

# Whitepaper

## ISO 13485



**Auditvision**  
IT-auditors

Uw partner  
in ISO 13485

# Inhoud

|                                                                                     |          |
|-------------------------------------------------------------------------------------|----------|
| <b>Introductie</b>                                                                  | <b>3</b> |
| Hoofdstuk 1 <b>Belang van ISO 13485 voor organisaties</b>                           | <b>4</b> |
| Hoofdstuk 2 <b>Wat houdt ISO 13485 in?</b>                                          | <b>5</b> |
| Hoofdstuk 3 <b>Onze aanpak: interne audit conform ISO 13485</b>                     | <b>6</b> |
| Hoofdstuk 4 <b>Waarom AuditVision?</b>                                              | <b>7</b> |
| Hoofdstuk 5 <b>Businesscase: succesvol ISO 13485 interne audit en adviestraject</b> | <b>8</b> |



# Introductie

AudITvision biedt hoogwaardige interne auditdiensten voor organisaties die actief zijn in de medische hulpmiddelensector. De ontwikkeling hiervan. Van productontwikkeling en productie tot distributie en post-market surveillance – wij ondersteunen uw kwaliteitsmanagementsysteem conform ISO 13485.

Onze interne auditdienst garandeert een gestructureerde, normconforme aanpak die bijdraagt aan aantoonbare naleving van wet- en regelgeving, waaronder de Medical Device Regulation (MDR) en andere wereldwijde eisen. Door gebruik van het AudITvision-keurmerk en de audit op de internationale auditstandaarden leveren we betrouwbare rapportages die vertrouwen wekken bij toezichthouders, klanten en certificerende instanties.

Onze audits identificeren tekortkomingen voordat deze risico's worden, en helpen uw organisatie bij het structureel verbeteren van processen. Zo beschermen we niet alleen uw compliancepositie, maar ook wat echt telt: de veiligheid en gezondheid van patiënten. Met AudITvision heeft u een onafhankelijke en ervaren partner aan uw zijde – niet alleen op het gebied van kwaliteitsborging, maar ook in risicobeheer, traceerbaarheid en documentcontrole binnen de sterk gereguleerde medische hulpmiddelensector.



# Hoofdstuk 1 Belang van ISO 13485 voor organisaties

Voor fabrikanten, distributeurs, leveranciers en andere actoren in de medische hulpmiddelensector is ISO 13485 dé wereldwijde standaard voor kwaliteitsmanagement. De norm vormt de basis voor naleving van regelgeving in Europa (MDR), de Verenigde Staten (FDA 21 CFR Part 820), Canada (CMDR), Japan (PMDA) en andere markten. De implementatie van ISO 13485 is essentieel voor:

- Toegang tot internationale markten
- Vertrouwen van klanten en toezichthouders
- Effectief risicobeheer in de productlevenscyclus
- Het aantonen van naleving tijdens inspecties en certificeringen

ISO 13485 stelt eisen aan onder meer documentatie, ontwerpcontrole, validatie, klachtenbeheer, CAPA-processen (Corrective and Preventive Actions), leveranciersbeheer en post-market surveillance. De norm is daarmee niet alleen een compliance-instrument, maar ook een strategisch hulpmiddel voor kwaliteits- en risicomanagement binnen de keten van medische hulpmiddelen.



# Hoofdstuk 2 Wat houdt ISO 13485 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 ISO 13485

De ISO 13485-norm richt zich op het opzetten, implementeren, onderhouden en continu verbeteren van een kwaliteitsmanagementsysteem (QMS) voor organisaties die medische hulpmiddelen ontwerpen, produceren, installeren of onderhouden. Dit systeem is bedoeld om aan te tonen dat een organisatie in staat is veilige en doeltreffende medische hulpmiddelen te leveren die voldoen aan zowel klantvereisten als relevante wet- en regelgeving. De norm is vooral van belang voor fabrikanten, leveranciers en distributeurs in de medische hulpmiddelensector.



