

6 STAPPEN NAAR NIS2-COMPLIANCE

Een Stappenplan Om Uw Organisatie
Voor Te Bereiden



SAMOERAI

INFORMATIEBEVEILIGING

Grip op NIS2 begint hier

Wat de NIS2 betekent voor uw organisatie en waarom u nu moet starten



De NIS2-richtlijn (Network and Information Security Directive 2) is de nieuwe Europese wetgeving die organisaties verplicht om aantoonbaar grip te hebben op hun informatiebeveiliging. In Nederland wordt deze richtlijn omgezet in de Cyberbeveiligingswet, die naar verwachting in 2026 van kracht wordt.

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 leveranciers en partners.
- 3 Meldplicht bij incidenten binnen 24 uur** - ernstige beveiligingsincidenten moeten binnen 24 uur gemeld worden aan de toezichthouder.
- 4 Continuïteitsbeheer en herstelvermogen** - u moet kunnen aantonen dat uw organisatie kan blijven functioneren tijdens storingen of aanvallen.
- 5 Bewustwording en training van medewerkers** - medewerkers moeten worden opgeleid en betrokken bij veilig werken.
- 6 Aantoonbare naleving en toezicht door bevoegde autoriteiten** - u moet kunnen bewijzen dat uw beveiliging op orde is en voldoet aan de wet.

Het doel is helder; u kunt vandaag starten met grip krijgen op NIS2

Hoe gebruikt u dit 6 stappen-plan

- 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 kunt toetsen of uw organisatie klaar is voor een audit

Grip op NIS2 begint hier

Wat de NIS2 betekent voor uw organisatie 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.

Maar ook bedrijven die onderdeel zijn van de keten van deze entiteiten, vallen vaak indirect onder de verplichtingen.

Waarom nu beginnen?

Hoewel de wet pas in 2026 officieel geldt, verwachten toezichthouders dat organisaties zich nu al voorbereiden.

Wie te laat begint, loopt risico op:

- Sancties en reputatieschade;
- Vertraging bij aanbestedingen of ketenverplichtingen;
- Niet te voldoen aan voorwaarden van relatie in landen waar de NIS2 al wel van kracht is;
- en 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 NIS, zonder overweldigd te raken.



Weet wat u moet beschermen en waarom

Weet wat de NIS2 betekent voor uw organisatie en waarom u nu moet starten



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



Leg de scope en verantwoordelijkheden vast

Dit document wordt later gebruikt tijdens audits, risicobeoordelingen en managementreviews.

Wat u vast legt:

- ✓ scopeomschrijving
- ✓ Uitsluitingen (en waarom)
- ✓ Processen / systemen die binnen scope vallen
- ✓ Verantwoordelijkheden

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 NIS2-reikwijdte?

