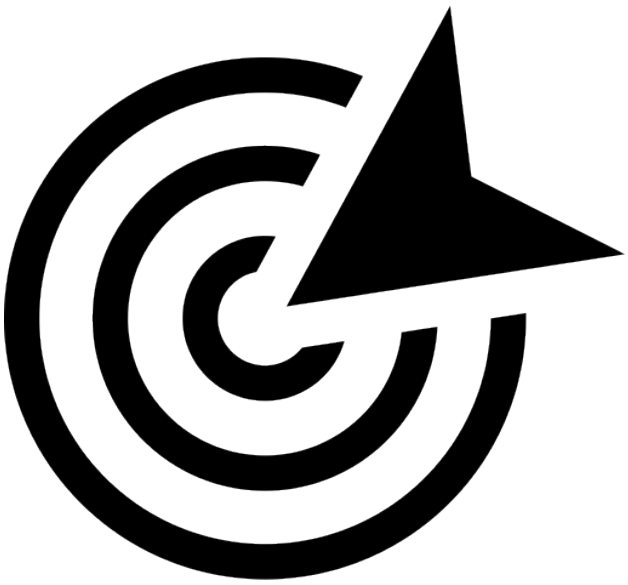
Rapportage Informatiebeveiliging 2023



Tijd om te scoren

CISO gemeente Nijmegen, december 2023

Informatiebeveiliging
2023

in maatregelen

Leveranciers toetsen

Roadmap: 1 raamwerk om te toetsen

Crisis bestrijding & Continuiteit plannen en oefenen

Scholing iBewustzijn
75% medewerkers
0% bestuur

sturen op KPI`s



Volwassenheidsniveau 3

in getallen

Inzage-verzoeken burgers

71x
Hoe wordt mijn info gebruikt?

Incidenten
84

22
Data-lekken

24 DPIA`s

Beheersmaatregelen geïmplementeerd
(baseline informatieveiligheid)

71%

Inhoudsopgave

1. Doel & wettelijk kader 4
2. Leeswijzer 4
3. Ambitie 5
4. Terugblik 6
4.1 Wat wilden we bereiken? 6
4.2 Wat hebben we bereikt? 6
5. Vooruitblik 17
5.1 Aanbevelingen uit externe toetsing 17
5.2 Komend jaar 19
5.3 Meerjarig 21
Bijlage: achtergrond & begrippen 24

1. Doel & wettelijk kader

Doel

In dit rapport informeert de CISO 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 2024 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. Een belangrijk document wat hieruit voortkomt is een 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 management beoordeling 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 ons doel van volwassenheidsniveau 3 te behalen,
- Een aantal getallen met betrekking tot informatiebeveiliging die wij jaarlijks in deze rapportage weergeven.

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 er naar 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:

- weet welke risico's en onzekerheden er bestaan op het terrein van de informatiebeveiliging
- daarbij weet welke (passende) maatregelen we nemen
- weet wie waar verantwoordelijk voor is
- zorgt voor een controleerbare planning van maatregelen die genomen moeten worden
- de planning van de implementatie van maatregelen bewaakt
- weet in hoeverre de maatregelen effectief zijn
- verantwoording af legt 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. Een ambitie die in 2022 nogmaals door de Nederlandse gemeenten bekrachtigd is, door af te spreken hier de benodigde middelen voor vrij te maken. 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.

Het team Stadscontrol binnen de gemeentelijke organisatie, met hier in ondergebracht de CISO en de FG, 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 er voor dat dit zo efficiënt mogelijk wordt ingevuld.

Ook 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?

In 2023 wordt de integrale **roadmap** opgesteld met daarin alle activiteiten op het vlak van informatiebeveiliging. Hier in worden alle aanbevelingen van zowel auditors als de accountant, als ook andere onderzoeken samengebracht.

In de **CyberManager** zijn implementatieacties uitgezet bij de afdelingen zelf. Door deze af te handelen ontstaat inzicht in de risico's die we lopen op het vlak van informatiebeveiliging en de status van de te treffen maatregelen.

In 2023 is het **iVeiligheidsteam** ingericht, met als eerste taak het elkaar ondersteunen met het ontwikkelen van een continuïteitsplan voor elke afdeling.

Het regionale **crisisproces** wordt verbeterd en opnieuw vastgesteld. In Nijmegen wordt geoefend door middel van een lokale table top oefening.

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 Let`s Connect.

4.2 Wat hebben we bereikt?

4.2.1 De gemeente Nijmegen

Activiteiten over de hele gemeente

- Het AVG-proof project is bij alle afdelingen (nagenoeg) afgerond.
- Het continuïteitsproject heeft voor zeven afdelingen continuïteitsplannen opgeleverd. Van de zeven plannen is voor de hele gemeente een samengestelde analyse opgesteld. Nadat de aanbevelingen zijn opgevolgd moet er een gemeentebreed continuïteitsplan liggen.
- Naar aanleiding van H@ckNijmegen 2022 zijn zwaardere wachtwoord eisen ingevoerd. Het gebruik van een wachtwoordmanager, zoals Bitwarden, wordt gestimuleerd door voorlichting en training.
- Het iBewustzijn communicatieplan is uitgevoerd. Tijdens Let`s Connect is er een Escape Truck geplaatst. Daarnaast is er aandacht geweest voor veilig mailen (gebruik Zivver), toegangspoortjes, phishing, ransomware en CEO fraude.
- De ransomware eLearning leerlijn is beschikbaar gesteld via Studytube. Iedere medewerker wordt geacht deze te volgen. Het aandeel afgeronde modules ligt op ruim 70%.
- Met de raad is het gesprek gevoerd over geschikte KPI`s om op te sturen. Een eerste set is gedefinieerd waarbij de aandacht met name uit gaat naar iBewustzijn en toegangsbeheer. Deze KPI`s worden in 2024 gevolgd.
- Het ICT crisisproces is in Nijmegen geoefend en geëvalueerd. Verbeteracties worden uitgevoerd.
- Het H@ckRijkVanNijmegen evenement heeft in Wijchen 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 viertal processen is gereed om te toetsen.
- Het team Stadscontrol ziet toe op het opvolgen van bevindingen en het nemen van de juiste maatregelen. Dit gebeurt door het voeren van advies gesprekken, het begeleiden van prestatie

dialogen 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.

