6 STAPPEN NAAR ISO 27001-COMPLIANCE

Een Stappenplan Om Uw Organisatie Voor Te Bereiden

SAMOERAI
INFORMATIEBEVEILIGING

Grip op ISO27001 begint hier

Wat de ISO27001 betekent voor uw organisatie en waarom u nu moet starten

De ISO27001-richtlijn is de belangrijkste norm om aantoonbaar grip te hebben op informatiebeveiliging. Voldoen aan deze norm betekend dat klanten en relaties verzekerd zijn van een partner die volledig in controle is op het gebied van Informatiebeveiling en security.

Steeds vaker is de ISO27001 een randvoorwaarde of zelfs een verplichting om duurzame werkrelatie op te bouwen met klanten en leveranciers. Daarnaast zal de organisatie een hoger volwassenheidsniveau bereiken en zijn processen beter geborgd.

Moet u ook voldoen aan de NIS2 Cyberveiligheidswet? De ISOdekt zo'n 90% hiervan af! Twee vliegen in één klap.

U wil bewijzen dat u aantoonbaar in control ben over uw digitale risico's en beveiligingsmaatregelen

De 6 kernverplichtingen van de ISO27001

1. **Scope en Context -** De organisatie moet vastleggen wat onder het ISMS valt, en aan welke eisen van stakeholders zij moet voldoen.
2. **Leiderschap & governance -** Het management moet eigenaarschap tonen door beleid vast te stellen, en verantwoordelijkheden te beleggen.
3. **Risicogedreven planning -** Beoordelen van informatiebeveiligingsrisico’s , passende maatregelen kiezen en een Verklaring van Toepasselijkheid.
4. **Support & randvoorwaarden -** Zorgen voor voldoende middelen, capaciteit, effectieve communicatie en beheerste documentatie.
5. **Operationele beheersing -** De maatregelen moeten aantoonbaar zijn geïmplementeerd en in de dagelijkse praktijk effectief functioneren.
6. **Evaluatie & verbetering - H**et ISMS periodiek meten, intern auditen, door management laten beoordelen en continu verbeteren op basis van bevindingen.

Het doel is helder; u kunt vandaag starten met grip krijgen op ISO27001

Hoe gebruikt u dit 6 stappen-plan

- U krijgt overzicht van alle uit te voeren activiteiten
- 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 ISO27001 begint hier

Wat de ISO27001 betekent voor uw organisatie en waarom u nu moet starten

Voor wie is de ISO27001?

ISO 27001 biedt een gestructureerde aanpak voor bedrijven die hun informatiebeveiliging willen waarborgen en hun bedrijfsrisico's op het gebied van cyberdreigingen willen verminderen. Daarnaast stellen klanten en relaties in toenemende mate compliance met de ISO 27001-norm als voorwaarde voor levering.

De norm is bedoeld voor alle organisaties die waardevolle, vertrouwelijke of kritische informatie verwerken en daar structureel, aantoonbaar en risicogedreven controle over willen hebben.

Waarom nu beginnen?

Veel organisaties en concurenten hebben deze stap al genomen. Wilt u niet uitgesloten worden van bestaande en nieuwe contracten is snel starten van belang.

Wie te laat begint, loopt risico op:

- Sancties en reputatieschade;
- Vertraging bij aanbestedingen of ketenverplichtingen;
- Niet te voldoen aan voorwaarden van relaties die wél voldoen aan de ISO27001;
- 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 Informatiebeveiling, 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 ISO27001 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 ISO27001-reikwijdte?

