SAMOERAI
INFORMATIEBEVEILIGING

STAPPENPLAN · EDITIE 2026

6 STAPPEN NAAR NEN7510 & NIS2-COMPLIANCE

Eén stappenplan om uw organisatie voor te bereiden op beide normen

HET TRAJECT IN ZES STAPPEN

01 Scope & Einddoel

02 Beleid & Planning

03 Risicomanagement

04 Beheersmaatregelen

05 Controle & Naleving

06 Audit & Externe toetsing

INTRODUCTIE

Grip op NEN7510 én NIS2 begint hier

Waarom één stappenplan voor twee normen

Veel organisaties in en rond de zorg krijgen op dit moment met twee verplichtingen tegelijk te maken. De NEN7510, de Nederlandse norm voor informatiebeveiliging in de zorg. En de NIS2, de Europese richtlijn die in Nederland is uitgewerkt in de Cyberbeveiligingswet. Die wet is op 15 augustus 2026 in werking getreden.

Het goede nieuws: beide normen rusten op hetzelfde fundament. Een managementsysteem voor informatiebeveiliging (ISMS) waarmee u risico's beheerst, maatregelen borgt en naleving aantoont. Wie het stappenplan in dit document doorloopt, bouwt dat fundament één keer en dekt daarmee de kern van beide verplichtingen af. Twee vliegen in één klap.

NEN7510

NEN7510 in het kort

De belangrijkste norm voor informatiebeveiliging in de Nederlandse zorg. Stelt expliciete eisen aan de bescherming van patiëntgegevens en is steeds vaker een randvoorwaarde in contracten met zorginstellingen, verzekeraars en ketenpartners.

NIS2

NIS2 / Cyberbeveiligingswet in het kort

Sinds 15 augustus 2026 van kracht voor ruim 8.000 organisaties in 18 sectoren, waaronder de zorg. Brengt een zorgplicht, een meldplicht en een registratieplicht in het entiteitenregister van het NCSC, met toezicht en sancties.

8.000+
organisaties vallen onder de Cyberbeveiligingswet

18
sectoren in scope, waaronder de zorg

1
ISMS als fundament voor beide normen

U moet als organisatie kunnen bewijzen dat u in control bent over uw digitale risico's en beveiligingsmaatregelen.

REIKWIJDTE

Voor wie is dit stappenplan, en waarom nu?

Voor wie?

NEN7510 De NEN7510 geldt voor zorgaanbieders én voor alle organisaties die patiëntgegevens verwerken, zoals ICT-leveranciers, administratiekantoren en andere ketenpartners van de zorg.

NIS2 De NIS2 geldt voor essentiële entiteiten zoals zorg-, energie-, transport- en overheidsorganisaties, en voor belangrijke entiteiten zoals IT-dienstverleners, maakindustrie, logistiek en digitale dienstverleners. Ook bedrijven die onderdeel zijn van de keten van deze entiteiten vallen vaak indirect onder de verplichtingen.

Valt uw organisatie onder beide normen? Dan is dit stappenplan precies voor u gemaakt. U doorloopt één traject en ziet per stap wat er voor elke norm extra nodig is.

Waarom nu beginnen?

De Cyberbeveiligingswet is geen verwachting meer, maar een feit. Sinds 15 augustus 2026 gelden de zorgplicht, de meldplicht en de registratieplicht. Toezichthouders verwachten dat organisaties nu aantoonbaar aan compliance werken. Veel organisaties en concurrenten hebben deze stap bovendien al genomen.

Wie te laat begint, loopt risico op:

- Sancties en reputatieschade;
- Vertraging bij aanbestedingen of ketenverplichtingen;
- Uitsluiting door klanten en partners die zelf wél voldoen;
- 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.

Hoe gebruikt u dit 6-stappenplan?

- ✓ U krijgt overzicht van alle verplichtingen en 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 starten met grip krijgen op NEN7510 én NIS2.

OVERLAP

Twee normen, één fundament

De zes stappen in dit document vormen de ruggengraat van een ISMS. De tabel hieronder laat zien hoe elke stap zich verhoudt tot de verplichtingen uit beide normen. Zo ziet u in één oogopslag: wie de stappen doorloopt, werkt aan beide normen tegelijk.

