NIS2-checklist voor bewijsaanvragen bij leveranciers

Het leveranciersregister dat NIS2 vereist, klaar om in te vullen: een register met toegangsniveau en gegevenscategorieën, een criticaliteitsrubriek met vier dimensies, tien bewijscategorieën (E1–E10) gemapt op artikel 21, lid 2, met frequenties per niveau, en een escalatieworkflow in vier fasen voor leveranciers die niet reageren.

Dit PDF is de veldgids. Het werkbestand is de XLSX (vier werkbladen met keuzelijsten); een machine-leesbare Markdown-variant is er voor AI-agents. Alle drie zijn gratis op orbiqhq.com/templates/nis2-supplier-evidence-request-checklist — geen e-mail vereist.

Rechtsgrondslag: Richtlijn (EU) 2022/2555 (NIS2), artikel 21, lid 2, onder d), en artikel 21, lid 3; Uitvoeringsverordening (EU) 2024/2690 van de Commissie; de technische implementatierichtlijn van ENISA (juni 2025). Dit sjabloon is een hulpmiddel, geen juridisch advies.

Leveranciersregister

Veldreferentie (de XLSX voert deze als kolommen; voorbeeldwaarden uit rij 1):

Kolom	Toelichting	Voorbeeldwaarde
Naam leverancier		Northcloud ApS
Geleverde dienst	Beschrijf de dienst die u afneemt, niet de catalogus van de leverancier	IaaS-hosting voor het productieplatform (EU-West)
Contractreferentie		MSA-2024-011
Commercieel eigenaar		J. Meyer
Security-reviewer		A. Kraus
Beveiligingscontact leverancier		security@northcloud.example
Toegangsniveau	Het hoogste niveau dat van toepassing is	production
Gegevenscategorieën		Persoonsgegevens van klanten, inloggegevens
Landen / gegevenslocatie		Denemarken / EU
Onderaannemers bekendgemaakt		yes
Criticaliteitsniveau	Scoor eerst met het werkblad Criticaliteitsrubriek	T1
Laatste volledige beoordeling		2026-03-14
Volgende beoordeling uiterlijk	Afgeleid van de frequentie van het niveau	2027-03-14
Status		active
Notities		SOC 2 Type II ontvangen; volgende pentestsamenvatting verwacht in Q3 2026

Toegestane waarden — Toegangsniveau: none, network, data-readonly, data-readwrite, production · Onderaannemers bekendgemaakt: yes, no, requested · Criticaliteitsniveau: T1, T2, T3 · Status: active, onboarding, under-review, escalated, offboarding.

Bewijschecklist

Veldreferentie (de XLSX voert deze als kolommen; voorbeeldwaarden uit rij 1):

Kolom	Toelichting	Voorbeeldwaarde
Naam leverancier		Northcloud ApS
ID	E1–E10 — de bewijscategorie	E2
Bewijscategorie		Certificeringen & onafhankelijke assurance
Wat u opvraagt		Het actuele certificaat of de actuele verklaring waarvan de scope de gehoste dienst dekt
Aanvaardbare bewijstypen		ISO/IEC 27001-certificaat met scope + vervaldatum; SOC 2 Type II-rapport (+ bridge letter als het ouder is dan 12 maanden); C5 waar relevant
NIS2-grondslag		Art. 21, lid 3 — kwaliteit van de praktijken
Frequentie (T1 / T2 / T3)		Jaarlijks + alerts bij verval / Jaarlijks / Elke 3 jaar
Datum aangevraagd		2026-02-10
Datum ontvangen		2026-03-01
Status		reviewed-accepted
Reviewer		A. Kraus
Notities		ISO 27001 geldig tot 2027-09; de scope dekt de regio EU-West

Toegestane waarden — ID: E1, E2, E3, E4, E5, E6, E7, E8, E9, E10 · Bewijscategorie: Securitygovernance / ISMS, Certificeringen & onafhankelijke assurance, Penetratietesten, Kwetsbaarheden- & patchbeheer, Veilige ontwikkeling, Openbaarmaking onderaannemers / vierde partijen, SLA voor incidentmelding, Bedrijfscontinuïteit & uitwijk, Toegangsbeheer & cryptografie, Personeelsbeveiliging & bewustzijn · Status: not-requested, requested, received, reviewed-accepted, reviewed-rejected, overdue, escalated, not-applicable.

