

Onafhankelijke audits NEN 7510 & ISO 27001

Weet u echt hoe uw informatiebeveiliging ervoor staat?

U weet nu niet of uw informatiebeveiliging echt werkt

Elk jaar tekent u het beleid af. De documenten zijn op orde, de risicoanalyses zijn ingevuld, de medewerkers zijn ingelicht. Maar niemand heeft het systeem ooit van binnenuit getoetst. Dat is het moment waarop uw externe auditor bevindingen doet — niet omdat het beleid slecht is, maar omdat papier en praktijk uit elkaar zijn gegroeid.

Ik los dat op. Als onafhankelijk auditor met meer dan 35 jaar ervaring in informatiebeveiliging kom ik niet om te keuren, maar om u te helpen sturen. U weet daarna exact waar u staat, wat er beter moet en hoe u dat aanpakt — vóórdat uw externe auditor er was.

Voor wie is dit?

Voor zorginstellingen die NEN 7510 willen behalen of behouden. Voor MKB-softwarebedrijven die ISO 27001 nodig hebben voor aanbestedingen of klanten. Voor farmaceutische toeleveranciers die GMP combineren met ISO 27001. En voor bestuurders die persoonlijke aansprakelijkheid serieus nemen — zeker met de Cyberbeveiligingswet in aantocht.

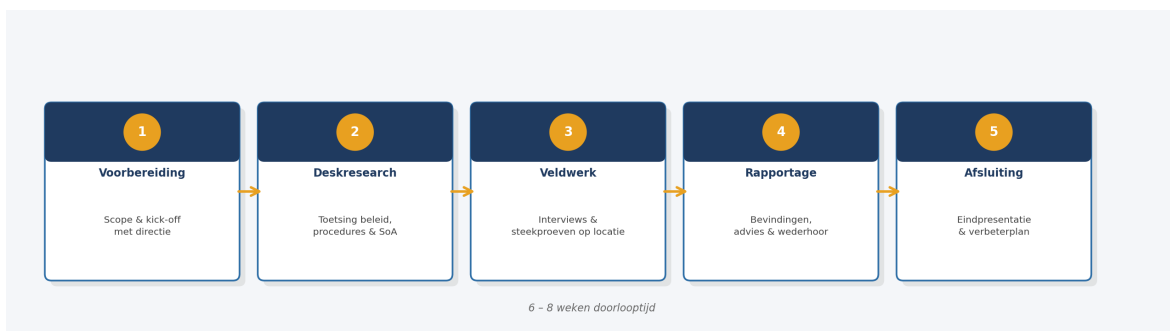
Wat u terugkrijgt

- ✓ Onafhankelijk auditoordeel — klaar voor directiebeoordeling
- ✓ lijst verbeterpunten, — geprioriteerd op risico
- ✓ Toepasbaarheidsverklaring per beheersmaatregel
- ✓ Bewijslast voor de externe certificeringsaudit
- ✓ Uw externe auditor vindt geen verrassingen

Doorlooptijd (voorbeeld)

| | | |
|-----------|-----------|-----------|
| ISO 27001 | · 6 weken | · 6 dagen |
| NEN 7510 | · 6 weken | · 6 dagen |
| Combi | · 8 weken | · 9 dagen |

Hoe ik werk — vijf fasen in zes tot acht weken



Vorbereiding. In de kick-off met directie en proceseigenaren stel ik de scope vast. Zo voorkom ik achteraf herwerk.

Deskresearch. Beleidsdocumenten, procedures, risicoregister en de Verklaring van Toepasselijkheid toets ik aan de norm. Lacunes markeer ik direct.

Veldwerk. Ik spreek zes tot tien medewerkers op locatie en doe steekproeven. Hier komt het verschil tussen papier en praktijk aan het licht.

Rapportage. Het rapport gaat ter wederhoor naar de organisatie. Feitelijke onjuistheden worden gecorrigeerd voordat ik het definitief maak.

Drie varianten

ISO 27001

Softwarebedrijven, dienstverleners, MKB

NEN 7510

Zorginstellingen, GGZ, Huisartsen

Combi

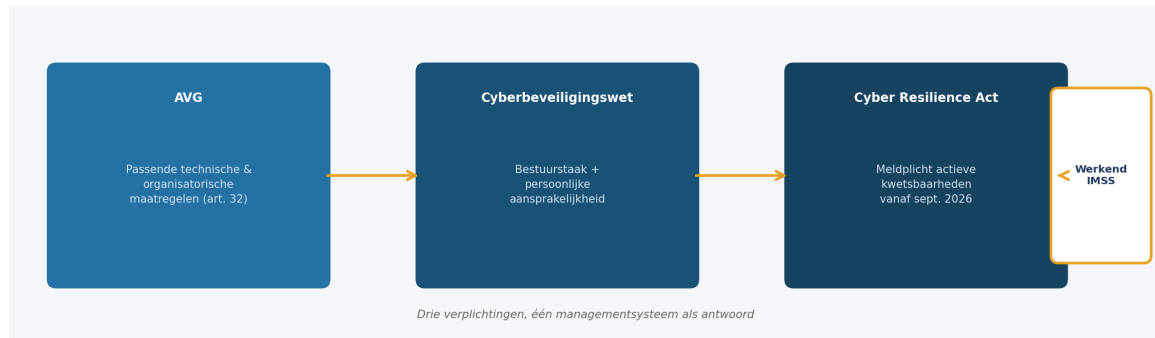
Softwareleveranciers in de zorg

Offerte binnen 3 werkdagen op aanvraag.

Afsluiting. Ik presenteer het eindrapport aan de stuurgroep en bespreek het verbeterplan. Nazorg is standaard inbegrepen.

Drie verplichtingen. Eén antwoord.

De AVG, de Cyberbeveiligingswet en de Cyber Resilience Act stellen allemaal dezelfde eis: aantoonbaar werken aan informatieveiligheid. Een werkend ISMS volgens ISO 27001 of NEN 7510 dekt 70–80% van die zorgplicht in één keer af.



Van twijfel naar certificaat in 12 weken

Een zorginstelling met 220 medewerkers en vier locaties wilde weten waar ze stonden vóórdat ze het NEN 7510-certificeringstraject in zouden gaan. Gemeenten vroegen er bij Wmo-aanbestedingen al naar.

In zes auditdagen bracht ik het systeem in kaart. Beleid en procedures waren grotendeels op orde — maar oud-medewerkers hadden tot vier weken na vertrek nog actieve toegang tot het elektronisch cliëntendossier. De HR-IT-koppeling bestond simpelweg niet.

Vijf verbeterpunten. Doorlooptijd acht weken. De externe certificeringsaudit daarna leverde één minor non-conformity op, dezelfde week opgelost.

Resultaat: Duidelijk verbeterplan opgesteld, tijdsplan erbij, Wmo-aanbesteding gewonnen.

||

*De interne audit was geen examen.
Het was de generale repetitie.*

— Bestuurder zorginstelling, NEN 7510

Over 258 Management

258 Management is mijn bureau. Met meer dan 35 jaar ervaring in ICT, informatiebeveiliging en governance werk ik voor zorginstellingen, farmaceutische bedrijven en zakelijke dienstverleners.

Certificeringen: C|CISO · CISM · CISA · CRISC



Normen zijn middelen, geen doel.

Klaar om te starten?

Plan een kennismakingsgesprek van 30 minuten. Ik vertel u welke variant past en wat de investering is.

+31 6 5269 8063

g.palm@258-management.nl

www.258-management.info