

FACTSHEET

BIO2

Informatiebeveiliging als bestuurlijke
verantwoordelijkheid

De BIO2

Informatiebeveiliging als bestuurlijke verantwoordelijkheid

Burgers en bedrijven zijn verplicht informatie met de overheid te delen en zijn afhankelijk van overheidsdiensten. Die afhankelijkheid brengt een zorgplicht mee: zorgvuldig omgaan met informatie en de continuïteit van dienstverlening waarborgen. De Baseline Informatiebeveiliging Overheid 2 (BIO2) is het instrument waarmee de overheid die zorgplicht invult.

De BIO2 is geen opgefriste versie van de oude baseline, maar een grondige herziening. De vaste basisbeveiligingsniveaus zijn verdwenen, risicomanagement staat centraal en de structuur volgt ISO/IEC 27001. Sinds 15 augustus 2026 is de BIO2 via de Cyberbeveiligingswet en de Cyberbeveiligingsregeling sector Overheid ook wettelijk verankerd, met de Rijksinspectie Digitale Infrastructuur als toezichthouder.

Daarmee verschuift informatiebeveiliging van een technisch vraagstuk naar een strategische bestuursverantwoordelijkheid. Niet langer óf de organisatie investeert in digitale weerbaarheid, maar hoe zij dat aantoonbaar en op de juiste manier doet.

In deze factsheet wordt het volgende behandeld:

- Wat er verandert ten opzichte van de BIO 1.04 en hoe de tijdlijn eruitziet
- Het wettelijk kader: Cyberbeveiligingswet, ministeriële regeling en wie eronder valt
- De opbouw van de BIO2 en de drie typen overheidsmaatregelen
- Governance: de rollen van bestuur, CISO en lijnmanagement
- Risicomanagement, aantoonbaarheid en transparantie
- Ketenhygiëne en de eisen aan leveranciers
- Toezicht, meldplicht en een praktisch stappenplan



I. Van BIO naar BIO2

Wat verandert er?

De BIO 1.04 werkte met drie basisbeveiligingsniveaus (BBN1, BBN2 en BBN3). Organisaties bepaalden per systeem het niveau en pasten de bijbehorende vaste set maatregelen toe. Dat gaf houvast, maar werkte in de praktijk vaak als afvinklijst.

De BIO2 laat de BBN's los. In plaats daarvan stemt de organisatie haar maatregelen af op de eigen context, dreigingen en risicobereidheid. De verplichte overheidsmaatregelen blijven het minimum; alles daarboven volgt uit de risicoanalyse. Je moet kunnen uitleggen waarom je bepaalde keuzes hebt gemaakt, welke risico's je accepteert en wie daarvoor bestuurlijk verantwoordelijk is.

Onderwerp	BIO 1.04	BIO2
Uitgangspunt	Drie basisbeveiligingsniveaus (BBN1 tot BBN3) met vaste maatregelen sets	Risicogedreven: verplichte overheidsmaatregelen plus maatregelen op basis van de eigen risicoanalyse
Structuur	Gebaseerd op de vorige generatie van ISO 27001/27002	Volgt ISO/IEC 27001:2023 en ISO/IEC 27002:2022; maatregelen genummerd naar de ISO-beheersmaatregel (bijv. 5.17.01)
Juridische status	Verplichtende zelfregulering, afgesproken tussen de overheidslagen	Wettelijk verankerd via de Cyberbeveiligingswet en de Cyberbeveiligingsregeling sector Overheid
Bestuur	Eindverantwoordelijk, maar in de praktijk vaak gedelegeerd aan IT	Bestuurders sturen aantoonbaar op risico's, keuren maatregelen goed en beschikken over voldoende kennis
Transparantie	Geen publicatieplicht	Publicatie van de reikwijdte van het ISMS en de Verklaring van Toepasselijkheid is verplicht
Toezicht	Geen publicatieplicht	Onafhankelijk toezicht door de Rijksinspectie Digitale Infrastructuur (RDI)

Tijdslijn BIO2

Sept. 2025

BIO2 vastgesteld; Rijk, provincies en waterschappen passen hem toe als verplichtende zelfregulering