Er waren een aantal opvallende gebeurtenissen in het afgelopen jaar.

In het afgelopen jaar heeft een onderzoeker van de Universiteit Twente, Koen van Hove, onderzoek gedaan naar het verwerken van coördinated vulnerability disclosures door gemeenten in Nederland (waaronder Nijmegen) en België. Dit is het proces waarbij een burger een kwetsbaarheid meldt die zij/hij gevonden hebben in bijvoorbeeld een website van de gemeente. Hij deed dit aan de hand van een melding van een lek (configuratie fout) die het mogelijk maakte om e-mails te versturen namens de gemeente. Over zijn onderzoek is gepubliceerd door diverse media. Hij heeft het onder andere op de One Conference gepresenteerd. Zie ook de website van UTwente.[2] Gemeente Nijmegen heeft de disclosure melding conform procedure opgepakt, maar wel lang gedaan over de afhandeling.

In 2023 zijn er 84 beveiligingsincidenten gemeld. Daarvan waren 64 meldingen intern en 20 meldingen extern. Er waren 22 datalekken. Van de datalekken zijn er 13 bij de Autoriteit Persoonsgegevens (AP) gemeld. Over een melding zijn door de AP aanvullende vragen gesteld. Daarbij ging het om 806 stempassen voor de Tweede Kamer verkiezingen. Deze waren verkeerd verstuurd. Als het gaat om beveiligingsincidenten dan gaat de verkeerd verstuurde mail nog steeds aan kop[3].

De inrichting van de CyberManager komt steeds meer op orde. Hierdoor kunnen we over de meldingen steeds meer informatie verstrekken.

De 84 van het afgelopen jaar kunnen we bijvoorbeeld categoriseren naar oorzaak:

Privacy of beveiligingsincident:	47
Verlies / diefstal:	9
Social engineering:	7
Storing beschikbaarheid:	1
Schending privacywetgeving	7
Kwetsbaarheid	13

Maar we kunnen de meldingen ook indelen naar afdeling:

FA: 5
SR: 5
SB: 1
ST: 5
IZL: 19
PIF: 12
PU: 12
BM: 3
VJB: 6
MO: 4
VSA: 1
Extern: 8
Intern door iRvN: 2
Onbekend: 1

2 https://www.utwente.nl/nieuws/2023/10/1169643/veel-gemeenten-reageren-nog-niet-adequaat-op-beveiligingslekken
3 https://www.nijmegen.nl/diensten/verkiezingen/stempas/

Deze indelingen zijn nog niet 100% betrouwbaar maar geven wel een beeld van wat mogelijk is. Zo zouden we trends kunnen signaleren op het moment dat het aandeel van een bepaalde oorzaak stijgt. Sommige afdelingen springen er van nature uit (IZL, PU en PIF) omdat zij relatief veel persoonsgegevens verwerken. Ook hier zijn onverwachte stijgingen of dalingen interessant. Op het moment dat we deze gegevens zouden kunnen combineren, bijvoorbeeld met gegevens over bewustzijn van de medewerkers, zouden we interessante conclusies kunnen trekken die wij kunnen gebruiken bij het kiezen en plannen van activiteiten op het vlak van iBewustzijn.

Invoering van de CyberManager afgerond

Implementatie taken op het vlak van informatiebeveiliging die zijn uitgezet bij de afdelingen werden door de ene afdeling beter afgehandeld dan de andere afdeling. Om die reden hebben wij in 2023 een project uitgevoerd samen met de leverancier van Cybermanager. Daarbij namen zij de begeleiding van de medewerkers op zich om hen te ondersteunen bij het afronden van de implementatie taken. Aansluitend hebben we een overzicht gekregen van de status door in de CyberManager een interne audit uit te voeren op de BIO 2023 maatregelen.
In de CyberManager is nu 71% van de maatregelen actief (bestaan), zie ook figuur 1. Dit betekent dat er een verbetering te zien is met het voorgaande jaar. De verklaring hier voor is dat er veel energie gestoken is in het beschrijven en toetsen van afspraken. In de eerste lijn hebben medewerkers onder begeleiding de tijd genomen om vast te leggen hoe gemeente Nijmegen maatregelen neemt, bijvoorbeeld op het vlak van personeel. Waar er nog onduidelijkheden waren, zijn verbetertaken uitgezet voor het komende jaar.
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 2022 is door het GMT de dreigingsanalyse informatiebeveiliging uitgevoerd en besproken. Continuïteit is een belangrijke pijler binnen de informatiebeveiliging en richt zich op het zo snel mogelijk herstellen van kritische bedrijfs- en dienstverleningsprocessen middels curatieve maatregelen op het moment dat een dreiging zich voordoet. Begin 2023 zijn de afdelingen aan de slag gegaan met het voor hun meest kwetsbare bedrijfs- en dienstverleningsprocessen in kaart brengen van preventieve en curatieve maatregelen, deze aanvullen waar nodig en implementeren. De bedoeling is dat elke afdeling voor haar cruciale bedrijfs- en dienstverleningsprocessen de belangrijkste risico’s die zij lopen inventariseert. Per risico brengt de afdeling de reeds getroffen preventieve maatregelen in kaart en bepaalt welke aanvullende maatregelen ze wil treffen. Die maatregelen worden opgenomen in een afdelingsplan. Elke afdeling heeft een aanspreekpunt/coördinator benoemd.
De plannen moeten praktisch uitvoerbaar zijn. Afhankelijkheden van andere afdelingen of derden moeten in de plannen opgenomen worden. Ook financiële risico’s dienen opgenomen te worden. Op het moment dat deze informatie op afdelingsniveau beschikbaar is wordt het makkelijker een gemeente brede afweging te maken als het gaat om wat voorrang moet krijgen bij een calamiteit die alle processen raakt.
De plannen worden jaarlijks gecontroleerd op actualiteit zodat ze geactualiseerd worden als er belangrijke ontwikkelingen geweest zijn. Elke drie jaar zou het overkoepelende beleid bijgewerkt moeten worden. Daarnaast moeten de plannen getest/geoefend worden door de afdelingen.
In de eerste helft van 2023 is onder leiding van de CISO het Netwerkteam I-veiligheid georganiseerd. Dit periodiek bijeen komende 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 om in januari 2024 aanbevelingen te

kunnen voor leggen aan het GMT. Het uitvoeren van deze aanbevelingen zal de continuïteit te verbeteren.

