SAMOERAI
INFORMATIEBEVEILIGING

STAPPENPLAN · NIS2

6 STAPPEN NAAR NIS2-COMPLIANCE

Een praktische route naar aantoonbare informatiebeveiliging

HET TRAJECT IN ZES STAPPEN

01
Scope & Einddoel

02
Beleid en planning

03
Risicomanagement

04
Beheersmaatregelen

05
Controle & Naleving

06
Audit & Externe toetsing

Grip op NIS2 begint hier

Een praktische route naar aantoonbare informatiebeveiliging

De NIS2-richtlijn (Network and Information Security Directive 2) is Europese wetgeving die organisaties verplicht om aantoonbaar grip te hebben op hun informatiebeveiliging. In Nederland is deze richtlijn uitgewerkt in de Cyberbeveiligingswet, die op 15 augustus 2026 in werking is getreden.

Waar eerdere wetgeving zich beperkte tot een paar vitale sectoren, geldt de NIS2 voor een veel bredere groep organisaties, óók binnen het mkb.

U moet als organisatie kunnen bewijzen dat u in control bent over uw digitale risico's en beveiligingsmaatregelen

De 6 kernverplichtingen van de NIS2

1. **Risicobeheer en passende beveiligingsmaatregelen.** U moet risico's identificeren en passende maatregelen treffen om ze te beperken.
2. **Beveiliging van de toeleveringsketen.** U bent verantwoordelijk voor de beveiliging van uw belangrijkste leveranciers en partners.
3. **Meldplicht bij incidenten.** Ernstige incidenten meldt u binnen 24 uur (eerste melding) en binnen 72 uur (uitgebreide melding) aan het CSIRT en de toezichthouder.
4. **Continuïteitsbeheer en herstelvermogen.** U moet kunnen aantonen dat uw organisatie kan blijven functioneren tijdens storingen of aanvallen.
5. **Bewustwording en training.** Medewerkers en bestuurders moeten worden opgeleid en betrokken bij veilig werken.
6. **Aantoonbare naleving en toezicht.** U moet kunnen bewijzen dat uw beveiliging op orde is en voldoet aan de wet.

Hoe gebruikt u dit 6-stappenplan

- ✓ U krijgt overzicht van de belangrijkste verplichtingen
- ✓ U ontdekt hoe u zelf al de eerste stappen kunt zetten
- ✓ U ziet hoe u risico's in kaart brengt en maatregelen prioriteert
- ✓ U ontdekt hoe u toetst of uw organisatie klaar is voor toezicht

Met dit stappenplan zet u vandaag de eerste stap richting NIS2-compliance.

NIS2 in 2026

Voor wie de wet geldt, wat er is veranderd en waarom u nu moet starten

Wie valt onder de NIS2?

De wet geldt voor:

- **Essentiële entiteiten**, zoals energie-, zorg-, transport- en overheidsorganisaties.
- **Belangrijke entiteiten**, zoals IT-dienstverleners, maakindustrie, logistiek, financiële en digitale dienstverleners.

In de regel gaat het om organisaties vanaf 50 medewerkers of € 10 miljoen jaaromzet. Overheidsorganisaties en een aantal digitale dienstverleners vallen er ongeacht hun omvang onder. Ook bedrijven die onderdeel zijn van de keten van deze entiteiten krijgen vaak indirect met de verplichtingen te maken.

Wat is er veranderd?

15 aug 2026

Cyberbeveiligingswet van kracht

Er is geen algemene overgangstermijn. De zorgplicht, de meldplicht en de registratieplicht gelden direct.

8.000+

Organisaties in 18 sectoren

Zij moeten zich registreren in het entiteitenregister van het NCSC en vallen onder toezicht.

€ 10 miljoen

Maximale boete

Voor essentiële entiteiten, of 2% van de wereldwijde jaaromzet. Voor belangrijke entiteiten is dat € 7 miljoen of 1,4%.

Waarom nu beginnen?

De Cyberbeveiligingswet is geen verwachting meer, maar een feit. Toezichthouders verwachten dat organisaties nu aantoonbaar aan compliance werken. Veel organisaties hebben deze stap bovendien al genomen.

