VeeHa B.V.
Cybersecurity and privacy

VeeHa B.V.
Aalsburg 1508
6602 TS Wijchen

Telefoon +31 6 125 749 24
Website www.veeha.nl
Email info@veeha.nl
KvK 97195618

WHITEPAPER 11 - 2026 Jan Willem van Hoorn

Nut en noodzaak van ISO 27001 en NEN 7510

Voordelen, wet- en regelgeving, stappenplan, doorlooptijd en kosten van certificering

Informatiebeveiliging is geen keuze meer, maar een aantoonbare plicht van het bestuur.

Sinds 15 augustus 2026 geldt de Cyberbeveiligingswet voor ruim 8.000 Nederlandse organisaties. Zorgaanbieders zijn al langer wettelijk gehouden aan NEN 7510. En klanten vragen steeds vaker om aantoonbaar bewijs dat hun leveranciers de beveiliging op orde hebben.

Deze whitepaper beschrijft wat ISO 27001 en NEN 7510 zijn, waarom ze nu nodig zijn, wat certificering oplevert en hoe een realistisch traject eruitziet: de stappen, de doorlooptijd en de kosten.

VeeHa B.V.

Praktische ondersteuning bij ISO 27001, NEN 7510, ISO 9001, privacy, risicoanalyse, beleid, implementatie en interne audits.

VeeHa B.V.
Cybersecurity and privacy

Managementsamenvatting

Informatiebeveiliging is sinds 15 augustus 2026 voor ruim 8.000 Nederlandse organisaties een wettelijke plicht met bestuurlijke aansprakelijkheid. Een ISMS volgens ISO 27001 of NEN 7510 is de snelste, aantoonbare route om daaraan te voldoen en om klanten, ketenpartners en toezichthouders vertrouwen te geven. De kernpunten:

1. **Wet- en regelgeving dwingt het af.** De Cyberbeveiligingswet (NIS2) geldt sinds 15 augustus 2026, met boetes tot € 10 miljoen of 2% van de wereldwijde omzet. Zorgaanbieders zijn via het Besluit elektronische gegevensverwerking al wettelijk gehouden aan NEN 7510.
2. **De normen zijn vernieuwd.** ISO 27001:2022 en NEN 7510-1:2024 sluiten op elkaar aan. Bestaande NEN 7510-certificaten op de oude versie vervallen op 20 februari 2027.
3. **Certificering loont commercieel.** Het certificaat is steeds vaker een harde eis in aanbestedingen en leverancierscontracten, en verkort beveiligingsvragenlijsten van klanten aanzienlijk.
4. **Realistische doorlooptijd: 6 tot 12 maanden** voor de meeste organisaties; 3 tot 6 maanden als de basis al op orde is.
5. **Realistische kosten eerste jaar: circa € 20.000 tot € 80.000** voor het mkb, waarvan het grootste deel interne uren zijn.

> **Advies:** bepaal eerst of u onder de Cyberbeveiligingswet valt en welke norm uw klanten vragen, kies dan een afgebakende scope en start met een nulmeting. Wachten maakt het traject niet goedkoper, wel krapper.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

VeeHa B.V.
Cybersecurity and privacy

1. Inleiding: waarom nu

De dreiging neemt toe terwijl de weerbaarheid achterblijft. Het Cybersecuritybeeld Nederland 2025 van de NCTV concludeert dat aanvallen gevarieerder en minder voorspelbaar worden, onder meer door statelijke actoren en generatieve AI. Tegelijk ontstaan veel incidenten nog steeds doordat de digitale basishygiëne niet op orde is.

In oktober 2026 waarschuwde het themarapport Cyberdreigingen van de Rijksbrede Risicoanalyse dat grootschalige cyberincidenten zeer waarschijnlijk zijn. Ook de afhankelijkheid van enkele buitenlandse techbedrijven wordt als groot risico genoemd.

De incidenten zijn concreet:

- **Openbaar Ministerie (2025):** het netwerk werd offline gehaald vanwege een Citrix-kwetsbaarheid, met grote gevolgen voor de strafrechtsketen.
- **Clinical Diagnostics (2025):** bij een cyberaanval op dit laboratorium lekten de medische gegevens van honderdduizenden mensen uit.
- **Bedrijfsleven:** volgens de CBS Cybersecuritymonitor 2025 kreeg 16% van de bedrijven met 250 of meer werknemers met een cyberincident te maken, terwijl slechts 13% van de kleinste bedrijven tien of meer van de twaalf onderzochte basismaatregelen heeft genomen.