5 maart 2026

BIO2 v1.3 in de Staatscourant, in lijn gebracht met de Cbw

15 april 2026

Tweede Kamer neemt de Cyberbeveiligingswet aan

7 juli 2026

Eerste Kamer neemt de Cbw en de Wet weerbaarheid kritieke entiteiten aan

5 augustus 2026

Cyberbeveiligingsregeling sector Overheid in de Staatscourant

15 augustus 2026

Cbw en regeling in werking: BIO2 wettelijk verplicht, ook voor gemeenten

Eind 2027

Beoogde volgende versie, na evaluatie in 2026



II. Het wettelijk kader

Cyberbeveiligingswet en de sector overheid

De Cyberbeveiligingswet (Cbw) is de Nederlandse uitwerking van de Europese NIS2-richtlijn. De wet legt aan essentiële en belangrijke entiteiten vier kernverplichtingen op. De overheid is daarbij als essentieel aangemerkt.

De Cyberbeveiligingsregeling sector Overheid werkt de zorgplicht voor overheidsorganisaties uit. Zij moeten een managementsysteem inrichten volgens ISO/IEC 27001:2023 en ten minste de beheersmaatregelen van ISO/IEC 27002:2022 toepassen, aangevuld met de voor hen relevante overheidsmaatregelen uit de BIO2 v1.3. Waterschappen vallen onder een eigen regeling en onder toezicht van de Inspectie Leefomgeving en Transport.



1 Registratieplicht

Registratie in het entiteitenregister van het Nationaal Cyber Security Centrum (mijn.ncsc.nl). Na registratie kan de organisatie aansluiten bij haar CSIRT.

2 Zorgplicht

Passende en evenredige technische, operationele en organisatorische maatregelen. Voor de overheid ingevuld met ISO 27001, ISO 27002 en de BIO2.

3 Meldplicht

Significante incidenten binnen 24 uur na ontdekking melden bij het CSIRT (vroegtijdige waarschuwing), gevolgd door een vervolgmelding binnen 72 uur en uiterlijk een maand daarna een eindverslag, inclusief oorzaakanalyse (RCA).

4 Bestuurlijke verantwoordelijkheid

Bestuurders keuren de maatregelen goed, zien toe op de uitvoering en volgen trainingen om over aantoonbaar voldoende kennis te beschikken.





Wat valt er onder de sector overheid?

Overheidsentiteiten: wie hoort erbij en wie is verantwoordelijk?

Overheid	Toelichting
Ministeries	Inclusief hun diensten en agentschappen. De minister is de verantwoordelijke bestuurder.
Provincies	Gedeputeerde Staten dragen de bestuurlijke verantwoordelijkheid.
Gemeenten	Het college van burgemeester en wethouders is verantwoordelijk. Tot 15 augustus 2026 gold de BIO 1.04zv als verplichtende zelfregulering; sindsdien is de BIO2 het wettelijk kader.
Zbo's en gemeenschappelijke regelingen	Zelfstandige bestuursorganen op centraal niveau en gemeenschappelijke regelingen vallen eronder wanneer zij aan de criteria uit de wet voldoen.
Uitgezonderd	Onder meer veiligheidsregio's, het ministerie van Defensie, het Openbaar Ministerie, de AIVD en MIVD, de politie, de rechterlijke macht, de Eerste en Tweede Kamer en De Nederlandsche Bank.

Twee uitzonderingen in de BIO2. De regeling zondert de ISO-beheersmaatregelen 5.32 (intellectueel eigendom) en 5.34 (privacy en bescherming van persoonsgegevens) en de bijbehorende overheidsmaatregelen uit van de wettelijke verplichting. Zij vallen buiten de reikwijdte van de Cbw, die zich beperkt tot de beveiliging van netwerk- en informatiesystemen. Voor de eigen informatiebeveiliging en de AVG blijven zij natuurlijk relevant.