Criticaliteitsrubriek

Scoor elke dimensie en ken vervolgens het niveau toe met de beslisregel. Dit operationaliseert artikel 21, lid 3, NIS2: de kwetsbaarheden die specifiek zijn voor elke directe leverancier, proportioneel beoordeeld.

Dimensie	Vraag	Score 3	Score 2	Score 1
Afhankelijkheid van de dienst	Zou uitval van de leverancier de levering van uw essentiële/belangrijke dienst verstoren?	Directe verstoring (< 24 u)	Verslechtering binnen enkele dagen	Geen materiële impact
Toegang & gegevens	Waar kan de leverancier bij?	Productiesystemen of gevoelige/grootschalige persoonsgegevens	Interne systemen of beperkte gegevens	Geen systeemtoegang, geen betekenisvolle gegevens
Vervangbaarheid	Hoe snel kunt u de leverancier vervangen?	Maanden of langer (diepe integratie, weinig alternatieven)	Weken (er zijn alternatieven)	Dagen (inwisselbaar)
Blootstelling aan incidenten	Zou een compromittering bij de leverancier voor u aannemelijk een meldplichtig incident onder artikel 23 NIS2 opleveren?	Ja, rechtstreeks	Indirect / onzeker	Nee

Beslisregel: totaal 10–12, of score 3 op ZOWEL Afhankelijkheid van de dienst ALS Blootstelling aan incidenten → T1. Totaal 7–9 → T2. Totaal 4–6 → T3.

Niveau	Bewijsset en ritme
T1 (Kritiek)	Volledige bewijsset (E1–E10); jaarlijkse herbeoordeling; monitoring per kwartaal; hernieuwde aanvragen bij gebeurtenissen
T2 (Belangrijk)	Kernset (E1–E4, E6–E8); jaarlijkse review
T3 (Standaard)	E2 of een eigen verklaring, E6, E7; elke 3 jaar / bij verlenging

Instructies

Stap	Actie	Waar
1	Leg elke directe leverancier en dienstverlener vast: dienst, contract, eigenaren, contactpersonen, toegangsniveau, gegevenscategorieën en de opgave van onderaannemers.	Leveranciersregister
2	Scoor de leverancier op de vier dimensies van de rubriek en ken met de beslisregel een niveau toe (T1/T2/T3). Herscoor bij elke materiële wijziging of elk incident.	Criticaliteitsrubriek
3	Maak de bewijsrijen aan die bij het niveau horen (T1 = E1–E10; T2 = E1–E4, E6–E8; T3 = E2/verklaring, E6, E7) en stuur de aanvragen naar het beveiligingscontact van de leverancier.	Bewijschecklist
4	Volg de status per rij. Controleer de scope van het certificaat, niet alleen het bestaan ervan. Wijs bewijs af dat ouder is dan het frequentievenster en vraag het opnieuw op, met opgave van reden.	Bewijschecklist
5	Escaleer bij stilte: een herinnering na 10 werkdagen; commerciële escalatie na 20; een formele aanmaning met een beroep op de audit-/bewijsbepaling uit het contract na 30; een gedocumenteerd risicobesluit (accepteren / compenseren / beperken / beëindigen) na 45. Log elke stap — het spoor is zelf compliancebewijs.	Notities in de Bewijschecklist
6	Ververs op frequentie (T1 jaarlijks + monitoring per kwartaal; T2 jaarlijks; T3 driejaarlijks/bij verlenging) en bij triggers op gebeurtenissen: een incident bij de leverancier, een wisseling van onderaannemer, een verlopen certificaat, een scopewijziging, of bevindingen uit de gecoördineerde risicobeoordeling van artikel 22, lid 1.	Alle werkbladen
7	Rechtsgrondslag: Richtlijn (EU) 2022/2555, art. 21, lid 2, onder d), en art. 21, lid 3; Uitvoeringsverordening (EU) 2024/2690; de technische implementatierichtlijn van ENISA (juni 2025) en Good Practices for Supply Chain Cybersecurity (juni 2023). Deze werkmap bevat algemene informatie, geen juridisch advies.	—