

Whitepaper NEN-7510

A stethoscope is positioned in the lower-left foreground, resting on a laptop keyboard. The background is a blurred laptop screen. Overlaid on the image is a futuristic digital interface with glowing blue lines and circular nodes. These nodes contain icons: a magnifying glass, a shield with a building, a person with a magnifying glass, and a document. A heart rate line is also visible within one of the nodes.

Auditvision
IT-auditors

Uw partner
in NEN-7510

Inhoud

Introductie	3
Hoofdstuk 1 Belang van NEN-7510:2024	4
Hoofdstuk 2 Wat houdt NEN-7510:2024 in	5
Hoofdstuk 3 Onze aanpak: interne audit conform NEN-7510:2024	6
Hoofdstuk 4 Waarom kiezen voor AudITvision?	7
Hoofdstuk 5 Businesscase: Interne audit en transitiebegeleiding NEN-7510:2024	8



Introductie

AudITvision ondersteunt organisaties in de zorgsector bij het realiseren van aantoonbare informatiebeveiliging. Met onze gestructureerde interne audits helpen wij instellingen en leveranciers bij het voldoen aan de Nederlandse norm voor informatiebeveiliging in de zorg: NEN-7510. Deze norm is cruciaal voor organisaties die omgaan met medische gegevens of digitale patiëntinformatie, zowel in Nederland als in bredere Europese context.

In 2024 is een nieuwe versie van de norm gepubliceerd. Deze update brengt niet alleen inhoudelijke wijzigingen met zich mee, maar stelt ook aanvullende eisen aan risicobeoordeling, governance en de toepassing van beveiligingsmaatregelen. AudITvision helpt organisaties om de overgang van eerdere versies naar NEN-7510:2024 succesvol te doorlopen.

Onze aanpak biedt inzicht in naleving, identificeert kwetsbaarheden en reikt praktische verbeteradviezen aan. Dit resulteert in een solide voorbereiding op externe toetsing, verkleint het risico op datalekken en verhoogt het vertrouwen van patiënten, zorgverleners en toezichthouders.



Hoofdstuk 1 Belang van NEN-7510:2024

NEN-7510:2024 is dé norm voor informatiebeveiliging in de zorgsector in Nederland. Ze stelt eisen aan het beveiligen van persoonsgegevens en medische informatie in zorginstellingen, softwareleveranciers en andere partijen die met patiëntgegevens werken. De norm is gebaseerd op internationale normen zoals ISO 27001, maar is specifiek toegespitst op de zorgcontext. Voor organisaties betekent naleving van NEN-7510 niet alleen het technisch beschermen van data, maar ook het aantoonbaar beheersen van risico's, processen en verantwoordelijkheden. De implementatie is van groot belang voor:

- het voldoen aan de eisen van de Autoriteit Persoonsgegevens en andere toezichthouders;
- het verkrijgen of behouden van vertrouwen bij cliënten, zorgverleners en partners;
- het voldoen aan contractuele verplichtingen van bijvoorbeeld zorgverzekeraars of samenwerkingsverbanden in e-health;
- en het voorbereiden op toekomstige certificeringstrajecten.

Met de nieuwe versie van 2024 wordt meer nadruk gelegd op continue verbetering, expliciete risicobeoordeling, ketenverantwoordelijkheid en de werking van interne controles. Dit vraagt om een gestructureerde aanpak bij zowel implementatie als toetsing.



Hoofdstuk 2 Wat houdt NEN-7510:2024 in?

De NEN-7510:2024 norm richt zich op het opzetten, implementeren, onderhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging, beter bekend als ISMS (Information Security Management System). Dit systeem is ontworpen om organisaties in de zorgsector te helpen hun informatiebeveiliging op een gedegen en gestructureerde manier vorm te geven. Binnen deze sector zijn er enkele specifieke aandachtspunten die NEN-7510 scherp benoemt en waar extra focus op ligt. Allereerst is er de patiëntveiligheid:



medische informatie moet te allen tijde correct zijn, beschikbaar zijn wanneer dat nodig is en beschermd

worden tegen ongeautoriseerde wijziging. Daarnaast is de privacy van patiënten cruciaal; de verwerking van persoonsgegevens dient te voldoen aan de Algemene Verordening Gegevensbescherming (AVG), waarbij transparantie, rechtmatigheid en zorgvuldigheid centraal staan. Verder is de continuïteit van zorgprocessen van groot belang, wat betekent dat beveiligingsincidenten nooit mogen leiden tot onderbrekingen in de levering van zorg of het functioneren van essentiële systemen.

