NIS2-compliance-checklist — Artikel 21(2)

Alle tien risicobeheermaatregelen met de ISMS-hiaatbeoordeling — v1.0 · 2026-07-16

#	Maatregel (art. 21(2))	ISMS-dekking	Het hiaat	Wat te doen	Prioriteit
(a)	**Beleid inzake risicoanalyse en informatiesysteembeveiliging**	Gedekt door ISMS	—	Zorg dat de risicoanalyse de NIS2-specifieke operationele aspecten dekt: incidentmelding, toeleveringsketen, bewijs van effectiviteit.	**Laag**
(b)	**Incidentafhandeling**	Fundament — operationele aanvulling nodig	Operationele 24u/72u-capaciteit onder tijdsdruk — coördinatie tussen security, legal, communicatie en bestuur.	Bouw incidentbeheer verder dan het plan: tabletop-oefeningen tegen de 24-uursdeadline; sjablonen voor alle drie meldfasen.	**Hoog**
(c)	**Bedrijfscontinuïteit en crisisbeheer**	Gedekt door ISMS	—	Controleer of de BCM-plannen cyberincidenten met gelijktijdige meldverplichtingen (artikel 23) dekken.	**Laag**
(d)	**Toeleveringsketenbeveiliging**	Fundament — operationele aanvulling nodig	Continue monitoring in plaats van jaarlijkse momentopnamen; gebeurtenisgestuurde herbeoordelingen; opvraagbaar leveranciersbewijs.	Bouw monitoringcapaciteit; verschuif van cyclische naar triggergestuurde beoordelingen; neem NIS2-clausules op in contracten; maak bewijs op afroep beschikbaar.	**Hoog**
(e)	**Beveiliging bij verwerving, ontwikkeling en onderhoud**	Gedekt door ISMS	Kwetsbaarheidsbekendmaking toetsen aan de ENISA-implementatierichtsnoeren.	Controleer of de bekendmakingsprocessen voldoen aan de NIS2-/ENISA-verwachtingen — die gaan verder dan typische ISMS-implementaties.	**Midden**
(f)	**Effectiviteitsbeoordeling van risicobeheermaatregelen**	Fundament — operationele aanvulling nodig	Continu beschikbaar bewijs in plaats van documentatie op auditritme.	Verschuif bewijsbeheer naar continue beschikbaarheid: versiebeheer, geldigheidsperioden, eigenaarschap; verzoeken van autoriteiten binnen dagen kunnen beantwoorden.	**Hoog**
(g)	**Cyberhygiëne en cybersecuritytraining**	Gedekt door ISMS	Aantoonbare trainingsdeelname van het bestuur.	Zorg dat het bestuur aantoonbaar deelneemt aan cybersecuritytraining — dit bewijs is direct aansprakelijkheidsrelevant.	**Laag**
(h)	**Cryptografie en encryptie**	Gedekt door ISMS	—	Houd het cryptografiebeleid actueel en afgestemd op de stand van de techniek.	**Laag**
(i)	**Personeelsbeveiliging, toegangscontrole en activabeheer**	Gedekt door ISMS	—	Bevestig de MFA-dekking waar NIS2 die vereist (zie maatregel (j)).	**Laag**
(j)	**MFA, beveiligde communicatie en noodcommunicatie**	Gedeeltelijk gedekt	Beveiligde noodcommunicatiekanalen die onafhankelijk van de reguliere (mogelijk gecompromitteerde) infrastructuur werken.	Auditeer de MFA-dekking; richt noodkanalen in die onafhankelijk zijn van de reguliere infrastructuur; borg versleutelde communicatie voor incidentcoördinatie.	**Midden**

Plichten art. 23 & art. 20

Verplichting	Deadline / regel	Rechtsgrondslag
Vroegtijdige waarschuwing aan het CSIRT of de bevoegde autoriteit	Binnen 24 uur na kennisname van een significant incident	Art. 23(4)(a)
Incidentmelding	Binnen 72 uur na kennisname — beoordeling incl. ernst, impact, indicatoren van compromittering	Art. 23(4)(b)
Eindverslag	Binnen één maand na de incidentmelding	Art. 23(4)(d)
Goedkeuring van en toezicht op de risicobeheermaatregelen door het bestuur	Doorlopend — het bestuur keurt de maatregelen goed, ziet toe op de uitvoering en kan aansprakelijk worden gesteld	Art. 20(1)
Cybersecuritytraining voor het bestuur	Regelmatig — bestuursleden zijn verplicht training te volgen	Art. 20(2)

Hoe u deze checklist gebruikt

1. Doorloop elk van de tien maatregelen uit artikel 21(2) en beoordeel eerlijk: niet 'hebben we een proces?', maar 'kunnen we dit operationeel uitvoeren onder tijdsdruk, richting externe partijen, met verifieerbaar bewijs?'

2. Gebruik de prioriteitskolom als startpunt: de drie Hoog-hiaten (incidentafhandeling, toeleveringsketen, bewijs van effectiviteit) dragen de hoogste regelgevende urgentie.

3. Plan per hiaat de operationele opbouw: welk systeem, proces of vermogen is concreet nodig?

4. Houd het ISMS als interne controlelaag en vul het aan met de operationele laag die NIS2 aanvullend vereist.

5. Volg status, eigenaar en bewijs per maatregel in het checklistblad — toezichthouders kunnen op elk moment bewijs opvragen.

Volledige toelichting per maatregel, bronnen en de ISMS-hiaatanalyse:
https://www.orbiqhq.com/nl/eu-regelgeving/nis2-compliance-checklist-artikel-21