Rapportage Informatiebeveiliging 2024

Tijd om te kiezen

CISO gemeente Nijmegen, december 2024

Informatiebeveiliging 2024

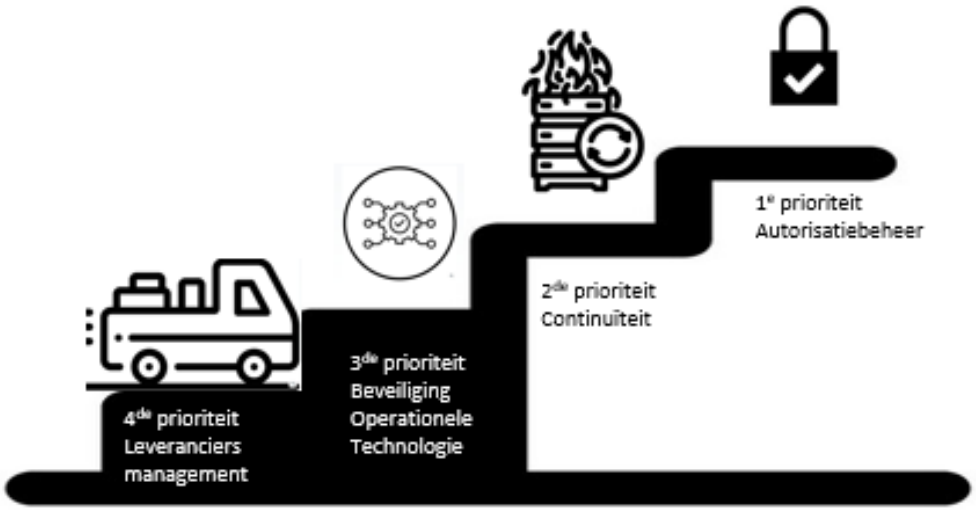
In getallen

96 incidenten,
10 datalekken

30 inzageverzoeken

101 DPIA`s
onder beheer

Geïmplementeerde
maatregelen 99%



Spotlight voor 2025

1e prioriteit
Beveilging
Operationele
Technologie

2de prioriteit
Leveranciers
Management

Voldoen aan
Cyberbeveiligingswet

Inhoudsopgave

1. Doel & wettelijk kader

Doel

In dit rapport informeert de Chief Information Security Officer van gemeente Nijmegen u over de ontwikkeling van de informatiebeveiliging bij de gemeente Nijmegen. We blikken terug op het afgelopen jaar en kijken vooruit naar de ontwikkelingen in 2025 en de jaren daarna. Dit rapport is onderdeel van de regelgeving 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. De voorliggende rapportage Informatiebeveiliging en Privacy is onderdeel van onze onderbouwing bij de collegeverklaring ENSIA, waarin het college aangeeft in welke mate gemeente Nijmegen voor DigiD, Reisdocumenten, de BRP en Suwinet aan de eisen voldoet. 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

Het eerste deel van dit rapport 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 en de langere termijn.

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 nieuwe wetgeving 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 zal worden.

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. Risico gestuurd werken zorgt ervoor dat dit zo efficiënt mogelijk wordt ingevuld. Met de invoering van de Cyberbeveiligingswet (de implementatie van de Europese NIS2 richtlijn in Nederland) zal aanleiding zijn om risicomanagement op steeds meer vlakken worden 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?

Terugkijkend naar vorig jaar, waren de vooraf geformuleerde doelen als volgt:

In 2024 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.

Gemeente Nijmegen gebruikt de CyberManager applicatie om de implementatie van maatregelen en de beoordeling van risico`s te beheren en te toetsen. De inhoud van de CyberManager wordt verder onder handen genomen om de **verantwoording** richting auditor en bestuur te verbeteren.

In 2024 gaat het **iVeiligheidsteam** aan de slag met het controleren van de autorisaties en de terugkoppeling hier over richting de CISO.

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. Een onderdeel van deze plannen is een eLearning module voor de gehele organisatie en een interventie tijdens Lets Connect. Om de effectiviteit van deze interventies beter te kunnen bepalen hebben we Hogeschool Saxion gevraagd om een onderzoek naar het iBewustzijn binnen de gemeente en het ontwikkelen van een instrument om deze op een efficiënte manier inzichtelijk te maken.

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. De controlerondes zijn bij een aantal afdelingen af. Bij andere afdelingen wordt eraan gewerkt.
- Het continuïteitsproject heeft voor alle afdelingen continuïteitsplannen opgeleverd. De laatste continuïteitsplannen worden begin 2025 geoefend.
- Het iBewustzijn communicatieplan is uitgevoerd. In 2024 omvatte dit onder andere een phishing campagne, een iBewustzijnsonderzoek door Hogeschool Saxion en inzet op het gebied van het gebruik van Zivver.
- De herhalings eLearning voor Informatiebeveiliging en Privacy is op Studytube beschikbaar gesteld. 60% van de medewerkers heeft deze gevolgd.
- Met de raad is het gesprek gevoerd over geschikte KPI`s om op te sturen. In 2024 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. De evaluatie met de studenten en iRvN was positief.
- iRvN is aan de slag met het beveiligingsproject evenals het traject naar certificering op basis van de BIO. Een achttal processen is getoetst.

