Rapportage Informatiebeveiliging 2025

Team IB & P

CISO gemeente Nijmegen, maart 2026

Informatiebeveiliging 2025

In getallen

118 incidenten,
36 datalekken

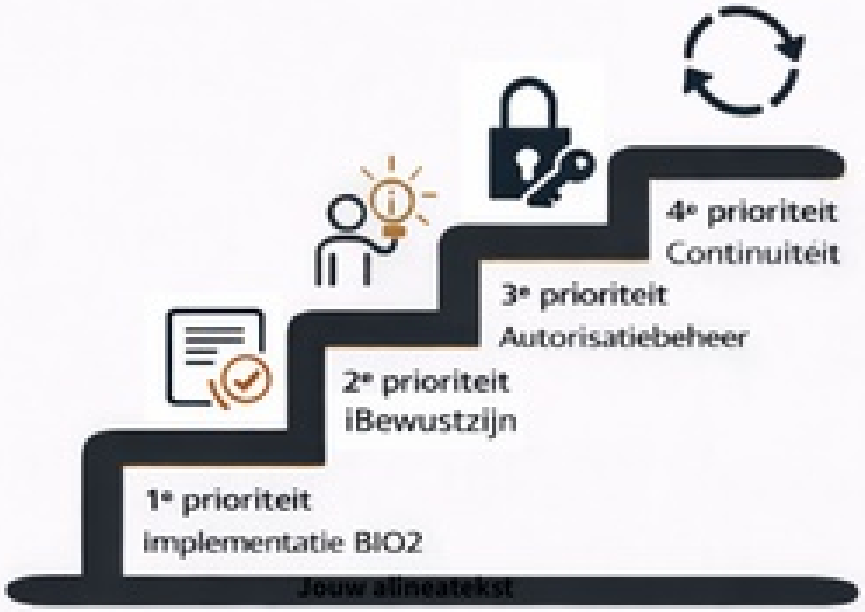
16 inzageverzoeken

41 DPIA's
onder beheer

60% eLearning gevolgd

Continuiteitsplannen
alle afdelingen

% geimplementeerde
maatregelen



Spotlight voor 2026

Voldoen aan
cyberbevelligingswet

Verhogen
weerbaarheid

AI &
Informatiebevelliging

Inhoudsopgave

1. Doel & wettelijk kader

Doel

Deze rapportage is een jaarlijks terugkerend stuk waarin de Chief Information Security Officer van gemeente Nijmegen u informeert over de ontwikkeling van de informatiebeveiliging bij de gemeente Nijmegen. We blikken terug op het afgelopen jaar en kijken vooruit naar de ontwikkelingen in 2026 en de jaren daarna. Dit rapport hoort bij de verantwoording rond de Eenduidige Normatiek Single Information Audit (hierna: ENSIA).
ENSIA is een systeem van zelfevaluaties op het vlak van informatiebeveiliging. Door dit systeem van verantwoording krijgen zowel de gemeenten als de rijksoverheid inzicht in het niveau van informatiebeveiliging bij gemeenten. Een belangrijk document wat hieruit voortkomt is de collegeverklaring. Hiermee legt het college verantwoording af aan de raad en aan landelijke toezichthouders over het gebruik van Suwinet. Daarnaast geeft de ENSIA auditor een assurance rapport af over het gebruik van DigiD. De voorliggende rapportage Informatiebeveiliging en Privacy geeft de achtergrondinformatie bij de collegeverklaring ENSIA, en de assurance rapportage. Daarnaast is in het resultaten overzicht van hoofdstuk 4 ook een in control verklaring/ management beoordeling van de informatiebeveiliging (ICV) opgenomen waarin over het geheel van de BIO wordt aangegeven hoe de stand van zaken is.

Wettelijk kader

Een periodieke rapportage aan alle managementlagen over de stand van zaken rond informatiebeveiliging is onderdeel van de Baseline Informatiebeveiliging Overheid (BIO). Met de passage over informatiebeveiliging in de jaarrekening en het onderbouwende rapport dat voor u ligt, verantwoordt het college zich aan de gemeenteraad over informatiebeveiliging in brede zin. In opvolging van de aanbevelingen van het regionale rekenkameronderzoek “Weten wat je moet weten” zal de rapportage ook beschikbaar gesteld worden aan de raad.

2. Leeswijzer

Dit rapport kent een vaste opbouw. Het eerste deel wijden we aan het schetsen van het onderwerp. Wat is het en hoe verhoudt de gemeente Nijmegen zich hiertoe. Daarna blikken we terug op het afgelopen jaar over de vooraf gestelde doelen en de behaalde resultaten. In eerste instantie voor de gemeente zelf en daarna waar het gaat om onze partners. Daarbij staan wij ook stil bij de managementbeoordeling van de effectiviteit van onze maatregelen. We sluiten af met een vooruitblik naar de toekomst, het komende jaar.

Ter ondersteuning vindt u voorin een infographic waarin de volgende onderwerpen zijn gevisualiseerd:

- Een aantal prominente maatregelen die wij op verschillende terreinen treffen om aan de Cyberbeveiligingswet te voldoen en ons doel van volwassenheidsniveau drie (1) te behalen,
- Een aantal getallen met betrekking tot informatiebeveiliging die wij jaarlijks in deze rapportage weergeven.
- Een visualisatie van de onderwerpen die onze aandacht vragen en de verschuiving daarin.

In de bijlage vindt u achtergrondinformatie over informatiebeveiliging & privacy inclusief een toelichting op veel gebruikte begrippen en afkortingen.

3. Ambitie

De gemeente Nijmegen wil haar volwassenheidsniveau[1] van de informatiebeveiliging verhogen. Wij streven ernaar om “in control” te zijn en daarover op professionele wijze verantwoording af te leggen, onder andere via de voorliggende rapportage. ‘In control’ betekent in dit verband dat de gemeente:

- inzicht heeft in de risico's en onzekerheden op het terrein van de informatiebeveiliging,
- toeziet op het nemen van (passende) maatregelen,
- daarbij helder de verantwoordelijkheden belegt,
- de controleerbare planning voor het implementeren maatregelen bewaakt ,
- toetst in hoeverre de maatregelen effectief zijn,
- verantwoording aflegt over de effectiviteit van de maatregelen,
- de risico’s die overblijven kent en bewust accepteert.

Deze ambitie hoort bij het zijn van een professionele gemeente. Het regionale rekenkameronderzoek “Weten wat je moet weten” wijst ons er op dat gemeente Nijmegen zwaarder zal moeten inzetten op het verwezenlijken van deze ambitie om volwassenheidsniveau drie te halen. Dit vindt zijn weerslag in ons nieuwe strategische informatiebeveiligingsbeleid dat in 2025 vastgesteld is.

Het team Stadscontrol binnen de gemeentelijke organisatie, met hierin ondergebracht de CISO en de FG (toezichthouders op het gebied van informatiebeveiliging en privacy), brengt de oordeelsvormende rol binnen de gemeente meer voor het voetlicht. Door meer aandacht te geven aan eigenaarschap, opvolging en verantwoording neemt het volwassenheidsniveau van processen toe. Door risico gestuurd te werken zorgen we ervoor dat dit zo efficiënt mogelijk wordt ingevuld. De invoering van de Cyberbeveiligingswet (de implementatie van de Europese NIS2 richtlijn in Nederland) is aanleiding om risicomanagement op steeds meer vlakken in te richten.