Wie te laat begint, loopt risico op:

- Sancties en reputatieschade;
- Vertraging bij aanbestedingen of ketenverplichtingen;
- Uitsluiting door klanten en partners die zelf wél voldoen;
- Verlies van vertrouwen bij klanten en partners.

Dit 6-stappenplan helpt u om vandaag nog te starten met een gestructureerde aanpak. Het laat zien wat u zelf kunt doen, waar de grootste valkuilen liggen, en hoe u stap voor stap grip krijgt op informatiebeveiliging, zonder overweldigd te raken.

→ Ga verder naar Stap 1 - Scope & Einddoel

STAP 1

Scope & Einddoel

01

Weet wat u moet beschermen en waarom

Zonder een duidelijke scope kunt u geen risico's inschatten, geen maatregelen onderbouwen en geen audit doorstaan.

WAAROM DEZE STAP BELANGRIJK IS

- U voorkomt dat u te veel (onnodig duur) of te weinig (risicovol) beveiligt.
- U creëert overzicht: welke systemen, processen en locaties horen erbij?
- U maakt helder wie verantwoordelijk is voor welke onderdelen.

Een onduidelijke scope is de #1 oorzaak van mislukte audits en incomplete beveiligingsmaatregelen

WAT U IN DEZE STAP GAAT DOEN

Beschrijf de scope van uw organisatie

Beantwoord vragen zoals:

- Welke diensten levert uw organisatie?
- Welke processen zijn essentieel?
- Welke IT-systemen ondersteunen deze processen?
- Welke locaties of afdelingen vallen binnen de reikwijdte?

Wijs verantwoordelijkheden toe

- Proceseigenaar
- Systeembeheerder
- Informatiebeheerder
- Security- of IT-verantwoordelijke

Leg de scope en verantwoordelijkheden vast

Dit document wordt later gebruikt tijdens audits, risicobeoordelingen en managementreviews. Wat u vastlegt:

- Scopeomschrijving
- Uitsluitingen (en waarom)
- Processen en systemen binnen scope
- Rollen en verantwoordelijkheden

NIS2 Stel vast of uw organisatie een essentiële of belangrijke entiteit is en registreer uw organisatie in het entiteitenregister van het NCSC. Dit is sinds 15 augustus 2026 een wettelijke verplichting.

VALKUILEN IN DEZE STAP

- ✕ Te breed starten → leidt tot onnodige maatregelen en kosten.
- ✕ Verantwoordelijkheden niet officieel vastleggen → auditors beoordelen dit als "niet aantoonbaar".
- ✕ Te smal starten → leidt tot gaten in de risicoanalyse.

→ Ga verder naar Stap 2 - Beleid en planning

STAP 2

Beleid en planning

02

Zorg voor richting, structuur en aantoonbare controle

De NIS2 vraagt niet alleen om maatregelen, maar vooral om duidelijk beleid en planning. Zonder beleid is er geen richting. Zonder planning is er geen borging.

Beleid vormt de fundering voor uw ISMS en bepaalt hoe u risico's beheert, maatregelen uitvoert en naleving organiseert.

WAAROM DEZE STAP BELANGRIJK IS

Een sterk beleid zorgt ervoor dat:

- Uw organisatie consistent en gestructureerd werkt;
- U kunt verantwoorden waarom bepaalde keuzes zijn gemaakt;
- en het management weet wat zijn verantwoordelijkheden zijn op het gebied van beveiliging.
- Iedereen dezelfde beveiligingsafspraken volgt;
- Audits soepel verlopen dankzij duidelijke documentatie;

WAT U IN DEZE STAP GAAT DOEN

Begin met de kern

Deze documenten vormen het fundament waarop andere maatregelen worden gebouwd:

- Informatiebeveiligingsbeleid
- Risicomanagement
- Toegangsbeheer
- Incidentmanagement
- Continuïteitsbeleid

Werk de scope- en documentatieplanning bij

Wanneer nieuwe beleidsregels worden opgesteld, vult u de scopedocumentatie aan met:

- Verantwoordelijkheden;
- Processen die nieuw zijn toegevoegd;
- Governance-afspraken;
- en reviewmomenten.