Wijs verantwoordelijkheden toe

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

Leg de scope en verantwoordelijkheden vast

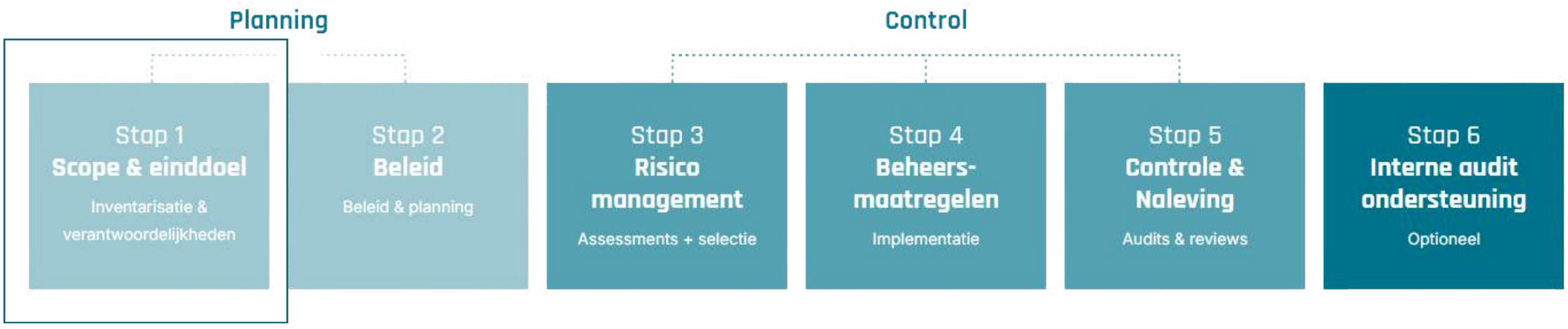
Dit document wordt later gebruikt tijdens audits, risicobeoordelingen en managementreviews.

Wat u vast legt:

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

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".



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

Stap 2 - Beleid en planning

Zorg voor richting, structuur en aantoonbare controle

De ISO27001 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

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
- Continuiteitsbeleid

Werk de scope- en documentatieplanning bij.
Wanneer nieuwe beleidsregels worden opgesteld, wordt de scope-documentatie aangevuld met:

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

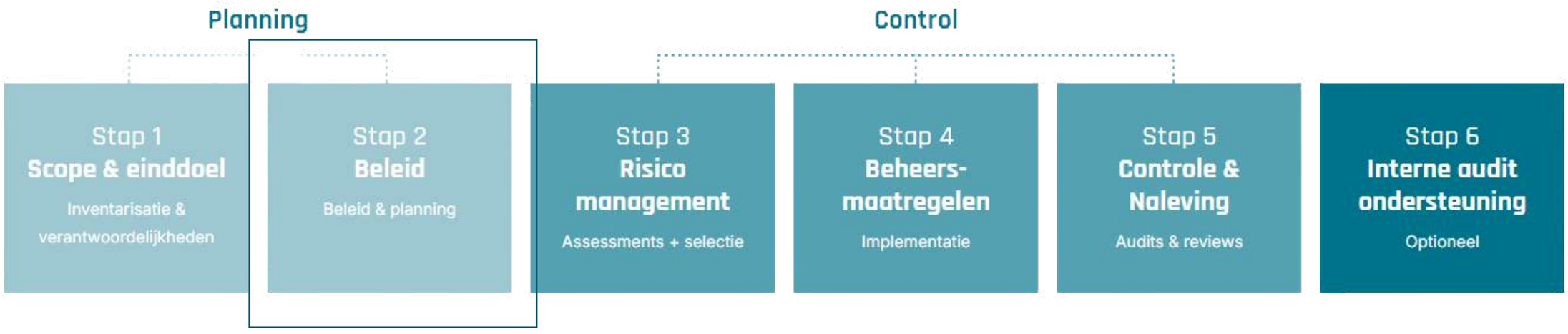
Plan de governance & reviews

ISO27001 verplicht organisaties om beleid periodiek te toetsen en bij te werken.
Dit omvat:

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

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 ISO27001-verplichtingen?
- Is vastgelegd wie eigenaar is van elk beleidsonderdeel?
- Zijn reviewmomenten, governance en planning gedocumenteerd?
- Is de scopedocumentatie bijgewerkt?