Ook de iRvN werkt aan professionalisering. Zij zijn gestart met een externe partij die hen naar certificering begeleidt. Hiermee geven zij gehoor aan de wens van gemeente Nijmegen tot meer transparantie en verantwoording in de ketens waar gemeente Nijmegen en iRvN verantwoordelijk voor zijn.

1 Het volwassenheidsniveau is gebaseerd op zowel de Norea handreiking als de BIO-SA (die gebaseerd is op de Capability Maturity Model Integration). Daarin zijn meerdere modellen geïntegreerd tot één model. Volwassenheidsniveau 1: ad-hoc / informeel. Volwassenheidsniveau 2: beheerst. Volwassenheidsniveau 3: vastgesteld / control gedefinieerd. Volwassenheidsniveau 4: voorspelbaar. Volwassenheidsniveau 5: geoptimaliseerd.

4. Terugblik

4.1 Wat wilden we bereiken?

Vorig jaar hebben we de volgende doelen als geformuleerdt:

In 2025 wordt de integrale **Roadmap** met daarin alle activiteiten op het vlak van informatiebeveiliging gebruikt bij het verantwoorden richting de accountant en de raad. Hierin worden alle aanbevelingen van zowel auditors als de accountant, als ook andere onderzoeken, samengebracht.

Het **informatiebeveiligingsbeleid** wordt herzien om aan te sluiten op de Cyberbeveiligingswet.

Gemeente Nijmegen gebruikt de CyberManager applicatie om de implementatie van maatregelen en de beoordeling van risico`s te beheren en te toetsen. Om met behulp van de CyberManager het **ISMS** beheer naar het niveau te tillen dat nodig is voor volwassenheidsniveau 3 wordt een Security Administrator toegevoegd aan het team Informatiebeveiliging

In 2025 gaat het **iVeiligheidsteam** aan de slag met het controleren van de autorisaties en de terugkoppeling hier over richting de CISO. Ook is er in dat jaar speciale aandacht voor leveranciersmanagement.

Met het inzetten van extra budget willen we de verantwoording in de **WPG audit** (met betrekking tot het gebruik van politiegegevens) beter borgen.

De afdelingen gaan aan de slag met het oefenen van de **continuïteitsplannen** en het verbeteren ervan.

Om meer gestructureerd aandacht te besteden aan **iBewustzijn** is verplichte scholing onderdeel van de jaarlijkse plannen. Daarnaast is bewustwording van de managementteams in de afdelingen een speerpunt voor 2025.

4.2 Wat hebben we bereikt?

4.2.1 De gemeente Nijmegen

Activiteiten over de hele gemeente

- Het iVeiligheidsteam is aan de slag gegaan met autorisatiematrices, waarin is opgenomen welke medewerker welke bevoegdheid heeft. Op het vlak van leveranciersmanagement heeft iedere afdeling hun lijst van applicaties beoordeeld en bepaald met welke leverancier ze een gesprek willen voeren.
- Het gemeentebrede continuiteitsplan (BCM plan) is vastgesteld. De laatste afdelingen hebben hun continuïteitsplannen in 2025 geoefend.
- Het iBewustzijn communicatieplan is uitgevoerd. In 2025 omvatte dit onder andere een phishing campagne, en een lezing door Daniel Verlaan.
- De herhaling eLearning voor Informatiebeveiliging en Privacy is op Studytube beschikbaar gesteld. 60% van de medewerkers heeft deze gevolgd.
- In 2025 is twee keer een informerende brief naar de raad gestuurd met betrekking tot de gekozen KPI`s.
- Het NYMACON hack evenement heeft bij Waalhalla in Nijmegen plaatsgevonden. Deze editie hebben ook professionele hackers deelgenomen. De evaluatie met de hackers en iRvN was zeer positief. De bevindingen worden verderop in dit document gedeeld.
- De CISO heeft in 2025 gezamenlijk met de FG de uitvraag van het controlplan uitgevoerd en hier over gerapporteerd aan het GMT en de directie. Dit controlplan had betrekking op de

processen van autoriseren, het evalueren van leveranciers, het borgen van continuïteit en het leren van incidenten.
- Met de afdelingsmanagementteams is een casusoefening uitgevoerd op het vlak van continuïteit.
- De Security Administrator is gestart met het herinrichten van de CyberManager.
- Met de toegekende claim voor informatiebeveiliging en privacy zijn er kandidaten geworven die in 2026 het team informatiebeveiliging en privacy (team IB&P) zullen versterken.

Opvallende zaken

In het afgelopen jaar was de NAVO top in Den Haag. Het belangrijkste dat gemeente Nijmegen in deze context gemerkt heeft is een aantal DDOS aanvallen waardoor onze website een paar keer kortstondig niet beschikbaar was. Aanvallen op infrastructuur nemen toe. Het aantal meldingen die gaan over kwetsbaarheden in apparatuur die netwerken moet beveiligen ligt in 2025 wereldwijd hoog. Dit leidt ook tot slachtoffers bij de Nederlandse overheid, zoals de Autoriteit Persoonsgegevens en de Dienst Justitiële Inrichtingen.

In 2025 zijn er 118 beveiligingsincidenten gemeld. Daarvan waren 103 meldingen intern en 15 meldingen extern. Er waren 36 datalekken. Van de datalekken zijn er 9 bij de Autoriteit Persoonsgegevens (AP) gemeld. Waaronder bijvoorbeeld een storing in de couverteermachine waardoor de verkeerde formulieren in enveloppen gestopt zijn en verstuurd. Niet alles wordt gemeld bij de AP omdat dit alleen geldt bij bepaalde potentiële schade die aangericht kan worden. De inrichting van de CyberManager komt steeds meer op orde. Hierdoor kunnen we over de meldingen steeds meer informatie verstrekken. Bijvoorbeeld over het aantal incidenten per afdeling. Sommige afdelingen springen er van nature uit (Zorg, Publiekszaken en Informatie) omdat zij relatief veel persoonsgegevens verwerken.

Incidenten per afdeling:
Financiën: 31
Stadsrealisatie: 6 (1 AP)
Stadsbeheer: 5
Stadsontwikkeling: 6
Inkomen, Zorg en Leerrecht: 24 (2 AP)
Personeel Informatie Facilitair: 15
Publiekszaken: 12 (2 AP)
Bestuur en Management: 1
Veiligheid, Juridische zaken en Bestuursondersteuning: 15 (2 AP)
Maatschappelijke Ontwikkeling: 6 (2 AP)
Vastgoed, Sport en Accommodaties: 4
Extern: 15
iRvN: 8

Een vergelijking tussen de verschillende jaren levert het volgende beeld op.

	2023	2024	2025
Incidenten	84	96	118
Waarvan datalekken	22	10	36
Waarvan gemeld	13	9	9

Het is positief dat er steeds meer gemeld wordt. Zonder consequent meld gedrag weten we te weinig, daarom is toenemend vertrouwen hierbij belangrijk. Het is ook goed om te zien dat daarbij het aantal meldingen aan de Autoriteit Persoonsgegevens (de privacy toezichthouder) stabiel blijft.