Plan de governance & reviews

De NIS2 verplicht organisaties om beleid periodiek te toetsen en bij te werken. Dit omvat:

- Managementreviews;
- Periodieke beleidsupdates;
- Risicobeoordelingen;
- en opvolging van verbeterpunten.

NIS2 Het bestuur is eindverantwoordelijk. Bestuurders moeten het cyberrisicobeleid aantoonbaar goedkeuren, erop toezien en zich erin laten trainen.

CHECKLIST VOOR STAP 2

- [ ] Zijn de basisbeleidsdocumenten opgesteld of bijgewerkt?
- [ ] Sluiten alle beleidsregels aan op de NIS2-verplichtingen?
- [ ] Zijn reviewmomenten, governance en planning gedocumenteerd?
- [ ] Zijn nieuwe beleidsregels toegevoegd op basis van risico's en scope?
- [ ] Is vastgelegd wie eigenaar is van elk beleidsonderdeel?
- [ ] Is de scopedocumentatie bijgewerkt?

→ Ga verder naar Stap 3 - Risicomanagement

STAP 3

Risicomanagement

03

Inzicht in risico's is inzicht in controle

De wet vraagt dat organisaties systematisch risico's identificeren, beoordelen en behandelen. Dat is niet alleen een wettelijke verplichting, maar ook de enige manier om gericht en effectief te beveiligen.

Inzicht in risico's = inzicht in waar uw organisatie kwetsbaar is én welke maatregelen het meest waarde toevoegen.

WAAROM DEZE STAP BELANGRIJK IS

- U ontdekt welke processen en systemen echt kritisch zijn.
- U voldoet aan de centrale verplichting van de NIS2.
- U creëert een aantoonbare, logische onderbouwing richting auditors.
- U kunt beveiligingsmaatregelen prioriteren op basis van impact.
- U voorkomt onder- of overbeveiliging.

WAT U IN DEZE STAP GAAT DOEN

Voer een Business Impact Assessment (BIA) uit

Met een BIA bepaalt u hoe essentieel processen zijn voor uw organisatie. Bijvoorbeeld:

- Wat is de impact als een proces 1 uur uitvalt?
- En als dat 24 uur duurt?
- Welke processen raken de klant direct?
- Welke processen raken de bedrijfsvoering het meest?

Identificeer dreigingen & kwetsbaarheden

Breng in kaart:

- Welke dreigingen relevant zijn;
- Welke kwetsbaarheden aanwezig zijn;
- en welke scenario's het meest realistisch zijn.

Voer een risicoanalyse uit

Per proces, applicatie en/of systeem beoordeelt u:

- Kans: hoe waarschijnlijk is het dat het risico optreedt?
- Impact: hoe groot is de schade als het gebeurt?
- Huidige beheersmaatregelen: wat is er al geregeld?
- Restrisico: wat blijft er over?

NIS2 Neem risico's in uw toeleveringsketen expliciet mee in de analyse. U bent verantwoordelijk voor de beveiliging van uw belangrijkste leveranciers en partners.

VALKUILEN IN DEZE STAP

- ✕ Te technisch kijken → risico's gaan niet alleen over IT; ook processen, menselijk gedrag en organisatie spelen mee.
- ✕ Geen sluitende risicoprocedure → zonder proces is er geen auditbare herhaalbaarheid.
- ✕ Te veel risico's tegelijk analyseren → begin bij de kritieke processen, niet bij elk detail.
- ✕ Maatregelen kiezen zonder risico-onderbouwing → auditors beoordelen dit als niet aantoonbaar.

→ Ga verder naar Stap 4 - Beheersmaatregelen

STAP 4

Beheersmaatregelen

04

Vertaal plannen naar aantoonbare actie

Dit is de fase waarin de strategie tastbaar wordt: u gaat beveiliging daadwerkelijk inrichten, verbeteren en borgen.

Een goed plan heeft pas waarde wanneer het is uitgevoerd én aantoonbaar werkt.

WAAROM DEZE STAP BELANGRIJK IS

- U verkleint direct de grootste risico's.
- U versterkt de digitale weerbaarheid van uw systemen en medewerkers.
- U creëert bewijs dat maatregelen niet alleen gepland zijn, maar ook echt uitgevoerd worden.
- U bouwt voort op de fundering uit stap 1 t/m 3.

