BMGRIP
Part of kader group

Herziening NEN7510:2024

Wat betekent dit voor u?

Whitepaper

Inhoudsopgave

1 Inleiding en achtergrond

De herziening van de NEN 7510 norm is in december 2024 door de NEN gepubliceerd. De NEN 7510:2024 bestaat net als zijn voorganger uit twee delen: deel 1: Managementsysteem en deel 2: Beheersmaatregelen. Deel 1 beschrijft de eisen waaraan het managementsysteem moet voldoen en in Deel 2 worden de beheersmaatregelen beschreven die organisatie kan inzetten voor het verlagen van informatiebeveiligingsrisico's. Of te wel voor het beschermen van de vertrouwelijkheid, het bewaken van de integriteit en het borgen van de beschikbaarheid van informatie en specifiek persoonlijke gezondheidszorggegevens.

De vorige versie, NEN 7510:2017, is gebaseerd op de ISO 27001:2015. Nadat de ISO 27001 in 2022 is herzien was een herziening van de NEN 7510 een kwestie van tijd. De NEN 7510:2024 volgt de wijzigingen en nieuwe onderdelen in de ISO 27001:2022. Ook zijn onderdelen te herkennen die zijn gebaseerd op de NIS2 waarvoor in Nederland nu de Cyberbeveiligingswet in de maak is. Net zoals in de voorgaande versie zijn zorg specifieke maatregelen bij bepaalde beheersmaatregelen toegevoegd aangevuld met extra HLT-beheersmaatregelen.

Met het uitkomen van deze herziening wordt van gecertificeerde organisaties verwacht een transitie uit te voeren en zich te certificeren tegen deze herziening. Na een overgangsperiode van 2 jaar na publicatie van de norm, waarbij beide certificeringen naast elkaar bestaan, moet elke gecertificeerde organisatie de transitie hebben uitgevoerd. Met de publicatie van deze herziening op 16 december 2024 moet de transitie uiterlijk 16 december 2026 hebben plaatsgevonden.