III. De opbouw van de BIO2

Kader, overheidsmaatregelen en toelichting

De BIO2 vervangt ISO 27001 en 27002 niet, maar bouwt erop voort. ISO 27001 vormt de basis voor het managementsysteem (ISMS), ISO 27002 levert de implementatierichtlijnen. Waar de BIO2 niets expliciet voorschrijft, gelden beide ISO-documenten. Daarbovenop komen de overheidsmaatregelen: concrete, verplichte eisen die voor iedere overheidsorganisatie gelden, ongeacht omvang of risicoprofiel.

De maatregelen zijn genummerd naar de ISO-beheersmaatregel waar ze bij horen, gevolgd door een volgnummer. Maatregel 5.17.01 hoort bijvoorbeeld bij ISO-control 5.17 (authenticatie-informatie). Hoofdstuk 5 gaat over organisatorische maatregelen, 6 over personeel, 7 over fysieke beveiliging en 8 over technologie.

Deel 1

BIO2-kader

De context waarin de overheid opereert, de doelstellingen, het risicomanagementproces en de rollen van bestuur, CISO en lijnmanagement.

Deel 2

BIO-overheidsmaatregelen

De verplichte maatregelen, geordend naar ISO 27001 bijlage A en aangevuld met specifieke overheids-eisen. Ook beschikbaar in Excel.

Deel 3

Toelichting

Praktische handvatten, voorbeelden en implementatietips. Wordt gefaseerd gepubliceerd via bio-overheid.nl.





Drie typen overheidsmaatregelen

Type	Waar het om gaat	Voorbeelden uit de BIO2
Basishygiëne	Het absolute minimum. Deze maatregelen zijn nodig om aan NIS2 en de Cbw te kunnen voldoen en gelden voor elke organisatie, ongeacht het risicoprofiel.	Een ISMS inrichten (5.35.01), multifactorauthenticatie (5.17.01), malwarescanning (8.07.03), logging, patchmanagement en incidentbeheer
Ketenhygiëne	Maatregelen die risico's in de keten van overheden en leveranciers beperken en waarbij gezamenlijk handelen nodig is. De organisatie blijft zelf verantwoordelijk, ook als zij uitbesteedt.	Leveranciers laten aantonen dat zij voldoen (5.20.03), delen van beveiligingsanalyses (5.27.02), elkaar waarschuwen bij dreigingen (7.02.01)
Overheidsrisico's	Universele risico's die voor de hele overheid gelden en verder gaan dan financiële schade: politiek gezichtsverlies, verlies van vertrouwen bij burgers, diplomatieke schade en verstoring van publieke dienstverlening.	Screeningsbeleid met VOG (6.01.01), testen van continuïteitsplannen (5.30.01), instructies voor het verwijderen en vernietigen van informatie (7.10.01)

Verplicht is verplicht. Overheidsmaatregelen kunnen niet op basis van een risico-inschatting worden geaccepteerd of weggelaten. Alleen wanneer een maatregel aantoonbaar niet van toepassing is, kan zij gemotiveerd in de Verklaring van Toepasselijkheid worden uitgesloten.

IV. Governance

Bestuurders in de hoofdrol

Waar informatiebeveiliging lang werd gezien als een IT-vraagstuk dat kon worden gedelegeerd, is de BIO2 helder: het bestuur is eindverantwoordelijk voor passende technische, organisatorische en operationele maatregelen en ziet toe op de naleving daarvan. Het bestuur laat zich adviseren door de CISO, de CIO en de functionaris gegevensbescherming, maar kan de verantwoordelijkheid niet overdragen.

Dat brengt concrete verplichtingen mee. Bestuurders moeten aantoonbaar over voldoende kennis en vaardigheden beschikken om de gevolgen van informatieveiligheidsrisico's voor de eigen dienstverlening te beoordelen. Dat vraagt om periodieke scholing van bestuur én medewerkers (5.04.01). Bij veel organisaties zit hier de grootste achterstand: de technische basis staat, maar de bestuurlijke sturing is nog niet aantoonbaar ingericht.

