SAMOERAI
INFORMATIEBEVEILIGING

STAPPENPLAN · BIO2

6 STAPPEN NAAR BIO2-COMPLIANCE

Wat de BIO2 betekent voor uw organisatie en waarom u nu moet starten

HET TRAJECT IN ZES STAPPEN

01 Scope & Einddoel

02 Beleid en planning

03 Risicomanagement

04 Beheersmaatregelen

05 Controle & Naleving

06 Audit & Toetsing

Grip op BIO2 begint hier

Wat de BIO2 betekent voor uw organisatie en waarom u nu moet starten

De BIO2 (Baseline Informatiebeveiliging Overheid) is het normenkader waarmee organisaties aantoonbaar grip houden op informatiebeveiliging. Voldoen aan de BIO2 laat zien dat uw organisatie volledig in control is op het gebied van informatiebeveiliging en security.

Voor overheidsorganisaties is de BIO2 verplicht. Voor leveranciers en ketenpartners van de overheid is de BIO2 steeds vaker een voorwaarde om opdrachten te krijgen en te behouden. Daarnaast bereikt uw organisatie een hoger volwassenheidsniveau en zijn uw processen beter geborgd.

> Valt u ook onder de Cyberbeveiligingswet (de Nederlandse invulling van NIS2)? De BIO2 dekt zo'n 90% hiervan af. Twee vliegen in één klap.

U wilt aantoonbaar laten zien dat u in control bent over uw digitale risico's en beveiligingsmaatregelen

De 6 kernverplichtingen van de BIO2

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** - Het ISMS periodiek meten, intern auditen, door management laten beoordelen en continu verbeteren op basis van bevindingen.

Hoe gebruikt u dit 6 stappenplan

- ✓ 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

Het doel is helder: u kunt vandaag nog starten met grip op BIO2.

Grip op BIO2 begint hier

Wat de BIO2 betekent voor uw organisatie en waarom u nu moet starten

Voor wie is de BIO2?

De BIO2 is het verplichte normenkader voor informatiebeveiliging binnen alle overheidslagen: het Rijk, provincies, gemeenten en waterschappen. De BIO2 bouwt voort op ISO 27001 en ISO 27002, aangevuld met specifieke overheidsmaatregelen.

Ook leveranciers en ketenpartners die informatie van of voor de overheid verwerken, krijgen met de BIO2 te maken. Overheidsopdrachtgevers stellen steeds vaker BIO2-compliance als voorwaarde in aanbestedingen en contracten.

Kortom: de BIO2 is bedoeld voor alle organisaties die overheidsinformatie verwerken en daar structureel, aantoonbaar en risicogedreven controle over willen hebben.

Waarom nu beginnen?

Veel organisaties hebben deze stap al genomen. Voor overheidsorganisaties is de BIO2 verplicht, en leveranciers die niet kunnen aantonen dat ze voldoen, lopen het risico buiten bestaande en nieuwe opdrachten te vallen. Snel starten is dus van belang.

Wie te laat begint, loopt risico op:

- Sancties en reputatieschade;
- Vertraging bij aanbestedingen of ketenverplichtingen;
- Niet voldoen aan de eisen van opdrachtgevers en ketenpartners;
- 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 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 BIO2-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 / 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

02

Zorg voor richting, structuur en aantoonbare controle

De BIO2 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 management richting krijgt in hun beveiligingsverantwoordelijkheden
- 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, wordt de scope-documentatie aangevuld met:

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

Plan de governance & reviews

BIO2 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?
- [ ] Sluiten alle beleidsregels aan op de BIO2-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. 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 voldoet aan de centrale verplichting van de BIO2.
- U creëert een aantoonbare, logische onderbouwing richting auditoren.
- 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?
- 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.
- ✕ 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 op basis van de verplichte overheidsmaatregelen en aanvullende maatregelen op basis van stap 3 Risicomanagement.

> **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. BIO2 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

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 BIO2 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 BIO2 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?
- [ ] Vindt er periodiek een managementreview plaats?
- [ ] Zijn bevindingen vastgelegd en opgevolgd?
- [ ] Is alle documentatie beschikbaar en actueel?

→ Ga verder naar Stap 6 - Audit & Toetsing

STAP 6

06

Audit & Toetsing

Aantonen dat uw organisatie klaar is voor toezicht

De BIO2 vereist géén verplichte externe certificeringsaudit. Maar aantoonbaarheid via onafhankelijke toetsing is wél expliciet onderdeel van governance, verantwoording en toezicht binnen de publieke sector.

Een interne 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 BIO2-verplichtingen.
- U voorkomt verrassingen, herstelacties en sancties.
- U bent voorbereid op controles door bijvoorbeeld de ADR, de Algemene Rekenkamer, gemeentelijke rekenkamers of uw overheidsopdrachtgever.
- 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 toetsing bestaan uit:

- Een interne audit;
- Een BIO2-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.

Doorloop de interne 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.

CHECKLIST VOOR STAP 6

- [ ] Is duidelijk welke vorm van interne toetsing van toepassing is?
- [ ] Zijn risico's, maatregelen en beleid logisch op elkaar afgestemd?
- [ ] Is de organisatie voorbereid op gesprekken met auditors/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 mate van compliance in een GAP analyse.

02

Implementatie fase

Uitvoeren van het 6-stappenplan, maatregelen, inrichten van processen en vastleggen van verantwoordelijkheden.

03

In control blijven fase

Diensten 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 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 BIO2 en 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 BIO2.

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 krijgen op BIO2? Start met de BIO2 Compliance scan

U heeft in dit e-book gezien wat er nodig is om BIO2-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 BIO2 Compliance scan

De BIO2 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 BIO2 Compliance scan:

- Brengen we uw huidige situatie in kaart;
- Toetsen we uw organisatie aan de belangrijkste BIO2-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 BIO2 Compliance scan is geschikt voor organisaties die:

- Weten dat BIO2 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 Zorg Groep · Driezorg Stichting voor wonen zorg en welzijn · 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 BIO2 Compliance scan

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

Plan mijn BIO2 scan →

samoerai.nl/contact

SAMOERAI · INFORMATIEBEVEILIGING