Een ander voorbeeld dat de inrichting van CyberManager steeds meer op orde komt, blijkt uit het feit dat in augustus 2025 binnen de gestelde termijn een WOO-verzoek met betrekking tot de geregistreerde datalekken in het jaar 2021 is afgehandeld.

Gebruik van de CyberManager

In 2025 is de Security Administrator aan de slag gegaan met het opschonen en herinrichten van de CyberManager om de verantwoording over 2026 op een hoger niveau te tillen. In het kader van de verantwoording is er een interne audit uit gevoerd op de verplichte BIO overheidsmaatregelen.
In de CyberManager is nu 100% van de maatregelen actief (bestaan), zie ook figuur 1. Dit betekent dat er een verbetering te zien is met het voorgaande jaar. De verklaring hiervoor is dat veel verbetertaken die waren uitgezet ook zijn afgerond. Daarnaast is er enige vervuiling verwijderd. Er staan wel nog een aantal verbetertaken open. Werking is in percentage gedaald. Het opvolgen en overdragen van controletaken moet in de komende tijd meer robuust ingericht worden.
In de CyberManager is ook een interne audit uitgevoerd op privacy op basis van het IBD AVG borgingsproduct. Hiermee is op organisatieniveau een meer actueel inzicht verkregen over de status van doorgevoerde maatregelen. De uitkomsten van de audit zullen het komende jaar een vast onderdeel gaan vormen van de control cyclus.

Resultaten 213a onderzoek doelmatigheid fysieke toegang

In 2025 is door Stadscontrol in samenwerking met Facilitaire Zaken een 213a onderzoek gedaan naar de doelmatigheid van de fysieke toegangsbeveiliging. De algemene conclusie is dat het beleid voor fysieke toegang en beveiliging in de kern doelmatig is. Met redelijke middelen wordt een goed basisniveau van fysieke toegang beveiliging bereikt dat vergelijkbaar is met dat van drie andere G40 - gemeenten. Tegelijkertijd blijkt uit de bevindingen dat met relatief kleine extra inspanningen en een aantal quick wins een nog hoger beveiligingsniveau kan worden bereikt. Denk hierbij aan het gebruiksvriendelijker maken van het registratieproces en meer/beter communiceren over gedragsregels. Dagelijkse incidenten zoals tailgaten (zonder eigen pas met iemand mee naar binnen lopen), onvolledige bezoekersregistratie en het niet terug begeleiden van bezoekers leiden tot risico's en extra werk voor de receptie. Verder kan de doelmatigheid worden verbeterd met een aantal gerichte grotere aanpassingen, bijvoorbeeld ter modernisering.

Resultaten uit NYMACON

In november 2025 vond in Waalhalla het NYMACON evenement plaats. Gemeente Nijmegen was gastheer voor dit regionale evenement. Studenten van de RU, maar ook andere universiteiten probeerden een aantal door de regio beschikbaar gestelde objecten te hacken. Bij deze editie deden ook een aantal professionele white hat hackers mee. De ter beschikking gestelde objecten waren onder andere een verkeerslicht, straatverlichting, een standaard laptop, een webapplicatie en de werkomgeving. Er zijn een aantal kwetsbaarheden gevonden waar leveranciers mee aan de slag zijn. De Gelderlander en RN7 hebben verslag gedaan van het evenement. Het evenement wordt samen met iRvN, cyber security dienstverlener Hunt&Hackett en het Institute for Computing and Information Sciences van de Radboud Universiteit Nijmegen georganiseerd.

Resultaat van management beoordeling informatiebeveiliging

In de hieronder weergegeven passage treft u een overzicht aan van de stand van zaken rond de implementatie van de maatregelen op het vlak van informatiebeveiliging bij gemeente Nijmegen. Dit is gebaseerd op de interne audit in de CyberManager, de uitvraag controlplan FG en CISO en de scores van de afdelingen op de Barobeter, een dashboard dat gebruikt wordt in de prestatiedialogen.

1. Beoordeling van de huidige situatie:
De status van de huidige informatiebeveiligingsmaatregelen en -processen binnen de organisatie is weergegeven in de CyberManager. Aan de hand van deze status kan door middel van een interne audit worden bepaald in hoeverre deze voldoen aan de eisen van de BIO. Deze interne audit wordt uitgevoerd op de BIO normen die getoetst worden in de ENSIA zelfevaluatie. Een algeheel overzicht van de stand van zaken als het gaat om opzet (is vastgelegd hoe de norm geïmplementeerd wordt), bestaan (is de norm op het moment van toetsing toegepast) en werking (is de implementatie van de norm effectief) wordt in onderstaand figuur getoond. Getoetst zijn de verplichte overheidsmaatregelen en de bijbehorende documenten.

Figuur 1: Opzet bestaan en werking van overheidsverplichte informatiebeveiligingsmaatregelen in CM

2. Identificatie van eventuele afwijkingen:
De scores voor opzet en bestaan zijn 100%, voor werking niet. Een aantal kanttekeningen zijn hierbij nodig. Bij de toetsing zijn alleen de verplichte overheidsmaatregelen meegenomen. In deze toetsing werken we risicogestuurd, wat wil zeggen dat we de opzet het meest kritisch beoordelen bij de meest risicovolle processen. Dit heeft te maken met beperkingen in de capaciteit door onze gehele organisatie (uitvoerende, ondersteunende en toetsende lijn), maar ook bij iRvN, die een deel van de (technische) maatregelen voor de gemeenten in de regio beheert. Dit betekent dat er met name als het gaat om werking voor de gemeente nog verbetering mogelijk is bij kritische processen, maar ook bij processen die niet tot de meest kritische behoren. Deze processen bevatten vaak wel gevoelige informatie en maken ons kwetsbaar. Een reden voor de dalende score van werking is dat de continuïteit bij het uitvoeren van de toetsing van werking nog niet geborgd is.

3. Implementatie van verbeteringen:
De taken om bovenstaande tekortkomingen te verbeteren staan in CyberManager en zijn toegewezen aan de verantwoordelijke gebruikers. Het inrichten en beheren van deze taken is een belangrijk onderdeel van het pakket van de Security Administrator. Het gaat met name om taken die toezien op de implementatie van maatregelen over de gehele organisatie. Veel maatregelen (op het vlak van gebruikersbeheer, leveranciersmanagement, continuïteit) zijn in bepaalde processen wel goed geïmplementeerd maar in andere nog niet. Om een consequente implementatie over de gehele organisatie te waarborgen is meer capaciteit en toezicht nodig.

