NIS2-Checkliste für Lieferantennachweise

Ein Arbeitsregister zum Anfordern, Nachverfolgen und Eskalieren von Sicherheitsnachweisen direkter Lieferanten und Dienstleister unter NIS2 (Richtlinie (EU) 2022/2555), Artikel 21(2)(d) und Artikel 21(3): Lieferantenregister, Kritikalitätsrubrik (T1/T2/T3), zehn Nachweiskategorien mit Kadenzen und ein dokumentierter Eskalationsprozess.

Dieses PDF ist der Begleiter zum Ausdrucken und Prüfen. Die Arbeitsdatei ist das XLSX (Dropdown-Listen, Lieferantenregister, Nachweis-Checkliste, Kritikalitätsrubrik); für KI-Agenten wird eine maschinenlesbare Markdown-Variante bereitgestellt. Alle drei Dateien sind kostenlos unter orbiqhq.com/templates/nis2-supplier-evidence-request-checklist verfügbar — ohne E-Mail-Adresse.

Rechtsgrundlage: Richtlinie (EU) 2022/2555 (NIS2), Artikel 21(2)(d) und 21(3); Durchführungsverordnung (EU) 2024/2690; ENISA Technical Implementation Guidance (Juni 2025) und Good Practices for Supply Chain Cybersecurity (Juni 2023). Diese Vorlage ist eine allgemeine Information, keine Rechtsberatung.

Lieferantenregister

Feldreferenz (das XLSX führt sie als Spalten; Beispielwerte aus Zeile 1):

Spalte	Beispielwert
Firmierung des Lieferanten	Northcloud ApS
Erbrachte Leistung	IaaS-Hosting für die Produktionsplattform (EU-West)
Vertragsreferenz	MSA-2024-011
Kaufmännischer Verantwortlicher	J. Meyer
Sicherheitsprüfer	A. Kraus
Sicherheitskontakt des Lieferanten	security@northcloud.example
Zugriffsebene	production
Datenkategorien	Personenbezogene Kundendaten, Zugangsdaten
Länder / Datenstandort	Dänemark / EU
Unterauftragnehmer offengelegt	yes
Kritikalitätsstufe	T1
Letzte vollständige Bewertung	2026-03-14
Nächste fällige Überprüfung	2027-03-14
Status	active
Anmerkungen	SOC 2 Type II erhalten; nächste Pentest-Zusammenfassung fällig Q3 2026

Kritikalitätsrubrik

Bewerten Sie jede Dimension und weisen Sie anschließend die Stufe anhand der Entscheidungsregel zu. Damit wird NIS2 Artikel 21(3) operationalisiert: die für jeden direkten Lieferanten spezifischen Schwachstellen, verhältnismäßig bewertet.

Dimension	Frage	Punktzahl 3	Punktzahl 2	Punktzahl 1
Serviceabhängigkeit	Würde ein Ausfall des Lieferanten die Erbringung Ihres wesentlichen/wichtigen Dienstes stören?	Sofortige Störung (< 24 h)	Beeinträchtigung innerhalb von Tagen	Keine wesentliche Auswirkung
Zugriff & Daten	Worauf kann der Lieferant zugreifen?	Produktionssysteme oder sensible / umfangreiche personenbezogene Daten	Interne Systeme oder begrenzte Daten	Kein Systemzugriff, keine nennenswerten Daten
Ersetzbarkeit	Wie schnell könnten Sie den Lieferanten ersetzen?	Monate oder länger (tiefe Integration, wenige Alternativen)	Wochen (Alternativen vorhanden)	Tage (Standardleistung)
Vorfallsexposition	Würde eine Kompromittierung des Lieferanten bei Ihnen plausibel einen nach NIS2 Artikel 23 meldepflichtigen Sicherheitsvorfall auslösen?	Ja, unmittelbar	Mittelbar / unklar	Nein

Entscheidungsregel: Gesamtpunktzahl 10–12, oder Punktzahl 3 SOWOHL bei Serviceabhängigkeit ALS AUCH bei Vorfallsexposition → T1. Gesamtpunktzahl 7–9 → T2. Gesamtpunktzahl 4–6 → T3.