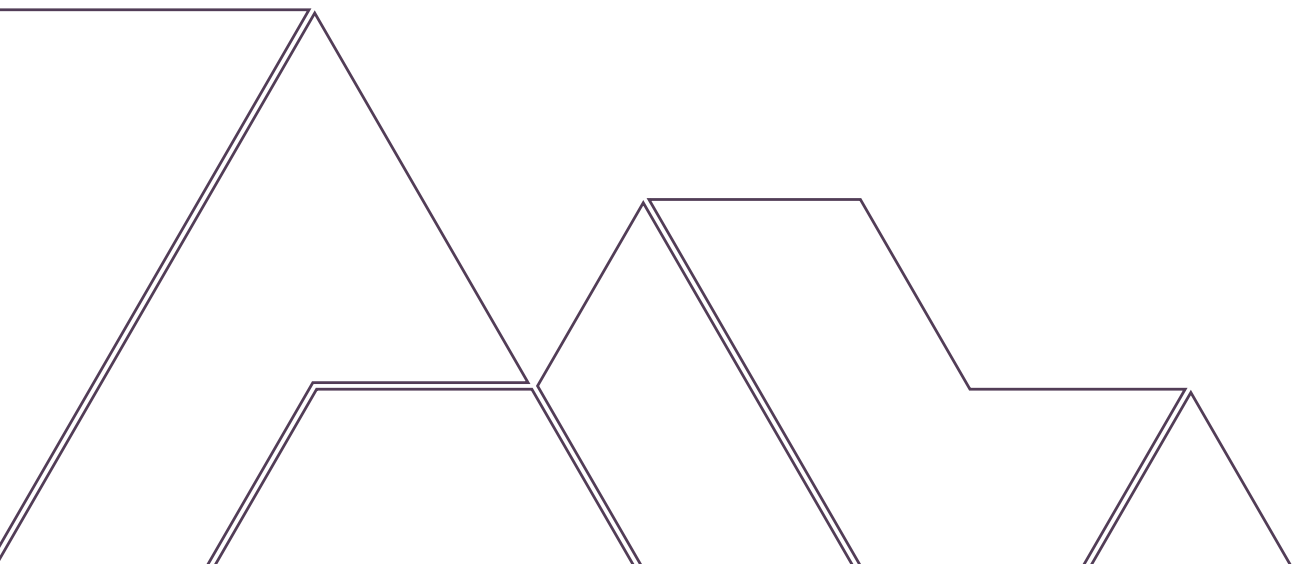
2 Herziening norm

2.1 Doel

In de herziening van de NEN 7510 is inhoudelijk veel verandert en verschoven. Het doel is ongewijzigd en blijft, net zoals de ISO 27001, om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen een organisatie risico gebaseerd te beschermen. Met het verplicht inrichten van een managementsysteem (deel 1) wordt continue verbetering gewaarborgd. Risico's worden verlaagd door het inzetten van beschreven beheersmaatregelen (deel 2) en/of eigen beheersmaatregelen.

2.2 Risico gebaseerd

Beheersmaatregelen beschreven in deel 2 blijven **geen** verplicht onderdeel van de norm, wel geldt hierbij het "voer uit of leg uit". Of je implementeert de beheersmaatregel of je legt uit waarom deze niet van toepassing is op jouw organisatie. Dit is het risico gebaseerd principe van de norm. Simpel geredeneerd: als je geen risico hebt of ervaart dan heb je ook geen beheersmaatregel nodig om deze te verlagen. Al moet gezegd worden dat de beheersmaatregelen in deel 2 veelal toegepast moeten worden voor een best-practice informatiebeveiliging. Ook blijft het mogelijk om extra beheersmaatregelen te beschrijven en te implementeren die niet in deel 2 worden genoemd.



2.3 Voor wie?

Aantoonbaar voldoen aan de NEN 7510 is voor organisaties met zorgverleners in Nederland sinds 2008 een wettelijke verplichting. Twee jaar geleden is de Inspectie voor Gezondheid en Jeugd (IGJ) gestart met het handhaven van de wettelijke verplichting. Het aantoonbaar voldoen staat niet gelijk aan het bezitten van een, door een geaccrediteerde Certificatie Instelling, uitgegeven certificaat. Wel stelt de IGJ een aantal voorwaarden aan het aantoonbaar voldoen zonder certificaat, deze zijn terug te vinden op de website van de IGJ.

Voor leveranciers van zorgverleners en zorgorganisaties is het voldoen aan de NEN 7510 optioneel. Aantoonbaar voldoen heeft twee voordelen voor een leverancier: het geeft (potentiële) klanten vertrouwen in een goede informatiebeveiliging. In verschillende wet- en regelgeving, bijvoorbeeld AVG artikel 32, wordt passende organisatorische en technische maatregelen vereist voor de bescherming van (persoons) gegevens. Met het aantoonbaar voldoen aan de, risico gebaseerde, NEN 7510 wordt hieraan voldaan.

3 NEN 7510:2024

3.1 Management systeem

De NEN 7510 beschrijft in de Harmonized Structure (HS) hoe je een managementsysteem voor het aandachtsgebied informatiebeveiliging kan inrichten. De Harmonized Structure (HS) is de opvolger van de High Level Structure (HLS). Dit managementsysteem laat je op hoofdlijnen herhaaldelijk 5 dingen doen om informatiebeveiliging binnen de organisatie te waarborgen en deze continu te verbeteren:

1. Inzichtelijk maken van de context van de organisatie door te beschrijven aan welke wet- en regelgeving de organisatie moet voldoen, aan welke externe invloeden de organisatie onderhevig is en welke eisen en verwachtingen belanghebbenden van de organisatie hebben.

2. Het opstellen van beleid en doelen als een antwoord op deze context. Hoe gaat de organisatie hiermee om en gaan ze de eisen en verwachtingen aan de organisatie waarmaken.

3. Het uitvoeren van een risicoanalyse om vast te stellen welke risico's de organisatie loopt waardoor mogelijk het beleid en de doelen, daarmee de eisen en verwachtingen, niet wordt uitgevoerd of worden behaald.

