VeeHa B.V.
Cybersecurity and privacy

VeeHa checklist ISO 27001 en NEN 7510

Van start tot certificaat: 57 punten in acht fasen om een managementsysteem voor informatiebeveiliging (ISMS) te implementeren en klaar te zijn voor de certificeringsaudit.

Verwijzingen naar clausules (4–10) en Annex A-maatregelen gelden voor ISO/IEC 27001:2022. Punten met **NEN 7510** zijn aanvullend voor zorgorganisaties en leveranciers in de zorg. Deze checklist is een hulpmiddel en geen formele conformiteitsbeoordeling; voor certificering gelden de actuele normteksten en het schema van de certificerende instelling.

Organisatie | **Ingevuld door** | **Datum**

Dit is een invulbare PDF: vink punten aan en vul de velden in met Adobe Acrobat Reader, de pdf-viewer van je browser of Voorvertoning op de Mac, en sla het bestand daarna op.

1. Voorbereiding en draagvlak

Zonder besluit, mandaat en tijd van de directie komt een ISMS niet van de grond.

☐	De directie heeft besloten een ISMS in te richten en stelt mensen, tijd en budget beschikbaar.	5.1, 7.1
☐	Er is een interne trekker (ISMS-eigenaar) aangewezen met mandaat en tijd, in de praktijk 1 tot 2 dagen per week tijdens de implementatie.	5.3
☐	De aanleiding en het doel zijn vastgelegd, bijvoorbeeld een klanteis, aanbesteding of de Cyberbeveiligingswet.	4.1
☐	Er is een nulmeting of gap-analyse uitgevoerd ten opzichte van de norm.	
☐	Er is een realistische planning tot de certificeringsaudit, meestal 6 tot 12 maanden.	6.2

Notities, acties en eigenaar

2. Context en scope

Bepaal waar het ISMS over gaat voordat je maatregelen kiest.

☐	Interne en externe factoren die van invloed zijn op informatiebeveiliging zijn vastgelegd.	4.1
☐	Belanghebbenden en hun eisen zijn bekend, inclusief klanten, toezichthouders en ketenpartners.	4.2
☐	Wet- en regelgeving en contractuele eisen zijn geïnventariseerd, zoals de AVG en de Cyberbeveiligingswet.	4.2, A.5.31
☐	De scope is vastgesteld: organisatieonderdelen, locaties, processen, systemen en raakvlakken met derden.	4.3
☐	**NEN 7510** Vastgesteld is welke persoonlijke gezondheidsinformatie de organisatie verwerkt en in welke systemen.	NEN 7510-1

Notities, acties en eigenaar

3. Leiderschap, beleid en rollen

Informatiebeveiliging wordt gedragen door het management, niet alleen door IT.

☐	Het informatiebeveiligingsbeleid is vastgesteld door de directie en bekendgemaakt.	5.2
☐	Rollen, verantwoordelijkheden en bevoegdheden zijn belegd en bekend.	5.3, A.5.2
☐	Er zijn meetbare doelstellingen voor informatiebeveiliging, met eigenaar en planning.	6.2
☐	Onderwerpspecifieke beleidsregels zijn opgesteld waar nodig, bijvoorbeeld voor toegang, thuiswerken en AI-gebruik.	A.5.1
☐	**NEN 7510** De governance sluit aan op de verantwoordelijkheden in de zorg, met de bestuurder als eindverantwoordelijke.	NEN 7510-1

Notities, acties en eigenaar

4. Risicomanagement en Verklaring van Toepasselijkheid

Het hart van het ISMS: maatregelen volgen uit risico's.

☐	Er is een vaste methode voor risicoanalyse, met criteria voor kans, impact en risicoacceptatie.	**6.1.2**
☐	Er is een overzicht van informatie en bedrijfsmiddelen, met een eigenaar per onderdeel.	**A.5.9**
☐	De risicoanalyse is uitgevoerd met sleutelpersonen uit de organisatie.	**6.1.2, 8.2**
☐	Er is een risicobehandelplan met maatregel, eigenaar en termijn per risico.	**6.1.3, 8.3**
☐	Restrisico's zijn expliciet geaccepteerd door de risico-eigenaren.	**6.1.3**
☐	De Verklaring van Toepasselijkheid motiveert voor alle 93 Annex A-maatregelen of en waarom ze van toepassing zijn.	**6.1.3 d**
☐	**NEN 7510** Risico's zijn ook beoordeeld op de gevolgen voor de cliënt, patiëntveiligheid en zorgcontinuïteit.	**NEN 7510-1**

Notities, acties en eigenaar

5. Maatregelen invoeren

Van papier naar praktijk: de maatregelen uit je Verklaring van Toepasselijkheid werken aantoonbaar.