Resultaten uit H@ckRijkVanNijmegen (Druten/Wijchen)

In november 2023 vond in het Kasteel van Wijchen het H@ckRijkVanNijmegen evenement plaats. Dit evenement was door gemeenten Wijchen en Druten en iRvN (in samenwerking met Hunt&Hackett en het Institute for Computing and Information Sciences van de Radboud Universiteit Nijmegen), georganiseerd. De studenten van de RU testten de technische informatiebeveiligingsmaatregelen van de regionale samenwerking. Het doel van dit evenement was het verhogen van de weerbaarheid van het samenwerkingsverband, en dus ook gemeente Nijmegen, doordat de gevonden kwetsbaarheden worden opgelost.
De studenten vonden met name kwetsbaarheden als het gaat om wachtwoordgebruik door de diverse gemeenten in de regio. Verder bleken de afgesproken doelwitten veelal nog te moeilijk te kraken in de beperkte tijd.

welkom	313
qwerty	104
test	36
appel	27
najaar	24
gemeente	16
wachtwoord	14
oversteek	14
fiets	12
vakantie	12
koffie	11
waalbrug	9
kerst	9
pizza	8
voorjaar	8
pensioen	7
telefoon	6

Een opsomming van woorden die in wachtwoorden voorkomen



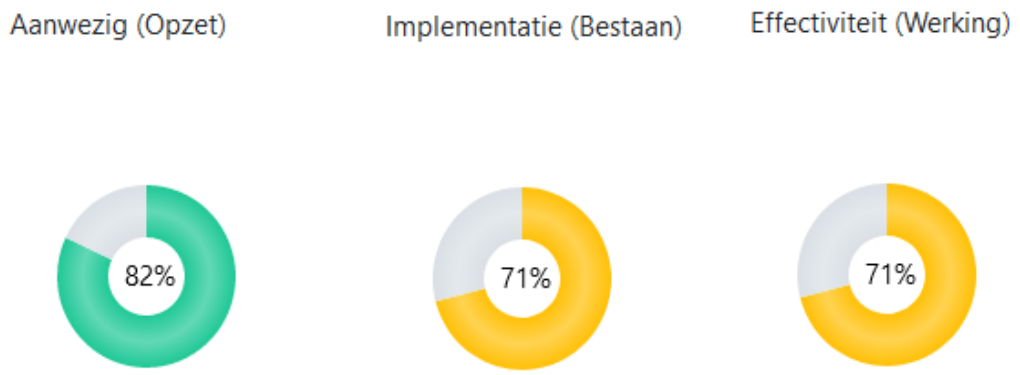




Resultaat van management beoordeling informatiebeveiliging

In de hier onder 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 waarvan bepaald kan worden in hoeverre deze voldoen aan de eisen van de BIO. Dit gebeurt door een Interne Audit uit te voeren 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.



Figuur 1: opzet bestaan en werking in CM

2. Identificatie van eventuele afwijkingen:
Zoals te zien is in bovenstaand figuur is de implementatie van het BIO normenkader niet 100%. Een deel van de tekortkoming is ontstaan doordat iRvN in 2023 niet de capaciteit had om hun CyberManager omgeving (waarvan een aantal maatregelen gekoppeld zijn aan de omgevingen van de deelnemende gemeenten in de regionale samenwerking) te administreren. Daarnaast heeft gemeente Nijmegen intern nog een aantal verbetertaken uit te voeren onder andere op het vlak van het expliciet accepteren van risico`s, gebruikersbeheer, en leveranciersrelaties. Meer details worden hier onder weergegeven.

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, leveranciers management, 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.

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 controle en de ENSIA auditor heeft met name oog voor de systemen die gekoppeld zijn aan DigiD. Beide pogen een breder beeld te zien vanuit hun perspectief. Met name de accountant slaagt daar in door in 2023 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.

6. In control statement:
Gemeente Nijmegen verklaart voor 71% te voldoen aan de BIO. Daarbij merkt zij op dat de implementatie status erg varieert per maatregel en per proces. Zo scoren de meest gevoelige systemen, met name die betrokken zijn bij DigiD en financiën 100%. Deze staan dan ook bovenaan bij het afwegen van risico`s.

IT Audit observaties van de Accountant over 2023

Op het vlak van Algemene IT beheersmaatregelen en Cybersecurity concludeert de accountant over 2023 dat de gemeente de bevindingen uit de verschillende audits oppakt en ook opvolgt. Hierbij wordt de IT Roadmap gebruikt als kader en communicatie vehikel. Daarnaast zijn er verschillende plannen die de gemeente uitvoert. Hierin worden stappen gezet waarmee verbetering bereikt wordt, bijvoorbeeld op het vlak van contractmanagement en toegang tot systemen.

De accountant merkt op dat het ontbreekt aan executiekracht om alle plannen tijdig uit te voeren. Het is niet alleen zo dat de IT-beheersing naar een hoger niveau getild moet worden. Tegelijkertijd vinden er ook veranderingen op het vlak van applicaties plaats die veel capaciteit vragen, zoals het project rond Coda. De accountant vraagt aandacht voor dit punt en adviseert het opstellen van een integraal plan om meer inzicht te krijgen in acties en tijdslijnen.