Daarmee is informatiebeveiliging geen IT-onderwerp meer maar een bestuursverantwoordelijkheid. Een managementsysteem volgens ISO 27001 of NEN 7510 geeft het bestuur grip: risico's zijn in beeld, maatregelen zijn aantoonbaar en er is een vaste cyclus van verbeteren.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

2. ISO 27001 en NEN 7510: wat zijn het?

Beide normen beschrijven een managementsysteem voor informatiebeveiliging (ISMS): een vaste cyclus van risico's bepalen, maatregelen nemen, controleren en verbeteren (Plan-Do-Check-Act). ISO 27001 is de internationale basis; NEN 7510 is de Nederlandse zorgvariant die daarop voortbouwt met extra zorgspecifieke eisen.

De NEN 7510-1:2024 sluit aan op ISO 27001:2022 en ordent de maatregelen in vier thema's: organisatie, mens, fysiek en technologie. Naast de 93 algemene beheersmaatregelen bevat zij acht zorgspecifieke maatregelen, deels gebaseerd op NIS2.

2.1 De verschillen op een rij

Kenmerk	ISO 27001:2022	NEN 7510-1:2024
Reikwijdte	Internationaal, elke sector	Nederland, zorg en beheerders van gezondheidsgegevens
Beheersmaatregelen (Annex A)	93, in 4 thema's	93 algemeen + 8 zorgspecifiek
Wettelijke status	Vrijwillig	Verplicht voor zorgaanbieders (voldoen, niet certificeren)
Aanvullende normen	ISO 27002 (implementatierichtlijn)	NEN 7510-2, NEN 7512 (uitwisseling), NEN 7513 (logging)
Erkenning	Wereldwijd, ruim 70.000 certificaten	Nederlandse zorgketen, IGJ, zorginkopers
Overgang oude versie	Certificaten op de 2013-versie zijn per 31 oktober 2025 vervallen	Certificaten op NEN 7510:2017 geldig tot 20 februari 2027

De herziene NEN 7510 is gepubliceerd op 16 december 2024. Wie al ISO 27001:2022-gecertificeerd is, maakt de overstap naar NEN 7510:2024 relatief eenvoudig, omdat de basis al is vernieuwd.

2.2 Ook voor leveranciers van de zorg

Ook leveranciers van zorgorganisaties vallen onder NEN 7510 als zij gezondheidsgegevens beheren, zoals hostingpartijen, zorgserviceproviders en gemeenten. Voor hen is het certificaat in de praktijk vaak een voorwaarde om zaken te doen met de zorg.

3. Wet- en regelgeving: de noodzaak

De Cyberbeveiligingswet (Cbw) geldt sinds 15 augustus 2026 en vervangt de Wbni. De wet geldt voor essentiële en belangrijke entiteiten in 18 sectoren, waaronder zorg, energie, digitale infrastructuur, overheid en vervoer. Organisaties moeten zelf vaststellen of zij eronder vallen; als vuistregel geldt 50 medewerkers of € 10 miljoen omzet in een aangewezen sector.

3.1 De vier kernverplichtingen van de Cbw

1. **Registratieplicht** in het entiteitenregister van het NCSC.
2. **Zorgplicht:** passende en evenredige maatregelen om risico's voor netwerk- en informatiesystemen te beheersen.
3. **Meldplicht:** significante incidenten binnen de wettelijke termijnen melden aan CSIRT en toezichthouder.
4. **Bestuurlijke verantwoordelijkheid:** het bestuur keurt de maatregelen goed, houdt toezicht en volgt verplicht een training.

3.2 Toezicht en sancties

Categorie	Toezicht	Maximale boete
Essentiële entiteit	Proactief (audits, controles)	€ 10 miljoen of 2% van de wereldwijde jaaromzet
Belangrijke entiteit	Reactief (na incident of signaal)	€ 7 miljoen of 1,4% van de wereldwijde jaaromzet

Bron boetes: ICTRecht factsheet Cbw. Bij ernstige nalatigheid kunnen bestuurders persoonlijk aansprakelijk worden gesteld.

3.3 ISO 27001 en de Cbw

De zorgplicht volgt dezelfde logica als ISO 27001: risicoanalyse, passende maatregelen, leveranciersbeheer, incidentbeheer en continuïteit. Een ISMS dekt daarmee het grootste deel van de zorgplicht af.