→ Ga verder naar. **Stap 3 - Risicomanagement**

Stap 3 - Risicomanagement

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 ISO27001.
- U voorkomt onder- of overbeveiliging.
- U creëert een aantoonbare, logische onderbouwing richting auditoren.

Wat u in deze stap gaat doen

Voer een Business Impact Assesment (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.

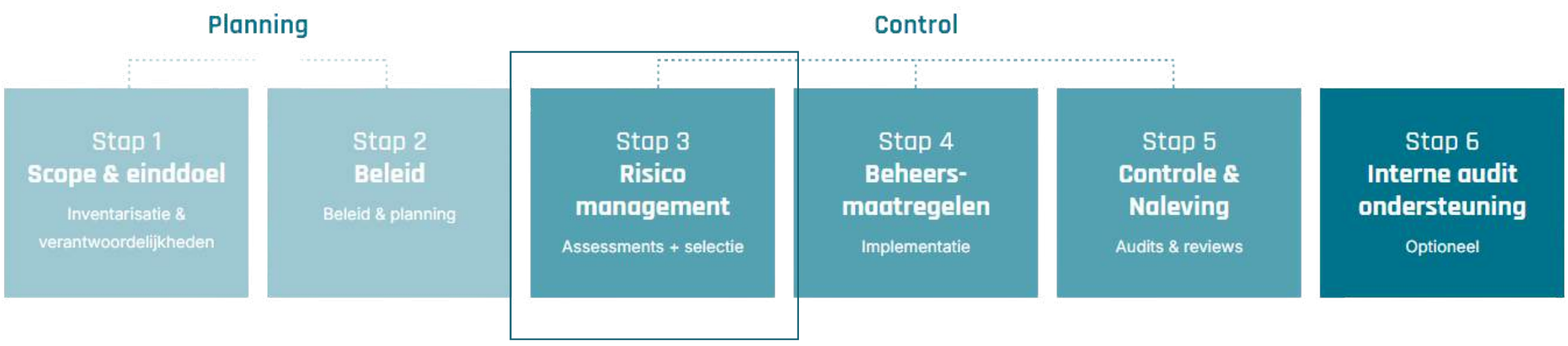
Voer een risicoanalyse uit

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?
- **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 → Auditors beoordelen dit als niet aantoonbaar.



→ Ga verder naar. **Stap 4 - Beheersmaatregelen**

Stap 4 - Beheersmaatregelen

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

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 beveiligingsincidenten een factor. ISO27001 verplicht daarom structurele bewustwording. Voorbeelden:

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

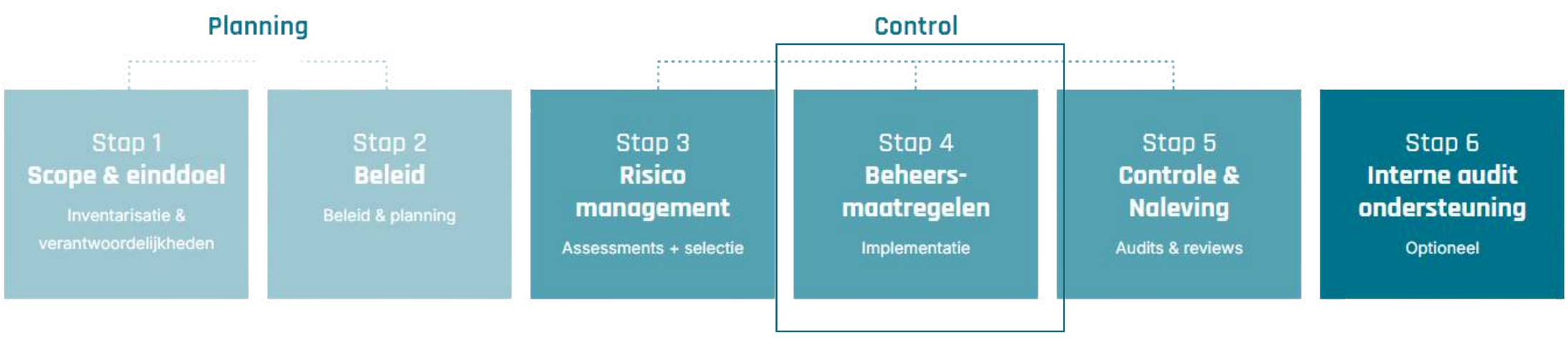
Documenteer alle maatregelen in uw ISMS

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.