- De CISO heeft in 2024 haar controleplan uitgevoerd en hier over gerapporteerd aan het GMT en de directie. Dit controleplan had betrekking op de processen van autoriseren, het afhandelen van incidenten en wijzigingen.
- Het team Stadscontrol ziet toe op het opvolgen van bevindingen en het nemen van de juiste maatregelen. Dit gebeurt door het voeren van adviesgesprekken, het begeleiden van prestatiedialogen en het toetsen van maatregelen, bijvoorbeeld door het uitvoeren van interne audits met behulp van de CyberManager en het uitvragen door de FG en de CISO.

Opvallende zaken

In het afgelopen jaar waren er een aantal verstoringen in de Microsoft omgeving waar wij soms in meer en op andere momenten in mindere mate last van hadden. Een voorbeeld hier van is de verstoring die wij ondervonden in het gebruik van multi-factor authenticatie (MFA). Daarnaast was er bijvoorbeeld de storing in het Nafin defensienetwerk die ook ons raakte omdat niet alleen de rijksoverheid maar ook veel gemeenten dit netwerk gebruiken voor vertrouwelijke communicatie. Het bewijst het belang van de acties die wij aan het uitvoeren zijn op het vlak van continuïteit. Het moet voor ons mogelijk zijn om de **kritische bedrijfsprocessen uit te blijven voeren op het moment dat de IT infrastructuur (deels) niet beschikbaar is**. Dit lukt steeds beter.

In 2024 zijn er 96 beveiligingsincidenten gemeld. Daarvan waren 81 meldingen intern en 15 meldingen extern. Er waren 10 datalekken. Van de datalekken zijn er 9 bij de Autoriteit Persoonsgegevens (AP) gemeld. 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.

<u>Incidenten per afdeling:</u>
Financiën: 3
Stadsrealisatie: 2
Stadsbeheer: 7
Stadsontwikkeling: 9 waarvan 1 gemeld datalek.
Inkomen, Zorg en Leerrecht: 13
Personeel Informatie Facilitair: 10
Publiekszaken: 16 waarvan 7 gemelde datalekken.
Bestuur en Management: 3
Veiligheid, Juridische zaken en Bestuursondersteuning: 9 waarvan 1 gemeld en 1 niet gemeld datalek.
Maatschappelijke Ontwikkeling: 7
Vastgoed, Sport en Accommodaties: 5
Extern: 6
iRvN: 6

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

	2022	2023	2024
Incidenten	56	84	96
Waarvan datalekken	21	22	10
Waarvan gemeld	6	13	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 2024 binnen de gestelde termijn een WOO-verzoek met betrekking tot de geregistreerde datalekken in het jaar 2021 is afgehandeld.

Gebruik van de CyberManager

Ook in 2024 hebben we Samoerai (de IT dienstverlener die de implementatie van CyberManager in Nijmegen al een aantal jaren begeleidt) gevraagd om de opvolging van de taken in Cybermanager te organiseren. Daarnaast zijn er een aantal opschoonacties uitgevoerd waardoor de kwaliteit van de verantwoording verbeterd is. Aansluitend hebben we een overzicht gekregen van de status door in de CyberManager een interne audit uit te voeren op de verplichte BIO overheidsmaatregelen.
In de CyberManager is nu 99% 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.
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 continuïteitsplannen

In de eerste helft van 2023 is onder leiding van de CISO het Netwerkteam I-veiligheid georganiseerd. Dit periodiek bijeenkomende gremium geeft de afdelingen meer steun bij het maken van de gevraagde plannen door de mogelijkheid te bieden om ervaringen te delen. Dat heeft ertoe geleid dat een flink aantal plannen nagenoeg gereed zijn, maar nog niet alle. In november zijn van 10 afdelingen de continuïteitsplannen resp. opgeleverde stukken geanalyseerd. In 2024 zijn de afdelingen aan de slag gegaan met het oefenen van de continuïteitsplannen en het bijstellen ervan. Naar verwachting zullen de meeste afdelingen hebben kunnen oefenen in 2024. Met de resultaten van de oefeningen zullen in 2025 de continuïteitsplannen van de afdelingen maar ook het gemeente brede continuïteitsplan worden bijgewerkt.