> **Let op:** ISO 27001 is geen automatische vrijbrief voor de Cbw. Meldtermijnen, registratie en bestuurstraining moeten apart worden geregeld. In België geldt een ISO 27001-certificaat via CyberFundamentals als vermoeden van NIS2-conformiteit; in Nederland bestaat zo'n formele koppeling niet, maar het certificaat is wel sterk bewijs richting de toezichthouder.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

3.4 Zorg: NEN 7510 is al wettelijk verplicht

Het Besluit elektronische gegevensverwerking door zorgaanbieders verplicht zorgaanbieders te werken volgens NEN 7510, NEN 7512 en NEN 7513, steeds in de laatste uitgave. Certificering zelf is niet verplicht, maar u moet wel kunnen aantonen dat u voldoet; een certificaat is daarvoor het sterkste bewijs. De IGJ gebruikt de norm in haar toetsingskader.

3.5 Overige drijfveren

De AVG (artikel 32) eist passende beveiliging van persoonsgegevens. Ook organisaties die zelf niet onder de Cbw vallen, krijgen de eisen via hun klanten: Cbw-entiteiten moeten de risico's in hun toeleveringsketen beheersen en vragen leveranciers om aantoonbaar bewijs.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

4. De voordelen

Het grootste voordeel is niet het certificaat aan de muur, maar dat de organisatie weet waar haar risico's zitten en daar aantoonbaar op stuurt. De opbrengsten vallen in vijf groepen.

Domein	Voordeel	Wat het concreet oplevert
Commercieel	Toegang tot aanbestedingen en grote klanten	Certificaat is vaak een knock-outcriterium in tenders van overheid, zorg en corporates
Commercieel	Snellere verkoop	Klantvragenlijsten en audits van honderden vragen worden beantwoord met één certificaat en de Verklaring van Toepasselijkheid
Juridisch	Aantoonbare naleving	Sterk bewijs voor zorgplicht (Cbw), AVG artikel 32 en, in de zorg, het Besluit elektronische gegevensverwerking
Juridisch	Bescherming bestuur	Vastgelegde risicoafwegingen en managementreviews laten zien dat het bestuur zijn verantwoordelijkheid neemt
Operationeel	Minder en kleinere incidenten	Basismaatregelen (toegangsbeheer, patching, back-ups, bewustwording) worden structureel geborgd in plaats van ad hoc
Operationeel	Grip op leveranciers	Eisen aan cloud- en IT-leveranciers zijn vastgelegd en worden periodiek getoetst
Operationeel	Continuïteit	Getest incidentresponse- en uitwijkplan verkort de hersteltijd na een aanval
Financieel	Lagere schade en premie	Minder incidenten, beter onderhandelbare cyberverzekering, minder boeterisico
Organisatie	Bewustzijn en cultuur	Medewerkers weten wat er van hen verwacht wordt; beveiliging wordt onderdeel van het werk

Een jaarlijkse toets door een onafhankelijke, geaccrediteerde auditor dwingt bovendien tot onderhoud: het ISMS verslapt niet na de eerste audit. Wie ook ISO 9001 of HKZ heeft, kan de systemen integreren en audits combineren in één traject, wat moeite en kosten bespaart.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

5. Hoe komt u over als u gecertificeerd bent?

Een certificaat vertelt de buitenwereld in één oogopslag dat een onafhankelijke partij heeft vastgesteld dat uw informatiebeveiliging systematisch is ingericht. Dat verandert hoe verschillende partijen naar u kijken.

- **Klanten en patiënten** zien een organisatie die zorgvuldig met hun gegevens omgaat. In de zorg, waar medische gegevens tot de gevoeligste horen, is dat een directe vertrouwenskwestie.
- **Inkopers en aanbestedende diensten** zien een leverancier die het risico in hun keten verkleint. Onder de Cbw moeten zij hun leveranciers beoordelen; een certificaat maakt die beoordeling kort.
- **Toezichthouders** (de sectorale Cbw-toezichthouder, IGJ, Autoriteit Persoonsgegevens) zien een organisatie die aantoonbaar werk maakt van haar zorgplicht. Bij een incident is het verschil tussen "we hadden het geregeld en het is toch misgegaan" en "we hadden het niet geregeld" groot.
- **Verzekeraars en financiers** zien een beter beheersbaar risico.
- **Medewerkers en sollicitanten** zien een professionele, volwassen organisatie.