De versie van 2024 brengt ten opzichte van eerdere versies diverse belangrijke updates en aanvullingen met zich mee. Zo maakt de norm nu expliciet melding van zorgspecifieke risico's die organisaties moeten adresseren, zoals het voorkomen van datalekken, het beperken van onjuiste toegang tot systemen en informatie, en het vermijden van storingen in cruciale zorgapplicaties. Daarnaast zijn de eisen rond leveranciersbeheer en het gebruik van cloud-diensten uitgebreid en aangescherpt, omdat deze vormen van externe dienstverlening steeds belangrijker en complexer worden binnen de zorgketen. Ook legt de norm meer nadruk op technische beveiligingsaspecten, zoals het systematisch vastleggen van gebeurtenissen (logging), het monitoren van systemen en het detecteren en herstellen van incidenten op een effectieve manier.

Een ander wezenlijk onderdeel van NEN-7510:2024 is de koppeling met governance. Dit betekent dat de verantwoordelijkheid voor informatiebeveiliging expliciet wordt belegd bij het topmanagement, zoals de raad van bestuur of directie, en dat zij betrokken zijn bij het sturen en bewaken van het ISMS. Tot slot is de integratie van security-awareness onder medewerkers een belangrijke pijler geworden. Organisaties moeten

aantoonbaar aandacht besteden aan bewustwording, training en gedragsverandering om het menselijk risico te verkleinen en een beveiligingscultuur te creëren.

Een interne audit vormt een cruciaal instrument om te beoordelen in hoeverre deze maatregelen adequaat en



doeltreffend zijn geïmplementeerd. Hiermee kan een organisatie bepalen waar nog verbeteringen nodig zijn en of het managementsysteem voldoende robuust is om een externe certificeringsaudit succesvol te doorstaan. Zonder een goed uitgevoerde interne audit blijft het lastig om risico's tijdig te herkennen en te mitigeren, wat uiteindelijk de kwaliteit en betrouwbaarheid van de informatiebeveiliging in de zorgsector onder druk kan zetten.

Hoofdstuk 3 Onze aanpak: interne audit conform NEN-7510:2024

AuditVision hanteert een gestructureerde auditaanpak gebaseerd op internationale auditprincipes en de eisen van NEN-7510:2024. We combineren documentanalyse met interviews, risico-inschattingen en toetsing van maatregelen in de praktijk. De stappen van onze interne auditdienst zijn als volgt:

1. Intake en scopedefinitie

We starten met een intakegesprek waarin we samen met de organisatie de scope van de audit bepalen. Welke locaties, processen, informatiesystemen en leveranciers vallen binnen het ISMS? Wat is de status van de transitie naar de 2024-versie?

2. Uitvoering audit en beoordeling ISMS

Onze auditoren analyseren beleid, procedures, risicoanalyses, gebruikersbeheer, logbestanden, incidentregistraties en awarenesscampagnes. We voeren gesprekken met sleutelfiguren binnen IT, zorg, security en management.

3. Gap-analyse en risicobeoordeling

De bevindingen worden afgezet tegen de normen van NEN-7510:2024. Afwijkingen worden gekwalificeerd (minor, major of aandachtspunt) en gekoppeld aan hun potentiële impact. Per onderdeel bieden wij heldere aanbevelingen en prioriteiten.

4. Begeleiding bij verbetering

Indien gewenst begeleiden we de organisatie bij het opstellen en uitvoeren van verbetermaatregelen. We ondersteunen bij het aanpassen van procedures, het verhogen van awareness of het invoeren van aanvullende technische controles.

5. Herbeoordeling (optioneel)

Na uitvoering van de verbetermaatregelen voeren wij – indien gewenst – een heraudit uit. Hierbij controleren we of de tekortkomingen zijn opgelost en het systeem klaar is voor externe certificering.



Hoofdstuk 4 **Waarom kiezen voor AudITvision?**

AudITvision biedt specifieke meerwaarde voor organisaties in de zorg en medische sector:

Gespecialiseerd in zorg & IT-beveiliging

Onze auditors combineren kennis van informatiebeveiliging met ervaring in zorgomgevingen. Wij begrijpen niet alleen de norm, maar ook de context waarin u werkt.

Onafhankelijk en objectief

We zijn geen leverancier van software of implementatietools, en hebben geen commercieel belang bij aanvullende trajecten. Onze audits zijn zuiver en betrouwbaar.