Resultaten uit NYMACON

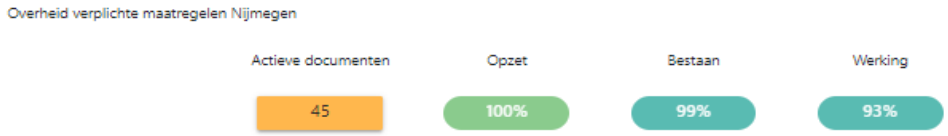
In november 2024 vond in Waalhalla het NYMACON evenement plaats. Gemeente Nijmegen was gastheer voor dit regionale evenement. Studenten van de RU, maar ook andere universiteiten probeerden een aantal door de regio beschikbaar gestelde objecten te hacken, zoals een robotstofzuiger, maar ook een kiosk PC en een webformulier. Met name de robotstofzuiger kon op grote belangstelling rekenen. Naast dat het een aantal studenten lukte om gebruik te maken van kwetsbaarheden in de objecten levert het evenement ook een impuls aan de samenwerking met de universiteit en het bedrijfsleven in Nijmegen. 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.

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. De actieve documenten die worden benoemd behoren bij verplichte overheidsmaatregelen die getoetst zijn in de interne audit.



Figuur 1: opzet bestaan en werking in CM

2. Identificatie van eventuele afwijkingen:
De scores voor opzet en bestaan zijn nagenoeg 100%, voor werking nog 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 (eerste, tweede en derde 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 processen die niet tot de meest kritische, maar wel gevoelige, processen behoren. Ook deze processen maken ons kwetsbaar.

3. Implementatie van verbeteringen:
De taken om bovenstaande tekortkomingen te verbeteren staan in CyberManager en zijn toegewezen aan de verantwoordelijke gebruikers. 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 coördinator dan wel de proceseigenaar van afdelingen, bijvoorbeeld in de prestatiedialoog. Deze 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 bedrijfsvoeringsaspecten waaronder informatiebeveiliging, geeft meer inzicht en aanleiding tot gesprek. In het kader van de verantwoording over werking van 2024 heeft de CISO een uitvraag met steekproef uitgevoerd die in 2025 zal worden gecombineerd met controlplan van de FG tot een gecombineerd controlplan FG en CISO.

5. Onafhankelijke beoordeling:
De externe beoordeling van de informatiebeveiligingsmaatregelen vindt elk jaar op 2 manieren plaats: via de IT audit van de accountant in de context van de controle van de jaarrekening, en via de DigiD audit in de context van de ENSIA zelfevaluatie. Beide 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 en de ENSIA auditor heeft met name oog voor de systemen die gekoppeld zijn aan DigiD en Suwinet. Beide pogen een breder beeld te zien vanuit hun perspectief. Met name de accountant slaagt daarin door in 2024 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 2024 is hier voor het eerst gekeken naar werking.

6. In control statement:
Gemeente Nijmegen verklaart voor 96% 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 2024

Op het vlak van Algemene IT beheersmaatregelen en Cybersecurity concludeert de accountant over 2024 dat de gemeente de IT Roadmap gebruikt om te prioriteren in de ontwikkelingen die in gang gezet moeten worden omdat de capaciteit te beperkt is om alles uit te voeren. Daarbij maakt gemeente Nijmegen de juiste keuzes maar het feit dat sommige gebieden (tijdelijk) minder voortgang laten zien is wel aanleiding tot zorg omdat de BIO2 richtlijnen groeien en de reikwijdte hiervan toeneemt. Het realiseren van de ambities uit de Roadmap is een belangrijk onderdeel om aan de BIO2 (en daarmee de Cbw) te kunnen voldoen.

Resultaat van de ENSIA Cyclus 2024

Deze zelfevaluatie, gebaseerd op de BIO, is tijdig afgerond. Alle vragenlijsten zijn ook dit jaar op tijd ingeleverd. Bij de definitieve audit in december was voor het merendeel van de DigiD aansluitingen en voor Suwinet de documentatie compleet. De laatste onderdelen met betrekking tot werking zijn in januari 2025? aangeleverd.

Een kanttekening bij het verantwoordingsproces is dat in 2024 voor het eerst verantwoording is afgelegd over de werking van een 5-tal maatregelen voor de periode juli tot en met december 2024. Een tweetal aanbevelingen komen uit de ENSIA audit naar voren. Voor een aantal applicaties vindt de terugkoppeling van wijzigingen in autorisaties door veranderingen van takenpakket (detachering bijvoorbeeld) nog niet (op tijd) plaats. Daarnaast is er een verbetering van de efficiëntie van het proces van de verbijzonderde controle mogelijk door de data centraal op te slaan.

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. Zo vindt u naast dit rapport ook bijlagen over DigiD, Suwinet, BRP, Reisdocumenten, BAG - BGT – BRO en WOZ bij de collegeverklaring over ENSIA. Een korte samenvatting per stelsel vindt u hier onder.

