobewertung und Restrisiken von der Leitung oder befugten Personen akzeptiert (Nr. 2.1.1).
- ☐ Regelmäßige Berichte zum Sicherheitsstand und zu unabhängigen Prüfungen (Nr. 2.2.1, 2.3.3).
- ☐ Jedes Mitglied der Geschäftsleitung geschult, Teilnahme dokumentiert (laut BCS genügen Mitarbeiter-schulungen nicht); den Mitarbeitenden werden regelmäßig Schulungen angeboten (§ 31 Abs. 2).
- ☐ Die Leitung unterzeichnet Prüfberichte mit den Prüfern (§ 33 Abs. 3) und gibt die Selbstdекlaration frei (Empfehlung).

Folgen: Geldstrafen nach § 45 kann die Bezirksverwaltungsbehörde gegen die juristische Person verhängen, laut Erläuterungen vorrangig (§ 44 Abs. 3 und 4). Daneben bleibt die Verantwortlichkeit nach § 9 VStG der zur Vertretung nach außen Berufenen wie der Geschäftsführung, soweit keine verantwortlichen Beauftragten bestellt sind; ist die juristische Person für denselben Verstoß bestraft, ist von ihrer Bestrafung abzusehen (§ 44 Abs. 5). Eigene Strafen für Leitungsorgane sieht das NISG 2026 laut Erläuterungen und BCS nicht vor; möglich ist Schadenersatz bei sorgfaltswidrigem Handeln. Wesentlichen Einrichtungen kann die Behörde Leitungsaufgaben vorübergehend untersagen (§ 39 Abs. 4 Z 2).

07

Verhältnismäßigkeit und kompensierende Maßnahmen

Wie Größe und Risiko die Umsetzung bestimmen und wann Sie begründet abweichen dürfen.

Für die Verhältnismäßigkeit zählen die Risikoexposition der Einrichtung und ihrer Dienste, ihre Größe sowie Wahrscheinlichkeit und Schwere von Vorfällen samt gesellschaftlichen und wirtschaftlichen Auswirkungen (§ 32 Abs. 3 NISG 2026, Art. 2 Abs. 2 DVO). Der Anhang ist laut den Erläuterungen zur NISV 2026 ein Rahmen, keine konkrete Umsetzungsbeschreibung. Ein Beispiel des BCS: Im Kleinstunternehmen können Inventar und Anbieterverzeichnis mit einer Tabellenkalkulation noch durchführbar sein.

Zwei Wege, von einer Anforderung abzuweichen

Kompensierende Maßnahme

§ 4 NISV 2026

Wer einer Anforderung vorübergehend oder wegen seiner Größe nicht entsprechen kann, setzt kompensierende Maßnahmen, die ihren Zweck auf Basis einer Risikobewertung möglichst erfüllen, dokumentiert sie begründet und prüft ihre Wirksamkeit mindestens jährlich. Vorübergehend heißt laut Erläuterungen etwa ein laufendes Vergabeverfahren; dafür erwartet das BCS einen konkreten Zeitplan für die eigentliche Umsetzung. Die Größe ist kein pauschales Argument.

Begründete Nichtanwendung

Art. 2 Abs. 2 UAbs. 2 DVO

Steht im Anhang „soweit angemessen“, „anwendbar“ oder „durchführbar“, genügt eine verständlich dokumentierte Begründung, warum die Anforderung für Sie nicht passt; kompensieren müssen Sie dann nicht (§ 4 Abs. 4 NISV 2026). Beispiele: Nr. 1.2.5, 3.2.2 und 11.7.1.

08

Selbstdeklaration, Prüfung und Fristen (§ 33 NISG 2026)

Selbstdeklaration bis 30. September 2027, Aufforderung zur Prüfung frühestens ab 1. Oktober 2028, Strafraumen.

Fristen ab Inkrafttreten des NISG 2026



1.10.2026

Pflichten gelten

§§ 31 bis 33 NISG 2026 in Kraft (§ 51 Abs. 2); NISV 2026 seit Ablauf dieses Tages (§ 9 NISV).



1.1.2027

Registrierung

Binnen drei Monaten ab Inkrafttreten (§ 29 Abs. 3) über NIS2-Services im USP; laut BCS bis 1. Jänner 2027, wegen § 33 Abs. 2 AVG spätestens 4. Jänner 2027. Die BCS-FAQ nennt 31. Dezember 2026.



30.9.2027

Selbstdeklaration

Binnen zwölf Monaten nach Eintritt der Registrierungs-pflicht (§ 33 Abs. 1), laut BCS bis 30. September 2027.



ab 1.10.2028

Prüfung möglich

Erste Aufforderung zum Nachweis durch eine un-abhängige Stelle frühestens zwei Jahre nach Inkrafttreten (§ 33 Abs. 2).