WAT U IN DEZE STAP GAAT DOEN

Implementeer technische maatregelen

Dit zijn maatregelen die uw systemen, netwerken en applicaties direct beschermen. Voorbeelden zijn:

- Multi-Factor Authenticatie (MFA)
- Patching & updatebeleid
- Firewalls & netwerksegmentatie
- Logging & monitoring
- Encryptie
- Back-ups & herstelprocedures

Implementeer organisatorische maatregelen

Deze omvatten:

- Beleid en procedures (incidenten, wijzigingen, toegangsbeheer)
- Governance-afspraken
- Verantwoordelijkheden per rol
- Leveranciersmanagement
- Documentatie en communicatie

Richt awareness & training in

Menselijk handelen is bij 80% van de beveiligingsincidenten een factor. De NIS2 verplicht daarom structurele bewustwording. Voorbeelden:

- Jaarlijkse security awareness-training
- Phishing-simulaties
- Onboarding met securityrichtlijnen
- Instructies voor meldplicht en incidentherkenning

Documenteer alle maatregelen in uw ISMS

Implementatie is niet klaar zonder documentatie. U moet kunnen aantonen:

- Welke maatregelen zijn uitgevoerd;
- Wanneer ze zijn uitgevoerd;
- Waarom ze gekozen zijn;
- Hoe ze worden beheerd en onderhouden.

NIS2 Richt uw meldproces in. Ernstige incidenten meldt u binnen 24 uur (eerste melding) en binnen 72 uur (uitgebreide melding) aan het CSIRT en de toezichthouder. Binnen een maand volgt een eindrapport.

VALKUILEN IN DEZE STAP

- ✕ Te veel tegelijk willen implementeren → begin met de risico's met de hoogste impact.
- ✕ Techniek inzetten zonder organisatorische borging → techniek werkt alleen binnen duidelijke processen.

→ Ga verder naar Stap 5 - Controle & Naleving

STAP 5

Controle & Naleving

05

Aantonen dat u structureel in control bent

Na het vaststellen van beleid, risico's en het implementeren van maatregelen is de volgende vraag essentieel: werkt het ook echt zoals bedoeld?

> **Wat u niet controleert, kunt u niet aantonen. En wat u niet kunt aantonen, is niet compliant.**

WAAROM DEZE STAP BELANGRIJK IS

- U toont aan dat uw beveiliging daadwerkelijk werkt.
- U ontdekt tekortkomingen vóórdat toezichthouders dat doen.
- U voldoet aan de eis van aantoonbare naleving (audit-proof).
- U creëert een continu verbeterproces.

WAT U IN DEZE STAP GAAT DOEN

Voer interne audits uit

Met een interne audit toetst u of:

- Beleid correct is geïmplementeerd;
- Maatregelen bestaan én functioneren;
- Procedures worden nageleefd;
- Verantwoordelijkheden duidelijk zijn belegd.

Toets opzet, bestaan en werking

Bij de NIS2 telt niet alleen of iets is vastgelegd, maar ook:

- Opzet: is het beleid logisch en passend?
- Bestaan: is het beleid daadwerkelijk geïmplementeerd?
- Werking: werkt het ook in de praktijk?

Registreer bevindingen en verbeteracties

Elke audit levert bevindingen op. Deze moeten worden:

- Vastgelegd;
- Geprioriteerd;
- Voorzien van een eigenaar;
- en opgevolgd binnen afgesproken termijnen.

Voer managementreviews uit

De NIS2 legt nadruk op bestuurlijke verantwoordelijkheid. Dat betekent dat het management periodiek beoordeelt:

- Of beveiligingsdoelstellingen worden behaald;
- Of risico's acceptabel zijn;
- Of aanvullende maatregelen nodig zijn.

NIS2 Bestuurders kunnen bij nalatigheid persoonlijk aansprakelijk worden gesteld. Managementreviews zijn dus geen formaliteit, maar bestuurlijke zelfbescherming.

CHECKLIST VOOR STAP 5

- [ ] Zijn interne audits gepland en uitgevoerd?
- [ ] Vindt er periodiek een managementreview plaats?
- [ ] Zijn bevindingen vastgelegd en opgevolgd?
- [ ] Is alle documentatie beschikbaar en actueel?