> **De keerzijde:** een certificaat schept verwachtingen. Een datalek bij een gecertificeerde organisatie trekt extra aandacht, en klanten verwachten dat u de norm echt naleeft. Daarom loont alleen een ISMS dat in de dagelijkse praktijk werkt, niet een papieren systeem voor de audit.

5.1 Communiceer het certificaat gericht

Vermeld de scope, de certificerende instelling en de RvA-accreditatie op uw website en in offertes, en bied de Verklaring van Toepasselijkheid aan op verzoek. Een certificaat zonder RvA-accreditatie wordt door professionele inkopers vaak niet geaccepteerd.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

6. Stappenplan naar certificering

Het traject bestaat uit tien stappen in vier fasen: voorbereiden, inrichten, invoeren en certificeren. De stappen zijn voor ISO 27001 en NEN 7510 gelijk; bij NEN 7510 komen de zorgspecifieke maatregelen en NEN 7512/7513 erbij. Na het certificaat volgen jaarlijkse surveillance-audits en na drie jaar een hercertificering: certificering is het begin van een cyclus, geen eindpunt.

6.1 Fase 1: voorbereiden

1. **Commitment van het bestuur.** Wijs een eigenaar aan (bijvoorbeeld een ISO/CISO), maak budget en uren vrij en leg vast waarom de organisatie certificeert.
2. **Scope bepalen.** Kies welke diensten, locaties, systemen en processen onder het ISMS vallen. Een scherpe scope die aansluit bij wat klanten vragen, verkort het traject aanzienlijk.
3. **Nulmeting (gap-analyse).** Vergelijk de huidige situatie met de eisen van de norm en de 93 (of 101) maatregelen. Dit levert de werkvoorraad op.

6.2 Fase 2: inrichten

4. **Context en risicoanalyse.** Breng belanghebbenden, informatie-assets en dreigingen in kaart en bepaal per risico de aanpak.
5. **Verklaring van Toepasselijkheid (VvT).** Leg per beheersmaatregel vast of die van toepassing is, waarom, en hoe die is ingevuld.
6. **Beleid en documentatie.** Informatiebeveiligingsbeleid, rollen, procedures en registraties. Houd het compact en werkbaar.

6.3 Fase 3: invoeren

7. **Maatregelen implementeren.** Technisch (MFA, patching, logging, back-ups), organisatorisch (leveranciersbeheer, incidentproces) en menselijk (bewustwordingstraining).
8. **Laten draaien en bewijs opbouwen.** Het systeem moet doorgaans 2 tot 3 maanden aantoonbaar werken voordat de auditor komt.
9. **Interne audit en directiebeoordeling.** Toets het ISMS zelf, los bevindingen op en laat het bestuur formeel de werking beoordelen.

6.4 Fase 4: certificeren

10. **Externe audit door een RvA-geaccrediteerde instelling.** De fase 1-audit toetst de documentatie en gereedheid; de fase 2-audit toetst de werking in de praktijk. Na een positief oordeel ontvangt u het certificaat, drie jaar geldig.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

7. Doorlooptijd: wat is realistisch?

De meeste organisaties zijn in 6 tot 12 maanden gecertificeerd; met een sterke bestaande basis kan het in 3 tot 6 maanden. De bepalende factoren zijn de omvang van de scope, de beschikbare interne capaciteit en de beginsituatie, niet de norm zelf.



Figuur 1. Een typisch certificeringstraject in vier fasen. De invoerfase duurt het langst, omdat de auditor wil zien dat maatregelen een aantal maanden aantoonbaar werken.

7.1 Doorlooptijd per situatie

Situatie	Realistische doorlooptijd	Kanttekening
Klein (< 50 mw), beperkte scope, basis op orde	3–6 maanden	Alleen haalbaar met een vaste trekker en snelle besluitvorming
Mkb (50–250 mw), gemiddelde volwassenheid	6–12 maanden	Meest voorkomende situatie
Groot of complex (meerdere locaties, veel systemen)	12 maanden of langer	Vaak gefaseerd: eerst kernscope, daarna uitbreiden
Al ISO 27001:2022, uitbreiding naar NEN 7510	Enkele maanden	Alleen zorgspecifieke maatregelen en NEN 7512/7513 toevoegen

> **Let op:** "in 8 weken gecertificeerd" is voor vrijwel geen organisatie realistisch. Een te kort traject leidt tot een papieren systeem en afwijkingen bij de fase 2-audit. Houd ook rekening met de wachttijd bij certificatie-instellingen; vraag de planning voor de fase 2-audit vroeg op.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

8. Kosten en inspanning

Voor een mkb-organisatie liggen de totale kosten in het eerste jaar doorgaans tussen € 20.000 en € 80.000. De grootste post wordt vaak onderschat: interne uren zijn 50 tot 70% van de totale kosten.