Binnen deze sector zijn er specifieke aandachtspunten die ISO 13485 expliciet benoemt en waar extra focus op ligt. Allereerst is er de patiëntveiligheid: producten en processen moeten zo worden beheerd dat risico's tot een minimum worden beperkt en de veiligheid van eindgebruikers wordt gewaarborgd. Daarnaast stelt de norm strikte eisen aan traceerbaarheid, documentatie en kwaliteitsborging gedurende de hele levenscyclus van een medisch hulpmiddel – van ontwerp en ontwikkeling tot post-market surveillance.

De laatste editie van de norm brengt ten opzichte van eerdere versies diverse belangrijke aanvullingen met zich mee. Zo wordt er meer nadruk gelegd op risicomanagement, niet alleen bij productontwikkeling, maar ook binnen ondersteunende processen zoals inkoop, productie en klachtbehandeling. Organisaties moeten kunnen aantonen dat zij risico's systematisch identificeren, evalueren en beheersen. Ook zijn de eisen rondom toeleveranciersbeheer aangescherpt: bedrijven moeten kunnen aantonen dat zij grip hebben op de prestaties van hun leveranciers, inclusief het gebruik van externe partijen zoals contractfabrikanten of laboratoria.

Een ander belangrijk onderdeel van ISO 13485 is de koppeling met governance en compliance. De verantwoordelijkheid voor kwaliteit en regelgeving ligt nadrukkelijk bij het topmanagement, dat betrokken moet zijn bij het sturen, bewaken en verbeteren van het QMS. Daarnaast vereist de norm dat medewerkers op alle niveaus voldoende bewust zijn van hun rol in het handhaven van productkwaliteit en patiëntveiligheid. Training en competentiebeheer vormen dan ook een belangrijke pijler binnen het systeem.

Een interne audit vormt een cruciaal instrument om te beoordelen in hoeverre het kwaliteitsmanagementsysteem doeltreffend is geïmplementeerd en wordt nageleefd. Hiermee kan een organisatie bepalen waar verbeteringen nodig zijn en of het systeem voldoende robuust is om een externe certificeringsaudit te doorstaan. Zonder een goed uitgevoerde interne audit blijft het lastig om afwijkingen, risico's en verbeterkansen tijdig te herkennen, wat uiteindelijk de kwaliteit en betrouwbaarheid van medische hulpmiddelen onder druk kan zetten.



# Hoofdstuk 4 **Waarom AudITvision?**

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

## **Gespecialiseerd in medische hulpmiddelen**

Onze auditors beschikken over diepgaande kennis van ISO 13485, MDR, FDA-eisen en andere relevante regelgeving. Wij begrijpen de impact van non-conformiteiten op patiëntveiligheid én markttoegang.

## **Praktisch, gestructureerd en normconform**

Geen wazige rapporten of theoretische analyses. Onze bevindingen zijn helder, toepasbaar en direct gekoppeld aan de normstructuur. U weet exact waar u staat en wat er moet gebeuren.

## **Onafhankelijk en objectief**

AudITvision is geen adviesbureau dat ook QMS'en verkoopt. Wij zijn 100% onafhankelijk en objectief in onze beoordelingen. Dat maakt ons betrouwbaar voor zowel klanten als externe certificerende instanties.

## **Transparante werkwijze en prijsafspraken**

U weet vooraf waar u aan toe bent: qua aanpak, tijdslijnen én kosten. Geen verrassingen achteraf.

## **Ervaring in complexe en gereguleerde omgevingen**

Van start-up tot multinational: wij hebben audits uitgevoerd in klinische, R&D- en productieomgevingen voor medische hulpmiddelen, implantaten, software (SaMD) en diagnostiek.