<table>
<tr><th>Stelsel</th><th>Samenvatting</th></tr>
<tr><td>DigiD</td><td>We voldoen voor alle DigiD aansluitingen aan de geldende normen als het gaat om opzet, bestaan en waar van toepassing werking, van de benodigde maatregelen. In 2024 is het toetsen van werking verplicht geworden.</td></tr>
<tr><td>Suwinet</td><td>Voor Suwinet-inkijk voldoet gemeente Nijmegen aan de geldende normen.</td></tr>
<tr><td>BRP</td><td>De BRP en RNI verantwoording zijn goed afgerond, zie behaalde score 2024.

<table>
<tr><td>1. ENSIA BRP</td><td>Max te behalen</td><td>Behaald in 2023</td><td>Behaald in 2024</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>360</td></tr>
</table></td></tr>
<tr><td>Reis-documenten</td><td>De verantwoording van reisdocumenten is goed afgerond, zie de behaalde score 2024.

<table>
<tr><td>Reisdocumenten</td><td>Max te behalen</td><td>Behaald in 2023</td><td>Behaald in 2024</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 2024:
De proceswijzigingen voor de BAG die nodig waren door de invoering van de Omgevingswet (Ow) en de Wet kwaliteitsborging voor het bouwen (Wkb) zijn succesvol uitgevoerd. Met een ingericht proces wordt bij nieuwe verblijfsobjecten, de gebruiksoppervlakte tussen de BAG en WOZ gelijk gehouden.
In 2024 waren er ongeveer 50 nevenadressen in de bag waarop burgers stonden ingeschreven in de BRP. In 2024 zijn meer dan de helft van die adressen onderzocht en hersteld in de BAG. Met de techniek mutatiesignalering registreren we jaarlijks alle wijzigingen aan panden en nieuwe panden, waarvoor geen omgevingsvergunning is afgegeven. De wet BAG geeft aan dat hierbij van de gemeente wordt verwacht dat de legaliteit van die onvergunde bouwactiviteiten wordt vastgesteld. Dat gebeurt nu niet omdat de Omgevingsdienst Regio Nijmegen (ODRN) daar geen opdracht van de gemeente voor heeft.
BAG vooruitblik op 2025:
Van een aantal verblijfsobjecten verschilt de "gebruiksoppervlakte" tussen de bag en de WOZ-registratie. Om die verschillen in bulk op te lossen, wordt in 2025 een nieuw proces ingericht. De pandcontour van 485 woningen met aangebouwde garages worden gecontroleerd en indien nodig gecorrigeerd.
Bij 216 panden wordt gecontroleerd of er een bestaand verblijfsobject aan gekoppeld moet worden.
Voor ongeveer 15 nevenadressen waarop mensen ingeschreven staan in de BRP zijn onderzoeken gestart. Voor 11 daarvan is een inspectieverzoek bij de bouwinspecteurs van de ODRN uitgezet. Het streven is om de onderzoeken in 2025 af te ronden.
Voor andere nevenadressen (zonder inschrijvingen in de BRP) wordt komende jaren onderzocht of ze voldoen aan de bepalingen uit de Wet BAG. Zo niet, dan worden ze ingetrokken.</td></tr>
<tr><td>BGT</td><td>BGT terugblik op 2024
We hebben alle terugmeldingen binnen 5 dagen in behandeling genomen en binnen 6-18 maanden afgerond. Aan de hand van de kwaliteitsdashboards, Tableau en de koppeling BGT-BOR, waaruit door het jaar heen veel BGT-mutaties naar voren kwamen, hebben we de BGT bijgewerkt. De koppeling BGT-BAG zorgt er doorlopend voor, dat over en weer de beide basisregistraties actueel blijven voor wat betreft de BAG-panden. Verder is de mutatiedetectie weer uitgevoerd en zijn de gevonden mutaties verwerkt.
Vooruitblik op 2025
De BGT werkvoorraad, die wordt gevuld met behulp van het berichtenverkeer BGT-BOR, proberen we zo klein mogelijk te houden, wat de actualiteit ten goede komt. Daarnaast raadplegen we zoveel mogelijk de kwaliteitsdashboards en lossen de genoemde fouten op. Bij Beheer Openbare Ruimte wordt verder gewerkt aan het project “Data op orde” en wanneer er een thema op orde is, nemen we deze op in de BGT. In 2024 is een start gemaakt met de “Revisieverwerking”. In dit project willen we met betrokken partijen de revisietekeningen verbeteren, zodanig, dat deze ook goed genoeg zijn om onder andere de BGT mee te muteren.</td></tr>
<tr><td>BRO</td><td>BRO terugblik op 2024
Voorgenomen verbetermaatregelen zijn niet overal uitgevoerd, vanwege andere prioriteitstelling in combinatie met personele uitval. Er is aandacht voor geweest maar dit heeft niet geleid tot verbetering</td></tr>
</table>