Kostenpost	Indicatie (mkb)	Toelichting
Interne uren	Grootste post (50–70%)	Eigenaar ISMS, procesverantwoordelijken, IT, management
Externe begeleiding (optioneel)	€ 30.000–€ 80.000 bij volledige begeleiding	Minder bij alleen nulmeting, templates of coaching
Certificatie-audit (fase 1 + 2)	€ 8.000–€ 25.000	Afhankelijk van aantal medewerkers, locaties en complexiteit IT
Technische maatregelen	Sterk wisselend	MFA, logging/SIEM, back-up, endpointbeveiliging; vaak al deels aanwezig
Normdocumenten en tooling	Enkele honderden tot enkele duizenden euro's per jaar	Normen via NEN; ISMS-software optioneel
Jaarlijkse surveillance-audit	Circa een derde tot de helft van de initiële audit	Jaar 2 en 3

Auditprijzen: Orbiq; de auditduur hangt af van organisatieomvang en IT-complexiteit. Vraag altijd twee tot drie offertes op bij RvA-geaccrediteerde instellingen.

Bedragen zijn indicaties uit marktbronnen, geen offerte. Wie al ISO 9001 heeft, bespaart op de managementsysteemkant; wie zowel ISO 27001 als NEN 7510 wil, betaalt meestal één gecombineerde audit met beperkte meerprijs.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

9. Valkuilen en succesfactoren

De meeste trajecten lopen niet vast op techniek, maar op eigenaarschap, scope en tijd.

Valkuil	Gevolg	Succesfactor
Het wordt "een IT-project"	Geen draagvlak, beleid sluit niet aan op de praktijk	Bestuur is eigenaar, IT is uitvoerder; beveiliging hoort bij de bedrijfsvoering
Scope te breed	Traject duurt maanden langer en kost meer	Begin bij de dienst of omgeving die klanten vragen; breid later uit
Papieren tijger	Documenten zonder werking; auditor vindt afwijkingen in fase 2	Weinig, korte documenten die mensen echt gebruiken
Risicoanalyse als formulier	Maatregelen die niet passen bij de werkelijke risico's	Risico's samen met de business bepalen, niet alleen met IT
Leveranciers vergeten	Grootste risico's zitten vaak bij cloud- en IT-partners	Leveranciersregister, contracteisen en periodieke toetsing
Te weinig tijd tussen invoeren en audit	Onvoldoende bewijs van werking	Reken op 2–3 maanden draaien vóór de fase 2-audit
Na certificaat stilvallen	Afwijkingen bij surveillance-audit, certificaat in gevaar	Vaste jaarkalender: risicoreview, interne audit, directiebeoordeling, oefening
Bewustwording als eenmalige e-learning	Phishing blijft de belangrijkste ingang	Doorlopend programma met korte sessies en phishingsimulaties

> **Vuistregel:** ontwerp het ISMS zo dat het ook zonder auditor waarde heeft. Dan is de audit een bevestiging in plaats van een examen.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

10. Keuzehulp: ISO 27001, NEN 7510 of beide?

De keuze volgt uit twee vragen: verwerkt u gezondheidsgegevens, en werkt u buiten de Nederlandse zorg? Wie beide met ja beantwoordt, kiest voor een gecombineerd traject.

Uw situatie	Advies	Waarom
Zorgaanbieder (ziekenhuis, GGZ, VVT, huisarts, apotheek)	NEN 7510	Wettelijk verplicht te voldoen; IGJ toetst erop
IT-, hosting- of softwareleverancier alleen voor de zorg	NEN 7510	Zorgklanten vragen erom; dekt zorgspecifieke eisen
Leverancier voor zorg én andere sectoren of internationaal	ISO 27001 + NEN 7510	Eén ISMS, één gecombineerde audit, beide markten bediend
Organisatie onder de Cbw, buiten de zorg	ISO 27001	Dekt het grootste deel van de zorgplicht, internationaal erkend
Leverancier van Cbw-organisaties	ISO 27001	Klanten moeten hun keten beoordelen; het certificaat maakt dat eenvoudig
Organisatie die veel persoonsgegevens verwerkt	ISO 27001, eventueel met ISO 27701	ISO 27701 breidt het ISMS uit met privacymanagement (AVG)