4. Interne controle en monitoring:
Monitoring van het functioneren van maatregelen op het vlak van gebruikersbeheer en incidentbeheer vindt plaats via systemen van iRvN (Topdesk). Vanuit dit systeem ontvangt gemeente Nijmegen rapportages over de afhandeling van meldingen en wijzigingen. Daarnaast wordt de voortgang gevolgd via gesprekken met de staf medewerkers dan wel de proceseigenaar van afdelingen, bijvoorbeeld in de prestatiedialoog. Deze dialoog vindt plaats tussen de directeur bedrijfsvoering en de concernmanagers, die ook proceseigenaar zijn. De introductie van de Barobeter, een nieuw kwalitatief dashboard dat een beeld geeft van de mate waarin een afdeling in control is op bepaalde aspecten van de bedrijfsvoering waaronder informatiebeveiliging, geeft meer inzicht en aanleiding tot gesprek. Over het afgelopen jaar is te zien dat het merendeel van de afdelingen een verbetering laat zien, en een enkeling een verslechtering. Een paar afdelingen blijven gelijk. In het kader van de verantwoording over werking van 2025 heeft de CISO met de FG een gecombineerde uitvraag via het controlplan uitgevoerd. De

uitwerking van de antwoorden is op dit moment nog niet compleet. In grote lijnen is het beeld dat het merendeel van de afdelingen een paar aandachtspunten heeft. Een paar afdelingen kunnen stellen dat zij in control zijn en een enkele afdeling scoort nog onvoldoende. Dit wordt veroorzaakt doordat de controle werkzaamheden niet voldoende zijn overgedragen.

5. Onafhankelijke beoordeling:
De externe beoordeling van de informatiebeveiligingsmaatregelen vindt elk jaar op 3 manieren plaats: via de IT audit van de accountant in de context van de controle van de jaarrekening, via de DigiD en Suwinet audit in de context van de ENSIA zelfevaluatie en via de WPG audit. Deze beoordelingen dekken een deel van het IT landschap af: de accountant heeft met name oog voor de systemen die betrokken zijn bij de financiële kritische bedrijfsprocessen, de ENSIA auditor heeft met name oog voor de systemen die gekoppeld zijn aan DigiD en Suwinet en de WPG audit heeft met name betrekking op processen die politie gegevens verwerken. Deze audits pogen een breder beeld te zien vanuit hun perspectief. Met name de accountant slaagt daarin door in 2025 het algehele volwassenheidsniveau van de gemeente op het gebied van informatiebeveiliging te adresseren. Zie de paragraaf over hun observaties hier onder. Ook de ENSIA cyclus heeft een eigen paragraaf onder aan deze pagina. Voor 2025 is hier voor het eerst gekeken naar werking.

6. In control statement:
Gemeente Nijmegen verklaart voor 94% te voldoen aan de BIO. Daarbij merkt zij op dat de implementatie status varieert per maatregel en per proces. Zo scoren de meest gevoelige systemen, met name die betrokken zijn bij DigiD, Suwinet en financiën 100%. Deze staan dan ook bovenaan bij het afwegen van risico`s.

IT Audit observaties van de Accountant over 2025

Op het vlak van Algemene IT beheersmaatregelen en Cybersecurity concludeert de accountant over 2025 dat het goed is dat er budget is vrij gemaakt om de implementatie van de BIO2 te realiseren en ook bij te blijven in de ontwikkelingen. Het advies is om te toetsen of de doelstellingen ook behaald worden en welke beleidskeuzes hiervoor gemaakt worden. Deloitte onderschrijft het belang van het houden van regie op onze leveranciers omdat de afhankelijkheid van leveranciers groter wordt. Zij adviseren te monitoren op het in kaart brengen van de meest kritische applicaties en leveranciers. Ook vanwege het belang van het garanderen van de continuïteit van deze applicaties en de bijbehorende processen.

Resultaat van de ENSIA Cyclus 2025

Deze zelfevaluatie, gebaseerd op de BIO, is tijdig afgerond. Alle vragenlijsten zijn ook dit jaar op tijd ingeleverd. Bij de audit in december is van alle DigiD aansluitingen en Suwinet opzet en bestaan getoetst. Werking is in januari 2026 gecontroleerd.

Het verantwoordingsproces over 2025 is anders dan voorgaande jaren omdat de auditor over onze vijf DigiD aansluitingen volgens de 3000D richtlijn rapporteert. Over Suwinet wordt nog volgens de tot nu gebruikte werkwijze, via een collegeverklaring, gerapporteerd.

Samenvatting van de ENSIA rapportages per stelsel
Wij rapporteren als gemeente Nijmegen op één moment in het jaar over de status van onze informatieveiligheid, via ENSIA. Deze Rapportage IB gemeente Nijmegen is daar een onderdeel van. Vanuit de gemeente brede zelfevaluatie wordt eveneens de verantwoording aan de stelselhouders bij de rijksoverheid afgeleid, de zogenaamde verticale verantwoording.

<table>
<tr><th>Stelsel</th><th>Samenvatting</th></tr>
<tr><td>DigiD</td><td>Voor DigiD geldt dat gemeente Nijmegen 5 aansluitingen heeft waarvoor getoetst is of de interne beheersingsmaatregelen, in opzet, bestaan en (waar van toepassing) werking, voldoen aan de door de Rijksoverheid verplicht gestelde geselecteerde normen inzake en DigiD. Voor vier aansluitingen is vastgesteld dat deze voldoen. Voor een van de aansluitingen is vastgesteld dat de werking van een van de zeven maatregelen niet aangetoond kon worden. Hierop wordt een herstelplan uitgevoerd.</td></tr>
<tr><td>Suwinet</td><td>Bij gemeente Nijmegen is op 31 december 2025 voor Suwinet geconstateerd is dat de interne beheersingsmaatregelen, in opzet, bestaan en (waar van toepassing) werking, voldoen aan de door de Rijksoverheid verplicht gestelde geselecteerde normen inzake en Suwinet.</td></tr>
<tr><td>BRP</td><td>De BRP en RNI verantwoording zijn goed afgerond, zie behaalde score 2025. Deze is gestegen tov 2024.

<table>
<tr><td>1. ENSIA BRP</td><td>Max te behalen</td><td>Behaald in 2024</td><td>Behaald in 2025</td></tr>
<tr><td>Organisatie beveiliging</td><td>400</td><td>400</td><td>400</td></tr>
<tr><td>Toegang</td><td>400</td><td>400</td><td>400</td></tr>
<tr><td>Naleving</td><td>400</td><td>350</td><td>400</td></tr>
</table>
</td></tr>
<tr><td>Reis-documenten</td><td>De verantwoording van reisdocumenten is goed afgerond, zie de behaalde score 2025. Deze is gestegen tov 2024