Rol	Verantwoordelijkheid BIO2	In de praktijk
Bestuur	Treft passende en evenredige maatregelen, keurt de maatregelen voor het beheer van cyberrisico's goed en ziet toe op de kwaliteit van de uitvoering. Beschikt over voldoende kennis.	Stelt het informatiebeveiligings-beleid en de risicobereidheid vast, bespreekt periodiek de rapportages van de CISO en besluit over restrisico's.
CISO	Coördineert de informatiebeveiliging en rapporteert aan het bestuur hoe het lijnmanagement het beleid implementeert. Is nadrukkelijk niet verantwoordelijk voor de implementatie zelf.	Adviseert gevraagd en ongevraagd, zonder belangenverstrengeling. Heeft een onafhankelijke positie met rechtstreekse lijn naar het bestuur.
Lijnmanagement	Is eigenaar van de informatie en informatiesystemen, identificeert dreigingen en past de maatregelen toe. Vraagt de CISO om advies bij afwijkingen.	Draagt de operationele uitvoering en het beheer van de systemen waarvan het eigenaar is, inclusief de bijbehorende risico's.
Proceseigenaar	Verantwoordelijk voor onder meer incidentafhandeling (5.24.03), beoordeling van leveranciers (5.22.01) en het identificeren van kritieke systemen (5.30.02).	Kent de praktijk en moet met de maatregelen werken; betrek proceseigenaren daarom al bij de gap-analyse.

Wie is de bestuurder?

Bij gemeenten het college van burgemeester en wethouders, bij provincies Gedeputeerde Staten en bij ministeries de minister. Zij dragen onder de Cbw de bestuurlijke verantwoordelijkheid en de opleidingsplicht.

Drie eerlijke vragen voor het bestuur

- Weet het bestuur wat de BIO2 van hén vraagt, en niet alleen van de CISO?
- Kun je vandaag aantonen hoe risico's worden gewogen en wie daarover beslist?
- Is er een realistisch pad van waar je nu staat naar wat de wet vereist?

V. Risicomanagement en aantoonbaarheid

Van papier naar praktijk

Risicomanagement is in de BIO2 geen eenmalige exercitie, maar een doorlopend proces dat de basis vormt voor alle verdere keuzes. De organisatie stelt haar context vast (minimaal de context die de BIO2 beschrijft), identificeert waardevolle informatie en middelen, brengt dreigingen in kaart, classificeert risico's op waarschijnlijkheid en impact en selecteert beheersmaatregelen. De methodiek omvat ten minste een quickscan, een volledige risicoanalyse, een risicoregister en een opvolgingsproces voor geaccepteerde risico's.

"We hebben een beleid" is niet langer voldoende. De BIO2 vraagt om aantoonbaarheid van opzet, bestaan en werking van maatregelen. Opzet blijkt uit beleid en verwijzingen; bestaan en werking uit self-assessments, interne audits, penetratietesten en red-team-oefeningen. Een vastgesteld auditplan bepaalt jaarlijks welke systemen op welke manier worden getoetst (5.35.02).

1

Context

Organisatie, dienstverlening, ketenpartners en dreigingsbeeld vaststellen

2

Identificatie

Waardevolle informatie en middelen benoemen, relevante dreigingen in kaart brengen

3

Analyse

Risico's classificeren op waarschijnlijkheid en impact, afgezet tegen de risicobereidheid

4

Behandeling

Maatregelen kiezen; overheidsmaatregelen zijn altijd verplicht, restrisico's worden bestuurlijk geaccepteerd

5

Monitoring

Interne audits, managementbeoordeling en continue verbetering van het ISMS

Aantoonbaarheid	Wat vraagt de BIO2?
Opzet, bestaan en werking	Maatregelen staan niet alleen op papier, maar zijn ingevoerd en functioneren aantoonbaar in de praktijk. Bewijs wordt vastgelegd en is opvraagbaar voor de toezichthouder.
Penetratiestesten	Internetfacing-systemen worden bij iedere nieuwe release of major update getest, bij voorkeur geautomatiseerd, en minimaal jaarlijks (8.08.05). Bevindingen met een hoog risico die niet anderszins gemitigeerd kunnen worden, betekenen: niet in productie.
Publicatie ISMS-scope	De organisatie publiceert welke bedrijfsprocessen en informatiesystemen onder haar managementsysteem vallen.
Publicatie Verklaring van Toepasselijkheid	De VvT laat zien welke maatregelen zijn geïmplementeerd en welke gemotiveerd niet van toepassing zijn. Publicatie is verplicht, zodat burgers, ketenpartners en toezichthouders kunnen beoordelen hoe serieus de organisatie informatiebeveiliging neemt.
ISO 27001-certificering	Niet verplicht. Een certificaat van een onafhankelijke auditor kan de verantwoording wel vereenvoudigen en het vertrouwen van ketenpartners versterken.