10.1 Combineren met andere systemen

ISO 27001 en NEN 7510 delen de hoofdstructuur met ISO 9001 (kwaliteit) en ISO 27701 (privacy). Eén geïntegreerd managementsysteem met gezamenlijke risicoanalyse, interne audits en directiebeoordeling voorkomt dubbel werk. In de zorg is de combinatie met HKZ of ISO 9001 gebruikelijk.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

11. Conclusie en aanbevelingen

ISO 27001 en NEN 7510 zijn in 2026 geen luxe meer: de Cyberbeveiligingswet legt de zorgplicht bij het bestuur, zorgaanbieders zijn al wettelijk aan NEN 7510 gebonden, en klanten eisen aantoonbaar bewijs van hun leveranciers.

Een gecertificeerd ISMS beantwoordt al die vragen tegelijk en maakt de organisatie aantoonbaar weerbaarder. Begin klein en scherp, en bouw van daaruit verder.

Checklist: aanbevolen eerste stappen

Actie	Ja	Actie nodig
Stel vast of u onder de Cbw valt (essentieel of belangrijk) en registreer zo nodig bij het NCSC	☐	☐
Inventariseer welke norm uw klanten en aanbestedingen vragen	☐	☐
Wijs een bestuurlijk eigenaar en een ISMS-verantwoordelijke aan	☐	☐
Laat bestuurders de verplichte Cbw-training volgen	☐	☐
Bepaal een scherpe scope en voer een nulmeting uit	☐	☐
Plan de certificatie-audit tijdig in; auditcapaciteit is krap	☐	☐
NEN 7510-certificaathouders: plan de transitie-audit naar NEN 7510-1:2024 vóór 20 februari 2027	☐	☐

Bronnen

[1] Rijksoverheid: Cyberbeveiligingswet en Wwke van kracht (15 augustus 2026)
[2] NJB: Cyberbeveiligingsbesluit, Stb. 2026, 189
[3] ICTRecht: factsheet NIS2 / Cyberbeveiligingswet
[4] ICTRecht: factsheet NEN 7510:2024
[5] Staatsblad 2017, 446: Besluit elektronische gegevensverwerking door zorgaanbieders
[6] Kiwa: herziene NEN 7510 gepubliceerd
[7] Kiwa: NEN 7510 for healthcare sector information security updated
[8] Brand Compliance: overgang naar NEN 7510-1:2024
[9] DEKRA: accreditatie NEN 7510-1:2024 en HKZ
[10] ActiZ: videocollege informatieveiligheid, bijlage 1A
[11] Brand Compliance: ISO 27001 en NIS2 (CyberFundamentals)
[12] ManageEngine: NIS2 (Cyberbeveiligingswet) vs ISO 27001
[13] Security Management: Cybersecuritybeeld Nederland 2025

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

VeeHa B.V.
Cybersecurity and privacy

[14] Dutch IT Channel: NCTV themarapport cyberdreigingen (oktober 2026)

[15] Accountancy Vanmorgen: CBS Cybersecuritymonitor 2025

[16] Orbiq: ISO 27001-certificering in 6 stappen

[17] Orbiq: kosten ISO 27001-certificering

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

VeeHa B.V.
Cybersecurity and privacy

Over VeeHa

VeeHa B.V. ondersteunt organisaties bij informatiebeveiliging, privacy en werkbare managementsystemen. De aanpak sluit aan op wat binnen de organisatie al aanwezig is. Wat goed werkt, blijft behouden. Beleid, risico's, planning, bewijs en verbeteracties worden zoveel mogelijk ingericht in bestaande omgevingen zoals Microsoft 365, SharePoint, Teams, Planner, Jira en Confluence.

De dienstverlening omvat consultancy, implementatie, gap-analyses en interne audits voor onder meer ISO 27001, NEN 7510, ISO 9001, ISO 27701, AVG, BIO en NIS2. De nadruk ligt op een aantoonbare balans tussen norm, risico en dagelijkse praktijk.

Meer weten of sparren over de eigen situatie? Neem contact op via info@veeha.nl of +31 6 125 749 24, of kijk op www.veeha.nl.

Deze whitepaper is algemene informatie en geen juridisch advies voor een concrete situatie. Wetgeving, norminterpretaties en bedragen kunnen wijzigen; toets altijd de actuele tekst en uw eigen situatie.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618