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 10 - 2026 Jan Willem van Hoorn

Leveranciersmanagement onder ISO/IEC 27001:2022

Kritische leveranciers beoordelen en een werkende exitstrategie voor uw data in de cloud

U kunt uw informatiebeveiliging uitbesteden, maar niet de verantwoordelijkheid ervoor.

Dat is de kern van leveranciersmanagement onder ISO/IEC 27001:2022. Wanneer uw klantdata, financiële administratie of bedrijfskritische processen bij een cloudleverancier draaien, is het beveiligingsniveau van die leverancier feitelijk uw beveiligingsniveau.

Deze whitepaper beschrijft wat de norm vraagt, hoe u kritische leveranciers beoordeelt en hoe u een exitstrategie opstelt die werkt op het moment dat het nodig is.

VeeHa B.V.

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

Managementsamenvatting

De norm vraagt in Annex A vijf samenhangende beheersmaatregelen (5.19 tot en met 5.23) voor leveranciers, waarvan 5.23 over clouddiensten in 2022 nieuw is toegevoegd. Wie deze maatregelen serieus invult, doet drie dingen goed:

1. **Weten wie kritisch is.** Niet elke leverancier verdient dezelfde aandacht. Een risicogebaseerde classificatie bepaalt waar u tijd en geld in steekt.
2. **Kritische leveranciers aantoonbaar beoordelen.** Vóór het contract, tijdens de looptijd en bij wijzigingen, met objectief bewijs zoals ISO 27001-certificaten (inclusief scope), ISAE 3402/SOC 2-rapporten en pentestresultaten.
3. **Een geteste exitstrategie hebben.** Voor elke kritische clouddienst ligt vast hoe u uw data in een bruikbaar formaat terugkrijgt, binnen welke termijn, tegen welke kosten en hoe de leverancier aantoonbaar verwijdert wat achterblijft.

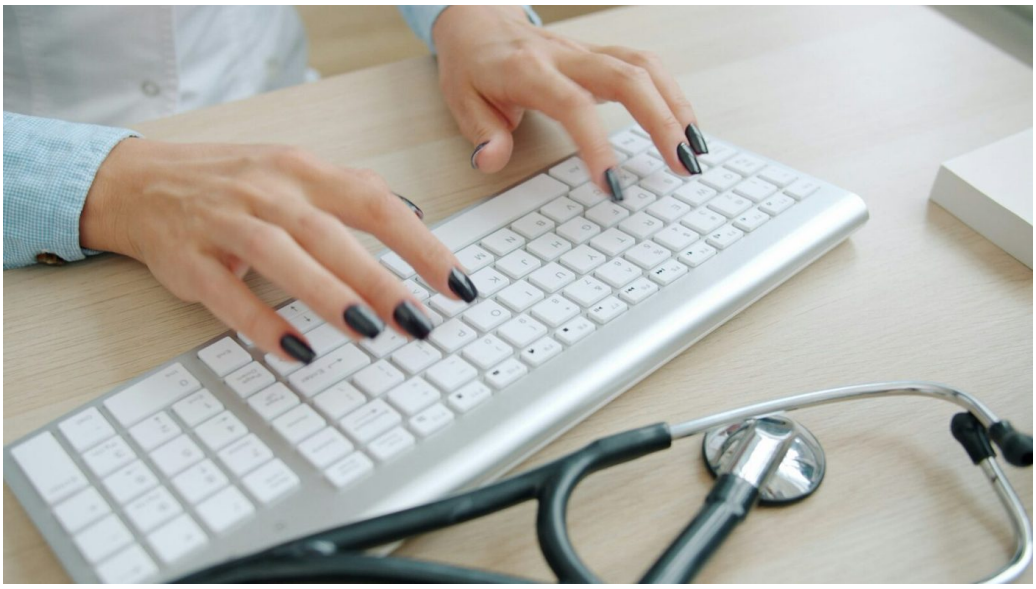
Vooral het derde punt ontbreekt in de praktijk vaak. Organisaties merken pas bij een faillissement, overname, prijsverhoging of datalek dat hun gegevens vastzitten in een eigen formaat, zonder afspraken over teruggave.

> De prijs van tekortschietend leveranciersmanagement is hoog: datalekken via leveranciers, stilstand van kernprocessen, verlies van data, boetes onder de AVG en de Cyberbeveiligingswet, persoonlijke aansprakelijkheid van bestuurders en verlies van klanten die aantoonbare ketenbeveiliging eisen. Paragraaf 1.3 zet deze risico's op een rij.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

1. Inleiding: de risico's van uitbesteden

Vrijwel geen organisatie werkt nog zonder externe leveranciers. Klantgegevens staan in een CRM in de cloud, de salarisadministratie draait bij een gespecialiseerde partij en een managed serviceprovider beheert de werkplekken. Dat levert schaalvoordelen en expertise op, maar het verplaatst ook een groot deel van uw informatie en uw processen naar een omgeving waar u zelf geen directe controle over heeft.



Of het nu om patiëntdossiers, klantgegevens of de financiële administratie gaat: de informatie staat steeds vaker bij een leverancier.

Daarmee verschuift ook het risico. Uw beveiliging is zo sterk als de zwakste schakel in de keten, en die schakel zit steeds vaker bij een leverancier, of bij de leverancier van uw leverancier. Recente incidenten laten zien hoe dat uitpakt:

- **Kaseya (2021):** via beheersoftware van één IT-dienstverlener werden honderden klanten tegelijk getroffen door ransomware.
- **MOVEit (2023):** een kwetsbaarheid in bestandsoverdrachtsoftware leidde tot datalekken bij een groot aantal organisaties, ook bij organisaties die de software zelf niet gebruikten, maar hun leveranciers wel.
- **CrowdStrike (2024):** een foutieve update van een beveiligingsleverancier legde wereldwijd miljoenen Windows-systemen plat, zonder dat er sprake was van een aanval.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

VeeHa B.V.
Cybersecurity and privacy

1.1 De belangrijkste leveranciersrisico's

Leveranciersrisico's gaan verder dan hacks. Ze raken alle drie de pijlers van informatiebeveiliging (vertrouwelijkheid, integriteit en beschikbaarheid) en daarnaast uw wettelijke positie en uw vrijheid om te kiezen.