→ Ga verder naar Stap 6 - Audit & Externe toetsing

STAP 6

Audit & Externe toetsing

06

Aantonen dat uw organisatie klaar is voor toezicht

De laatste stap in het NIS2-traject is het moment van waarheid: kunt u extern aantonen dat uw organisatie grip heeft op informatiebeveiliging?

Een audit is geen doel op zich, maar een bevestiging dat uw organisatie structureel in control is.

WAAROM DEZE STAP BELANGRIJK IS

- U kunt aantonen dat u voldoet aan de NIS2-verplichtingen.
- U voorkomt verrassingen, herstelacties en sancties.
- U bent voorbereid op toezicht en controles.
- U versterkt vertrouwen bij klanten, partners en ketenpartijen.

WAT U IN DEZE STAP GAAT DOEN

Bepaal de vorm van externe toetsing

Afhankelijk van uw organisatie en sector kan externe toetsing bestaan uit:

- Een externe audit of certificering, bijvoorbeeld ISO 27001;
- Een NIS2-assessment;
- Toezicht door de bevoegde autoriteit;
- of toetsing vanuit ketenpartners of opdrachtgevers.

Bereid de auditdocumentatie voor

Zorg dat alle kernonderdelen compleet en actueel zijn, zoals:

- Scope- en beleidsdocumentatie;
- Risicoregisters en BIA's;
- Rapportages en verbeteracties;
- Bewijs van implementatie en werking.

Doorloop de externe audit of toetsing

Tijdens de audit of toetsing wordt beoordeeld:

- Of uw aanpak logisch en consistent is;
- Of maatregelen aantoonbaar bestaan en werken;
- Of verantwoordelijkheden duidelijk zijn belegd;
- En of u structureel stuurt op verbetering.

NIS2 Er bestaat geen NIS2-certificaat. De bevoegde autoriteit houdt toezicht en u moet naleving op elk moment kunnen aantonen. Essentiële entiteiten kunnen ook zonder aanleiding worden gecontroleerd. Bij belangrijke entiteiten volgt toezicht meestal achteraf, bijvoorbeeld na een incident.

CHECKLIST VOOR STAP 6

- [ ] Is duidelijk welke vorm van externe toetsing van toepassing is?
- [ ] Zijn risico's, maatregelen en beleid logisch op elkaar afgestemd?
- [ ] Is de organisatie voorbereid op gesprekken met auditors en toezichthouders?
- [ ] Is alle documentatie actueel en compleet?
- [ ] Zijn eerdere bevindingen aantoonbaar opgevolgd?
- [ ] Zijn auditresultaten geborgd en vastgelegd?

DE SAMOERAI-AANPAK

Van implementatie naar structureel in control

Innovatie en verandering binnen een organisatie brengen altijd uitdagingen met zich mee. Nieuwe werkwijzen kosten tijd, vragen investeringen en roepen vaak scepsis op binnen verschillende lagen van de organisatie. Dit geldt in het bijzonder voor informatiebeveiliging en risicobeheer, waar technische, organisatorische en menselijke aspecten samenkomen.

De Samoerai-aanpak is ontwikkeld om deze complexiteit beheersbaar te maken. Niet met losse maatregelen of een eenmalig project, maar met een helder, gefaseerd model dat zorgt voor grip, draagvlak en structurele borging binnen alle bedrijfslagen.

DRIE FASES NAAR AANTOONBARE CONTROLE

01
Compliancescan-fase
Het vaststellen van de huidige situatie en de mate van compliance in een GAP-analyse.

02
Implementatiefase
Het uitvoeren van het 6-stappenplan: maatregelen implementeren, processen inrichten en verantwoordelijkheden vastleggen.

03
In control blijven-fase
Het structureel evalueren, verbeteren en aanpassen van informatiebeveiliging aan nieuwe risico's, eisen en ontwikkelingen.

De in-control fase: continu grip houden

Na de implementatie van een ISMS begint de fase waarin veel organisaties vastlopen: het actueel houden van informatiebeveiliging. In de in-control fase ligt de focus op:

- Het continu evalueren van beleid en maatregelen;
- Het tijdig reageren op nieuwe dreigingen en incidenten;
- Het doorlopen van de Plan-Do-Check-Act (PDCA)-cyclus;
- En het aantoonbaar blijven voldoen aan wet- en regelgeving zoals de Cyberbeveiligingswet.

