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

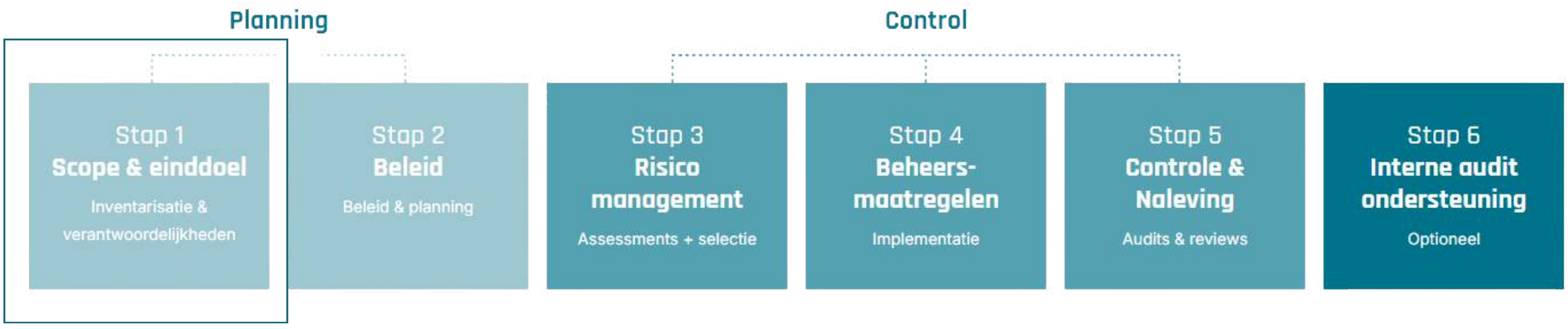
Dit document wordt later gebruikt tijdens audits, risicobeoordelingen en managementreviews.

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**