Risico	Hoe het zich voordoet	Mogelijk gevolg voor u
Datalek bij de leverancier	Inbraak, configuratiefout of misbruik door een medewerker van de leverancier	Meldplicht bij de Autoriteit Persoonsgegevens, schadeclaims, reputatieschade
Leverancier als toegangspoort	Aanvallers misbruiken de beheertoegang of koppeling die een leverancier tot uw systemen heeft	Ransomware of spionage in uw eigen netwerk
Gecompromitteerde software of updates	Kwaadaardige code of fouten in software die u van de leverancier ontvangt (supply-chainaanval)	Aantasting van de integriteit van systemen en data
Uitval en storingen	Technische storing, cyberaanval of fout bij de leverancier	Kernprocessen liggen stil; RTO en RPO worden niet gehaald
Ketenrisico (onderaannemers)	De leverancier besteedt zelf uit aan partijen die u niet kent of niet heeft beoordeeld	Data bij onbekende partijen en op onbekende locaties
Continuïteit van de leverancier	Faillissement, overname, stopzetten van een dienst	Abrupt einde van de dienst, data mogelijk niet meer bereikbaar
Vendor lock-in	Data in een eigen formaat, geen goede exportfunctie, hoge overstapkosten	Geen realistische uitweg; afhankelijkheid van prijs en voorwaarden van de leverancier
Jurisdictie en privacy	Opslag of beheer buiten de EER, buitenlandse wetgeving die toegang tot data kan afdwingen	Strijdigheid met de AVG, verlies van controle over gevoelige informatie
Eenzijdige wijzigingen	De leverancier wijzigt functionaliteit, voorwaarden, datalocatie of prijs	Het risicoprofiel verandert zonder dat u dat merkt
Schaduw-IT	Afdelingen sluiten zelf clouddiensten af, buiten IT en inkoop om	Bedrijfsdata bij leveranciers die nooit zijn beoordeeld

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618



Figuur 1. De leveranciersrisico's uit de tabel, gegroepeerd naar wat er wordt aangetast.

1.2 Waarom dit uw verantwoordelijkheid blijft

U kunt de uitvoering uitbesteden, maar niet de verantwoordelijkheid. Bij een datalek bij een verwerker blijft u als verwerkingsverantwoordelijke aanspreekbaar onder de AVG. Onder de Cyberbeveiligingswet is het bestuur zelf verantwoordelijk voor de beveiliging van de toeleveringsketen. En voor uw klanten maakt het niet uit of de storing bij u of bij uw leverancier ontstond.

Vooral twee risico's worden in de praktijk onderschat. Het eerste is dat een leverancier die bij de selectie goed scoorde, jaren later een ander bedrijf is geworden. Het tweede is lock-in: data die jarenlang in een SaaS-omgeving is opgebouwd, blijkt zonder voorbereiding lastig, duur of onvolledig terug te halen. Dat merkt u pas op het moment dat u weg wilt of weg moet.

ISO/IEC 27001:2022 erkent deze risico's expliciet en behandelt leveranciers als integraal onderdeel van het managementsysteem voor informatiebeveiliging (ISMS). De rest van deze whitepaper laat zien hoe u ze beheerst: door kritische leveranciers te herkennen, ze aantoonbaar te beoordelen en te volgen, en door voor uw data in de cloud een werkende exitstrategie te hebben.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

1.3 Wat er op het spel staat als het niet op orde is

Leveranciersmanagement dat half is ingericht voelt veilig, maar is het niet. Een leverancierslijst zonder classificatie, een certificaat dat niemand heeft gelezen of een contract zonder exitafspraken geeft schijnzekerheid. De gevolgen worden pas zichtbaar als het misgaat, en dan is het te laat om ze te herstellen.

Wat ontbreekt	Wat er dan gebeurt	Gevolg voor uw organisatie
Geen zicht op kritische leveranciers	Aandacht gaat naar de verkeerde partijen; schaduw-IT blijft buiten beeld	Bedrijfskritische data staat bij leveranciers die nooit zijn beoordeeld
Geen of oppervlakkige beoordeling	Een certificaat blijkt de afgenomen dienst niet te dekken; zwakke plekken worden niet ontdekt	Een datalek of aanval via de leverancier die voorkomen had kunnen worden
Zwakke contracten	Geen meldplicht, geen auditrecht, geen afspraken over onderaannemers of verwijdering	Bij een incident hoort u het te laat of niet; u kunt niets afdwingen
Geen exitstrategie	Data zit vast in een eigen formaat, zonder afspraken over teruggave	Bij faillissement of conflict raakt u data kwijt of betaalt u de hoofdprijs om weg te komen

De gevolgen raken de hele organisatie:

- **Financieel.** Boetes onder de AVG en de Cyberbeveiligingswet (zie paragraaf 7.1), schadeclaims van klanten, kosten voor incidentherstel en onverwachte migratiekosten.
- **Bestuurlijk en juridisch.** Onder de Cyberbeveiligingswet kunnen bestuurders persoonlijk worden aangesproken. Als verwerkingsverantwoordelijke blijft u onder de AVG aanspreekbaar voor fouten van uw verwerker.
- **Operationeel.** Kernprocessen liggen stil zolang de leverancier niet levert, en zonder eigen kopie van de data is er geen terugvalpositie.
- **Certificering.** Een auditor die vaststelt dat maatregelen 5.19 tot en met 5.23 niet werken, kan een grote afwijking (major non-conformity) uitschrijven. Wordt die niet tijdig opgelost, dan kan het certificaat worden geschorst of ingetrokken.
- **Commercieel en reputatie.** Klanten die zelf onder de Cbw of DORA vallen, eisen aantoonbaar leveranciersmanagement. Wie dat niet kan laten zien, verliest opdrachten en aanbestedingen. Een datalek via een leverancier wordt door klanten en media gewoon aan u toegerekend.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