☐	Informatie is geclassificeerd en er zijn regels voor het omgaan met elke klasse.	**A.5.12, A.5.13**
☐	Toegangsbeheer werkt op basis van least privilege, met periodieke controle van rechten.	**A.5.15–A.5.18, A.8.2**
☐	Leveranciers zijn geclassificeerd; kritische leveranciers zijn beoordeeld en contracten bevatten beveiligingseisen.	**A.5.19–A.5.22**
☐	Voor clouddiensten zijn aanschaf, gebruik, beheer en exit geregeld.	**A.5.23**
☐	Er is een incidentprocedure, inclusief meldplichten (AVG binnen 72 uur, Cbw binnen 24 en 72 uur).	**A.5.24–A.5.28**
☐	Continuïteit en ICT-gereedheid zijn geregeld en getest.	**A.5.29, A.5.30**
☐	Medewerkers zijn gescreend waar nodig en hebben geheimhoudingsafspraken getekend.	**A.6.1, A.6.6**
☐	Fysieke beveiliging is geregeld: toegang tot gebouwen en ruimten, clear desk en clear screen.	**A.7**
☐	Werkplekken en mobiele apparaten zijn beveiligd, met bescherming tegen malware.	**A.8.1, A.8.7**
☐	Technische kwetsbaarheden worden structureel opgespoord en opgelost (patchbeleid).	**A.8.8**
☐	Configuratie- en wijzigingsbeheer zijn ingericht.	**A.8.9, A.8.32**
☐	Back-ups worden gemaakt en het herstel wordt periodiek getest.	**A.8.13**
☐	Logging en monitoring zijn ingericht en worden gebruikt om afwijkingen te signaleren.	**A.8.15, A.8.16**
☐	Cryptografie en sleutelbeheer zijn geregeld.	**A.8.24**
☐	Veilige ontwikkeling is geborgd, als de organisatie zelf software ontwikkelt.	**A.8.25–A.8.29**
☐	**NEN 7510** Toegang tot gezondheidsinformatie is afgestemd op de behandelrelatie.	**NEN 7510-2**
☐	**NEN 7510** Inzage in en wijzigingen van dossiers worden gelogd volgens NEN 7513, en die logging wordt gecontroleerd.	**NEN 7510-2, NEN 7513**
☐	**NEN 7510** Medische apparatuur en zorginformatiesystemen zijn meegenomen in risicoanalyse en beheer.	**NEN 7510-2**
☐	**NEN 7510** Gegevensuitwisseling met ketenpartners is betrouwbaar geregeld.	**NEN 7512**

Notities, acties en eigenaar

6. Mensen en documentatie

Iedereen weet wat er van hem of haar wordt verwacht, en je kunt het laten zien.

☐	Benodigde competenties zijn vastgesteld en aantoonbaar aanwezig.	7.2
☐	Er is een bewustwordingsprogramma voor alle medewerkers, afgestemd op hun rol.	7.3, A.6.3
☐	**NEN 7510** Zorgprofessionals en management hebben zorgspecifieke awareness gekregen.	NEN 7510-2
☐	Interne en externe communicatie over informatiebeveiliging is geregeld.	7.4
☐	Documenten worden beheerd: versie, goedkeuring, beschikbaarheid en bewaartermijn.	7.5
☐	Registraties worden bijgehouden, zoals incidenten, wijzigingen, trainingen en toegangsreviews.	7.5

Notities, acties en eigenaar

7. Evaluatie

Laat zien dat het ISMS werkt voordat de auditor komt.

☐	Er wordt gemeten of het ISMS effectief is, met indicatoren die terugkoppelen naar de doelstellingen.	9.1
☐	Er is een intern auditprogramma en het hele ISMS is minstens één keer onafhankelijk intern geaudit.	9.2
☐	De management review is gehouden, met alle verplichte onderwerpen en vastgelegde besluiten.	9.3
☐	Het ISMS draait aantoonbaar al enige tijd, met registraties over meerdere maanden.	

Notities, acties en eigenaar

8. Verbetering en certificeringsaudit

De laatste stappen naar het certificaat en daarna.

☐	Afwijkingen en verbeterpunten worden geregistreerd, de oorzaak wordt onderzocht en ze worden opgevolgd.	10.2
☐	Een door de RvA geaccrediteerde certificerende instelling is gekozen en de audit is ingepland.	
☐	Fase 1-audit: documentatie en gereedheid zijn beoordeeld, bevindingen zijn opgelost.	
☐	Fase 2-audit: medewerkers zijn voorbereid op interviews en steekproeven in de praktijk.	
☐	Er is een aanpak om eventuele afwijkingen na de audit binnen de gestelde termijn op te lossen.	10.2
☐	Er is een jaarplanning na certificering: controle-audits, interne audits en management review.	10.1

Notities, acties en eigenaar

Hulp nodig? Plan een vrijblijvend kennismakingsgesprek via www.veeha.nl/contact of mail naar info@veeha.nl. Je krijgt binnen 24 uur een reactie. Wil je eerst meten waar je staat? Doe de gratis ISMS-volwassenheidsscan op www.veeha.nl/volwassenheidsscan.