Ervoor zorgen dat informatiebeveiliging geen project blijft, maar een vast onderdeel wordt van de bedrijfsvoering

Continuïteit, bewustwording en leveranciersmanagement

Leveranciersmanagement
Organisaties zijn steeds afhankelijker van ketenpartners. Samoerai ondersteunt bij het beoordelen, monitoren en vastleggen van leveranciersrisico's, zodat u grip houdt op uw toeleveringsketen, een expliciete eis binnen de NIS2.

Bewustwording binnen de organisatie
Techniek alleen is onvoldoende. Medewerkers spelen een cruciale rol in het voorkomen en herkennen van incidenten. Daarom ondersteunt Samoerai bij het vergroten van security awareness, met praktische richtlijnen en structurele aandacht voor veilig gedrag.

Samenwerking en ondersteuning
Tijdens de in-control fase biedt Samoerai geen theoretisch kader, maar praktische ondersteuning: meedenken, meekijken en bijsturen waar nodig, altijd afgestemd op uw organisatie en risicoprofiel.

Klaar om grip te krijgen op NIS2? Start met de NIS2 Quickscan

U heeft in dit stappenplan gezien wat er nodig is om aan de NIS2 te voldoen en te blijven voldoen. De zes stappen geven u structuur en richting, maar de praktijk leert dat veel organisaties vastlopen op tijd, capaciteit en prioriteit.

De vraag is daarom niet óf u moet starten, maar hoe snel en hoe gecontroleerd.

De NIS2 Quickscan

De NIS2 Quickscan is een laagdrempelige eerste stap om inzicht te krijgen in waar uw organisatie nu staat en wat er concreet nodig is om in control te komen. Geen theoretisch rapport, maar een praktisch en eerlijk beeld van uw situatie.

WAT KUNT U VERWACHTEN

Tijdens de NIS2 Quickscan:

- Brengen we uw huidige situatie in kaart;
- Toetsen we uw organisatie aan de belangrijkste NIS2-verplichtingen;
- Identificeren we de grootste risico's en uitdagingen;
- Bepalen we welke stappen prioriteit hebben;
- Geven we inzicht in wat u zelf kunt oppakken en wat niet.

Na afloop weet u precies waar u staat en welke vervolgstap logisch is.

VOOR WIE IS DE QUICKSCAN BEDOELD?

De NIS2 Quickscan is geschikt voor organisaties die:

- Weten dat de NIS2 impact heeft, maar nog geen duidelijk plan hebben.
- Grip willen krijgen op risico's, beleid en maatregelen.
- Voorbereid willen zijn op toezicht en audits.
- Geen tijd hebben om alles zelf uit te zoeken.
- Willen voorkomen dat ze te laat of ongericht starten.

WAAROM STARTEN MET SAMOERAI?

Samoerai combineert diepgaande inhoudelijke kennis met een pragmatische aanpak. Geen onnodige complexiteit, maar focus op wat werkt en wat aantoonbaar is.

Wat u mag verwachten:

- ✓ Ervaring met complexe organisaties en regelgeving.
- ✓ Structuur, rust en overzicht in een complex speelveld.
- ✓ 100% slagingspercentage bij compliance-projecten.
- ✓ Mensgerichte aanpak met draagvlak binnen de organisatie.
- ✓ Begeleiding van start tot structureel in control.

ORGANISATIES DIE MET SAMOERAI WERKEN

Bravis ziekenhuis · ZZG zorggroep · De Zorggroep · Driezorg · NCare By CareConnections · Rijksdienst voor het Cultureel Erfgoed, Ministerie van Onderwijs, Cultuur en Wetenschap · provincie limburg · Universiteit van Amsterdam · eleos, specialist in christelijke ggz · JUMBO

Plan uw NIS2 Quickscan

Wilt u weten waar uw organisatie staat en welke stappen nu het meeste effect hebben?

Plan mijn NIS2 Quickscan →

samoerai.nl/contact

SAMOERAI INFORMATIEBEVEILIGING