ZELFEVALUATIE

NIS2 zelfevaluatie checklist

De NIS2-richtlijn is in Nederland ingevoerd als de Cyberbeveiligingswet, die op 15 augustus 2026 in werking is getreden. Met tien vragen schat u in of uw organisatie onder de wet valt en hoe ver u bent met de kernverplichtingen. Reken op tien minuten; meer dan uw organogram en omzetcijfers heeft u niet nodig.

Deel A Valt u onder de wet?

1	**Behoort uw organisatie tot een sector van hoog kritiek belang?** Energie, vervoer, bankwezen, financiële marktinfrastructuur, gezondheidszorg, drinkwater, afvalwater, digitale infrastructuur, beheer van ICT-diensten, overheid of ruimtevaart.	☐ ja	☐ nee
2	**Behoort uw organisatie tot een andere kritieke sector?** Post- en koeriersdiensten, afvalbeheer, chemie, levensmiddelen, industrie (onder meer medische hulpmiddelen en elektronica), digitale aanbieders of onderzoek.	☐ ja	☐ nee
3	**Is uw organisatie middelgroot of groter?** Vijftig of meer medewerkers, of een jaaromzet en balanstotaal boven de 10 miljoen euro.	☐ ja	☐ nee
4	**Bent u kleiner, maar de enige aanbieder van een essentiële dienst?** Voor organisaties met een onmisbare rol voor samenleving of economie kan de wet ook onder de omvangsgrens gelden.	☐ ja	☐ nee
5	**Levert u aan organisaties die zelf onder de wet vallen?** Via de ketenbeveiliging stellen die klanten eisen aan u, ook wanneer u zelf buiten de wet valt.	☐ ja	☐ nee

Tussenstand. Vraag 1 of 2 én vraag 3 met ja beantwoord: uw organisatie valt vrijwel zeker onder de wet. Alleen vraag 4 of 5 met ja: de wet raakt u direct of via uw klanten, behandel deel B als uw werklijst. Overal nee: de wet geldt niet voor u, maar klanten en verzekeraars stellen steeds vaker dezelfde eisen.

Deel B Hoe ver bent u?

6 **Heeft u een actuele risicoanalyse?** ☐ ja ☐ nee
Van uw belangrijkste systemen en processen, niet ouder dan een jaar en vastgesteld door het bestuur.

7 **Kunt u een ernstig incident binnen 24 uur melden?** ☐ ja ☐ nee
Het meldproces is beschreven, de contactgegevens van het NCSC en uw toezichthouder zijn bekend en het proces is geoefend.

8 **Is uw bestuur aantoonbaar betrokken?** ☐ ja ☐ nee
Bestuurders keuren de maatregelen goed, volgen opleiding en zijn persoonlijk aanspreekbaar op de naleving.

9 **Stelt u beveiligingseisen aan uw leveranciers?** ☐ ja ☐ nee
Vastgelegd in contracten of inkoopvoorwaarden, met periodieke toetsing.

10 **Kunt u uw maatregelen bewijzen?** ☐ ja ☐ nee
Beleid, procedures en logboeken zijn gedocumenteerd, actueel en klaar voor een audit.

Drie vervolgstappen

Elke nee in deel B is een werkpunt. Begin met de drie stappen die de meeste urgentie hebben.

1. **Bepaal uw categorie.** Essentiële entiteiten vallen onder actief toezicht, belangrijke entiteiten worden achteraf getoetst. De verplichtingen zijn vrijwel gelijk; het verschil zit in het toezicht en de boetes.
2. **Beleg het eigenaarschap.** Wijs één bestuurder aan met cyberbeveiliging in de portefeuille en laat het bestuur de risicoanalyse vaststellen. De wet spreekt bestuurders persoonlijk aan.
3. **Richt het meldproces in.** Een incident wacht niet op kantooruren. Leg vast wie meldt, binnen welke termijn en bij wie — de Meldprocedure en meldingenlogboek (C3) uit de Toolbox geeft hiervoor het format.

De kernvereisten op een rij

Risicobeheer	Gestructureerde identificatie en beheersing van cyberrisico's
Incidentmelding	Vroegtijdige waarschuwing binnen 24 uur, volledige melding binnen 72 uur, eindverslag binnen een maand
Kritieke diensten	Hogere norm voor organisaties in kritieke sectoren
Ketenbeveiliging	Eisen aan leveranciers en partners
Audit en bewijs	Uitgebreide documentatie en periodieke audits

Verder met documenten.nl. Hoe de vijf kaders samenhangen, van wet naar techniek, leest u op documenten.nl/compliancy. De Positiescan en de overige instrumenten vindt u op documenten.nl/toolbox.