van de borging van het proces rondom de BRO. Ook moet gezegd worden dat sommige processen rondom de BRO goed zijn ingericht. Hier is de BRO goed onder de aandacht en worden de afspraken ook nageleefd.
BRO vooruitblik op 2025
Terugkijkend op voorgaande jaren trekken we de conclusie dat het BRO coördinatorschap anders belegd moet worden in de organisatie. Om het proces goed aan te sturen is er meer doorzettingsmacht nodig in de primaire processen. Tot op heden is het coördinatorschap belegd in een beheerteam in de bedrijfsvoering. De facilitering voor de BRO zal hier blijven liggen, maar het aanjagen en borgen van het proces gaan we voor 2025 dichter op het primaire proces beleggen. De huidige coördinator en primaire processen hebben momenteel een te grote afstand.

Resultaat op het vlak van privacy

Afhandeling klachten

In 2024 zijn er in totaal 8 klachten ingediend door burgers betreffende een onrechtmatige verwerking van hun persoonsgegevens. Dit is stabiel ten opzichte van 2022 en 2023.

Rechten van betrokkenen

In 2024 zijn er bij de gemeente 28 verzoeken ingediend (t/m half december). Dit zijn allemaal inzageverzoeken. Het aantal van 28 is een behoorlijke daling ten opzichte van het aantal verzoeken in 2023. Dit is echter te verklaren doordat er een apart formulier gekomen is voor BRP-verzoeken. Deze komen daarom niet meer binnen als een AVG-verzoek.

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

Bij aanvang van 2024 hadden 9 van de 10 afdelingen het traject ‘Mijn afdeling AVG proof’ afgerond. De afdeling IZL zal in december 2024 de laatste hand leggen aan afronding van dit traject. Afronding van het traject - Mijn afdeling AVG-proof - betekent nog niet dat de afdelingen ook daadwerkelijk AVG proof zijn. De eerste stap hiertoe is dan gemaakt. In de trits ‘opzet – bestaan – werking’ is de eerste fase dan afgerond: de opzet. De processen zijn in beeld, er is duidelijk wat er (nog) moet gebeuren en deze acties zijn ingepland. In 2024 is die planning gevolgd (afronding ‘bestaan’) en zullen de acties beoordeeld worden (volgen van de ‘werking’). Dit komt tot uitdrukking in het jaarverslag van de FG, welke later in 2025 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 2024 zijn in totaal 30 DPIA’s uitgevoerd op verschillende soorten risicovolle gegevensverwerkingen.

Naleving Wet politiegegevens (Wpg)

In 2022 heeft de (verplichte) externe audit op naleving van de Wpg plaatsgevonden. 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. In het najaar 2024 is er reeds een interne (derde) audit geweest op dit domein door een interne auditeur, die hiervoor in de organisatie benoemd is. Hier werden reeds de eerste vorderingen opgemerkt. De resultaten hiervan zijn beschikbaar gekomen eind december 2024. De conclusies hiervan en de voorgenomen acties voor 2025 zullen benoemd worden in het jaarverslag van de FG (later in 2025).

Naleving AVG

In het najaar 2024 heeft de Functionaris voor de gegevensbescherming, zoals inmiddels gebruikelijk, een interne controle uitgevoerd op naleving van de AVG door de gemeentelijke organisatie. Object van onderzoek was:

- 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.

Ondanks dat er grote stappen zijn gezet op het vergroten van het informatiebewustzijn en het werken conform de AVG zijn er een drietal belangrijke constateringen op te maken:

- Er is voortgang op het traject mijn afdeling AVG—proof. Inmiddels hebben negen afdelingen dit traject –zo goed als - afgerond (van de 10). De laatste afdeling heeft haar afronding eind december 2024.
- Naleving van de DPIA’s gaat al beter dan voorgaande jaren. Evidenced based aanleveren (aantoonbaar laten zien dat het werkt zoals afgesproken) is nog geen gemeengoed. Hier moet de organisatie nog steeds een duidelijke stap in maken.
- De uitvoering van verwerkersovereenkomsten wordt onvoldoende getoetst op naleving bij leveranciers. Bij navraag vanuit de toezichthoudende rol gebeurt dit wél als resultante van de hercontrole, echter als regulier onderdeel van de normale bedrijfsvoering is dit géén gemeengoed.
- In 2024 is voor het eerst een uitvraag geweest op alle binnen de gemeente bekende leveranciers en/of verwerkingsovereenkomsten. Doel is beter inzicht te krijgen wat we allemaal hebben, welke nog valide zijn en welke een update verdienen. Resultaten hiervan komen terug in het jaarverslag van de FG over 2024, later in 2025.
- Er is nu een betere inventarisatie van de aanwezigheid van privacyprotocollen in de organisatie. Dit geeft al een goed beeld. Naleving staat nog in de kinderschoenen.