Resultaat van de ENSIA Cyclus 2023

Deze zelfevaluatie, gebaseerd op de BIO, is tijdig afgerond. Alle vragenlijsten zijn ook dit jaar op tijd ingeleverd. De proefaudit DigiD en Suwinet in oktober heeft nog een aantal acties opgeleverd op het vlak van het opleveren van voorbeelden en aanvullende documentatie. Bij de definitieve audit in december was voor het merendeel van de DigiD aansluitingen de documentatie compleet. De laatste onderdelen zullen in januari worden aangeleverd. Dit geldt ook voor de Suwinet verantwoording. Hierbij blijkt dat het niet tijdig zal lukken om aan de normen voor DKD-inlezen te voldoen. Daarom zullen wij zo snel mogelijk in 2024 stoppen met DKD-inlezen.

Een kanttekening bij het verantwoordingsproces is dat wij in 2023 een nieuwe auditor gekozen hebben voor de toetsing van de Suwinet en DigiD zelfevaluatie. Dit betekent dat het proces voor 2023 meer afstemming heeft gevraagd dan in de jaren daarvoor wat op een aantal punten voor vertraging zorgde.

Een tweetal aanbevelingen komen uit de ENSIA audit naar voren. De eerste is het zorg dragen voor een tijdige aanlevering van het dossier zodat de audit goed kan worden voorbereid. Ten tweede is een aanbeveling om de bezetting in de organisatie en de overdracht van taken die te maken hebben met de zelfevaluatie en de DigiD/Suwinet audit beter te bewaken. Dit met name ook met het oog op de toetsing van werking (met ingang van 2024), waar het tijdelijk niet uitvoeren van monitoring taken tot grotere problemen zal leiden bij de audit dan nu.

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 en Privacy 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 en bestaan van de benodigde maatregelen. In 2024 is het toetsen van werking verplicht.</td></tr>
<tr><td>Suwinet</td><td>Voor Suwinet-inkijk voldoet gemeente Nijmegen aan de geldende normen. Voor DKD-inlezen niet. Omdat de benodigde inspanning om te voldoen voor DKD-inkijk op dit moment niet geleverd kan worden is besloten om het gebruik van deze functionaliteit zo snel mogelijk te beëindigen.</td></tr>
<tr><td>BRP</td><td>De BRP en RNI verantwoording zijn goed afgerond, zie behaalde score 2023 t.o.v. de maximaal te behalen score.

<table>
<tr><td>1. ENSIA BRP</td><td>Max te behalen</td><td>Behaald in 2022</td><td>Behaald in 2023</td></tr>
<tr><td>Organisatie beveiliging</td><td>400</td><td>290</td><td>400</td></tr>
<tr><td>Toegang</td><td>400</td><td>385</td><td>400</td></tr>
<tr><td>Naleving</td><td>400</td><td>360</td><td>350</td></tr>
<tr><td>Beleid en organisatie</td><td>228</td><td>nvt</td><td>210</td></tr>
<tr><td>Uitvoering bijhouden</td><td>418</td><td>385</td><td>371</td></tr>
<tr><td>Uitvoering verstrekking</td><td>76</td><td>nvt</td><td>58</td></tr>
<tr><td>Uitvoering incidentafhandeling</td><td>78</td><td>nvt</td><td>58</td></tr>
<tr><td colspan="4">2. RNI</td></tr>
<tr><td>Organisatie beveiliging</td><td>100</td><td>100</td><td>75</td></tr>
<tr><td>Toegang</td><td>50</td><td>15</td><td>25</td></tr>
<tr><td>Naleving</td><td>50</td><td>34</td><td>50</td></tr>
<tr><td>Bijhouding van de BRP</td><td>150</td><td>150</td><td>150</td></tr>
<tr><td>Verstrekking gegevens</td><td>25</td><td>max</td><td>25</td></tr>
<tr><td>Aanbeveling</td><td>25</td><td>max</td><td>25</td></tr>
</table></td></tr>
<tr><td>Reis-documenten</td><td>De verantwoording van reisdocumenten is prima.

<table>
<tr><td>Reisdocumenten</td><td>Max te behalen</td><td>Behaald in 2022</td><td>Behaald in 2023</td></tr>
<tr><td>Organisatie beveiliging</td><td>400</td><td>330</td><td>400</td></tr>
<tr><td>Toegangsbeveiliging</td><td>400</td><td>340</td><td>400</td></tr>
<tr><td>Naleving</td><td>400</td><td>315</td><td>360</td></tr>
<tr><td>Aanvraag-en uitgifteproces</td><td>400</td><td>400</td><td>385</td></tr>
<tr><td>Overig proces</td><td>300</td><td>300</td><td>300</td></tr>
<tr><td>Aanbeveling</td><td>100</td><td>75</td><td>76</td></tr>
</table></td></tr>
<tr><td>BAG</td><td>BAG terugblik op 2023:
De gestelde kwaliteitsnorm van het verwerken van definitieve pandgeometrie hebben we dit jaar gehaald. Voor een groot aantal verblijfsobjecten is gecontroleerd of ze aan de juiste panden zijn gekoppeld en de koppeling in de registratie is verbeterd. De 3D-mutatiesignalering is gebruikt om wijzigingen aan bestaande panden en nieuwe panden, waarvoor geen omgevingsvergunning is verleend, te registreren in de BAG. We voldoen aan de eis om de vergunde situatie te registreren. De ambitie bestaat om daarnaast ook het feitelijk gebruik te registreren en te toetsen op legaliteit. In 2023 is voor deze onderwerpen een overleg geweest met de verantwoordelijken van het VTH-beleid waarna is besloten dat hier nu geen actie op gewenst is en dat er geen proces ingericht hoeft te worden.
BAG vooruitblik op 2024:
Van een aantal verblijfsobjecten verschilt de geregistreerde "gebruiksoppervlakte" tussen de BAG en de WOZ-registratie. Om dit op te lossen wordt in 2024 een nieuw proces ingericht.
De Rijksdienst voor Identiteitsgegevens (RvIG) stelt in 2024 een wijziging vast van het Logisch Ontwerp Basisregistratie Personen (BRP). Bewoners in de BRP kunnen dan niet meer ingeschreven worden op een zogenaamd 'nevenadres' uit de BAG. Voor de BAG wordt in 2024 op basis van dossieronderzoek gecontroleerd of een 'nevenadres' als 'hoofadres' moet worden geregistreerd, gekoppeld aan een zelfstandig verblijfsobject. De invoering van de Omgevingswet (Ow) en de Wet kwaliteitsborging voor het bouwen (Wkb) per 1-1-2024 leidt tot proceswijzigingen voor de BAG.</td></tr>
<tr><td>BGT</td><td>BGT terugblik op 2023
We hebben terugmeldingen ouder dan 18 maanden verwerkt. Eén melding hebben we doorgezet naar Prorail omdat deze in het bronhoudergebied van Prorail lag.</td></tr>
</table>