• T1: vollständiger Nachweissatz (E1–E10); jährliche Neubewertung; vierteljährliches Monitoring; ereignisgesteuerte Neuanforderungen

• T2: Kern-Nachweissatz (E1–E4, E6–E8); jährliche Überprüfung

• T3: E2 oder Selbstattestierung, E6, E7; alle 3 Jahre / bei Vertragsverlängerung

Nachweis-Checkliste

Feldreferenz (das XLSX führt sie als Spalten; Beispielwerte aus Zeile 1):

Spalte	Beispielwert
Firmierung des Lieferanten	Northcloud ApS
ID	E2
Nachweiskategorie	Zertifizierungen & unabhängige Prüfung
Was anzufordern ist	Aktuelles Zertifikat bzw. aktuelle Attestierung, deren Geltungsbereich die gehostete Leistung abdeckt
Akzeptable Nachweistypen	ISO/IEC 27001-Zertifikat mit Geltungsbereich + Ablaufdatum; SOC 2 Type II-Bericht (+ Bridge Letter, wenn älter als 12 Monate); C5, sofern relevant
NIS2-Anker	Art. 21(3) — Qualität der Praktiken
Kadenz (T1 / T2 / T3)	Jährlich + Ablauf-Benachrichtigungen / Jährlich / Alle 3 Jahre
Datum der Anforderung	2026-02-10
Datum des Eingangs	2026-03-01
Status	reviewed-accepted
Prüfer	A. Kraus
Anmerkungen	ISO 27001 gültig bis 2027-09; Geltungsbereich deckt die Region EU-West ab

Die zehn Nachweiskategorien

Fordern Sie jede für die Stufe des Lieferanten geltende Kategorie an. Anwendbarkeit je Stufe: T1 = E1–E10 · T2 = E1–E4, E6–E8 · T3 = E2 (oder eine unterzeichnete Selbstattestierung), E6, E7.

ID	Nachweiskategorie
E1	Sicherheits-Governance / ISMS
E2	Zertifizierungen & unabhängige Prüfung
E3	Penetrationstests
E4	Schwachstellen- & Patch-Management
E5	Sichere Entwicklung
E6	Unterauftragnehmer- / Vierte-Partei-Offenlegung
E7	SLA zur Vorfallsmeldung
E8	Business Continuity & Disaster Recovery
E9	Zugriffskontrolle & Kryptografie
E10	Personalsicherheit & Sensibilisierung

Anleitung

Schritt	Maßnahme	Wo
1	Erfassen Sie jeden direkten Lieferanten und Dienstleister: Leistung, Vertrag, Verantwortliche, Kontakte, Zugriffsebene, Datenkategorien, Offenlegung der Unterauftragnehmer.	Lieferantenregister
2	Bewerten Sie den Lieferanten anhand der vier Dimensionen der Rubrik und weisen Sie mit der Entscheidungsregel eine Stufe zu (T1/T2/T3). Bewerten Sie bei jeder wesentlichen Änderung oder jedem Vorfall neu.	Kritikalitätsrubrik
3	Legen Sie die für die Stufe geltenden Nachweiszeilen an (T1 = E1–E10; T2 = E1–E4, E6–E8; T3 = E2/Attestierung, E6, E7) und senden Sie die Anforderungen an den Sicherheitskontakt des Lieferanten.	Nachweis-Checkliste
4	Verfolgen Sie den Status je Zeile. Prüfen Sie den Geltungsbereich des Zertifikats, nicht nur dessen Existenz. Lehnen Sie Nachweise ab, die älter sind als das Kadenzfenster, und fordern Sie sie mit Begründung erneut an.	Nachweis-Checkliste
5	Eskalieren Sie bei ausbleibender Antwort: Erinnerung nach 10 Arbeitstagen; kaufmännische Eskalation nach 20; formelle Aufforderung unter Berufung auf die Audit-/Nachweisklausel des Vertrags nach 30; dokumentierte Risikoentscheidung (akzeptieren / kompensieren / einschränken / kündigen) nach 45. Protokollieren Sie jeden Schritt — der Verlauf ist selbst Compliance-Nachweis.	Anmerkungen in der Nachweis-Checkliste
6	Frischen Sie im Turnus auf (T1 jährlich + vierteljährliches Monitoring; T2 jährlich; T3 alle drei Jahre bzw. bei Verlängerung) sowie bei Ereignisauslösern: Sicherheitsvorfall beim Lieferanten, Wechsel eines Unterauftragnehmers, Zertifikatsablauf, Änderung des Geltungsbereichs, Feststellungen aus koordinierten Risikobewertungen nach Artikel 22(1).	Alle Blätter
7	Rechtsgrundlage: Richtlinie (EU) 2022/2555 Art. 21(2)(d) und 21(3); Durchführungsverordnung (EU) 2024/2690; ENISA Technical Implementation Guidance (Juni 2025) und Good Practices for Supply Chain Cybersecurity (Juni 2023). Diese Arbeitsmappe ist eine allgemeine Information, keine Rechtsberatung.	—