3.1.1 iRvN

iRvN heeft 2024 afgesloten met de eerste externe (deel) BIO TPM-audit. Voor deze TPM is iRvN onafhankelijk getoetst op de mate waarin naast Opzet en Bestaan ook de Werking is gecontroleerd. Zoals regionaal is afgesproken, wordt de uitslag van deze audit met de regio gedeeld. De scope van de audit omvatte de belangrijkste iRvN (core) processen: Back-up & Restore, Technische Kwetsbaarheden, Change Management, Cryptografie, Security Incident Management, Gebruikersauthenticatie, Autorisatiemanagement en Logging & Monitoring. Voor de Werking-toets zijn de drie maanden (september, oktober en november) voorafgaand aan de daadwerkelijke audit (begin december) gekozen.
Op het moment van dit schrijven is de conceptrapportage van de audit beschikbaar gekomen en is iRvN nog bezig met het lezen en verwerken ervan. Significante wijzigingen zijn echter in de definitieve versie niet te verwachten. De resultaten zijn positief. Naast Opzet en Bestaan blijkt ook de Werking voor de hierboven genoemde processen de toets te kunnen doorstaan. Uiteraard heeft de auditor ook enkele punten voor verbetering gevonden. Het belangrijkste onderdeel is de periodieke review voor accounts met verhoogde rechten. iRvN heeft een beperkt aantal beheerders die een veelheid aan werkzaamheden, waarvoor hogere rechten nodig zijn, uitvoeren. Hiervoor zijn veel rollen en autorisaties nodig. Daar komt nog bij dat, om continuïteit te kunnen bieden, beheerders elkaars taken moeten kunnen overnemen. De huidige autorisatiematrices zijn te complex, waardoor effectieve reviews niet voldoende kunnen worden uitgevoerd. Dit is een belangrijk verbeterpunt voor de volgende audit. De andere punten betreffen kleine procesaanpassingen en documentatieverbeteringen.

iRvN is blij met dit resultaat. Het geeft aan dat de inspanningen van het afgelopen jaar effectief zijn geweest en dat de planning haalbaar is.

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 de opname van de NIS2 richtlijn 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 de komende tijd extra aandacht aan het opvolgen van leveranciers- en verwerkersovereenkomsten. De CISO adviseert over passende maatregelen in de inkoopfase en zal adviseren over 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. Een voorbeeld hier van zijn gesprekken die de CISO voert, samen met de privacy officer, met de buurtteams volwassenen over incidenten en de verbeteringen die op basis hiervan worden uitgevoerd. Net als bij gemeente Nijmegen komt hier het versturen/afgeven van persoonsgegevens aan de verkeerde ontvanger het meest voor. In reactie hierop wordt het meest geïnvesteerd in het verspreiden van kennis en instructies over de te volgen processen.

In het kader van het gastheerschap vult de gemeente Nijmegen voor de Meervoudige Gemeenschappelijke Regeling (MGR) en de Omgevingsdienst Rijk van Nijmegen (ODRN) 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 ODRN en de MGR hebben een eigen verantwoordelijkheid voor hun verwerkingen en kunnen gemeente Nijmegen bevragen op de voortgang van de implementatie van maatregelen die wij als gastheer voor onze rekening nemen. Hiervoor is nog geen standaard proces afgesproken.

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 regio gemeenten 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 weer aanbevelingen op die we meenemen in de ontwikkelingen van dat jaar. Dit naast aanbevelingen die uit andere onderzoeken naar voren komen.

IT toetsing bij de jaarrekeningcontrole

Voorafgaande aan de controle van de jaarrekening 2024 heeft de accountant onze (bedrijfs)processen beoordeeld. In een boardletter zijn deze bevindingen gerapporteerd en voorzien van aanbevelingen. De accountant ziet dat er keuzes gemaakt moeten worden omdat de capaciteit te beperkt is om op alle trajecten die in de IT Roadmap staan vooruitgang te kunnen boeken. Hierdoor laten sommige trajecten beperkte voortgang zien terwijl in het komende jaar het nieuwe normenkader (BIO2) van kracht wordt en wettelijk verankerd wordt in de Cyberbeveiligingswet (Cbw). In de BIO2 zijn enkele belangrijke veranderingen doorgevoerd:

- De BIO2 hanteert een risicogebaseerde aanpak; De basis beveiligingsniveau's zijn losgelaten;
- Het inrichten van een Information Security Management System (ISMS), zoals wij doen in de CyberManager, is verplicht gesteld;
- De indeling van de controls/beheersmaatregelen en overheidsmaatregelen sluit aan bij vernieuwde indeling van de ISO 27002.