Toegankelijke rapportage, gericht op actie

Onze rapportages zijn helder en praktisch. U ontvangt geen theoretisch normverslag, maar een werkbaar verbeterplan op basis van concrete bevindingen.

Ervaring met NEN-7510:2024-transitie

Wij hebben ervaring met organisaties die overstappen van NEN-7510:2017 naar NEN-7510:2024. We weten waar de verschillen zitten en hoe u dat aantoonbaar kunt maken.

Zorgbreed inzetbaar

Van GGZ-instelling tot ziekenhuis, van ICT-dienstverlener tot apotheekketen – wij kennen de sector, de risico's én de best practices.



Hoofdstuk 5 Businesscase: Interne audit en transitiebegeleiding NEN-7510:2024

Klantprofiel

Een regionaal IT-dienstverlener actief in de zorgsector beheerde de hosting- en databeveiliging voor meerdere huisartsenpraktijken en GGZ-instellingen. De organisatie was al jarenlang gecertificeerd volgens NEN-7510:2017, maar wilde tijdig en aantoonbaar overstappen naar de nieuwe NEN-7510:2024.

Uitdaging

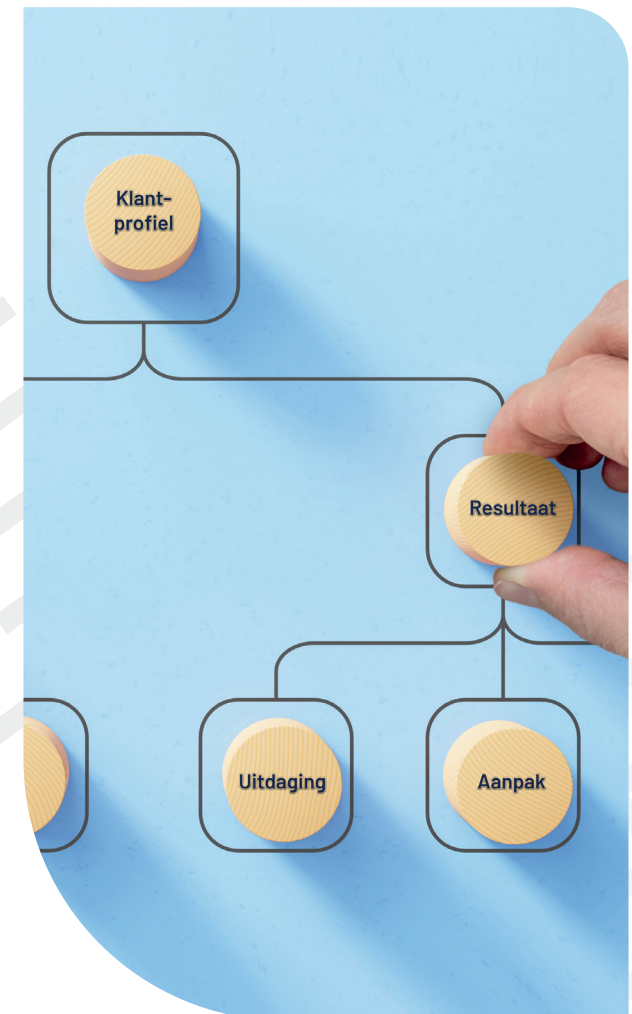
De normwijziging bracht een grotere nadruk op risicogebaseerd werken en governance met zich mee. Dit betekende dat bestaande procedures en maatregelen herzien moesten worden, en dat aanvullende documentatie nodig was rondom logging, beheer van cloudleveranciers en het trainen van personeel.

Aanpak

AuditVision werd ingeschakeld om een volledige interne audit uit te voeren, gericht op de NEN-7510:2024-eisen. Tijdens deze audit werden zowel beleid als operationele praktijk doorgelicht. In overleg met directie en security officers zijn nieuwe risicobeoordelingen opgesteld en is de bestaande awareness-aanpak geüpdatet. Ook zijn leveranciersbeoordelingen aangescherpt en is het incidentmanagementproces aangepast aan de nieuwe vereisten.

Resultaat

Na implementatie van de voorgestelde maatregelen voerden wij een herbeoordeling uit. Daarbij werd vastgesteld dat de organisatie aantoonbaar voldeed aan NEN-7510:2024. De transitie werd succesvol afgerond en de klant is inmiddels voorbereid op certificering onder de nieuwe norm.



audITvision b.v.
Van der Houven van Oordtlaan 2
7316 AH Apeldoorn
t. 088-2028700

info@auditvision.nl
www.auditvision.nl

AudITvision
IT-auditors

**Uw partner
in NEN-7510**