<table>
<tr><td>Reisdocumenten</td><td>Max te behalen</td><td>Behaald in 2024</td><td>Behaald in 2025</td></tr>
<tr><td>Organisatie beveiliging</td><td>400</td><td>400</td><td>400</td></tr>
<tr><td>Toegangsbeveiliging</td><td>400</td><td>400</td><td>400</td></tr>
<tr><td>Naleving</td><td>400</td><td>360</td><td>370</td></tr>
</table>
</td></tr>
<tr><td>BAG</td><td>BAG terugblik op 2025:
Van een aantal verblijfsobjecten verschilt de "gebruiksoppervlakte" tussen de BAG en de WOZ-registratie. Om die verschillen in bulk op te lossen, heeft in 2025 een analyse plaats gevonden.
Bij 216 panden is gecontroleerd of aan die panden een bestaand verblijfsobject gekoppeld moest worden. Wanneer dat nodig was, is dat uitgevoerd.
Voor ongeveer 15 nevenadressen waarop mensen ingeschreven waren in de BRP zijn onderzoeken gestart. Voor 11 daarvan is een inspectieverzoek bij de bouwinspecteurs uitgezet. In 2025 zijn 6 onderzoeken afgerond.
De Dienst Toeslagen van het Ministerie van Financiën is een onderzoek gestart om na te gaan of ze dezelfde regels als de BAG kunnen hanteren. De Dienst heeft een lijst van 385 “ontbrekende adressen” met de gemeente gedeeld met de vraag ze te onderzoeken. De lijst is grotendeels onderzocht maar een terugkoppeling aan de Rijksbelastingdienst heeft nog niet plaats gevonden. In december is de opdracht intern besproken met VTH, WOZ en JZ en is besloten een Memorandum te schrijven voor een PO met de wethouder.
BAG vooruitblik op 2026:
Van een aantal verblijfsobjecten verschilt de "gebruiksoppervlakte" tussen de BAG en de WOZ-registratie. In 2026 wordt verder onderzocht of er een nieuw proces ingericht kan worden. De inzet is om die verschillen in bulk op te lossen.
De Dienst Toeslagen heeft meldingen gemaakt van 385 mogelijk ontbrekende verblijfsobjecten. In 2026 wordt gekeken of in een projectvorm meldingen afgehandeld kunnen worden. Hiervoor wordt een memorandum voor een PO met de wethouder opgesteld.
Per 1 januari 2025 is een nieuw VTH-systeem ingevoerd waarbij de werkvoorraad voor de BAG handmatig aangemaakt moet worden; dit is foutgevoeliger. De betrokken medewerkers worden hiervoor extra geïnstrueerd om de termijnen wel te halen. Ook wordt een monitoring gestart om te beoordelen of we werkvoorraad missen.</td></tr>
<tr><td>BGT</td><td>BGT terugblik op 2025
Het actualiseren, up-to-date houden van de BGT gaat goed. De koppelvlakken met BOR, BAG en de kwaliteitsdashboards helpen daar goed bij mee. Het is de bedoeling, dat in de toekomst steeds meer BOR-thema’s met een GEO-component een koppelvlak hebben met de BGT.
Vooruitblik op 2026
Voor 2026 staat helaas noodgedwongen de aanbesteding van de BGT-applicatie op de planning. 1 Januari 2027 moet de nieuwe BGT-applicatie zijn geïmplementeerd. Het actualisatieproces van de BGT zal dan op bepaalde punten moeten worden aangepast.</td></tr>
</table>

BRO	**BRO terugblik op 2025** Wegens gezondheidsredenen van de BRO-coördinator heeft de BRO minder aandacht gekregen dan voorgaande jaren. Door het ontbreken van een beleidsdocument is het lastig om de juiste mensen in beweging te krijgen. **BRO vooruitblik op 2025** Er wordt op hoger niveau gekeken hoe we het beste een beleidsdocument kunnen opstellen en uitrollen binnen de organisatie. In welke vorm en hoedanigheid is voor nu nog onbekend.

Resultaat op het vlak van privacy

Afhandeling klachten

In 2025 zijn er in totaal 2 klachten ingediend door burgers betreffende een onrechtmatige verwerking van hun persoonsgegevens. Dit is stabiel ten opzichte van 2023 en 2024 (laatste keer 8).

Rechten van betrokkenen

In 2025 zijn er bij de gemeente 16 verzoeken ingediend. Dit zijn allemaal inzageverzoeken. Het aantal van 16 is een behoorlijke daling ten opzichte van het aantal verzoeken in 2024 (28). Voor BRP-inzageverzoeken is een apart formulier gemaakt, deze komen dus niet binnen als een AVG-verzoek.

Uitvoering van de plannen van aanpak ‘elke afdeling privacy-proof’

Het traject mijn ‘afdeling AVG-proof’ is eind 2024 eindelijk door alle afdelingen afgerond. Dit wil niet zeggen dat de afdelingen hiermee volledig aan de AVG voldoen. Wél dat alle afdelingen een ‘privacy risico scan’ hebben gemaakt en daarmee inzicht hebben in welke acties nog ondernomen moeten worden. De voorwaarden voor het naleven van de AVG zijn daarmee gecreëerd (realisatie ‘opzet’). Vanaf 2025 dient de organisatie (conform vastgesteld volwassenheidsniveau) een beweging te maken van ‘opzet’, naar ‘bestaan’ en tenslotte naar ‘werking’ volgens de AVG. Hierop is de toetsing van 2025 gericht. Dit komt tot uitdrukking in het jaarverslag van de FG over 2025, welke later in 2026 beschikbaar komt.

DPIA als continu bijstuurproces

Het instrument DPIA (waarmee de privacy risico`s van een gegevensverwerking in kaart worden gebracht) wordt steeds beter ingezet. Door middel van de uitvraag voor het controlplan, worden de maatregelen die in de DPIA’s genoemd zijn getoetst op naleving. Daarmee is de controle van DPIA’s een blijvend onderdeel van de verantwoordingsplicht geworden. In 2025 zijn in totaal 20 DPIA’s afgerond met oordeel/advies van de FG op verschillende soorten risicovolle gegevensverwerkingen. Eind december 2025 waren er 41 DPIA’s onder beheer.

Naleving Wet politiegegevens (Wpg)

Uit artikel 33 van de Wpg volgt een auditplicht voor verwerkingsverantwoordelijken van politiegegevens. Als gemeente vallen wij daar ook onder, wat betekent dat er elk jaar een audit wordt gedaan op het gebied van de Wpg en eens in de vier jaar door een externe auditeur. In 2025 heeft deze (verplichte) externe audit op naleving van de Wpg plaatsgevonden over de controleperiode van 1 januari 2022 t/m 31 december 2024. Daarbij wordt de gemeente getoetst op hoe wij omgaan met persoonsgegevens die worden gebruikt in politietaken zoals opsporing. De resultaten hiervan zijn verstuurd aan de Autoriteit Persoonsgegevens (AP).

Inmiddels is er een traject gestart om de noodzakelijke verbeteringen in dit traject op te pakken en vorm te geven. De conclusies hiervan en de voorgenomen acties zullen benoemd worden in het jaarverslag van de FG (later in 2026). In 2026 zal ook een her controle door de externe auditeur plaatsvinden.

Naleving AVG

In het najaar 2025 heeft de Functionaris voor de gegevensbescherming, zoals inmiddels gebruikelijk, een schriftelijke uitvraag (interne controle) gedaan naar de naleving van de AVG door de gemeentelijke

organisatie. De afdelingen hebben in januari 2026 de stukken hiervoor aangeleverd. Het analyseren van de aangeleverde documentatie en het opstellen van het jaarverslag vindt, net als in voorgaande jaren, plaats in de periode februari t/m mei. Object van onderzoek is:

- voortgang ‘Mijn afdeling AVG-proof’;
- registraties datalekken, klachten en incidenten zoals opgenomen in de CyberManager;
- naleving van afspraken gemaakt in de DPIA en in de beoordelingen daarvan;
- naleving van privacy protocollen;
- naleving van de afspraken gemaakt in verwerkersovereenkomsten.
- Resultaten hiervan komen terug in het jaarverslag van de FG over 2025, welke later in mei 2026 beschikbaar komt.