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.



→ Ga verder naar. **Stap 5 - Controle & Naleving**

Stap 5 - Controle & Naleving

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.

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 **ISO27001** 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?

Registreer bevindingen en verbeteracties

Elke audit levert bevindingen op.
Deze moeten worden:

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

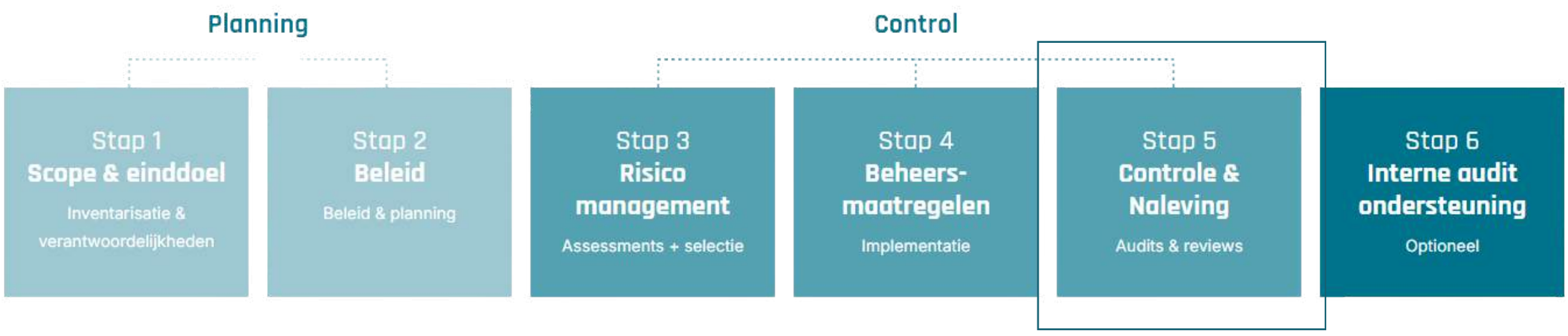
Voer managementreviews uit

De ISO27001 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.

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?



→ Ga verder naar. **Stap 6 - Audit & Externe toetsing**

Stap 6 - Audit & Externe toetsing

Aantonen dat uw organisatie klaar is voor toezicht

De laatste stap in het ISO27001-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 ISO27001-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 ISO27001-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. **Compliancescan fase**
   Het vaststellen van de huidige situatie en mate van compliance in een GAP analyse.

2. **Implementatie fase**
   Uitvoeren van het 6-stappenplan, maatregelen, inrichten van processen en vastleggen van verantwoordelijkheden.

3. **In control blijven fase**
   Dinesten voor het structureel evalueren, verbeteren en aanpassen van informatie-beveiliging aan nieuwe 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 ISO27001 (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 ISO27001.

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.

Grip te krijgen op ISO27001?

Start met de **ISO27001 Compliance scan**

U heeft in dit e-book gezien wat er nodig is om ISO27001-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 ISO27001 Compliance scan

De ISO27001 Compliance scan 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 ISO27001 Compliance scan:

- ✓ Brengen we uw huidige situatie in kaart;
- ✓ Toetsen we uw organisatie aan de belangrijkste ISO27001-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 Compliance scan bedoeld?

De ISO27001 Compliance scan is geschikt voor organisaties die:

- ✓ Weten dat ISO27001 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.
- 100% succesrate van compliance projecten

Plan uw ISO27001 Compliance scan

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

☞ **Plan mijn ISO27001 scan**

SAMOERAI

INFORMATIEBEVEILIGING