Die Selbstdeklaration informiert über die umgesetzten Maßnahmen, insbesondere über die genutzten Netz- und Informationssysteme, die Sicherheit der Lieferketten und die Ergebnisse der Risikoanalyse (§ 33 Abs. 1). Laut BCS wird sie ein Formular mit kurzen, konkreten Fragen im Unternehmensserviceportal (USP) sein und keine Prüfung ersetzen. Wer später wesentlich oder wichtig wird, rechnet die zwölf Monate ab Erfüllung der Voraussetzungen (Erläuterungen zu § 33). Vorbereitung, empfohlen von TOMORIS:

- ☐ Inventar der Dienste und Systeme (Anhang Nr. 12.4) und Verzeichnis der direkten Anbieter (Nr. 5.2) aktuell.
- ☐ Risikoanalyse mit den vier Kategorien des § 3 NISV 2026 (technologisch, menschlich, IKT-Lieferkette, standortbezogen), Behandlungsplan und akzeptierten Restrisiken.
- ☐ Stand je Zeile der Checklisten 1 bis 3 erhoben, mit Verantwortlichen und Terminen; Abweichungen begründet dokumentiert.
- ☐ Zugang zum USP geklärt; festgelegt, wer ausfüllt und wer freigibt; Angaben mit den Nachweisen abgeglichen.

Nachweis durch eine unabhängige Stelle (§ 33 Abs. 2 bis 5 NISG 2026)

PUNKT	REGELUNG
Aufforderung	Laut BCS frühestens ab 1. Oktober 2028; bei wichtigen Einrichtungen nur, wenn die Behörde aus Nachweisen wie der Selbstdeklaration oder aus sonstigen begründeten Hinweisen erfährt, dass die Einrichtung ihre Pflichten mutmaßlich nicht erfüllt (§ 33 Abs. 2, § 38 Abs. 2).

Fristen	Zwei Jahre ab Aufforderung; wesentliche Einrichtungen weisen die operative und organisatorische Umsetzung binnen zwei Monaten nach (§ 33 Abs. 2).
Zertifikate	Gültige einschlägige Zertifikate können die operative und organisatorische Umsetzung belegen (§ 33 Abs. 2), laut BCS nicht die technische. Der Scope muss die ganze Einrichtung erfassen; eine Teilanerkennung ist möglich, den Rest weisen Sie durch Prüfung nach. Scope, Abweichungen und allfällige Prüfberichte gehen mit dem Zertifikat an die Behörde.
Prüfbericht	Von Leitungsorganen und Prüfern unterzeichnet, mit Mängeln und Maßnahmenplan (§ 33 Abs. 3); Prüfplan einen Monat vorher an die Behörde (Abs. 5).

Strafrahmen (§§ 45 und 46 NISG 2026)

VERSTOSS	FUNDSTELLE	STRAFRAHMEN
Maßnahmen nach § 32 nicht umgesetzt, außer die Behörde kennt das nur aus der Selbstdeklaration; Schulungen nach § 31 Abs. 2 nicht vorgesehen	§ 45 Abs. 1 Z 1 bis 3	wesentliche Einrichtung bis 10 Mio. Euro oder 2 %, wichtige bis 7 Mio. Euro oder 1,4 % des weltweiten Vorjahresumsatzes des Unternehmens, dem sie angehört, der höhere Betrag
Registrierung, Selbstdeklaration oder Prüfbericht nicht fristgerecht; Selbstdeklaration wesentlich falsch; Prüfung nicht angekündigt	§ 45 Abs. 4 Z 1, 7 bis 10	bis 50.000 Euro, im Wiederholungsfall bis 100.000 Euro
Behörden und sonstige Stellen der öffentlichen Verwaltung, auch Gemeinden	§ 46 Abs. 2, § 39 Abs. 6	keine Geldstrafe nach § 45: Feststellung mit Bescheid und Frist, bei Nichtbefolgung Veröffentlichung; keine Untersagung von Leitungsaufgaben

09

Häufige Fehler

Was die Umsetzung von § 32 NISG 2026 und den Nachweis gegenüber der Cybersicherheitsbehörde in der Praxis erschwert.

- Leitung nur informiert: Genehmigung des Konzepts und die eigene Schulung jedes Mitglieds sind Aufgaben der Leitungsorgane; Restrisiken akzeptiert die Leitung oder eine befugte Person, die ihr berichtet (Anhang Nr. 1.1.1.1 lit. k, 2.1.1 DVO; § 31 Abs. 2 NISG 2026).
- Auslagerung als Entlastung: Laut BCS bleibt die Einrichtung selbst verantwortlich, auch wenn ein Dienstleister die IT betreibt; Anforderungen gehören soweit angemessen in den Vertrag (Nr. 5.1.4).
- Pläne nie getestet: Vorfalldreaktion, Notfallplan, Wiederherstellung und Krisenmanagement sind in geplanten Abständen zu testen (Nr. 3.5.5, 4.1.4, 4.2.6, 4.3.4).