	De geometrieverschillen tussen de BGT- en BAGpanden zijn bij veertien van de vijftien panden opgelost. Bij 1 pand lukt dat nog niet, omdat het betreffende pand wordt verbouwd. Wanneer de verbouwing gereed is lossen we het verschil in geometrie op. Bij Beheer Openbare Ruimte vinden het hele jaar door mutaties plaats in de buitenruimte, die ook verwerkt moeten worden in de BGT. De piekwerkzaamheden zijn vooral in het voor- en najaar, met als gevolg, dat we in die periodes veel mutaties voor de BGT kunnen verwachten. **Vooruitblik op 2024** 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 gewerkt aan het project “Data op orde”. Wanneer een thema op orde is, actueel en volledig, dan nemen we dat thema op in de BGT en leveren deze aan de landelijke voorziening. De leverancier van onze BGT applicatie ontwikkelt een nieuwe BGT applicatie. De ontwikkelingen volgen we nauwgezet. De leverancier biedt de mogelijkheid om, indien gereed, de eerste versie en daarna de updates ervan te installeren naast de huidige BGT-applicatie, om zo de ontwikkelingen goed te kunnen volgen.
BRO	In 2023 werden alle BRO relevante ondergrondgegevens geleverd aan het bronhouderportaal. In 2024 komt het BRO coördinatieteam per kwartaal bij elkaar om de stand van zaken te bespreken. In 2023 was het BRO coördinatieteam nog niet compleet.

Resultaat op het vlak van privacy

Afhandeling klachten

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

Rechten van betrokkenen

In 2023 zijn er bij de gemeente 72 verzoeken (t/m november) ingediend. Hier zat één verwijderverzoek bij. De rest waren inzageverzoeken. Het aantal van 72 betreft een behoorlijke stijging ten opzichte van het aantal verzoeken in 2022. De stijging is echter te verklaren doordat middels het AVG inzageproces een groot aantal BRP inzageverzoeken zijn ingediend. De BRP kent echter in de vorm van de Wet BRP een eigen wettelijk kader gericht op inzage in de BRP. Deze verzoeken zijn dan ook doorgezet naar de afdeling Publiekszaken.

Vernieuwd privacy beleid

In juli 2023 is het nieuwe privacybeleid vastgesteld. Het oude beleid stamde uit 2018 en was toe aan vervanging, gelet op het feit hoe de rol van het thema ‘privacy’ binnen de gemeente sinds 2018 gegroeid is. Het nieuwe beleid schetst onze visie op het respecteren van de persoonlijke levenssfeer van onze inwoners, de gewenste transparantie naar de inwoner, het belang van het beschermen van persoonsgegevens en de afweging die gemaakt dient te worden tussen dienstverlening enerzijds en het beschermen van persoonsgegevens anderzijds. Daarnaast wordt de ethische kant van privacy belicht. Verder wordt de ambitie uitgesproken om binnen vier jaar het volwassenheidsniveau 3 te bereiken.

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

Medio 2022 zijn de afdelingen begonnen om de uitvoering van de “elke afdeling AVG-proof” plannen weer op te pakken, na stilstand door de Coronapandemie. De afdelingen Financiën, PIF, Publiekszaken en de afdeling Vastgoed, Sport en Accommodaties en het team Stadscontrol hebben dit traject (zo goed als) afgerond.

De afdelingen Maatschappelijke Ontwikkeling, IZL, Stadsrealisatie en VJB zijn in de afrondende fase. De afdelingen Stadsontwikkeling en Stadsbeheer zijn nog druk doende het traject vóór 14 jan 2024 (deadline project) af te ronden. Het volledige beeld wordt beschreven in het jaarverslag van de FG.

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 zal die planning gevolgd worden (afronding 'bestaan') en zullen de acties beoordeeld worden (volgen van de 'werking').

DPIA als continu bijstuurproces

Het instrument DPIA is nog steeds teveel een momentopname van de privacyrisico's die spelen bij een gegevensverwerking. Ook wordt het instrument nog niet voldoende ingezet als monitoring op de implementatie en de borging van de ingezette maatregelen op de langere termijn. Hier schuilt dan ook nog steeds een kwetsbaarheid in. Door de ombuiging van implementatie naar beheer / controle wordt de DPIA een blijvend onderdeel van de (interne) verantwoordingsplicht. In 2023 zijn in totaal (stand 01/12/23) 24 DPIA's uitgevoerd op (bestaande) grote complexe gegevensverwerkingen binnen het fysiek, sociaal en veiligheidsdomein. In de jaarlijkse controle wordt getoetst in hoeverre uitvoering en borging wordt gegeven aan de risico's en maatregelen zoals opgenomen in de DPIA's .

Naleving Wpg

In 2022 heeft de (verplichte) externe audit op naleving van de Wpg plaatsgevonden. 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 2022 is er reeds een interne (tweede) audit geweest op dit domein door een interne auditeur, die hiervoor in de organisatie benoemd is. Hier werden reeds de eerste vorderingen opgemerkt.

In het voorjaar 2023 is de verplichte (externe) hercontrole op de eerste audit Wpg uitgevoerd. Ook deze is verzonden aan de AP. De resultaten waren op het eerste oog teleurstellend. In het sociale domein waren wel stappen gezet, in het fysieke domein was sprake van achteruitgang. Inzoomend is dat te verklaren: de opzet was in eerste instantie nog als redelijk bestempeld, en nu als onvoldoende. Oorzaak was dat ten tijde van de hercontrole de gehele opzet vernieuwd werd en dat proces was nog gaande.