De IT roadmap en de KPI`s die twee keer per jaar door middel van een raadsinformatiebrief met de raad gedeeld worden zijn de sturingsinstrumenten waarmee de voortgang inzichtelijk wordt gemaakt. Hierbij heeft de raad gekozen voor KPI`s op het vlak van toegangsbeveiliging, iBewustzijn, dataveiligheid en databeheer. De status wordt geagendeerd in het Gemeentelijk Management Team (GMT) en in de raad.

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 belangrijk het bestuur niet alleen te voorzien van KPI`s die weer geven hoe de stand van zaken nu is, maar daarbij ook de relevante bestuurlijke keuzes te presenteren die geraakt worden door de ontwikkelingen. Door deze relatie als vertrekpunt te gebruiken wordt het gesprek verduidelijkt. Daarbij ziet de accountant het juist implementeren en monitoren van de Roadmap nog als actiepunt.

Onderstaand vindt u een overzicht van de IT Roadmap. Daarin worden een viertal gebieden aangegeven waarin maatregelen worden geïmplementeerd. 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 DigiD en Suwinet normen. Met betrekking tot de controle werkzaamheden zijn er een aantal aandachtspunten voor 2024.

- De opbouw en overdracht van controle dossiers moet beter bewaakt worden zodat de werking continue aangetoond kan worden.
- Het is van belang tijdig de leveranciers aan te spreken op de stukken die zij moeten leveren.
- Mutatie informatie met betrekking tot autorisaties moet eerder aangeleverd worden bij de medewerker die de toegang tot de applicatie beheert.

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.

Onzeker is welk effect de omzetting van de Europese NIS2 richtlijn naar Nederlandse wetgeving via de Cbw zal betekenen. 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. 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 2025 staan de volgende stappen gepland:

- 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.
- De verbeterde continuïteitsplannen (na het afronden van alle oefeningen) combineren tot een bedrijfscontinuïteitsplan dat voldoet aan de Cbw.
- De Barobeter inzetten in de prestatiedialogen om regelmatig op afdelingsniveau de aandacht op informatiebeveiliging te vestigen
- Vaststellen geactualiseerd strategisch informatiebeveiligingsbeleid en de uitwerking ervan.
- Alle medewerkers volgen de jaarlijkse herhaling informatiebeveiliging en privacy eLearning.
- 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.
- Implementatie Cbw inclusief verantwoording via de Cybermanager verder inrichten om ook in 2025 te voldoen aan de wet. Door de implementatie van de BIO2 (het normenkader behorend bij de Cbw) in 2025 zullen er meer taken worden uitgezet in de organisatie.
- Controlplan FG en CISO op een lijn brengen inclusief de verantwoording via ENSIA
- 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.
- iBewustzijn promoten door o.a. Let's Connect, een lezing van Daniël Verlaan, NYMACON het hack evenement en door het verzorgen van interventies ‘Veilig mailen’ bij de afdelingen MO, en I,Z & L.
- Registratieplicht bij het NCSC (Nationaal Cyber Security Centrum) invullen.

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. 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. Onderdeel van het beter controleerbaar maken van de omgeving is de verantwoording hier over via het BIO TPM project. Het afgelopen jaar is gebleken dat de planning voor het in 2026 kunnen afgeven van een volledig BIO TPM haalbaar is. Voor 2025 staan, naast de verbeterpunten in bovengenoemde processen, een aantal nieuwe processen op de planning. In 2026 zal het BIO TPM-project de projectstatus verlaten en verdergaan als standaard onderdeel van de reguliere jaarlijkse auditronden.

5.3 Meerjarig

5.3.1 Informatiebeveiliging

Toetsing van onszelf en onze partners wordt uitgebreid

Informatiebeveiliging en privacy vormen een essentieel onderdeel van de jaarplannen van Stadscontrol. Ook zijn deze thema`s een cruciaal onderdeel van de opgave “digitale transformatie”. Het verhogen van ons volwassenheidsniveau naar niveau drie zal een aantal jaren in beslag nemen waarbij verschillende aspecten van de organisatie geraakt zullen worden. Organisatorische processen, technische maatregelen maar ook de bedrijfscultuur. Dit proces zal gemonitord worden en er zal over gerapporteerd worden. Daarbij neemt de druk toe door het toenemend aantal richtlijnen dat afgevaardigd wordt vanuit Europa in het kader van de “digital decade”.