3.1.1 iRvN

In 2025 heeft iRvN voor de tweede maal een onafhankelijk assurance-onderzoek conform Richtlijn 3000D (TPM) laten uitvoeren op een specifiek deel van de BIO 2.0. De selectie van de getoetste normen is in nauwe afstemming met de deelnemers tot stand gekomen.
De audit richtte zich op de processen, procedures en onderliggende systemen die primair relevant zijn voor de dienstverlening van iRvN. Binnen de scope vielen de volgende domeinen: Back-up & restore, technische kwetsbaarheden, change Management, cryptografie, security Incident Management, gebruikersauthenticatie, autorisatiemanagement en logging & Monitoring. De beoordeling had betrekking op het beheer van centrale ICT-hardware, applicaties en basis- en kernregistraties ten behoeve van onze afnemers.
De auditor heeft de geschiktheid, opzet, het bestaan en de werking van de getroffen beheersmaatregelen getoetst aan de overeengekomen normen. De uitkomsten van het onderzoek zijn positief. Voor de genoemde processen is vastgesteld dat de maatregelen adequaat zijn ingericht, maar ook aantoonbaar functioneren.
Wel zijn enkele verbeterpunten geïdentificeerd. Het belangrijkste aandachtspunt betreft de periodieke review van accounts met verhoogde rechten. Hoewel de controle op toegangsrechten feitelijk plaatsvindt, is de vastlegging hiervan onvoldoende. Daardoor zijn uitgevoerde controles niet altijd navolgbaar en vindt hierover geen structurele managementrapportage plaats.
In vervolg hierop zet iRvN in op verdere professionalisering van haar vastlegging en rapportage.
.

4.2.2 Overige samenwerkingen

Afspraken met externe partijen

Om haar doelstellingen op een zo effectief en efficiënt mogelijke manier te kunnen behalen maakt de gemeente voor een aantal taken gebruik van samenwerkingsverbanden of externe relaties. Om deze samenwerkingen tot een succes te maken worden data en informatie uitgewisseld. Dit betekent dat er afspraken gemaakt moeten worden die vastgelegd worden in dienstverleningsovereenkomsten, privacy protocollen en verwerkersovereenkomsten. Met het omzetten van de NIS2 richtlijn in de BIO2 en de opname hiervan in de Cyberbeveiligingswet (Cbw) neemt de verantwoordelijkheid voor het beheren van cyberveiligheidsrisico`s in toeleveringsketens en leveranciersrelaties toe. Op basis van risico-inschattingen zullen wij verwerkers van gegevens intensiever beoordelen op hun verantwoordingsplicht vanuit de privacy en informatiebeveiligingswetgeving. De FG en de CISO besteden in het controlplan extra aandacht aan het opvolgen van leveranciers- en verwerkersovereenkomsten. De CISO adviseert over passende maatregelen in de inkoopfase en de invulling van de gesprekken met leveranciers. Leveranciersmanagement (het maken en opvolgen van afspraken met leveranciers) is een punt van aandacht in het bevragen van proceseigenaren.

In het kader van het gastheerschap vult de gemeente Nijmegen voor de Meervoudige Gemeenschappelijke Regeling (MGR) een aantal maatregelen in. Het betreft maatregelen die te maken hebben met voorzieningen op het gebied van facilitair, personeel en juridische zaken. Denk daarbij aan maatregelen op het vlak van contractbeheer, toegangsbeleid en telewerken. De MGR heeft een eigen verantwoordelijkheid voor hun verwerkingen en kan gemeente Nijmegen bevragen op de voortgang van de implementatie van maatregelen die wij als gastheer voor onze rekening nemen.

Het Werkbedrijf Rijk van Nijmegen (WBRN) gebruikt een eigen Suwinet aansluiting om client gegevens op te zoeken voor haar werkzaamheden in het uitvoeren van de participatiewet. De IT-auditor geeft voor de regiogemeenten die deelnemen aan de WBRN een verklaring af over het gebruik van de Suwinet aansluiting volgens de geldende normen. Daarnaast rapporteert de WBRN in het kader van verwerkingsrelaties zoals die bijvoorbeeld geldt voor de “Doe je mee” regeling.

5. Vooruitblik

5.1 Aanbevelingen uit externe toetsing

De externe controle door de accountant en de IT-audit in het kader van ENSIA leveren elk jaar aanbevelingen op die we meenemen in de ontwikkelingen van dat jaar. Dit naast aanbevelingen die uit andere onderzoeken naar voren komen.

Aanbevelingen van de accountant

De accountant beveelt aan om periodiek te inventariseren wat de gerealiseerde voortgang op de ambities is en passende bestuurlijke keuzes te maken om tijdig op alle onderdelen in control te komen. Gemeente Nijmegen ligt op een aantal onderdelen op schema, maar het normenkader waar aan voldaan moet worden heeft zich ondertussen verder ontwikkeld in de BIO2. Dit betekent dat het normenkader groeit en in reikwijdte toeneemt. Het is belangrijk om blijvend in dit onderdeel te investeren omdat de ontwikkelingen op dit domein elkaar snel opvolgen en er nog een hoop te doen is.

Onderstaand vindt u een overzicht van de IT Roadmap. Daarin worden een viertal gebieden aangegeven waarin maatregelen worden geïmplementeerd. In de Roadmap van 2025 zijn toegevoegd maatregelen op het vlak van het gebruik van bedrijfsmiddelen en het ISMS. Deze maatregelen worden beschreven in deze rapportage en in de eerder genoemde raadsinformatiebrieven.

Figuur 2 IT Roadmap

Aanbevelingen van de IT-auditor (ENSIA)

Bij de controle ten behoeve van het rapport dat de IT-auditor (Accoris) afgeeft bij de collegeverklaring ENSIA zijn er geen afwijkingen geconstateerd als het gaat om opzet, bestaan en werking voor de relevante Suwinet normen. Bij de beoordeling van de DigiD normen is geconstateerd dat we aan de normen voor opzet en bestaan voldoen. Aan de normen voor werking voldoen we bij een van de vier aansluitingen niet op dit moment. Op dit moment wordt een herstel plan uitgevoerd. Met betrekking tot de controle zijn er een aantal aandachtspunten voor 2025.

- Continuïteit van de controle werkzaamheden (overdracht en verdeling van werkzaamheden) moet geborgd zijn om jaar naar jaar ons proces op orde te hebben.
- De opbouw van controle dossiers moet op een centrale plek beter bewaakt worden zodat de werking continue aangetoond kan worden.
- Het is van belang leveranciers aan te spreken op het tijdig aanleveren van de afgesproken stukken.

5.2 Komend jaar

Gezamenlijk stippelen Stadscontrol en de adviseurs van Ontwikkeling I&A (Informatie & Automatisering) het groeipad uit voor de organisatie naar meer volwassenheid. Op het moment dat de door de toenemende reikwijdte van regelgeving de druk toeneemt terwijl de middelen beperkt blijven is het nodig weloverwogen keuzes te benoemen en voor te leggen aan de juiste gremia.