Bij de interne controle die in het najaar 2023 op het fysieke domein is gehouden, bleek dat dit inmiddels weer hersteld is. De nieuwe opzet is beter dan de oude en ook in het fysieke domein is sprake van een goede vooruitgang ten opzichte van de eerste externe audit.

Naleving AVG

In het najaar 2023 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.

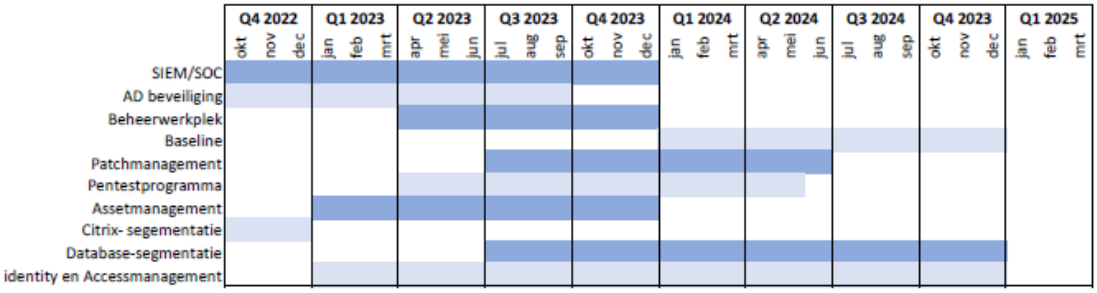
Ondanks dat er grote stappen zijn gezet op het vergroten van het informatiebewustzijn en het werken conform de AVG zijn er een drietal belangrijke constateringen op te maken:

- Er is voortgang op het traject mijn afdeling AVG—proof. Inmiddels hebben acht afdelingen dit traject –zo goed als - afgerond (van de 10). De laatste twee afdelingen zijn goed op weg en naderen de afronding.
- Naleving van de DPIA's gaat al beter dan voorgaande jaren. Evidence 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.
- 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.

4.2.2 iRvN

Op dit moment loopt bij iRvN het tweede veiligheidsproject. Dit project wordt uitgevoerd samen met Hunt & Hackett. Projecten die op dit moment lopen hebben te maken met het verder scheiden van de gemeentelijke omgevingen, het verbeteren van het beheren van ICT middelen en het certificeren van iRvN op basis van het BIO normenkader. Daarnaast wordt de implementatie van het beheersysteem van mobiele apparaten in dit jaar afgerond.
Veel maatregelen die te maken hebben met het ontdekken van problemen via het detectiesysteem (EWS) en het beheersysteem voor mobiele apparaten (MDM) zijn in 2020 ingevoerd. De implementatie heeft in 2023 gelopen en wordt in 2023 voortgezet.



Figuur 2 planning projecten iRvN

Er worden steeds meer rapportages opgeleverd door iRvN gebaseerd op de monitoring die wordt verricht. Hierdoor ontstaat steeds meer inzicht in de stand van zaken rond de geïmplementeerde maatregelen.

4.2.3 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 vernieuwde Wbni 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 besteedt de komende tijd extra aandacht aan het opvolgen van verwerkersovereenkomsten. De CISO adviseert over passende maatregelen in de inkoopfase en zal adviseren over de invulling van de gesprekken met leveranciers. Leveranciersmanagement 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 hier op 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) de beschikking gebruikt een eigen Suwinet aansluiting voor haar werkzaamheden ten behoeve van 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.

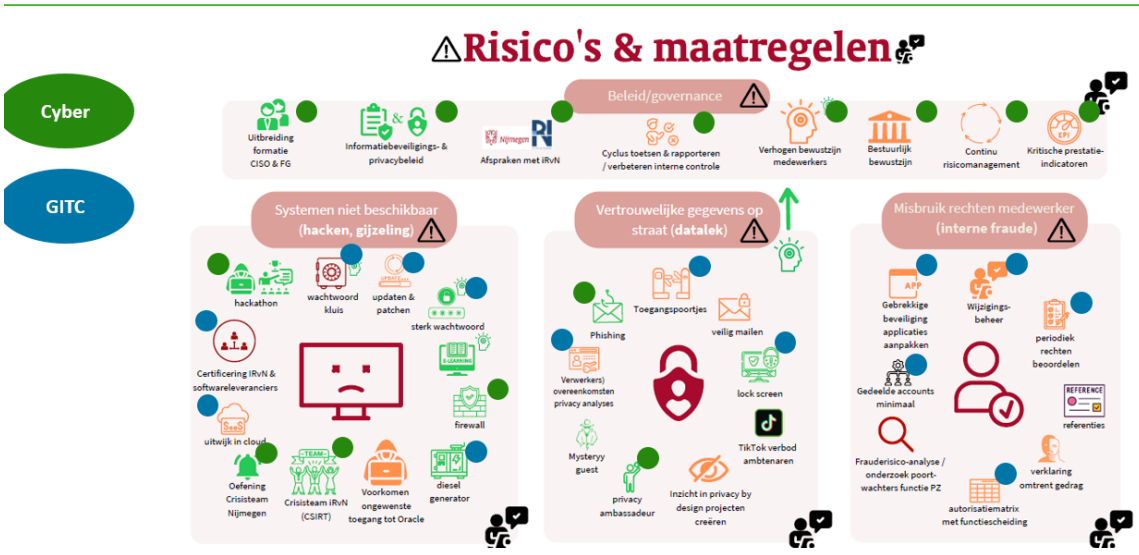
IT toetsing bij de jaarrekeningcontrole

Voorafgaande aan de controle van de jaarrekening 2023 heeft de accountant onze (bedrijfs)processen beoordeeld. In een boardletter zijn deze bevindingen gerapporteerd en voorzien van aanbevelingen. De accountant ziet dat verbeteringen zijn ingezet en worden uitgevoerd zoals geformuleerd in onze meerjaren ambitie. Hierbij adviseert de accountant het college kritisch te kijken naar het tijdspad van de aangegeven ambities en daarbij de beschikbare capaciteit en middelen in ogenschouw te nemen. Dit om te voorkomen dat door te weinig focus het doel niet gehaald wordt.
Ons college heeft bij het aanbieden van de boardletter aan de raad aangeven dat “de bevindingen worden erkend en (waar nodig) passende verbetermaatregelen zullen worden ingevoerd.” De roadmap en de KPI`s zijn daarbij de sturingsinstrumenten. De status wordt drie keer per jaar geagendeerd in het Gemeentelijk Management Team (GMT) en twee keer per jaar in de raad.