> **Een herkenbaar scenario.** Een organisatie gebruikt al zeven jaar een SaaS-pakket voor haar klantadministratie. Er is geen exitplan en nooit een volledige export gemaakt. Op een maandagochtend blijkt de leverancier failliet; de dienst gaat binnen enkele dagen uit de lucht. Er is geen bruikbare kopie van de data, de curator heeft andere prioriteiten en de bewaarplicht voor klantgegevens loopt gewoon door. Tegelijk moet de organisatie beoordelen of er sprake is van een meldplichtig incident. Wat met een jaarlijkse exporttest en een paar contractbepalingen te voorkomen was geweest, wordt nu een crisis van weken.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

2. Wat ISO/IEC 27001:2022 vraagt

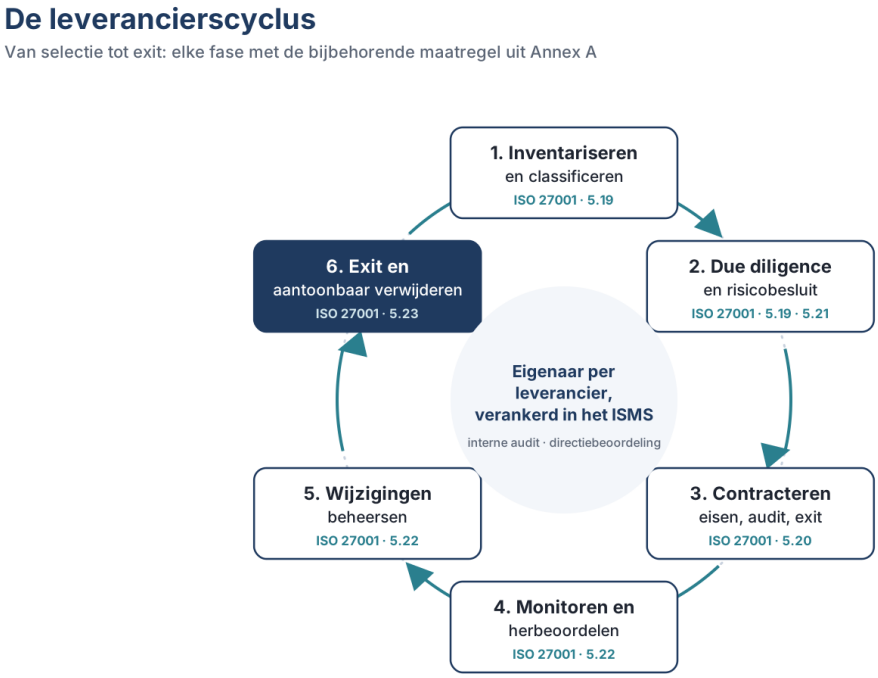
De norm verankert leveranciersmanagement op twee niveaus. In de hoofdtekst eist clausule 8.1 dat extern geleverde processen, producten en diensten die relevant zijn voor het ISMS beheerst worden. In Annex A staan vijf specifieke beheersmaatregelen, uitgewerkt in de richtlijn ISO/IEC 27002:2022.

Maatregel	Onderwerp	Wat u moet kunnen aantonen
5.19	Informatiebeveiliging in leveranciersrelaties	Een vastgesteld proces en beleid voor het beheersen van risico's rond leveranciers, inclusief classificatie
5.20	Informatiebeveiliging in leveranciersovereenkomsten	Contracten met concrete beveiligingseisen, afgestemd op het type leverancier
5.21	Informatiebeveiliging in de ICT-toeleveringsketen	Zicht op en eisen aan onderaannemers (de leverancier van uw leverancier)
5.22	Monitoren, beoordelen en wijzigingsbeheer van leveranciersdiensten	Periodieke beoordeling van prestaties en beveiliging, en beheersing van wijzigingen
5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Processen voor aanschaf, gebruik, beheer en beëindiging van clouddiensten

Leveranciersmanagement raakt ook aan andere maatregelen: 5.14 (informatieoverdracht), 5.30 (ICT-gereedheid voor bedrijfscontinuïteit), 5.31 (wettelijke en contractuele eisen), 5.34 (privacy en persoonsgegevens), 8.10 (verwijderen van informatie) en 8.13 (back-up). Een goede invulling verbindt deze maatregelen in één samenhangend proces in plaats van losse documenten.

> **Let op:** de Verklaring van Toepasselijkheid (VvT/SoA) moet per maatregel motiveren of en hoe deze is geïmplementeerd. Wie clouddiensten gebruikt, kan 5.23 vrijwel nooit uitsluiten.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618



Figuur 2. De leverancierscyclus: elke fase met de bijbehorende maatregel uit Annex A.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

3. Kritische leveranciers identificeren en classificeren

Een leverancier is kritisch wanneer uitval, een datalek of het einde van de relatie direct de vertrouwelijkheid, integriteit of beschikbaarheid van uw kernprocessen raakt. Begin daarom niet bij de leverancierslijst van inkoop, maar bij uw eigen processen en informatie.

Stap 1: inventariseer. Breng alle leveranciers in beeld die informatie verwerken, opslaan of toegang hebben tot uw systemen. Vergeet de schaduw-IT niet: SaaS-abonnementen die afdelingen zelf hebben afgesloten met een creditcard.

Stap 2: beoordeel per leverancier vijf vragen.

1. Welke informatie verwerkt de leverancier, en hoe gevoelig is die (classificatie, persoonsgegevens, bijzondere persoonsgegevens)?
2. Welke processen stoppen als de dienst een dag, een week of definitief uitvalt?
3. Heeft de leverancier toegang tot uw netwerk, systemen of beheeromgevingen?
4. Hoe makkelijk is de leverancier te vervangen, en hoeveel data zit er in hun omgeving?
5. Gelden er wettelijke of contractuele eisen (AVG, sectorale regelgeving, klanteisen)?



Stap 3: deel in. Een indeling in drie niveaus is in de praktijk goed werkbaar.