De omzetting van de Europese NIS2 richtlijn naar Nederlandse wetgeving via de Cbw zal in 2026 afgerond worden. Gemeenten zijn als essentieel aangemerkt dus een intensivering op het vlak van continuïteit, scholing en de beveiliging van operationele technologie is zeker aan de orde. In die context wordt de opvolger van de BIO, de BIO2 wettelijk verplicht via het Cyberbeveiligingsbesluit. Hieruit vloeien extra maatregelen voort die we zullen gaan volgen en implementeren via de CyberManager. Daarnaast zijn er meer Europese richtlijnen die gemeenten raken. Ook de effecten van AI op de ontwikkeling van algoritmen en de onzekerheid die ontstaat door de onstabiele geopolitieke situatie zullen gevolgen hebben voor de keuzes die gemeente Nijmegen zal maken.

In 2026 staan de volgende stappen gepland:

- Het vormen van het team IB en P dat aan de slag gaat met de opdrachten die nodig zijn om gemeenten Nijmegen, over een periode van een aantal jaar, naar volwassenheidsniveau 3 te brengen op het gebied van informatiebeveiliging en privacy.
- Starten met het implementeren van de uitwerking van ons informatiebeveiligingsbeleid.
- Met het iVeiligheidsteam en de contractmanager aan de slag gaan met leveranciersmanagement. Dit gebeurt door middel van het onderzoeken van afspraken, het voeren van evaluatiegesprekken en het bijstellen waar nodig.
- Het vergroten van de weerbaarheid van gemeente Nijmegen door het verbeteren van de continuïteitsplannen op alle niveaus en het inrichten en oefenen van de bijbehorende processen.
- De Barobeter inzetten in de prestatiedialogen om regelmatig op afdelingsniveau de aandacht op informatiebeveiliging te vestigen
- Alle medewerkers volgen de jaarlijkse herhaling informatiebeveiliging en privacy eLearning. Er wordt gestart met het maken van eigen eLearning modules die voor meer relevantie en flexibiliteit zullen zorgen.
- Bijzondere aandacht voor het risicobewustzijn van het bestuur en het management op het vlak van informatiebeveiliging en privacy.
- Investeren op het vlak van iBewustzijn, met name als het gaat om het meten van vooruitgang in de afdelingen.

- Inventariseren OT (operationele technologie) t.b.v. het voldoen aan de Cbw.
- Technische maatregelen uit de accountantscontrole/ENSIA/Cbw.
- Organisatorische maatregelen in het kader van de accountantscontrole/ENSIA/Cbw.

De NIS2-richtlijn is gericht op de verbetering van de digitale weerbaarheid van essentiële diensten en organisaties in Europa. Voor gemeenten geldt een wettelijke verplichting om gegevens aan te leveren voor het entiteitenregister. Dit is in 2025 gebeurd. Het NCSC kan op basis van de gegevens gericht producten en diensten aanbieden om de weerbaarheid van de gemeente te vergroten. Ook is het NCSC in staat om in het geval van incidenten gemakkelijk contact op te nemen.

Het controlplan van de FG en van de CISO zal onder andere gevoed worden door informatie over de implementatie status van de normen zoals dat is opgebouwd in de CyberManager. Daarnaast zal gebruik gemaakt worden van informatie verkregen van de afdelingen die door hen wordt aangeleverd in de uitvraag van FG en CISO.

Als het gaat om de samenwerking met iRvN dan laat het informatiebeveiligingsplan van de MGR (waar iRvN onderdeel van is) zien hoe zij de gemeente Nijmegen ondersteunt door het implementeren van maatregelen voor de kritische systemen en het nemen van generieke maatregelen om de IT omgeving voorspelbaarder te maken. Het belangrijkste aandachtspunt voor het komende jaar betreft de periodieke review van accounts met verhoogde rechten. Hoewel de controle op toegangsrechten feitelijk plaatsvindt, is de vastlegging hiervan onvoldoende. Daardoor zijn uitgevoerde controles niet altijd navolgbaar en vindt hierover geen structurele managementrapportage plaats.
In vervolg hierop zet iRvN in op verdere professionalisering van haar vastlegging en rapportage.

Bijlage: achtergrond & begrippen

Wat is Informatiebeveiliging

Informatiebeveiliging is de verzamelnaam voor een pakket aan maatregelen, die getroffen worden om de betrouwbaarheid van processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te garanderen, en te beschermen tegen bedreigingen. Het begrip 'informatiebeveiliging' heeft te maken met:

- *beschikbaarheid / continuïteit*: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- *exclusiviteit / vertrouwelijkheid:* het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- *integriteit / betrouwbaarheid:* het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

  Er is ook een sterke samenhang met de archiefwet. In het Informatiebeveiligingsbeleid van gemeente Nijmegen wordt daarom in deze context ook verwezen naar duurzame opslag:
- *duurzaamheid:* het zorg dragen voor de tijdige archivering van informatie zodat ook in de toekomst verantwoording en geschiedschrijving mogelijk blijft. Dit aspect komt voort uit de archiefwet.

Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente. Toegankelijke en betrouwbare informatie is essentieel voor een gemeente. Gemeente Nijmegen wil zich verantwoordelijk gedragen, aanspreekbaar en servicegericht zijn. Gemeente Nijmegen wil bovenal transparant en proactief verantwoording afleggen aan burgers en raadsleden en met minimale middelen maximale resultaten behalen. De bescherming van waardevolle informatie is datgene waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden. Het informatiebeveiligingsbeleid van gemeente Nijmegen is eind 2025 geactualiseerd zodat het de BIO2 volgt.

Wat is Privacy

De Algemene verordening gegevensbescherming (AVG) is mei 2018 van kracht geworden. Er is in 2017 een Functionaris Gegevensbescherming (FG) aangesteld alsook een Privacy Officer (PO). Het privacybeleid van gemeente Nijmegen is in 2024 geactualiseerd en legt de nadruk op:

- Transparantie
- De ethische kant van privacy
- Het beschermen van persoonsgegevens en het belang daarvan
- De afweging tussen dienstverlening en het beschermen van persoonsgegevens
- Het respecteren van de wettelijke kaders en de bescherming van de persoonlijke levenssfeer van inwoners
- Privacy by design

Wat zijn de kaders & hoe toetsen we daarop?

De AVG spreekt van het beschermen van persoonsgegevens met afdoende technische en organisatorische maatregelen. De BIO2 is het normenkader dat voor een gemeente (overheid) bepaalt of technische en organisatorische maatregelen afdoende zijn.

De standaard voor het toetsen van deze normen kaders is geformuleerd door de beroepsvereniging van register auditors in Nederland, de NOREA.

Deze normenkaders en de toetsing van de toepassing daarvan door middel van de vragen die geformuleerd zijn door de NOREA zijn de basis voor de inhoud van ISMS en PIMS systemen zoals de CyberManager die door gemeente Nijmegen gebruikt wordt.

Waar liggen de bevoegdheden?