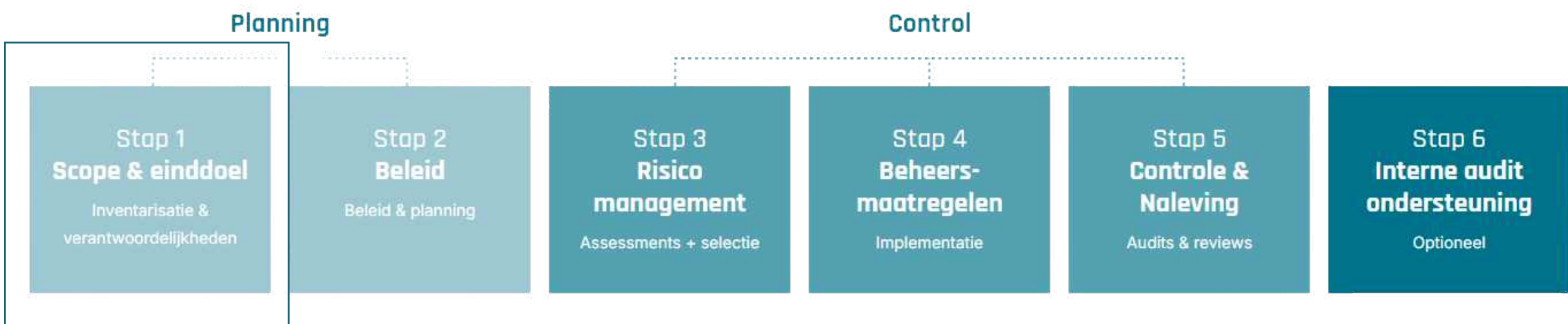


Wijs verantwoordelijkheden toe

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

Valkuilen in deze stap

- ✓ Te breed starten → leidt tot onnodige maatregelen en kosten.
- ✓ Te smal starten → leidt tot gaten in risicoanalyse.
- ✓ Verantwoordelijkheden niet officieel vastleggen → auditoren beoordelen dit als “niet aantoonbaar”.



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
- ✓ Iedereen dezelfde beveiligingsafspraken volgt
- ✓ U kunt verantwoorden waarom bepaalde keuzes zijn gemaakt
- ✓ Audits soepel verlopen dankzij duidelijke documentatie
- ✓ en management richting krijgt in hun beveiligingsverantwoordelijkheden



Plan de governance & reviews

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

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

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



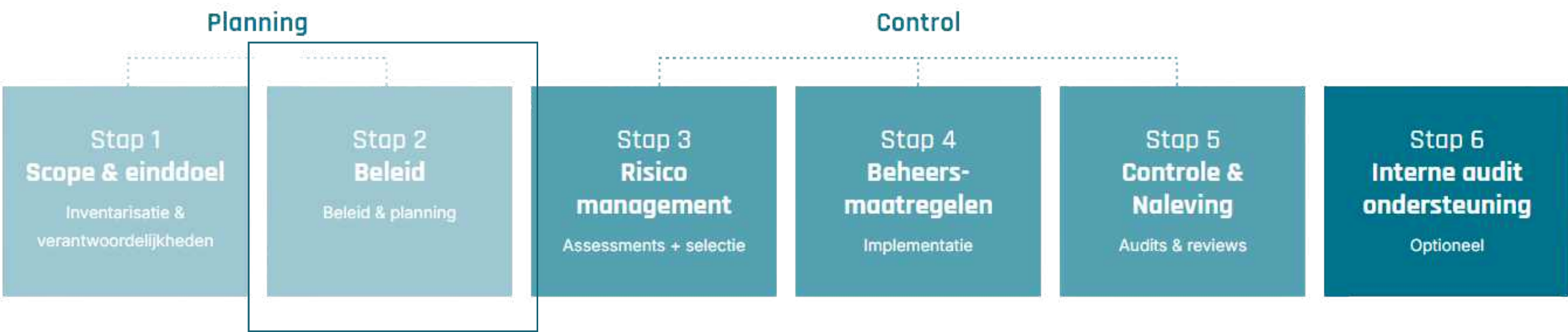
Werk de scope- en documentatieplanning bij.

Wanneer nieuwe beleidsregels worden opgesteld, wordt de scope-documentatie aangevuld met:

- Verantwoordelijkheden,
- processen die nieuw zijn toegevoegd,
- governance-afspraken,
- en reviewmomenten

Checklist voor stap 2

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



Inzicht in risico's is inzicht in controle

De wet vraagt dat organisaties systematisch risico's identificeren, beoordelen en behandelen. Niet omdat het moet, maar omdat dit de enige manier is 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 kunt beveiligingsmaatregelen prioriteren op basis van impact.
- ✓ U voldoet aan de centrale verplichting van de NIS2.
- ✓ U voorkomt onder- of overbeveiliging.
- ✓ U creëert een aantoonbare, logische onderbouwing richting auditoren.



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?
- **Rest-risico:** wat blijft er over?