VI. Ketenhygiëne

Van inkoop naar risicobeheersing

Overheidsorganisaties zijn steeds afhankelijker van externe leveranciers voor hun informatievoorziening. Die afhankelijkheid brengt risico's mee die de organisatie zelf moet beheersen, ook als de dienstverlening buiten de eigen muren plaatsvindt. Uitbesteden is nooit het uitbesteden van verantwoordelijkheid.

De BIO2 stelt daarom expliciete eisen aan de hele levenscyclus van een leveranciersrelatie: van de risicoafweging vóór de aanbesteding, via de eisen in offerteaanvraag en contract, tot de jaarlijkse toetsing en de exit. Voor de juridische kant betekent dit dat inkoopvoorwaarden, verwerkersovereenkomsten en SLA's opnieuw tegen het licht moeten.

Fase	Wat de BIO2 vraagt	Wat je contractueel regelt
Vóór het contract	Een expliciete risicoafweging wijst uit of de afhankelijkheid van de leverancier beheersbaar is. Informatiebeveiligingseisen (beschikbaarheid, integriteit, vertrouwelijkheid) zijn onderdeel van het hele pakket inkoopseisen (5.19.01).	Beveiligingseisen in de aanbestedingsstukken en als gunningscriterium; toets op eigenaarschap, locatie van data en subverwerkers.
In het contract	De leverancier toont jaarlijks aan dat hij aan alle eisen voldoet in opzet, bestaan en werking, op basis van onderzoek door onafhankelijke derden (5.20.03).	Rapportageplicht (bijvoorbeeld assurancerapporten of certificaten), auditrecht voor de organisatie, meldplicht voor kwetsbaarheden en incidenten.
Toeleveringsketen	De leverancier is verantwoordelijk voor het borgen van de eisen bij zijn toeleveranciers (5.21.01); de organisatie beoordeelt of de ketenrisico's acceptabel zijn (5.21.02).	Doorlegverplichting naar subleveranciers, transparantie over de keten, goedkeuring bij wijziging van subleveranciers.
Gedurende looptijd	De organisatie voert zelfstandig onderzoek uit, ook ter validatie van de rapportages die de leverancier aanlevert.	Contractueel vastgelegde mogelijkheid voor externe audits en penetratietesten, escalatie- en herstelafspraken.
Exit	Een expliciete uitwerking van de exit-strategie is een vast onderdeel van het contract (5.20.06).	Overdracht en verwijdering van data, medewerking bij migratie, continuïteit tijdens de transitie.

Ook de leverancier heeft er belang bij. Leveranciers die zelf onder de Cbw vallen of die aan meerdere overheden leveren, kunnen hun compliance het beste één keer goed inrichten en aantonen, bijvoorbeeld met een ISO 27001-certificaat en een assurancerapport dat de BIO2-overheidsmaatregelen afdekt.

VII. Toezicht en meldplicht

De tanden van de Cbw

Binnen de sector Overheid houdt de Rijksinspectie Digitale Infrastructuur (RDI) toezicht op de naleving van de Cyberbeveiligingswet. De RDI toetst of organisaties aan hun zorgplicht voldoen en of het ISMS, inclusief de verplichte overheidsmaatregelen, naar behoren functioneert. Voor waterschappen is de Inspectie Leefomgeving en Transport de toezichthouder.

De RDI kiest voor een stelselbenadering: datagedreven, risicogericht en proportioneel, gericht op verbetering van het geheel in plaats van op losse inspecties. Dat neemt niet weg dat iedere organisatie op verzoek moet kunnen aantonen dat zij aan de zorgplicht voldoet. De gepubliceerde ISMS-scope en Verklaring van Toepasselijkheid zijn daarbij het startpunt.