Het verhogen van de volwassenheid beslaat een aantal sporen. De CyberManager zal heringericht worden passend bij de Cbw. Hierbij zullen alle niveaus van de organisatie betrokken zijn. Van het invoeren van informatie in de lijn tot het sturen op de geproduceerde informatie door het management en het bestuur. Het ondersteunen van en bijdragen aan initiatieven op het vlak van iBewustzijn spelen een centrale rol. Denk hierbij aan een periodieke enquête van medewerkers en gesprekken met concernmanagers. Maar ook investeren in meer kennis en het (monitoren op het) veranderen van gedrag. Alle voortgangsinformatie wordt gebruikt in het controlplan van de FG en de CISO om inzicht te geven. In de komende jaren zullen controle mechanismen verder toegepast worden op de toetsing van informatiebeveiligingsmaatregelen, intern maar ook bij externe relaties door middel van evaluerende gesprekken met leveranciers. Op deze manier maken wij onze partners sterker en kunnen wij vertrouwen geven aan relaties die gegevens aan ons toevertrouwen, dan wel van ons afnemen.

ENSIA blijft het ijkpunt voor informatiebeveiliging

Als het gaat om de eenduidige toetsing door de rijksoverheid dan is daar in 2024 de toetsing van werking bij gekomen voor een aantal maatregelen. Toetsen op werking zal de volwassenheid van de gemeente Nijmegen ten goede komen. Een dergelijke ontwikkeling zal ook gevolgen hebben voor de eisen die wij stellen aan de partijen waar wij mee samen werken. Informatieveiligheid bij de overheid zal een wettelijke basis krijgen in 2025. Dit moet gebeuren via een zorgplicht waaraan meer regelgeving kan worden gehangen, zoals een geactualiseerde versie van de BIO. Door het wettelijk verplichten van de BIO2 is de vrijblijvendheid voorbij. Bij het toezicht zal niet alleen worden gekeken naar de naleving van algemene regels zoals die van de BIO. Er wordt ook toezicht gehouden op specifieke regels die aanvullend worden gesteld door de verschillende ministeries, bijvoorbeeld rond operationele technologie. Dit alles voert terug naar het aantoonbaar serieus nemen van digitale veiligheid en daarom de basis in de gehele keten op orde hebben.

Contact met de Nijmegenaar verbeteren

In het contact met de burger zien wij dat er steeds meer verwacht wordt van de digitale mogelijkheden om diensten te verlenen en te communiceren. Zie bijvoorbeeld de ontwikkelingen rond manieren om je als burger te identificeren, zoals DigiD, Yivi en eIDAS. Dit geldt ook voor niet Nederlandse burgers uit Europa. Anderzijds is het zo dat er geen “one size fits all” burger is. Voor de gemeente is het van belang rekening te houden met burgers die om redenen van ongeletterdheid of geestelijke dan wel lichamelijke beperkingen, niet de mogelijkheid hebben om gebruik te maken van de digitale voorzieningen. Websites en achterliggende procedures moeten met dit punt in gedachten onderhouden worden. Het ontstaan, dan wel vergroten, van een kloof tussen diegenen die mee kunnen komen met de ontwikkelingen en degenen die dat niet lukt moet voorkomen worden. Het bieden van alternatieve voorzieningen moet indien nodig meer aandacht krijgen om te voorkomen dat sommige burgers belemmerd worden in hun toegang tot voorzieningen en het uitoefenen van hun rechten. Het klantportaal “mijn Nijmegen” wordt verder ontwikkeld en er wordt gewerkt aan de beschikbaarheid van verschillende kanalen voor de burger om contact op te nemen met onze gemeente. Deze aanpak wordt “omni channel” genoemd en heeft als doel de bereikbaarheid te verbeteren. Dit moet op een veilige en eenduidige manier mogelijk gemaakt worden en ook hiervoor gelden in Europa richtlijnen.

Bewustwording en weerbaarheid

Op het gebied van bewustwording wordt jaarlijks een (herhalings)module aangeboden via eLearning. Via het intranet vindt steeds vaker communicatie plaats over relevante onderwerpen op het vlak van informatiebeveiliging en privacy om twee redenen:
- er zijn steeds vaker ontwikkelingen die onder de aandacht gebracht moeten worden zoals AI en nieuwe aanvalstechnieken.
- communicatie m.b.t. iBewustzijn behoort tot het takenpakket van de operational security officer.
Het instrument dat opgeleverd zal worden uit het traject met Hogeschool Saxion zal ingezet worden om een meer informatieveilige cultuur bij gemeente Nijmegen te bereiken. Naast permanente scholing van alle medewerkers zal er jaar na jaar ook specifieke aandacht zijn voor bepaalde groepen zoals bijvoorbeeld het management, de privacy ambassadeurs of medewerkers die zich bezig houden met de verantwoording.

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.

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 2023 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 2023 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.
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

Afkorting	Uitleg
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.
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.
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.

Afkorting	Uitleg
SO	Security Officer. Degene die de eerste lijn adviseert en (mede) beleid ontwikkelt op het vlak van informatiebeveiliging.
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).