Valkuilen in deze stap

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



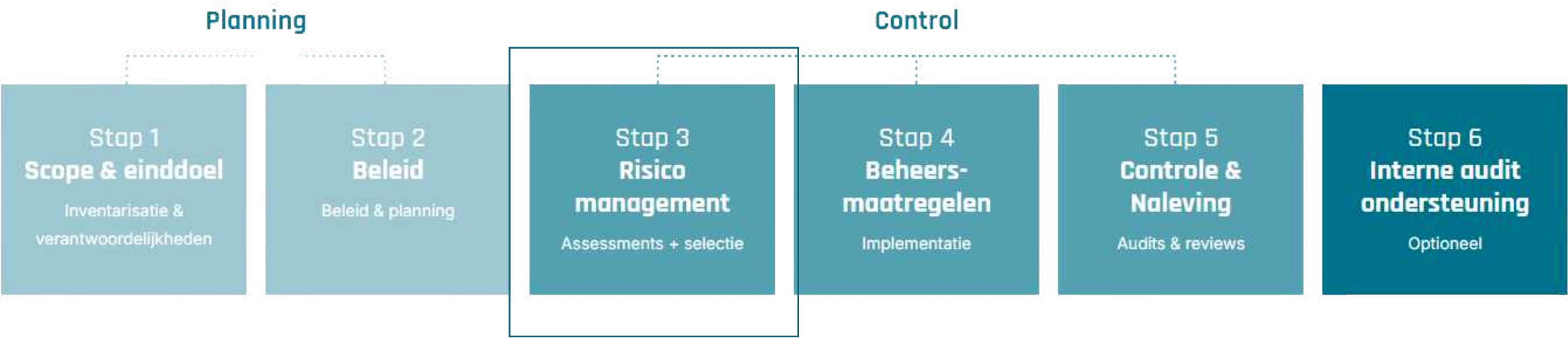
Voer een Business Impact Assessment (BIA) uit Met een BIA bepaalt u hoe essentieel processen zijn voor uw organisatie. Bijvoorbeeld:

- 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.



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 creëert bewijs dat maatregelen niet alleen gepland zijn, maar ook echt uitgevoerd worden
- ✓ U versterkt de digitale weerbaarheid van uw systemen en medewerkers
- ✓ U bouwt voort op de fundering uit stap 1 t/m 3



Richt awareness & training in

Menselijk handelen is bij 80% van beveiligingsincidenten een factor. 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.



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

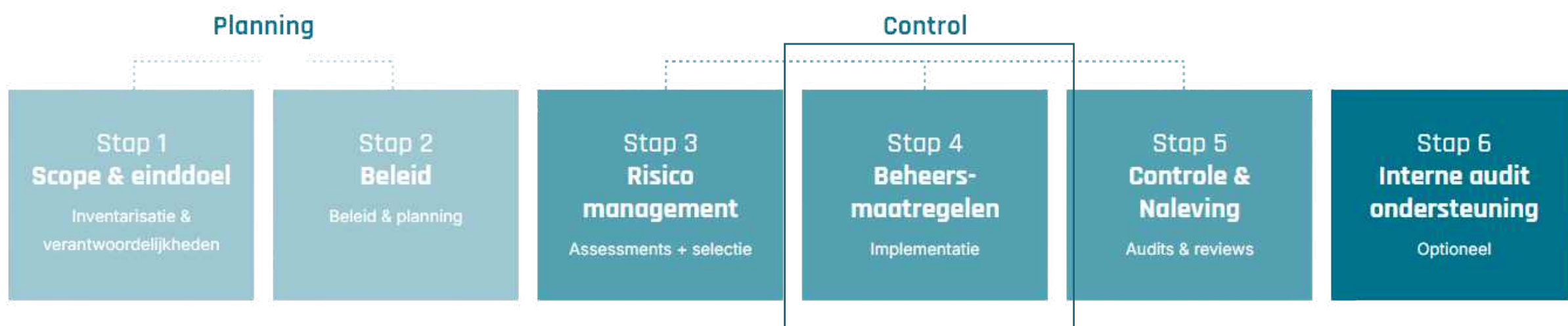


Implementeer organisatorische maatregelen

- deze omvatten:
- beleid en procedures (incidenten, wijzigingen, toegangsbeheer)
 - governance-afspraken
 - verantwoordelijkheden per rol
 - leveranciersmanagement
 - documentatie en communicatie

Valkuilen in deze stap

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



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



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 moet beoordelen:

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



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 NIS2 gaat het niet alleen om 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?