Verplichting	Wat betekent dit concreet?
Registratie	Iedere organisatie onder de Cbw registreert zich in het entiteitenregister bij het NCSC en houdt de gegevens actueel.
Vroegtijdige waarschuwing	Binnen 24 uur na ontdekking van een significant incident: een eerste melding bij het CSIRT.
Vervolgmelding	Binnen 72 uur een vervolgmelding met een eerste beoordeling van het incident, de ernst en de gevolgen.
Eindverslag	Uiterlijk een maand na de vervolgmelding een eindverslag met een gedetailleerde beschrijving van het incident, de oorzaak (root cause analysis), de getroffen maatregelen en eventuele grensoverschrijdende gevolgen.
Significant incident	De regeling bevat drempelwaarden voor centrale en decentrale overheden, onder meer bij uitval van dienstverlening van vier uur of langer, ernstige financiële gevolgen of dood of ernstig letsel. Leg de drempels vast in het eigen incidentproces.
Samenloop met de AVG	Een significant incident is vaak ook een datalek. De melding bij de Autoriteit Persoonsgegevens (binnen 72 uur) en de informatieplicht richting betrokkenen blijven onverkort gelden, naast de Cbw-melding.

Geen standaard is voldoende op zichzelf

De BIO2 vult de zorgplicht in, maar de registratieplicht, de meldplicht en de bestuurlijke verplichtingen uit de Cbw worden niet door de norm afgedekt. Richt deze processen apart in en leg ze vast.

Cbw Control Framework

De Auditdienst Rijk en NOREA publiceerden het Cbw Control Framework als praktische vertaalslag van NIS2 en Cbw naar toetsbare maatregelen. Het bouwt voort op ISO 27001 en de BIO2 en is bruikbaar als hulpmiddel bij de gap-analyse.



VIII. Praktisch aan de slag

Van analyse naar actie

De implementatie van de BIO2 vraagt om een gestructureerde aanpak. Begin niet met het lukraak doorvoeren van maatregelen, maar volg een pad dat start bij inzicht en leidt naar concrete verbetering. De BIO2 is geen sprint maar een marathon; wat telt is een realistisch plan met heldere mijlpalen en bestuurlijk eigenaarschap.

Voor wie al onder de BIO 1.04 werkte, is de technische basis vaak redelijk op orde. De grootste stappen liggen meestal in de bestuurslaag: risicobereidheid vaststellen, rapportagelijnen inrichten, de publicatieplicht invullen en het leveranciersmanagement contractueel sluitend maken.

1 Breng de reikwijdte in kaart

Bepaal welke processen en systemen onder het ISMS vallen en of de organisatie (of een gemeenschappelijke regeling waarin zij deelneemt) onder de Cbw valt. Registreer bij het NCSC.

4 Voer een gap-analyse uit

Gebruik de BIO Self Assessment en de BIO2 in Excel van bio-overheid.nl, of het Cbw Control Framework. Kijk niet alleen naar ontbrekende maatregelen, maar ook naar de volwassenheid ervan. Betrek proceseigenaren.

2 Richt risicomanagement in, nu al

Wacht niet tot alle maatregelen zijn doorgevoerd. Kies een methodiek, stel de context en de risicobereidheid vast en laat het bestuur besluiten over restrisico's.

5 Organiseer de governance

Leg de rolverdeling tussen bestuur, CISO en lijnmanagement vast, regel de onafhankelijke positie van de CISO en plan de scholing van bestuurders en medewerkers.

3 Maak de keten sluitend

Inventariseer leveranciers en subleveranciers, toets contracten op beveiligingseisen, rapportage- en auditrechten en exit-afspraken, en pas inkoopvoorwaarden aan.

6 Werk planmatig en maak het aantoonbaar

Begin met quick wins zoals MFA en patchmanagement of met de hoogste risico's. Stel een auditplan op, publiceer de ISMS-scope en de Verklaring van Toepasselijkheid en richt het meldproces in.