Aanbevelingen van de accountant

De accountant ziet de gecombineerde weergave van de aanbevelingen uit de onderzoeken in een raamwerk als een generiek model waarlangs zij kunnen toetsen. In de figuur hier onder heeft de accountant de voor hen belangrijkste maatregelen in de Roadmap gemarkeerd.

IT Roadmap: Hoe doen we het nu samen?



Figuur 3 Maatregelen accountant in roadmap

Door dit telkens als vertrekpunt te gebruiken wordt het gesprek verduidelijkt. Daarbij ziet de accountant het juist implementeren en monitoren van de Roadmap nog als actiepunt.



Figuur 4 Samenvatting boardletter 2023

In de samenvatting van de boardletter hier boven zien we dan ook het generieke model (single audit aanpak) als speerpunt terug komen. Die bal is opgepakt en we zijn er mee aan het lopen.

Drie aanbevelingen van vorig jaar zijn opgevolgd. Voor de komende tijd staan er vier ontwikkelpunten open, waaronder ook het gebruiken van de IT Roadmap als gereedschap voor verantwoording. Dat is het doel waar we moeten scoren.

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 afwijkingen geconstateerd als het gaat om het onderdeel DKD-inlezen bij Suwinet. Voor alle DigiD aansluitingen en het inkijk gebruik van Suwinet geldt dat we voldoen aan de huidige normen. Omdat de maatregelen rond de DKD-inlezen functie al eerder niet voldeden, en de capaciteit die nodig is om deze op orde te krijgen niet beschikbaar is, heeft de proces eigenaar besloten om te stoppen met het gebruik van deze functie. Deze zal weer in gebruik genomen worden op het moment dat het bijbehorende verantwoordingsproces goed uitgevoerd kan worden.

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.
- Controle acties die door derden uitgevoerd worden moeten eerder gepland worden.

5.2 Komend jaar

Gezamenlijk stippelen Stadscontrol en de Informatiemanagers het groeipad uit voor de organisatie naar meer volwassenheid. Hierbij moeten we aandacht hebben voor focus en keuzes maken, zoals ook in de reactie op het regionale rekenkameronderzoek en de directiebrief worden weergegeven. Door de juiste speerpunten te kiezen en efficiënte combinaties te maken binnen de opgave “digitale transformatie” verwachten wij belangrijke stappen vooruit te kunnen zetten op het vlak van informatieveiligheid. Het is tijd om de doelen die we gesteld hebben te behalen en te scoren!

Onzeker is daarbij welk effect de omzetting van de Europese NIS2 richtlijn naar Nederlandse wetgeving via de Wbni zal betekenen. Gemeenten zijn daarbij als essentieel aangemerkt dus een intensivering op het vlak van continuïteit, scholing en de beveiliging van operationele technologie is zeker aan de orde. Ook de effecten van AI op de ontwikkeling van algoritmen en de onzekerheid daaromtrent mag verbeteringen niet in de weg staan.

In 2024 staan de volgende stappen gepland:

- Met het iVeiligheidsteam aan de slag gaan met role based access. Autorisatiematrices opstellen voor de top40 applicaties en de toetsing van de autorisaties inrichten.
- Op afdelingsniveau oefenen met en verbeteren van de continuïteitsplannen.
- Over de gekozen KPI`s en aan de hand van de IT roadmap door middel van raadsbrieven terugkoppeling geven aan de raad zodat deze hier op kan sturen.
- Maatregelen die volgen uit de AVG afdelingsplannen plannen en uitvoeren.
- Alle medewerkers volgen de eLearning herhalingsmodule Informatiebeveiliging en Privacy.
- Leden van het college scholen op het vlak van informatiebeveiligingsrisico`s.
- Investeren op het vlak van iBewustzijn, met name als het gaat om het meten van vooruitgang.
- Onderhoud van de verantwoording via de Cybermanager inrichten.
- Technische maatregelen uit de accountantscontrole/ENSIA/H@ckRijkVanNijmegen/NIS2.
- Organisatorische maatregelen in het kader van de accountantscontrole/ENSIA/NIS2.

Het controleplan 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 en toetsingen door het jaar heen.

Deze informatie wordt verkregen door gesprekken zoals de prestatiedialoog en uitvragen via rapportages.

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. Met name in de context van het Veiligheidsproject dat iRvN in 2023 heeft afgerond zijn een aantal acties uitgevoerd. In 2023 groeit het Veiligheidsproject door het Hunt & Hackett project waarin een aantal maatregelen worden genomen, gebaseerd op de gap analyse die zij hebben uitgevoerd.

Deze maatregelen zijn niet uitsluitend technisch. De effectieve verbetering van de veiligheid is het resultaat van een combinatie van technische maatregelen, het correcte gebruik ervan en de opvolging van geïdentificeerde zwakheden (Design and Operational effectiveness). De gecombineerde effectiviteit van de ontworpen maatregel en het gebruik er van wordt getest en verbeterd aan de hand van het test resultaat.

In 2022 is iRvN daarom gestart met het BIO TPM-project, het verkrijgen van een derdenverklaring over de kwaliteit van haar ICT dienstverlening op basis van het BIO normenkader. Het doel van dit project is om een voorspelbare kwaliteit te leveren en deze inzichtelijk en controleerbaar te maken door middel van een jaarlijks uit te geven TPM voor die informatieverwerkingen waarvoor iRvN optreedt als Verwerker in het kader van de AVG. Kwaliteitsbeheersing is alleen mogelijk als prestaties meetbaar en toetsbaar zijn.