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

NIS2-Betroffenheitscheck

tomoris.com/tools/nis2-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

10

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 **NISG 2026, BGBl. I Nr. 94/2025, geltende Fassung im RIS**
Fassung vom 25.10.2026 (Stammfassung); §§ 3 Z 11, 27, 29, 31 bis 33, 38, 39, 44 bis 46, 51; gelesen am 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=1051257
- 2 **NISV 2026, BGBl. II Nr. 290/2026, authentische Kundmachung im RIS**
§§ 2 bis 4 Risikomanagementmaßnahmen, § 7, § 9 Inkrafttreten; gelesen am 25.10.2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 3 **Bundesamt für Cybersicherheit: Erläuterungen zur NISV 2026 (PDF)**
Allgemeiner Teil, zu §§ 2, 4 und 8: Rahmen, DORA, § 7 analog, kompensierende Maßnahmen, Verweise; gelesen am 25.10.2026
www.bundesamt-cybersicherheit.gv.at/501/files/nisv-2026-erlaeut...
- 4 **Erläuterungen zur Regierungsvorlage NISG 2026 (308 d. B. XXVIII. GP), beim Bundesamt für Cybersicherheit (PDF)**
Zu §§ 31, 44 und 45 (Billigung, Strafadressat, § 9 VStG) und zu § 33 (Selbstdeklaration); gelesen am 25.10.2026
www.bundesamt-cybersicherheit.gv.at/501/files/nis-2026-gesetzes...
- 5 **Verwaltungsstrafgesetz 1991 (VStG), § 9, im RIS**
§ 9 Abs. 1 Verantwortlichkeit der zur Vertretung nach außen Berufenen; gelesen am 25.10.2026
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=1051257
- 6 **Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie), Art. 20 und 21**
Art. 20 Abs. 1 und Art. 21 Abs. 2; ABL L 333 vom 27.12.2022; gelesen am 25.10.2026
eur-lex.europa.eu/eli/dir/2022/2555/oj/deu
- 7 **Durchführungsverordnung (EU) 2024/2690, Art. 2 und Anhang**
Art. 1, 2 und Anhang Nr. 1 bis 13; ABL L vom 18.10.2024; gelesen am 25.10.2026
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu
- 8 **ENISA: NIS2 Technical Implementation Guidance, Juni 2025, Version 1.0**
Examples of evidence zu Nr. 1 bis 13, Guidance zu 4.3.2; laut ENISA nicht verbindlich; gelesen am 25.10.2026
www.enisa.europa.eu/publications/nis2-technical-implementation-...
- 9 **Bundesamt für Cybersicherheit: Registrierung**
Erstregistrierung bis 1.1.2027, spätestens 4.1.2027 (§ 33 Abs. 2 AVG), NIS2-Services; Seite vom 2.10.2026, gelesen am 25.10.2026
www.bundesamt-cybersicherheit.gv.at/303/registrierung.html
- 10 **Bundesamt für Cybersicherheit: Häufig gestellte Fragen, Registrierung**
Registrierung bis 31.12.2026 über das USP; Seite vom 25.9.2026, gelesen am 25.10.2026
www.bundesamt-cybersicherheit.gv.at/faq/registrierung.html
- 11 **Bundesamt für Cybersicherheit: Häufig gestellte Fragen, Geschäftsleitung**
Leitungsorgan, Schulung je Mitglied, keine Verwaltungsstrafen; Seite vom 25.9.2026, gelesen am 25.10.2026
www.bundesamt-cybersicherheit.gv.at/faq/geschaeftsleitung.html
- 12 **Bundesamt für Cybersicherheit: Häufig gestellte Fragen, Maßnahmen**
Verantwortung bei ausgelagerter IT; Seite vom 15.10.2026, gelesen am 25.10.2026
www.bundesamt-cybersicherheit.gv.at/faq/massnahmen.html
- 13 **Bundesamt für Cybersicherheit: Häufig gestellte Fragen, § 2 Anforderungen an Risikomanagementmaßnahmen**
Verhältnismäßigkeit mit Beispiel Tabellenkalkulation; Seite vom 20.10.2026, gelesen am 25.10.2026
www.bundesamt-cybersicherheit.gv.at/faq/anforderungen-an-risiko...
- 14 **Bundesamt für Cybersicherheit: Häufig gestellte Fragen, § 4 Kompensierende Maßnahmen**
Zeitplan bei vorübergehenden Abweichungen; Seite vom 20.10.2026, gelesen am 25.10.2026
www.bundesamt-cybersicherheit.gv.at/faq/kompensierende-massnahm...
- 15 **Bundesamt für Cybersicherheit: Häufig gestellte Fragen, Nachweise**
Selbstdeklaration bis 30.9.2027 über das USP, ISO 27001, Scope, Teilanerkennung; Seite vom 25.9.2026, gelesen am 25.10.2026
www.bundesamt-cybersicherheit.gv.at/faq/nachweise.html
- 16 **Bundesamt für Cybersicherheit: Überprüfungen durch unabhängige Stellen**
Aufforderung frühestens ab 1.10.2028, Fristen, Zertifikate mit Scope; Seite vom 21.9.2026, gelesen am 25.10.2026
www.bundesamt-cybersicherheit.gv.at/303/ueberpruefung-durch-una...