Beschikbare hulpmiddelen via bio-overheid.nl: de BIO2 (Nederlands en Engels), de BIO2 in Excel, de was-woordt-lijst ten opzichte van de BIO 1.04, de BIO Self Assessment, de Handreiking BIO2-op-maat, de Quickscan Information Security en de mapping tussen NIS2, ISO 27002:2022 en de BIO2.



FAQ: veelgestelde vragen

De abstracte normen van de BIO2 en de Cbw roepen in de praktijk vaak concrete vragen op. Hieronder behandelen wij enkele vragen die wij regelmatig van overheidsorganisaties krijgen.

Vraag

Wij zijn een gemeente en werkten nog met de BIO 1.04. Hoeveel tijd hebben we?

Antwoord

Sinds 15 augustus 2026 is de BIO2 via de Cyberbeveiligingsregeling sector Overheid het wettelijk kader, ook voor gemeenten. De regeling kent geen algemene overgangstermijn voor de zorgplicht. Wel kiest de RDI voor risicogericht en proportioneel toezicht. Zorg dat je nu een gap-analyse, een risicoanalyse en een realistisch implementatieplan hebt: daarmee laat je zien dat je in control bent, ook als nog niet alles is afgerond.

Vraag

Moeten we ons laten certificeren tegen ISO 27001?

Antwoord

Nee. De BIO2 en de regeling verplichten het toepassen van ISO 27001 voor het ISMS, niet een certificaat. Een certificering door een onafhankelijke auditor kan de verantwoording richting toezichthouder en ketenpartners wel aanzienlijk vereenvoudigen.

Vraag

Mogen we een verplichte overheidsmaatregel weglaten als het risico laag is?

Antwoord

Nee. Overheidsmaatregelen zijn altijd verplicht en kunnen niet op basis van een risico-inschatting worden geaccepteerd. Alleen als een maatregel aantoonbaar niet van toepassing is, kan zij gemotiveerd worden uitgesloten in de Verklaring van Toepasselijkheid. Uitzondering zijn de maatregelen bij ISO 5.32 en 5.34, die buiten de Cbw-verplichting vallen.

Vraag

Wat moeten we precies publiceren?

Antwoord

De reikwijdte van het ISMS (welke processen en systemen vallen eronder) en de Verklaring van Toepasselijkheid (welke maatregelen zijn geïmplementeerd en welke gemotiveerd niet van toepassing zijn). Publiceer op een vindbare plek, bijvoorbeeld de eigen website, en houd de documenten actueel. Vertrouwelijke details over de concrete inrichting hoeven niet openbaar.

Vraag

Onze leverancier zegt dat hij ISO 27001-gecertificeerd is. Is dat voldoende?

Antwoord

Een certificaat is een goed begin, maar dekt niet automatisch de BIO2-overheidsmaatregelen of jullie specifieke eisen. De BIO2 vraagt dat de leverancier jaarlijks aantoont dat hij aan alle gestelde eisen voldoet in opzet, bestaan en werking, en dat jullie dit zelf valideren. Leg daarom in het contract vast welke eisen gelden, hoe daarover wordt gerapporteerd en dat jullie mogen auditen.

Vraag

Wat is de rol van de functionaris gegevensbescherming?

Antwoord

De FG adviseert het bestuur over gegevensbescherming en houdt toezicht op de naleving van de AVG. De BIO2 noemt de FG als een van de adviseurs van het bestuur, naast de CISO en de CIO. Informatiebeveiliging en privacy raken elkaar voortdurend: een significant incident onder de Cbw is vaak ook een datalek dat binnen 72 uur bij de Autoriteit Persoonsgegevens moet worden gemeld.



Zou je extra informatie willen ontvangen?

Meer weten? Aan de slag met de BIO2 en de Cyberbeveiligingswet? Wij helpen overheidsorganisaties de verplichtingen te vertalen naar concrete acties: van gap-analyse en risicomanagement tot governance, leverancierscontracten en kennissessies voor bestuurders.

Neem dan contact op met ons:
e-mail: contact@ictrecht.nl
telefoonnummer: 020 663 19 41

www.ictrecht.nl/bio2
020 - 663 1941