De functie van CISO is verplicht gesteld via de BIO. Met de invoering van de Cbw en de bijbehorende ministeriele regelingen wordt via de ministeriele regeling van Binnenlandse zaken de BIO2 nu ook voor gemeenten wettelijk verplicht gesteld.

De CISO is verantwoordelijk voor het beveiligen van de informatie om in de beschikbaarheid, integriteit en vertrouwelijkheid te kunnen voorzien die nodig is voor de dienstverlening. De CISO heeft een derdelijns toetsende rol maar geeft ook advies.

De functie van FG is verplicht gesteld (voor een gemeente) via de AVG. Is verantwoordelijk voor de bescherming van de privacy van burgers en medewerkers van gemeente Nijmegen. Het accent van de derdelijns FG rol ligt meer op toetsing en minder bij advies.

In het normenkader van de BIO2 is het College van B&W eindverantwoordelijk voor de risico`s die aanvaard worden en de maatregelen die getroffen worden. Deze verantwoordelijkheid begint bij de eigenaren in de lijn die voor hun processen bepalen welke keuzes zij willen maken bij het bereiken van hun doelen. Aangezien het college van B&W eindverantwoordelijk is zijn zij uiteindelijk de enigen die risico`s kunnen accepteren.

Afkortingen

Afkorting	Uitleg
AP	Autoriteit Persoonsgegevens. Toezichthouder op de bescherming van persoonsgegevens in Nederland
AVG	Algemene Verordening Gegevensbescherming. In werking getreden op 25 mei 2018. Sinds dat moment geldt in de gehele Europese Unie dezelfde privacywetgeving.
AMvB	Algemene Maatregel van Bestuur die een nadere uitwerking bevat van (in dit geval) de Cbw. Hierin worden de verplichtingen zoals de zorgplicht en de scholingsverplichting verder geduid.
BAG	Basisregistratie Adressen en Gebouwen bevat gemeentelijke basisgegevens van alle adressen en gebouwen in een gemeente.
BGT	Basisregistratie Grootschalige Topografie is een digitale kaart van Nederland waarop gebouwen, wegen, waterlopen, terreinen en spoorlijnen eenduidig zijn vastgelegd.
BIO	Baseline Informatiebeveiliging Overheid. Van kracht sinds 1 januari 2020. Een gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid gebaseerd op de internationaal erkende en actuele ISO-normatiek. In verband met de inwerkingtreding van de Europese Netwerk- en informatiebeveiligingsrichtlijn (NIS2) is begin 2024 besloten de oplevering van de BIO2 te koppelen aan de Cyberbeveiligingswet (Cbw). Dat is de wetgeving die uit de NIS2 volgt. Volgens de huidige planning wordt de BIO2 in Q3 van 2025 wettelijk verankerd onder de nadere regelgeving van de Cbw.

Afkorting	Uitleg
BRO	Basisregistratie Ondergrond bevat gegevens over geologische en bodemkundige opbouw van de Nederlandse ondergrond.
BRP	Basisregistratie Personen bevat persoonsgegevens van inwoners van Nederland en van personen die Nederland hebben verlaten
Cbw	Cyberbeveiligingswet (naar verwachting van kracht najaar 2025). De implementatie van de NIS2 richtlijn in Nederland.
CISO	Chief Information Security Officer verantwoordelijk voor het informatiebeveiligingsbeleid. Dit betreft zowel het implementeren van beleid als het toezicht houden op de uitvoering ervan
CMM	Capability Maturity Model. Amerikaans model dat gebruikt wordt om het stadium van volwassenheid van een proces (organisatie) uit te drukken.
DigiD	Digitale Identiteit s een systeem waarmee Nederlandse overheden op internet iemands identiteit kunnen verifiëren, een soort digitaal paspoort voor overheidsinstanties.
DPIA	Data Protection Impact Assessement oftewel gegevensbeschermingseffectbeoordeling is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.
ENSIA	Eenduidige Normatiek Single Information Audit heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door toezicht te bundelen en aan te sluiten op de gemeentelijke P&C cyclus
EWS	Early Warning System. Systeem voor het analyseren van log informatie en het voeden van het SIEM systeem
FG	Functionaris voor de Gegevensbescherming is een onafhankelijke deskundige op het gebied van gegevensbescherming die binnen een organisatie (of een aantal organisaties) wordt aangewezen om te adviseren, informeren en toezicht te houden op de naleving van de AVG.
GITC	General IT Controls zijn IT beheersmaatregelen (beleid en processen) die betrekking hebben op het beheer van alle systemen.
ISMS	Information Security Management System is een verzameling van alle (onderling gerelateerde) informatiebeveiligingselementen van een organisatie die ervoor moet zorgen dat beleid, procedures en doelstellingen samenhangend kunnen worden gecreëerd, geïmplementeerd, gecommuniceerd en geëvalueerd om de algehele veiligheid van de informatie van een organisatie beter te garanderen.
ISO	Information Security Officer. Degene die de eerste lijn adviseert en (mede) beleid ontwikkelt op het vlak van informatiebeveiliging.
MDM	Mobile device management. Het (op afstand) beheren van mobiele apparaten zoals laptops, smartphones en tablets.
NAFIN	Netherlands Armed Forces Integrated Network. Het netwerk dat vitale onderdelen van de rijksoverheid veilig en vertrouwelijk met elkaar laat communiceren.
NIS2	Europese richtlijn op het vlak van informatiebeveiliging. In Nederland omgezet in de Cbw.
NOREA	Nederlandse Orde van Register EDP-Auditors is de beroepsorganisatie van IT-auditors in Nederland.
OSO	Operational Security Officer. Degene die de toepassing van informatiebeveiliging in de eerste lijn tot aandachtsgebied heeft.
PIMS	Privacy Information Management System ondersteunt in het managen van een aantal registraties (Datalekken, Verwerkingsregister, Data Protection Impact Assessments (DPIAs), Risico’s, Maatregelen, Verzoeken, Toestemmingen) om AVG compliant te zijn.

Afkorting	Uitleg
PO	Privacy Officer is degene die de eerste lijn van advies dient, tot op casus niveau, en (mede) beleid ontwikkelt op het vlak van privacy en het voldoen aan de AVG.
RMC	Regionale Meld- en Coördinatiefunctie voortijdig schoolverlaten richt zich op jongeren tussen 18 en 23 jaar, met het doel voorwaarden te scheppen zodat zij een passende onderwijs- en/of arbeidsmarktpositie kunnen bereiken.
SIEM	Security Incident and Event Monitoring. Systeem voor het analyseren van log informatie vanuit verschillende gemeenten zodat informatie over gebeurtenissen snel gedeeld kan worden.
SUWI	Wet Structuur Uitvoering Werk en Inkomen. Suwinet is de elektronische infrastructuur gebruikt voor de uitvoering van de taken in het kader van de wet SUWI, en sommige ook niet-SUWI taken.
TPM	Third Party Memorandum (derdenverklaring) is een verklaring afgelegd door een onafhankelijke derde partij (auditor) met betrekking tot de kwaliteit van de ICT dienstverlening van de eerste partij (leverancier) ten behoeve van de tweede partij (klant).