Niveau	Kenmerken	Voorbeelden	Beoordelingsdiepgang
Kritisch	Verwerkt vertrouwelijke of bedrijfskritische data, kernproces stopt bij uitval, moeilijk vervangbaar	ERP- of CRM-platform in de cloud, hostingpartij, managed service provider, salarisadministratie	Volledige due diligence, jaarlijkse herbeoordeling, getest exitplan
Belangrijk	Verwerkt interne data of ondersteunt belangrijke processen, vervangbaar binnen weken	Projectmanagementtool, e-mailmarketingplatform	Vragenlijst plus certificaat, herbeoordeling elke twee jaar, exitplan op hoofdlijnen

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

Niveau	Kenmerken	Voorbeelden	Beoordelingsdiepgang
Standaard	Geen of openbare data, eenvoudig vervangbaar	Kantoorartikelen, openbare informatiediensten	Standaard inkoopvoorwaarden



Figuur 3. Risicomatrix: de combinatie van impact en afhankelijkheid bepaalt of een leverancier standaard, belangrijk of kritisch is. De voorbeelden zijn indicatief.

Leg de classificatie vast in een leveranciersregister met per leverancier een eigenaar binnen uw organisatie. Herzie de indeling bij elke significante wijziging, zoals een nieuwe module, meer data of een overname van de leverancier.

> **Risico als dit ontbreekt:** zonder classificatie krijgt elke leverancier evenveel (en dus te weinig) aandacht. De partij die uw klantdata beheert, wordt dan net zo licht beoordeeld als de leverancier van kantoorartikelen, en clouddiensten die afdelingen zelf hebben afgesloten blijven volledig buiten beeld.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

4. Kritische leveranciers goed beoordelen

Een goede beoordeling steunt op bewijs, niet op beloftes. Een ingevulde vragenlijst met alleen ‘ja’ zegt weinig; een certificaat zonder passende scope evenmin. De beoordeling bestaat uit drie onderdelen: due diligence vooraf, contractuele borging en een besluit over het restrisico.

4.1 Due diligence vooraf



Vraag en beoordeel voor kritische leveranciers ten minste:

- **ISO/IEC 27001-certificaat.** Controleer de geldigheid, de certificerende instelling (geaccrediteerd?) en vooral de **scope**: valt de dienst die u afneemt, inclusief de betrokken locaties en datacenters, er echt onder? Vraag ook de Verklaring van Toepasselijkheid op.
- **Assurancerapportages.** Een ISAE 3402 type II of SOC 2 type II-rapport laat zien dat maatregelen gedurende een periode daadwerkelijk werkten. Lees de afwijkingen en de *complementary user entity controls*: de maatregelen die ú moet nemen.
- **Cloudspecifieke normen.** Voor clouddiensten zijn ISO/IEC 27017 (cloudbeveiliging) en ISO/IEC 27018 (persoonsgegevens in de publieke cloud) relevante aanvullingen.
- **Technische toetsing.** Recente penetratietestresultaten (samenvatting), het kwetsbaarheidsbeheerproces en de aanpak voor versleuteling en sleutelbeheer.
- **Locatie en jurisdictie.** Waar staat de data, waar zit de supportorganisatie en onder welk recht valt de leverancier? Dit is relevant voor de AVG en voor buitenlandse wetgeving die toegang tot data kan afdwingen.
- **Onderaannemers.** Welke subverwerkers en hostingpartijen gebruikt de leverancier, en hoe worden wijzigingen daarin aan u gemeld?

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

- **Continuïteit en financiële gezondheid.** Kredietwaardigheid, eigendomsstructuur, afhankelijkheid van investeerders, en het bedrijfscontinuïteitsplan inclusief testresultaten.
- **Incidentrespons.** Hoe snel en via wie meldt de leverancier een beveiligingsincident, en wat is hun staat van dienst?

4.2 Contractuele borging (maatregel 5.20)

Wat niet in het contract staat, is achteraf niet af te dwingen. Leg voor kritische leveranciers minimaal vast:

Onderwerp	Minimale afspraak
Beveiligingseisen	Verwijzing naar concrete eisen of normen, plus de verplichting die te handhaven gedurende de looptijd
Incidentmelding	Meldtermijn in uren (bijvoorbeeld binnen 24 uur), contactpersonen en informatieplicht
Auditrecht	Recht op eigen audit of op onafhankelijke rapportages, met jaarlijkse aanlevering
Onderaannemers	Voorafgaande melding van nieuwe onderaannemers en recht van bezwaar; doorlegging van dezelfde eisen
Verwerkersovereenkomst	Bij persoonsgegevens verplicht onder artikel 28 AVG
Beschikbaarheid	SLA met meetbare beschikbaarheid, hersteltijden (RTO) en maximaal dataverlies (RPO)
Exit	Teruggave van data, formaat, termijn, kosten, ondersteuning en aantoonbare verwijdering (zie hoofdstuk 6)
Wijzigingen	Melding vooraf van wijzigingen in dienst, locatie of eigendom



Leg beveiligings-, audit- en exitafspraken vast vóór de handtekening; daarna is uw onderhandelingspositie veel kleiner.

Bij grote cloudleveranciers zijn de voorwaarden vaak niet onderhandelbaar. Beoordeel dan of hun standaardvoorwaarden en documentatie uw eisen afdekken, en leg de restrisico's vast.

4.3 Besluit over het restrisico

De beoordeling eindigt met een expliciet besluit: accepteren, aanvullende maatregelen eisen of nemen, of afzien van de leverancier. Leg vast wie het restrisico accepteert. Bij kritische leveranciers hoort dat de risico-eigenaar op managementniveau te zijn, niet alleen de inkoper of IT-beheerder.

> **Risico als dit ontbreekt:** een beoordeling die alleen bestaat uit het opvragen van een certificaat mist de vragen die ertoe doen. Valt de dienst binnen de scope? Welke afwijkingen staan in het auditrapport? Welke maatregelen moet u zelf nemen? Zonder contractuele borging hebt u na een incident geen meldtermijn, geen auditrecht en geen hefboom om verbetering af te dwingen. En zonder expliciet besluit over het restrisico draagt uiteindelijk niemand het, totdat het bestuur er alsnog op wordt aangesproken.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

5. Monitoren en herbeoordelen tijdens de looptijd

Een leverancier die bij contractering goed scoorde, kan drie jaar later een ander bedrijf zijn. Maatregel 5.22 vraagt daarom om doorlopende monitoring en beheerste wijzigingen.