STAP	WAT U REGELT	NEN7510	NIS2 (CYBERBEVEILIGINGSWET)
1 · Scope & Einddoel	Vastleggen wat onder het ISMS valt en wie waarvoor verantwoordelijk is	Scope en context van het ISMS	Vaststellen of u een essentiële of belangrijke entiteit bent; registratie in het entiteitenregister
2 · Beleid & Planning	Beleid, governance en reviewcyclus	Leiderschap en governance; beleid gericht op patiëntgegevens	Bestuurlijke verantwoordelijkheid voor cyberrisicobeheer
3 · Risicomanagement	BIA, dreigingen en risicoanalyse	Risicogedreven planning en Verklaring van Toepasselijkheid	Risicobeheer en passende beveiligingsmaatregelen (zorgplicht)
4 · Beheersmaatregelen	Technische en organisatorische maatregelen, awareness	Operationele beheersing; toegangsbeheer op patiëntgegevens	Ketenbeveiliging, continuïteit, meldproces, training van medewerkers
5 · Controle & Naleving	Interne audits en managementreviews	Evaluatie en verbetering	Aantoonbare naleving
6 · Audit & Externe toetsing	Extern aantonen dat u in control bent	NEN7510-audit of certificering	Toezicht door de bevoegde autoriteit

Een goed ingericht ISMS volgens dit stappenplan dekt daarmee het overgrote deel van beide normen af.

→ Ga verder naar Stap 1 · Scope & Einddoel

STAP 1 VAN 6

01

Scope & Einddoel

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 reikwijdte?

Wijs verantwoordelijkheden toe. Denk aan: 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 en systemen die binnen scope vallen, rollen en verantwoordelijkheden.

NEN7510

Neem alle processen mee waarin patiëntgegevens worden verwerkt, ook waar u die verwerking heeft uitbesteed.

NIS2

Stel vast of uw organisatie een essentiële of belangrijke entiteit is en registreer uw organisatie in het entiteitenregister van het NCSC. Dit is sinds 15 augustus 2026 een wettelijke verplichting.

VALKUILEN IN DEZE STAP

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

→ Ga verder naar Stap 2 · Beleid en planning

Beleid en planning

02

Zorg voor richting, structuur en aantoonbare controle

Beide normen vragen 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, continuïteitsbeleid.

Werk de scope- en documentatieplanning bij. Wanneer nieuwe beleidsregels worden opgesteld, wordt de scopedocumentatie aangevuld met: verantwoordelijkheden, processen die nieuw zijn toegevoegd, governance-afspraken en reviewmomenten.

Plan de governance & reviews. Beide normen verplichten organisaties om beleid periodiek te toetsen en bij te werken. Dit omvat: managementreviews, periodieke beleidsupdates, interne audits, risicobeoordelingen en opvolging van verbeterpunten.

NEN7510

Uw beleid moet expliciet ingaan op de bescherming van patiëntgegevens.

NIS2

Het bestuur is eindverantwoordelijk. Bestuurders moeten het cyberrisicobeleid aantoonbaar goedkeuren, erop toezien en zich erin laten trainen.

CHECKLIST VOOR STAP 2

- [ ] Zijn de basisbeleidsdocumenten opgesteld of bijgewerkt?
- [ ] Sluiten alle beleidsregels aan op de verplichtingen uit beide normen?
- [ ] 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

Risicomanagement

03

Inzicht in risico's is inzicht in controle

Beide normen vragen 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 beide normen.
- U voorkomt onder- of overbeveiliging.
- U creëert een aantoonbare, logische onderbouwing richting auditoren.

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? Restrisico: wat blijft er over?

NEN7510

Weeg patiëntveiligheid en continuïteit van zorg expliciet mee als impactcriteria.

NIS2

Neem risico's in uw toeleveringsketen expliciet mee in de analyse. U bent verantwoordelijk voor de beveiliging van uw belangrijkste leveranciers en partners.

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.

→ Ga verder naar Stap 4 · Beheersmaatregelen

STAP 4 VAN 6

04

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 versterkt de digitale weerbaarheid van uw systemen en medewerkers.
- U creëert bewijs dat maatregelen niet alleen gepland zijn, maar ook echt uitgevoerd worden.
- 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: 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 de beveiligingsincidenten een factor. Beide normen verplichten daarom structurele bewustwording. Voorbeelden: jaarlijkse security-awarenesstraining, 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, en hoe ze worden beheerd en onderhouden.