# Hoofdstuk 5 Businesscase: succesvol ISO 13485 interne audit en adviestraject

## Klantprofiel

Een innovatieve startup uit Zuid-Nederland, actief in de medische technologie, ontwikkelde diagnostische hulpmiddelen bedoeld voor thuisgebruik. De onderneming bevond zich in een cruciale groeifase en wilde toetreden tot de Europese markt. Hiervoor was naleving van de Europese Medical Device Regulation (MDR) noodzakelijk. ISO 13485-certificering werd beschouwd als de fundamentele basis om aan de MDR-eisen te voldoen en vertrouwen op te bouwen bij toezichthouders, zorgverleners en distributeurs.

## Uitdaging

De startup beschikte over een jong en groeiend kwaliteitsmanagementsysteem (QMS), maar had beperkte ervaring met interne audits en certificeringstrajecten. Dit leidde tot onzekerheid over de volledigheid van de technische documentatie en het QMS als geheel. Daarnaast waren er vragen over de mate waarin processen zoals validatie en traceerbaarheid voldeden aan de eisen van ISO 13485. De organisatie wilde een objectieve beoordeling om te bepalen waar zij stond en wat er nog nodig was om klaar te zijn voor certificering.

## Aanpak

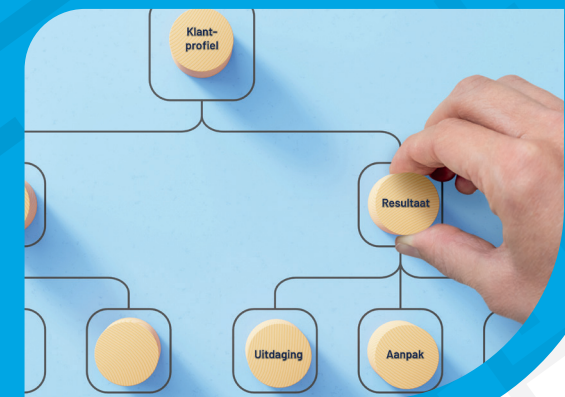
AudITvision werd ingeschakeld om een volledige interne audit uit te voeren, met als doel het identificeren van gaps en bevindingen ten opzichte van ISO 13485 en het begeleiden van verbetermaatregelen. Tijdens het traject werd het volledige kwaliteitsmanagementsysteem en de technische documentatie grondig beoordeeld. In gesprekken met de verantwoordelijke teams voor kwaliteit, regelgeving en productontwikkeling werden processen getoetst op consistentie, effectiviteit en naleving van de norm. De bevindingen werden per hoofdstuk van ISO 13485 in kaart gebracht in een gedetailleerde gap-analyse, voorzien van concrete aanbevelingen. Vervolgens ondersteunden wij de organisatie bij het opstellen en uitvoeren van Corrective and Preventive Actions (CAPA's). Ter voorbereiding op de externe certificeringsaudit voerden wij een herbeoordeling uit, waarin we toetsten of de verbeteracties doeltreffend waren geïmplementeerd.

## Resultaat

Binnen een periode van drie maanden wist de organisatie de belangrijkste tekortkomingen effectief aan te pakken. Tijdens de daaropvolgende externe certificeringsaudit werden slechts enkele kleine afwijkingen vastgesteld, waarvoor geen heraudits

nodig was. De organisatie verkreeg succesvol het ISO 13485-certificaat en kon daardoor sneller dan gepland haar product op de Europese markt introduceren. De interne audit vormde niet alleen een toetsmoment, maar ook een belangrijk leermoment voor het team en een solide basis voor toekomstige kwaliteitsborging.

AudITvision helpt organisaties in de medische hulpmiddelensector om met vertrouwen het certificeringstraject in te gaan. Onze audits zijn meer dan een checklist – ze zijn gericht op inhoudelijke versterking van uw systeem, zodat kwaliteit aantoonbaar en werkbaar wordt.



audITvision b.v.

Van der Houven van Oordtlaan 2  
7316 AH Apeldoorn

t. 088-2028700

[info@auditvision.nl](mailto:info@auditvision.nl)  
[www.auditvision.nl](http://www.auditvision.nl)

**AudITvision**  
IT-auditors

**Uw partner  
in ISO 13485**