- **Periodieke herbeoordeling.** Kritische leveranciers minstens jaarlijks: nieuw certificaat of auditrapport opvragen, afwijkingen beoordelen en de classificatie herzien.
- **Serviceoverleg.** Bespreek SLA-rapportages, incidenten, wijzigingen en openstaande verbeterpunten in een vast overleg, met verslaglegging.
- **Signalen van buitenaf.** Volg nieuws over overnames, datalekken, kwetsbaarheden in de producten van de leverancier en financiële problemen.
- **Wijzigingsbeheer.** Nieuwe functionaliteit, een nieuwe onderaannemer of een andere datalocatie kan het risicoprofiel veranderen. Laat wijzigingen langs dezelfde beoordeling lopen.
- **Toegangsbeheer.** Controleer periodiek welke medewerkers van de leverancier toegang hebben tot uw omgevingen en trek die in als die niet meer nodig is.
- **Tekortkomingen opvolgen.** Registreer bevindingen als risico's of verbeteracties in het ISMS, met een eigenaar en een termijn.

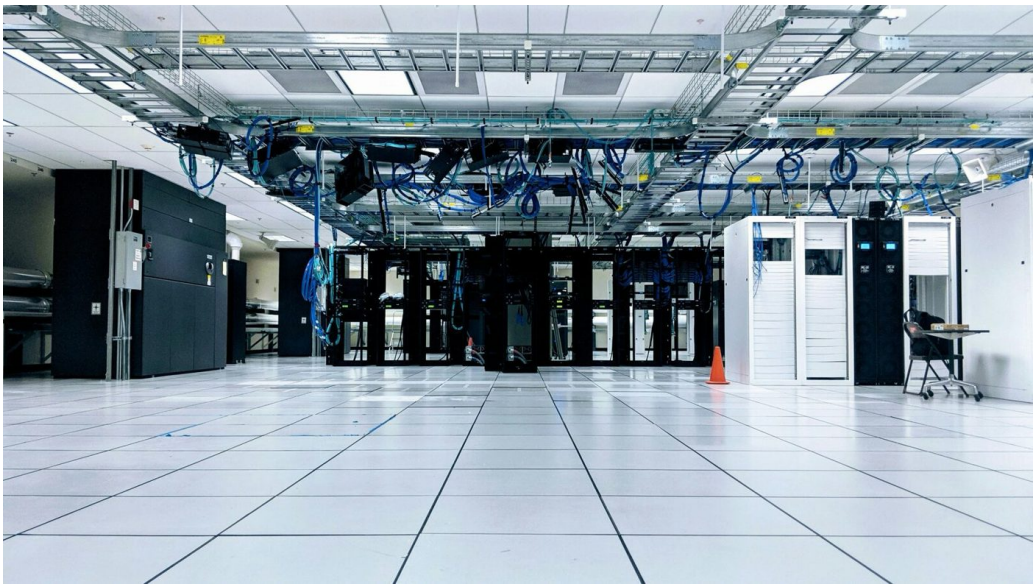
Maak de leveranciersbeoordeling onderdeel van de interne audit en de directiebeoordeling. Zo blijft leveranciersmanagement geen eenmalige inkoopactiviteit, maar een vast onderdeel van de Plan-Do-Check-Act-cyclus.

> **Risico als dit ontbreekt:** een eenmalige beoordeling veroudert snel. Een overname door een partij buiten de EU, een nieuwe onderaannemer, een verlopen certificaat of een structureel probleem in de dienstverlening verandert uw risico, zonder dat iemand het opmerkt of accepteert. Bij een audit of incident blijkt dan dat de laatste beoordeling jaren oud is.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

6. De exitstrategie voor uw data in de cloud

Een exitstrategie beantwoordt één vraag: kunt u, als de relatie morgen eindigt, uw informatie volledig, bruikbaar en op tijd terugkrijgen, en weet u zeker dat er niets achterblijft? De beste plek om dat te regelen is vóór de handtekening. Na een faillissement of conflict is uw onderhandelingspositie verdwenen.



Uw data staat fysiek in het datacenter van een ander. Een exitstrategie bepaalt of u die data ook weer terugkrijgt.

6.1 Waarom een exit plaatsvindt

Plan niet alleen voor de nette, geplande overstap. De lastigste scenario's zijn de onverwachte:

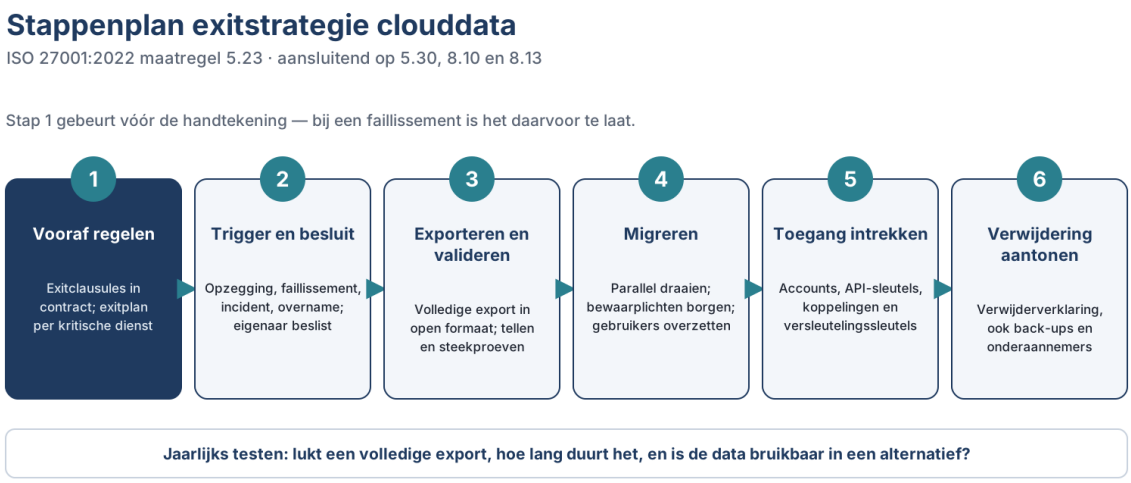
- **Gepland:** contract loopt af, betere alternatieven, strategische keuze voor een ander platform.
- **Gedwongen door de leverancier:** faillissement, overname, stopzetten van de dienst, forse prijsverhoging of eenzijdige wijziging van voorwaarden.
- **Gedwongen door risico:** ernstig of herhaald datalek, structureel slechte prestaties, verlies van certificering.
- **Gedwongen door wetgeving:** gewijzigde regels rond doorgifte buiten de EU, of nieuwe sectorale eisen.