NEN7510

Logging en controle van toegang tot patiëntgegevens is een expliciete eis. Leg vast wie wanneer welk dossier heeft ingezien.

NIS2

Richt uw meldproces in. Ernstige incidenten meldt u binnen 24 uur (eerste melding) en binnen 72 uur (uitgebreide melding) aan het CSIRT en de toezichthouder.

VALKUILEN IN DEZE STAP

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

→ Ga verder naar Stap 5 · Controle & Naleving

STAP 5 VAN 6

05

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, en verantwoordelijkheden duidelijk zijn belegd.

Toets opzet, bestaan en werking. Het gaat 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. Beide normen leggen nadruk op bestuurlijke verantwoordelijkheid. Het management moet periodiek beoordelen: of beveiligingsdoelstellingen worden behaald, of risico's acceptabel zijn, en of aanvullende maatregelen nodig zijn.

NIS2

Bestuurders kunnen bij nalatigheid persoonlijk aansprakelijk worden gesteld. Managementreviews zijn dus geen formaliteit, maar bestuurlijke zelfbescherming.

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 & Externe toetsing

STAP 6 VAN 6

06

Audit & Externe toetsing

Aantonen dat uw organisatie klaar is voor toezicht

De laatste stap 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 verplichtingen uit beide normen.
- U bent voorbereid op toezicht en controles.
- U voorkomt verrassingen, herstelacties en sancties.
- 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 externe toetsing bestaan uit: een externe audit of certificering, een assessment of maturityscan, 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, Verklaring van Toepasselijkheid (SoA), auditrapportages en verbeteracties, managementreviewverslagen, en bewijs van implementatie en werking.

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.

NEN7510

Certificering door een onafhankelijke instelling is mogelijk en wordt steeds vaker gevraagd door opdrachtgevers en zorgverzekeraars.

NIS2

Er bestaat geen NIS2-certificaat. De bevoegde autoriteit houdt toezicht en u moet naleving op elk moment kunnen aantonen.

CHECKLIST VOOR STAP 6

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

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

FASE 01

Compliancescan-fase

Het vaststellen van de huidige situatie en mate van compliance in een GAP-analyse.

FASE 02

Implementatiefase

Het uitvoeren van het 6-stappenplan: maatregelen implementeren, processen inrichten en verantwoordelijkheden vastleggen.

FASE 03

In control blijven-fase

Het structureel evalueren, verbeteren en aanpassen van informatiebeveiliging aan nieuwe risico's, eisen en ontwikkelingen.

De in-control fase: continu 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 NEN7510 en de Cyberbeveiligingswet.

Ervoor zorgen dat informatiebeveiliging geen project blijft, maar een vast onderdeel wordt van de bedrijfsvoering.

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 beide normen.

Bewustwording

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

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.

VOLGENDE STAP

Klaar om grip te krijgen op NEN7510 én NIS2? Start met de Compliance Quickscan

U heeft in dit stappenplan gezien wat er nodig is om aan beide normen te voldoen en te blijven voldoen. 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 Compliance Quickscan

De Compliance 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. Voor de NEN7510, de NIS2, of beide tegelijk. Geen theoretisch rapport, maar een praktisch en eerlijk beeld van uw situatie.

WAT KUNT U VERWACHTEN?

Tijdens de Compliance Quickscan:

- Brengen we uw huidige situatie in kaart;
- Toetsen we uw organisatie aan de belangrijkste verplichtingen uit de NEN7510 en de NIS2;
- 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?

Voor organisaties die:

- Weten dat NEN7510 en/of NIS2 impact hebben, 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% succesratio op compliancetrajecten.
- ✓ Mensgerichte aanpak met draagvlak binnen de organisatie;
- ✓ Begeleiding van start tot structureel in control;

ORGANISATIES DIE MET SAMOERAI WERKEN

Bravis ziekenhuis · ZZG zorggroep · De Zorggroep · 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 mijn Compliance Quickscan →

samoerai.nl/contact

SAMOERAI · INFORMATIEBEVEILIGING