Het BIO TPM-project heeft een geplande looptijd van drie jaar. Gedurende deze periode worden de processen van iRvN beoordeeld, gedocumenteerd en klaargemaakt voor audits. De voltooide processen worden jaarlijks beoordeeld door een externe auditor. Elk jaar worden er nieuwe elementen toegevoegd. Na het derde jaar, mits alles volgens plan verloopt, wordt de volledige TPM uitgereikt en wordt het project formeel afgesloten. Alle interne en externe beoordelings- en auditactiviteiten worden vanaf dat moment opgenomen in een jaarlijkse standaard verantwoordingscyclus.

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 verder ingevoerd worden, waarbij alle niveaus van de organisatie betrokken zullen 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 de controleplannen 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. 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 werken wij in 2024 aan de toetsing van werking. Binnen gemeente Nijmegen is deze ontwikkeling aangekondigd en is er in de verantwoording over 2023 mee geoefend. 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. Het ministerie van Binnenlandse Zaken heeft aangekondigd dat het streven is om informatieveiligheid bij de overheid een wettelijke basis te geven. Dit moet gebeuren via een zorgplicht waaraan meer regelgeving kan worden gehangen, zoals de BIO. Door het wettelijk verplichten van de BIO via de Wbni is de vrijblijvendheid voorbij. Bij het toezicht zal niet alleen worden gekeken naar de naleving van algemene regels zoals 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 zijn de ontwikkelingen 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. 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 hierop 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. Er zal in de komende jaren gewerkt worden aan een centraal klantportaal “mijn Nijmegen” en aan de beschikbaarheid van verschillende kanalen voor de burger om contact op te nemen met onze gemeente “omni channel”. Dit moet op een veilige en eenduidige manier mogelijk gemaakt worden.

5.3.2 Privacy

De uitdagingen op het terrein van privacy en informatiebeveiliging zijn ook in de komende jaren onverminderd groot. Om daarop in te spelen wordt verder ingezet op:

Van implementatie naar beheer / controle

De inrichting van de CyberManager voor informatiebeveiliging, privacy en de Wpg heeft in 2023 een volgend stadium bereikt door het invoeren van normenkaders en het daaraan koppelen van maatregelen om naleving te monitoren. Voor het verkrijgen van inzicht in de risico’s die we lopen op het vlak van informatiebeveiliging en de status van de te treffen maatregelen is het nu nodig dat de afdelingen zelf aan de slag gaan met de risico analyses en de implementatie van maatregelen.
De eerste stap hiertoe is eind november 2023 genomen. In een werksessie met de privacy-ambassadeurs is een zelf-evaluatie gedaan gebaseerd op genoemde normenkaders. De resultaten hiervan worden opgenomen in het jaarverslag van de FG.

De check op de “in control-maatregelen” (= de onderdelen van het controlplan) willen we als volgt invullen:

- Via het systeem CyberManager kunnen we zien welke maatregelen getroffen zijn en welke nog niet. Hier kan een actie uit voortkomen. Dit betreft informatie die voorradig is in het systeem (werkwijze: check melding in systeem en opvolging daarvan).
- Via gerichte vragen kunnen we nagaan of met name ‘nalevingen’ plaatsvinden i.c. wordt ook datgene gedaan wat we afgesproken hebben. Dit gaat met name over houding en gedrag. Deze vragen worden aan de afdelingshoofden - als gegevensverantwoordelijke – gesteld (medium = vragenlijst).

Tenslotte gaan we via gerichte steekproeven “checken” wat de kwaliteit van maatregelen is.

Het is noodzakelijk het komend jaar verder aan de slag te gaan met de ingezette lijn. Dat betekent dat de volgende stappen staan gepland:

- Het gebruik van de CyberManager verder uitrollen;
- Maatregelen die volgen uit de afdelingsplannen op basis van het project “mijn afdeling AVG proof” implementeren;
- Maatregelen op het vlak van de kwaliteit van data (in de context van datagestuurd werken) zullen per bron worden opgepakt;
- Implementeren van de aanbevelingen van de Functionaris voor de Gegevensbescherming op basis van het uitgevoerde controleplan over 2023.
- Het sturen op ‘spontane naleving’. Dat wil zeggen dat de aspecten (zoals kennis en kunde, kosten/baten, mate van acceptatie etc.) ten behoeve van spontane naleving terugkomen in de aansturing van medewerkers; denk aan afspraken rond opleiding.

Bewustwording en weerbaarheid

Op het gebied van bewustwording heeft in 2019 een ‘mystery visit’ plaatsgevonden. Hier zijn een aantal verbeterpunten uit naar voren gekomen. Die hebben wij in 2020 en 2022 geïmplementeerd. Dit heeft onder andere geleid tot een voorstel tot het benoemen van i-bewustzijn als belangrijk thema voor de Nijmegen School in 2022. In de digitale opleidingsmodule zijn verplichte leerlijnen over Privacy en Informatiebeveiliging opgenomen voor alle medewerkers. De uitkomsten van deze actie worden meegenomen in het opleidingsprogramma. Dit heeft (mede) geleid tot de implementatie van een wachtwoordmanager en mobile device management.
In 2023 is het Gedragsteam Nijmegen van Nu opgericht. Dat is een team waarin verschillende expertises (communicatie, gedrag, P&O, privacy, informatiebeveiliging, dienstverlening) samen zijn gebracht. Dit team zorgt voor gecoördineerde interventies, onder andere op het vlak van privacy en informatiebeveiliging. Verder is in 2023 de leerlijn ‘ransomware’ verplicht gesteld aan al onze medewerkers.

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 BIO 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. 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 BIO 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 de enige die risico`s kunnen accepteren.

Afkortingen

Afkorting	Uitleg
AVG	Algemene Verordening Gegevensbescherming. In werking getreden op 25 mei 2018. Sinds dat moment geldt in de gehele Europese Unie dezelfde privacywetgeving.
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.
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
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.
DKD-inlezen	Digitaal Klantdossier gegevens die ingelezen kunnen worden vanaf het Inlichtingenbureau met betrekking tot werk en inkomen.
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.

Afkorting	Uitleg
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.
NOREA	Nederlandse Orde van Register EDP-Auditors is de beroepsorganisatie van IT-auditors in Nederland.
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, 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).