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 ben 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. **Continuiteitsbeheer 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

SAMOERAI
INFORMATIEBEVEILIGING

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.

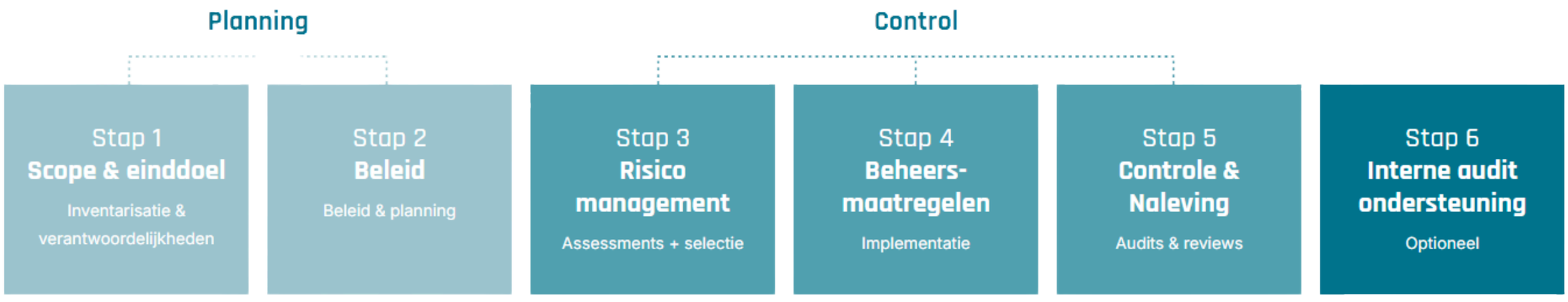
Waarom nu beginnnen?

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.



→ Ga verder naar. **Stap 1 - Scope & Einddoel**

Stap 1 - Scope & Einddoel

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

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

Leg de scope en verantwoordelijkheden vast

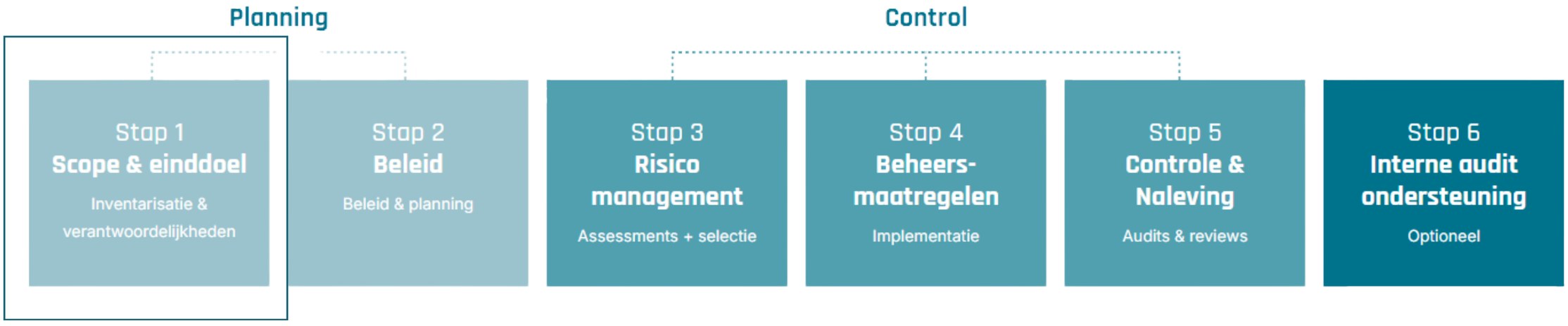
Dit document wordt later gebruikt tijdens audits, risicobeoordelingen en managementreviews.

Wat u vast legt:

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

Valkuilen in deze stap

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



→ Ga verder naar. **Stap 2 - Beleid en planning**