4. Het beschrijven en implementeren van beheersmaatregelen om de risico's van de organisatie te verlagen en de kans te vergroten dat het beleid wordt uitgevoerd en de doelen worden behaald.

5. Controleren van de werking en effectiviteit van de beheersmaatregelen en indien nodig bijstellen, verbeteren of invoeren van extra beheersmaatregelen.

Bovenstaande beschrijft de Plan-Do-Check-Act-cirkel ofwel kwaliteitscirkel, de basis van elk managementsysteem. De NEN 7510 beschrijft dit specifiek voor het aandachtsgebied informatiebeveiliging in de zorg.

3.2 Beheersmaatregelen

Deel 2 van de NEN 7510 beschrijft 93 beheersmaatregelen om risico's op het gebied van informatiebeveiliging van een organisatie te verlagen. De beheersmaatregelen zijn onderverdeeld in 4 categorieën:

1. Organisatorische beheersmaatregelen (37).
2. Mensgerichte beheersmaatregelen (8).
3. Fysieke beheersmaatregelen (14).
4. Technologische beheersmaatregelen (34).

Beheersmaatregelen worden gekoppeld aan risico's bij de uitvoering van de risicoanalyse en daarmee welke van toepassing zijn. Beheersmaatregelen die worden ingezet worden beschreven in de Verklaring van Toepasselijkheid. Op basis van de beschreven scope van het managementsysteem en de Verklaring van Toepasselijkheid kan een belanghebbende van de organisatie de waarborgen voor een goede informatiebeveiliging vaststellen. Deze waarborgen zijn de basis van een vertrouwensrelatie tussen belanghebbende en de organisatie.

Om beheersmaatregelen volgens de norm te implementeren moet de PDCA aantoonbaar zijn. De eisen waaraan een beheersmaatregel volgens de organisatie moet voldoen moet zijn beschreven (Plan). De beheersmaatregel moet aantoonbaar zijn genomen (Do). De werking en effectiviteit van de beheersmaatregel moet worden gemeten door het uitvoeren van controles of interne audits (Check). Indien nodig moet de beheersmaatregel worden aangepast, verbeterd of aangevuld (Act).

4 Aan de slag

4.1 Beginners

Voor organisatie die willen beginnen met de NEN 7510 is het aan te raden om te starten met een 0-meting. Met de 0-meting kan in beperkte tijd een beeld worden gevormd waar een organisatie staat ten opzichte van de eisen van de NEN 7510. Veel organisaties hebben al ervaring met een managementsysteem voor het aandachtsgebied kwaliteit en/of hebben, al dan niet bewust, beheersmaatregelen geïmplementeerd. Het resultaat van de 0-meting is een organisatie specifiek implementatieplan waarmee de organisatie zelfstandig of met behulp van een adviesorganisatie zoals BMGRIP aan de slag kan.

Om het beheer en onderhoud van het managementsysteem en alle daarbij behorende documentatie te verlichten is het raadzaam om hiervoor een systeem in te zetten. BMGRIP gebruikt ter ondersteuning bij alle implementaties SmartManSys. SmartManSys is een systeem waarin zowel het managementsysteem wordt opgebouwd en templates beschikbaar zijn voor vereiste documentatie.

Een implementatie van de NEN 7510 wordt voltooid met het uitvoeren van een interne audit. Met een interne audit wordt de werking en effectiviteit van het managementsysteem beoordeeld. Om aantoonbaar te voldoen moet deze audit door een onafhankelijke zijn en moeten de auditors voldoende kennis van de norm hebben.

Indien gewenst kan, of wanneer een belanghebbende dit vereist moet, de organisatie een externe audit laten uitvoeren door een geaccrediteerde Certificatie Instelling. Bij een positieve uitkomt van de audit ontvangt de organisatie een certificaat. Een door een Certificatie Instelling verstrekt certificaat is de ultieme vorm om aan te tonen dat de organisatie voldoet aan de eisen die de NEN 7510:2024 stelt. Met het behalen van een certificaat voldoet je organisatie zeker aan alle, aantoonbaar voldoen, eisen van de IGJ.