6.2 De onderdelen van een exitplan

Stel voor elke kritische clouddienst een exitplan op met ten minste deze elementen:

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

Onderdeel	Vragen die het plan beantwoordt
Data-inventaris	Welke data staat er (inclusief metadata, logbestanden, bijlagen, audit trails, configuraties en historie)? Wat is de omvang?
Formaat	In welk open, gangbaar en machineleesbaar formaat krijgt u de data (bijvoorbeeld CSV, JSON, XML, SQL-dump)? Blijven relaties tussen gegevens behouden?
Methode	Via export in de applicatie, API of bulkoverdracht? Is die methode getest en gedocumenteerd?
Termijnen	Opzegtermijn, overgangsperiode, periode waarin data nog op te halen is
Verwijdering	Hoe en wanneer verwijdert de leverancier alle kopieën, ook in back-ups en bij onderaannemers? Welk bewijs krijgt u (verwijderverklaring)?
Toegang en sleutels	Intrekken van accounts, API-sleutels, koppelingen en federatie; teruggave of vernietiging van versleutelingssleutels
Alternatief	Welke vervangende oplossing of noodvoorziening is er, en hoelang duurt het om die in gebruik te nemen?
Bewaarplichten	Welke data moet u wettelijk bewaren (fiscaal, archiefwet, sectoraal) en waar blijft die na de exit?
Rollen	Wie besluit tot een exit, wie voert hem uit, wie communiceert met klanten en toezichthouders?



Figuur 4. De exit in zes stappen. Stap 1 moet geregeld zijn vóór de handtekening.

6.3 Verminder afhankelijkheid tijdens de looptijd

Een exitplan op papier helpt weinig als de data in de praktijk niet los te krijgen is. Neem daarom maatregelen die al tijdens het gebruik werken:

- **Eigen periodieke export.** Maak voor kritische SaaS-diensten regelmatig een volledige export naar een omgeving onder eigen beheer. Dit is ook uw vangnet bij een plotseling faillissement (koppeling met maatregel 8.13, back-up).
- **Eigen sleutelbeheer.** Waar mogelijk *bring your own key* of *hold your own key*, zodat u controle houdt over de toegang tot versleutelde data.
- **Open standaarden.** Geef bij selectie de voorkeur aan diensten met open exportformaten en gedocumenteerde API's.
- **Escrow.** Voor maatwerk- of nichesoftware kan een escrowregeling voor broncode en data de continuïteit borgen bij faillissement.
- **Architectuur.** Vermijd onnodig gebruik van eigen, niet-overdraagbare functies van één cloudplatform voor kritische toepassingen, of accepteer dat bewust als risico.

6.4 Test het plan

Een niet-geteste exitstrategie is een aanname. Test minstens jaarlijks voor kritische diensten of een volledige export lukt, hoelang die duurt, of de data compleet is en of die te importeren is in een alternatieve omgeving. Een tabletop-oefening met het scenario ‘de leverancier is vandaag failliet verklaard’ brengt snel aan het licht welke afspraken en kennis ontbreken. Leg de resultaten vast als bewijs voor maatregelen 5.23 en 5.30.

6.5 Steun vanuit de EU Data Act

De Europese Data Act versterkt uw positie als afnemer van clouddiensten. De overstapregels gelden sinds 12 september 2025, voor IaaS, PaaS en SaaS. Volgens artikel 29 mogen aanbieders tot 12 januari 2027 alleen kosten rekenen die direct samenhangen met de overstap; vanaf die datum zijn overstapkosten, inclusief egress-kosten voor de overstap, helemaal verboden. De Data Act verplicht aanbieders ook om overstapafspraken in het contract op te nemen, zoals een maximale opzegtermijn, een overgangsperiode en een periode om data op te halen.

Dit neemt de noodzaak van een eigen exitplan niet weg. De wet geeft u een recht, maar regelt niet dat uw data compleet, bruikbaar en op tijd bij u terug is. Controleer bovendien of uw bestaande contracten vóór 12 januari 2027 in lijn worden gebracht, met name bij automatische verlengingen.

> **Risico als dit ontbreekt:** zonder exitstrategie bent u afhankelijk van de goede wil van de leverancier precies op het moment dat die het minst te bieden heeft: bij faillissement, conflict of overname. U loopt het risico dat data onvolledig of onbruikbaar terugkomt, dat bewaarplichten niet meer na te komen zijn, dat de overstap maanden duurt en dat kopieën van uw gegevens achterblijven bij een partij waar u geen grip meer op hebt.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

7. Samenhang met wet- en regelgeving

Een goed ingericht leveranciersproces volgens ISO 27001 levert een groot deel van het bewijs dat ook wetgevers en toezichthouders vragen. De belangrijkste raakvlakken:



Waar het datacenter staat en onder welk recht de leverancier valt, bepaalt welke wetgeving op uw data van toepassing is.

Regeling	Relevantie voor leveranciersmanagement
AVG	Verwerkersovereenkomst verplicht (artikel 28); beoordeling van passende beveiliging bij de verwerker; teruggave of verwijdering van persoonsgegevens na afloop; regels voor doorgifte buiten de EER
Cyberbeveiligingswet (NIS2)	Van kracht sinds 15 augustus 2026; de zorgplicht voor essentiële en belangrijke entiteiten omvat beveiliging van de toeleveringsketen, en het bestuur is zelf verantwoordelijk
DORA	Voor de financiële sector sinds januari 2025: register van ICT-dienstverleners en verplichte exitstrategieën voor ICT-diensten die kritieke of belangrijke functies ondersteunen
EU Data Act	Recht op overstap tussen clouddiensten, contractuele overstapafspraken en het verbod op overstapkosten vanaf 12 januari 2027 (zie paragraaf 6.5)

Ook organisaties die zelf niet onder de Cyberbeveiligingswet of DORA vallen, krijgen ermee te maken. Klanten die wel onder deze regels vallen, stellen dezelfde eisen door aan hun leveranciers. Een aantoonbaar leveranciersproces is daarmee ook een commercieel voordeel.