Checklist voor stap 5

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



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 bent voorbereid op toezicht en controles.
- ✓ U voorkomt verrassingen, herstelacties en sancties.
- ✓ U versterkt vertrouwen bij klanten, partners en ketenpartijen.



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.

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;
- Een NIS2-assessment;
- Toezicht door een bevoegde autoriteit;
- Of toetsing vanuit ketenpartners of opdrachtgevers.



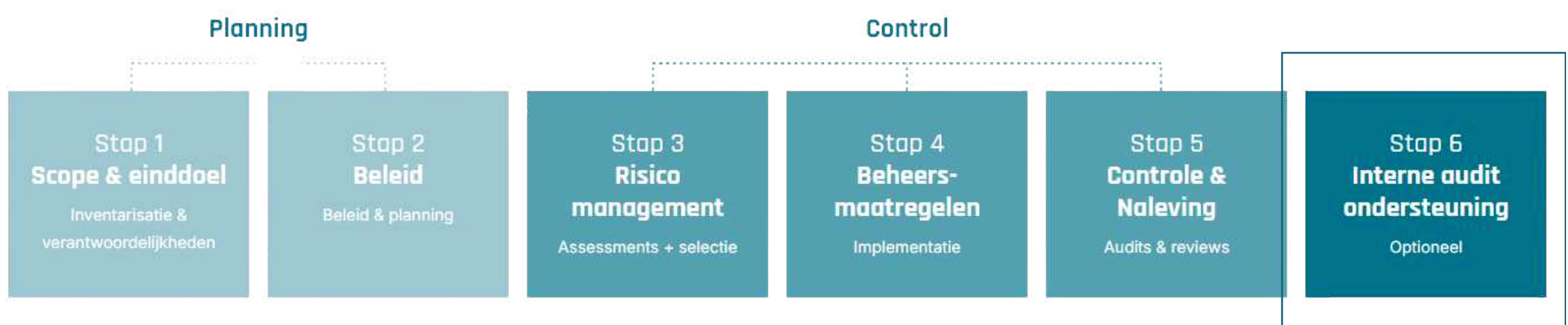
Bereid auditdocumentatie voor.

Zorg dat alle kernonderdelen compleet en actueel zijn, zoals:

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

Checklist voor stap 6

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

- 1 Structuur aanbrengen**
Het vaststellen van scope, beleid, risico's en maatregelen zoals beschreven in dit 6-stappenplan.
- 2 Implementeren en borgen**
Het daadwerkelijk uitvoeren van maatregelen, inrichten van processen en vastleggen van verantwoordelijkheden.
- 3 In control blijven**
Het structureel evalueren, verbeteren en aanpassen van informatiebeveiliging aan nieuwe risico's, eisen en ontwikkelingen.

De in-control fase: Continue 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 doorlopen van de Plan-Do-Check-Act (PDCA)-cyclus;
- Het tijdig reageren op nieuwe dreigingen en incidenten;
- En het aantoonbaar blijven voldoen aan wet- en regelgeving zoals de NIS2 (Cyberbeveiligingswet).

“ Ervoor zorgen dat informatiebeveiliging geen **project blijft**, maar een **vast onderdeel** word 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 e-book gezien wat er nodig is om NIS2-compliant te worden en te blijven. 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 exact waar u staat en welke vervolgstap logisch is.

Voor wie is de Quickscan bedoeld?

De NIS2 Quickscan is geschikt voor organisaties die:

- ✓ Weten dat 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.
- Mensgerichte aanpak met draagvlak binnen de organisatie.
- Structuur, rust en overzicht in een complex speelveld.
- Begeleiding van start tot structureel in control.



Plan uw NIS2 Quickscan

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



[Plan mijn NIS2 Quickscan](#)



SAMOERAI
INFORMATIEBEVEILIGING