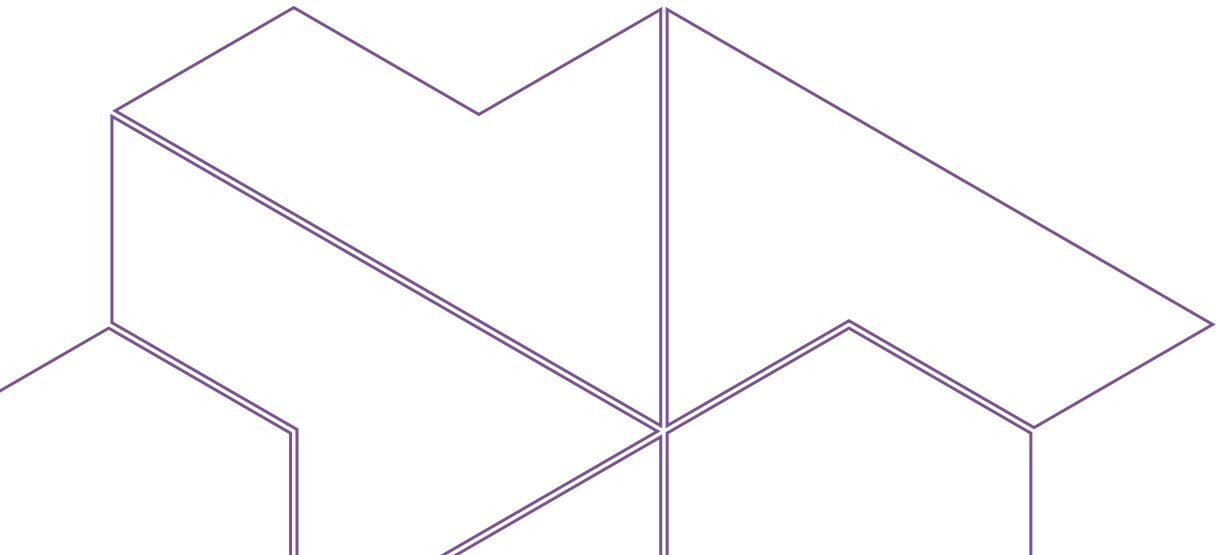
4.2 Organisaties met certificaat

Organisaties met een NEN 7510:2017 certificaat moeten voor 16 december 2026 de transitie uitvoeren. Met een GAP-analyse gericht op de nieuwe elementen maakt de organisatie inzichtelijk wat aangepast moet worden. In een Plan van Aanpak wordt beschreven wie, wat en wanneer uitvoert. De Security Officer kan de uitvoering van dit Plan van Aanpak coördineren in samenwerking met het ingerichte IBMF of vergelijkbaar overleg.

Met een interne audit moeten alle normelementen en beheersmaatregelen die van toepassing zijn verklaard worden beoordeeld. Tijdens de externe audit, die uitgebreid wordt met een transitie audit, beoordeeld de Certificatie Instelling van de organisatie of alle nieuwe elementen volgens de norm zijn geïmplementeerd. Wanneer het oordeel positief is ontvangt de organisatie een NEN 7510:2024 certificaat. Wanneer de transitie wordt uitgevoerd tijdens een hercertificering heeft het ontvangen certificaat een geldigheidstermijn van 3 jaar. Wanneer de transitie wordt uitgevoerd tijdens een tussentijdse controle neemt het NEN 7510:2024 certificaat de geldigheidstermijn over van het NEN7510:2017 certificaat.

5 Tot slot

In de bijlagen van dit soort documenten staan vaak veel details waar alleen de echte kenners in geïnteresseerd zijn. Maar niet in de bijlagen van de NEN 7510:2024. In de bijlagen van deel 1 staat een inhoudelijke vergelijking tussen versie 2017 en 2024 van zowel het managementsysteem als de beheersmaatregelen en een overzicht van gerelateerde Nederlandse en Europese wet- en regelgeving. De bijlagen van deel 2 geeft een uitleg van het gebruik van attributen die zijn toegekend aan de beheersmaatregelen, vertaaltabellen tussen de 2017 en 2024 norm en een mapping van de NIS2 op de NEN7510. Een mooi cadeau gegeven door de opstellers van deze herziening.