7.1 Verantwoordelijkheden onder de Cyberbeveiligingswet (NIS2)

Sinds 15 augustus 2026 geldt de Cyberbeveiligingswet (Cbw), de Nederlandse uitwerking van de Europese NIS2-richtlijn. De wet vervangt de Wbni en stelt eisen aan ruim 8.000 organisaties die als essentiële of belangrijke entiteit worden aangemerkt. Het Cyberbeveiligingsbesluit werkt de zorgplicht en de kennisplicht van bestuurders verder uit. Organisaties stellen zelf vast of zij onder de wet vallen.

Voor leveranciersmanagement is de kernboodschap: de zorgplicht stopt niet bij de eigen voordeur. Beveiliging van de toeleveringsketen is een expliciet onderdeel van de verplichte maatregelen, en het bestuur is er zelf verantwoordelijk voor.

Verantwoordelijkheden van het bestuur

Verantwoordelijkheid	Wat dit betekent voor leveranciersmanagement
Maatregelen vaststellen en goedkeuren	Het bestuur keurt het leveranciersbeleid, de classificatie en de risicoacceptatie voor kritische leveranciers goed
Toezien op de uitvoering	Het bestuur laat zich periodiek rapporteren over de status van kritische leveranciers, incidenten in de keten en openstaande risico's
Kennis en opleiding	Bestuurders volgen verplicht training, zodat zij risico's, ook die in de keten, kunnen herkennen en maatregelen kunnen beoordelen
Persoonlijke aansprakelijkheid	Bestuurders kunnen persoonlijk worden aangesproken als de organisatie de zorgplicht schendt; ‘het lag bij de leverancier’ is geen verweer

Zorgplicht: beveiliging van de toeleveringsketen

De zorgplicht vraagt passende en evenredige technische, operationele en organisatorische maatregelen. Voor de keten betekent dat onder meer:

- **Risico's per directe leverancier beoordelen.** Kijk naar de kwetsbaarheden die specifiek zijn voor die leverancier, de kwaliteit van hun producten en hun beveiligingspraktijk, inclusief veilige ontwikkeling.
- **Beveiligingseisen contractueel vastleggen.** Inclusief eisen aan onderaannemers, auditrechten en incidentmelding.
- **Aanschaf, ontwikkeling en onderhoud beveiligen.** Ook bij de inkoop van ICT-producten en -diensten, inclusief het afhandelen van kwetsbaarheden.
- **Bedrijfscontinuïteit borgen.** Back-ups, crisisbeheer en herstel moeten ook werken als een kritische leverancier uitvalt. Hier sluit de exitstrategie uit hoofdstuk 6 direct op aan.
- **Effectiviteit toetsen.** Periodiek beoordelen of de maatregelen, ook die bij leveranciers, daadwerkelijk werken.

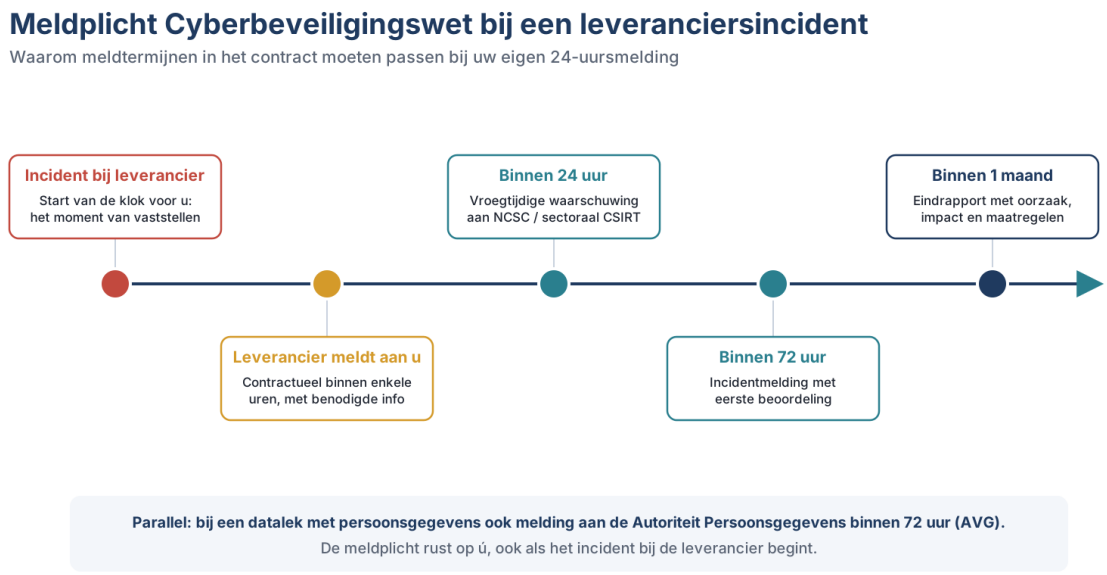
Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

Meldplicht: een incident bij uw leverancier kan uw incident zijn

Een significant incident moet gefaseerd worden gemeld bij het NCSC of het sectorale CSIRT, en waar nodig bij de toezichthouder:

1. **Binnen 24 uur:** een vroegtijdige waarschuwing.
2. **Binnen 72 uur:** een incidentmelding met een eerste beoordeling.
3. **Binnen één maand:** een eindrapport.

Valt uw dienstverlening uit door een storing of aanval bij een leverancier, dan rust de meldplicht op u. Die termijn haalt u alleen als de leverancier u snel en volledig informeert. Leg daarom in het contract vast dat kritische leveranciers incidenten binnen enkele uren melden, met de informatie die u voor uw eigen melding nodig hebt. Stem deze route af op de datalekmelding onder de AVG, die daar los van blijft bestaan.