6 BMGRIP

Jouw organisatie is specifiek en daarmee uniek. Er is dus geen one-size-fits-all aanpak. De implementatie en het onderhoud van een NEN 7510 managementsysteem of certificaat is maatwerk. BMGRIP helpt organisaties met het inrichten van een maatwerk managementsysteem in drie smaken.

1. Helpen: ‘Hulp bij zelf doen’
2. Samen: ‘Samen inrichten’
3. Ontzorgen: ‘uit handen nemen’

De praktijk van de afgelopen jaren heeft laten zien dat we daarmee aan iedere klantwens tegemoet kunnen komen. Ons systeem SmartManSys en de daarin aanwezige templates is de basis voor iedere smaak. U kunt zelf bepalen hoeveel u zelf wilt of kunt doen en welke smaak het beste bij uw organisatie past.

Voor de NEN 7510:2024 ondersteunen wij organisaties met het uitvoeren van 0-metingen en bij het inrichten van managementsystemen. NEN 7510:2017 gecertificeerde organisaties ondersteunen wij met een GAP-Analyse en het uitvoeren van voor de transitie benodigde activiteiten. Ook leveren bij Professionals as a Service bijvoorbeeld als Security Officer, Privacy Officer of Functionaris Gegevensbescherming.

Certificering een stap te ver maar wel aantoonbaar voldoen? Dan kan BMGRIP een onafhankelijke interne audit uitvoeren volgens de eisen van de IGJ. Hiermee kunnen organisaties wel aantoonbaar voldoen aan de NEN 7510:2024 maar besparen op de kosten van een externe audit door een geaccrediteerde Certificerende Instelling.

Over Kader en BMGRIP

Kader Group verbetert de kwaliteit, veiligheid en duurzaamheid van organisaties, zodat een ieder goed kan zorgen voor mens, milieu en maatschappij. Dat doen we met onze consultancy & interim diensten, digitale oplossingen en opleidingen op de gebieden kwaliteit, veiligheid & gezondheid, cyber security en milieu & duurzaamheid. Onze missie: het creëren van een veilige en duurzame leefomgeving om door te geven aan toekomstige generaties. We zijn daarin pragmatisch, innovatief, persoonlijk en vakkundig. Kader Group startte in 1994 en bestaat inmiddels uit ruim 350 gedreven medewerkers.

BMGRIP is expert op het gebied van integrale informatiebeveiliging en privacy. Als onderdeel van de Kader Group helpen we organisaties verantwoord te moderniseren en stellen daarbij mens, milieu en maatschappij centraal. Onze aanpak is gebaseerd op de zes Kader Kapitalen: medewerkerswelzijn, arbeidsveiligheid, technische veiligheid, organisatiekwaliteit, informatiebeveiliging en duurzaamheid; alle aspecten die bepalend zijn voor een verantwoorde bedrijfsvoering. Samen met jou bouwen we aan een moderne, veerkrachtige organisatie, zodat deze voldoet aan de eisen van nu en die van de toekomst. We begrijpen als geen ander dat complexe wet- en regelgeving uitdagend kan zijn. Dit beschouwen we niet als een beperking, maar als een kans. Onze aanpak, gebaseerd op de zes Kader Kapitalen, biedt een unieke combinatie van consultancy, opleidingen en digitale oplossingen.

Met 400 toegewijde Kader-collega's en meer dan 30 jaar ervaring, ondersteunen we ruim 100.000 opdrachtgevers en hebben we 125.000 mensen opgeleid. We hebben 7.500 bedrijven geassisteerd bij het behalen van certificeringen en 60.000 professionals ontzorgd met een software-oplossing. Met Kader aan onze zijde zijn we beter uitgerust dan ooit om jouw organisatie te helpen haar doelen te bereiken. Wij hebben met de zes Kader Kapitalen alles in huis om bedrijven effectief te begeleiden en klaar te stomen voor de toekomst.

Verbeter met visie!

BMGRIP

Part of kader group

Computerweg 22
3542 DR UTRECHT

030 - 200 8243
info@bmgrip.nl

V.0325

www.bmgrip.nl