Figuur 5. De meldtermijnen van de Cyberbeveiligingswet beginnen ook te lopen als het incident bij de leverancier ontstaat.

Toezicht en sancties

Toezichthouders kunnen bindende aanwijzingen geven en boetes opleggen. Onder NIS2 lopen die voor essentiële entiteiten op tot € 10 miljoen of 2% van de wereldwijde jaaromzet, en voor belangrijke entiteiten tot € 7 miljoen of 1,4%, welk bedrag het hoogst is. Daarnaast bestaat er een registratieplicht.

Ook als u zelf niet onder de wet valt

Levert u aan een organisatie die wel onder de Cbw valt, dan krijgt u de eisen via het contract doorgelegd. U kunt dan vragen verwachten over certificering, incidentmelding, onderaannemers

en exitondersteuning. Een ISMS volgens ISO/IEC 27001:2022 met een aantoonbaar leveranciersproces is in dat geval het sterkste bewijs dat u kunt leveren.

Hoe ISO 27001 en de Cbw op elkaar aansluiten

Cbw-verplichting	Aansluitende ISO/IEC 27001:2022-onderdelen
Bestuursverantwoordelijkheid en training	Clausule 5 (leiderschap), 7.2 (competentie), 9.3 (directiebeoordeling)
Risicobeheer in de toeleveringsketen	Maatregelen 5.19 tot en met 5.23
Bedrijfscontinuïteit bij uitval van een leverancier	Maatregelen 5.29, 5.30 en 8.13, plus de exitstrategie
Meldplicht	Maatregelen 5.24 tot en met 5.26 (incidentbeheer), aangevuld met contractuele meldtermijnen voor leveranciers
Effectiviteit toetsen	Clausule 9 (monitoring, interne audit) en maatregel 5.22

> ISO 27001-certificering betekent niet automatisch dat u aan de Cbw voldoet, maar het dekt een groot deel van de zorgplicht af. Controleer vooral of de scope van uw ISMS alle diensten omvat die onder de wet vallen, en of de 24-uursmelding ook werkt als het incident bij een leverancier begint.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

8. Stappenplan en checklist

Gebruik dit stappenplan om leveranciersmanagement in uw ISMS in te richten of aan te scherpen.

1. Stel een leveranciersbeleid vast met rollen, classificatiecriteria en minimale eisen per niveau (5.19).
2. Breng alle leveranciers die informatie verwerken in kaart in een leveranciersregister, inclusief schaduw-IT.
3. Classificeer elke leverancier en wijs een interne eigenaar toe.
4. Voer voor kritische leveranciers een volledige due diligence uit en leg het restrisicobesluit vast.
5. Werk contracten en verwerkersovereenkomsten bij met beveiligings-, audit- en exitafspraken (5.20, 5.21).
6. Stel voor elke kritische clouddienst een exitplan op (5.23).
7. Richt periodieke monitoring, serviceoverleg en wijzigingsbeheer in (5.22).
8. Test de exit en de data-export minstens jaarlijks en verwerk de lessen.
9. Neem leveranciersmanagement op in de interne audit en de directiebeoordeling.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

Checklist per kritische leverancier

Controlepunt	Ja	Actie nodig
Leverancier staat in het register met classificatie en eigenaar	☐	☐
ISO 27001-certificaat geldig en scope dekt de afgenomen dienst	☐	☐
Recent ISAE 3402 of SOC 2 type II-rapport beoordeeld, inclusief eigen aanvullende maatregelen	☐	☐
Datalocaties, jurisdictie en onderaannemers bekend	☐	☐
Contract bevat beveiligingseisen, meldtermijn incidenten (passend bij de 24-uursmelding onder de Cbw) en auditrecht	☐	☐
Verwerkersovereenkomst afgesloten (bij persoonsgegevens)	☐	☐
SLA met RTO en RPO passend bij het eigen continuïteitsplan	☐	☐
Exitplan vastgelegd: formaat, termijnen, kosten, ondersteuning en verwijdering	☐	☐
Periodieke eigen export van data ingericht	☐	☐
Exit of export in het afgelopen jaar getest	☐	☐
Restrisico geaccepteerd door de risico-eigenaar	☐	☐
Jaarlijkse herbeoordeling ingepland	☐	☐

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618

9. Conclusie

Leveranciersmanagement is de plek waar informatiebeveiliging het vaakst lekt, en tegelijk een van de best te beheersen onderwerpen in ISO/IEC 27001:2022. De norm geeft met maatregelen 5.19 tot en met 5.23 een helder kader. Het verschil zit in de uitvoering: weet welke leveranciers kritisch zijn, beoordeel ze op bewijs in plaats van beloftes, en blijf ze volgen gedurende de hele looptijd.

Het sluitstuk is de exitstrategie. Uw data is van u, ook als die bij een ander staat. Zorg dat u die terug kunt halen in een bruikbaar formaat, binnen een afgesproken termijn, en dat u kunt aantonen dat er niets achterblijft. Regel dat bij de start van de relatie, test het periodiek, en u staat sterk op het moment dat het er echt toe doet.

Bronnen

[1] ISO/IEC 27001:2022 en ISO/IEC 27002:2022, Annex A maatregelen 5.19 tot en met 5.23

[2] Data Act, artikel 29: geleidelijke afschaffing overstapkosten

[3] Xictron: Data Act en overstappen tussen cloudaanbieders

[4] Rijksoverheid: Cyberbeveiligingswet en Wwke van kracht (15 augustus 2026)

[5] Security Management: verwachte inwerkingtreding Cbw en Wwke op 15 augustus

[6] NJB: Cyberbeveiligingsbesluit, Stb. 2026, 189

[7] Aon: NIS2 en de Cyberbeveiligingswet (boetebedragen)

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 leveranciersvoorwaarden kunnen wijzigen; toets altijd de actuele tekst en contracten.

Aalsburg 1508 • 6602 TS Wijchen • KvK 97195618