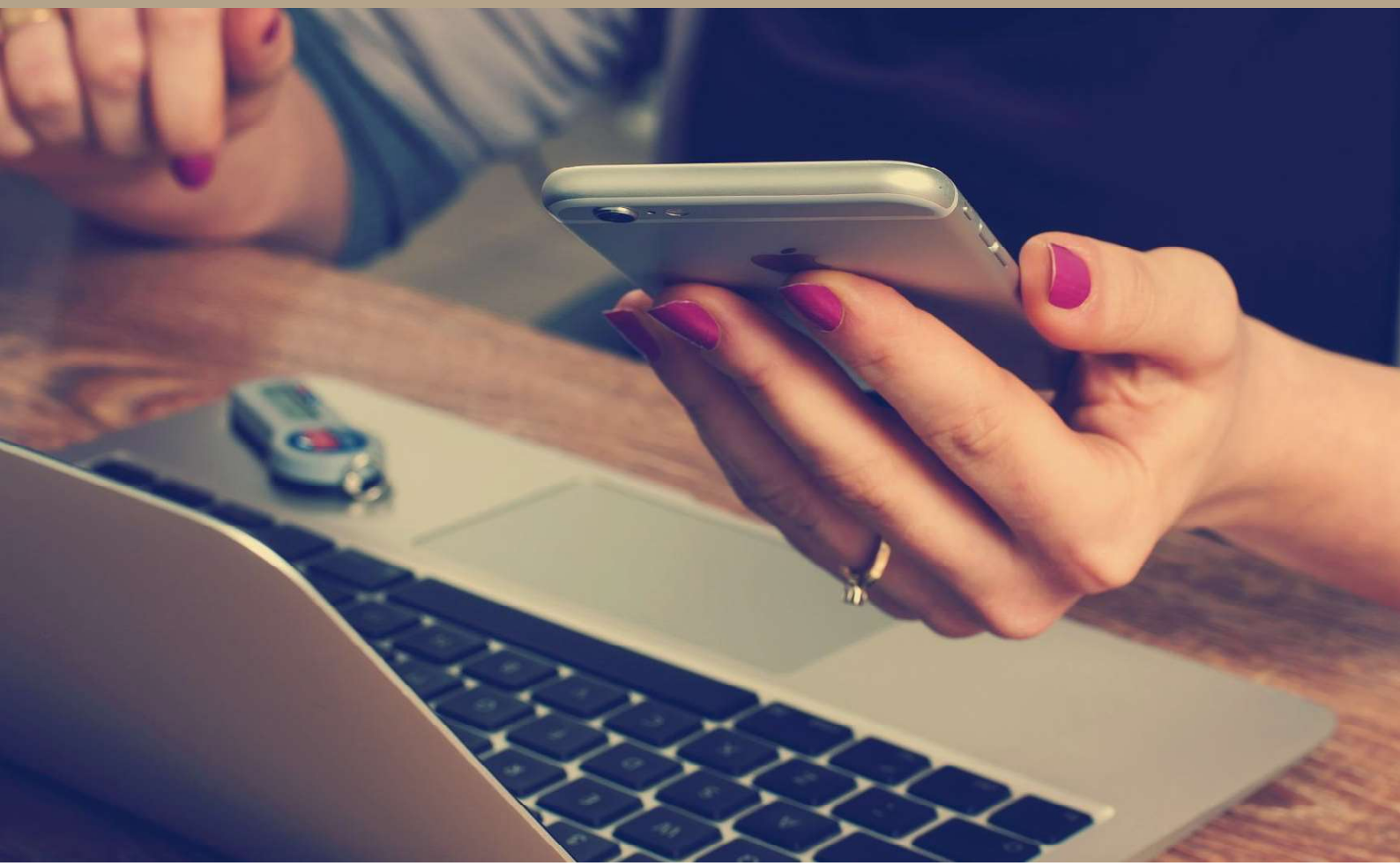
BMC
YACHT GROUP

Breed onderzoek informatiebeveiliging en privacy

Eindrapportage



Eindrapport | 29 november 2021

Partners in verbetering

Breed onderzoek informatiebeveiliging en privacy

Eindrapportage

Definitief
BAR-organisatie

BMC
YACHT GROUP

Inhoudsopgave

Samenvatting

Inleiding

De BAR-organisatie omvat de ambtelijke organisatie van de gemeenten Barendrecht, Albrandswaard en Ridderkerk. Voor deze gemeenten zijn informatiebeveiliging en privacy van groot belang. Daarom heeft de directieraad in 2020 besloten tot het instellen van een programma Informatieveiligheid en Privacy, aangestuurd door een stuurgroep met vertegenwoordigers uit directie en management. Naar aanleiding van een rekenkameronderzoek en een onderzoek van Concerncontrol en recente calamiteiten elders in het land - zoals de ransomwareaanval bij de gemeente Hof van Twente - is er eind 2020 een uitvoeringsplan opgesteld in opdracht van het dagelijks bestuur (DB) van de BAR-organisatie. Daarbij heeft het DB besloten in 2021 pilots te starten om op gebieden met de grootste risico's extra beveiligingsmaatregelen te nemen. Tussentijds hebben de drie verantwoordelijke bestuurders in de zomer van 2021 ook nog opdracht gegeven tot het nemen van aanvullende maatregelen om de risico's van cyberaanvallen te verkleinen. Tevens heeft het DB de opdracht aan de BAR-organisatie gegeven om eind 2021 met een totaalplan te komen ten aanzien van informatieveiligheid en privacy. Daarbij is het de vraag waar de BAR-organisatie staat op het gebied van informatiebeveiliging en privacy, wat relevante ontwikkelingen zijn, wat een acceptabel niveau is en hoe daar te komen. De stuurgroep heeft daarom gevraagd om een plan van aanpak gebaseerd op een breed onderzoek.

Ontwikkelingen in risico's en bedreigingen

De risico's en bedreigingen ten aanzien van informatiebeveiliging en privacy worden voor de BAR-gemeenten en de BAR-organisatie groter door:

- voortschrijdende digitalisering, datagedreven werken en samenwerking met andere organisaties;
- laagdrempeliger inzet van technologie, zoals clouddiensten en Internet of Things, dat zich mogelijk buiten het blikveld van de CISO en/of Privacy Officer voltrekt;
- een blijvende stroom van kwetsbaarheden in software;
- toegang tot gegevens via en afhankelijkheid van leveranciers en intranet; beide mogelijke aanvalsroutes voor kwaadwillenden;
- toenemende activiteit van buitenlandse overheden ('statelijke actoren') en cybercriminelen, al dan niet gedoogd door door die overheden;
- toenemend bewustzijn in de samenleving en handhaving door toezichthouders.

De BAR-gemeenten en de BAR-organisatie zijn net als andere gemeenten kwetsbaar, omdat de weerbaarheid nog niet voldoende is, zoals onder andere blijkt uit de beperkte implementatie van BIO, AVG en Wpg.

Ambitie - wat is een acceptabel niveau?

De BAR-gemeenten en de BAR-organisatie willen *aantoonbaar* voldoen aan wet- en regelgeving. Daarnaast wil men 'in control' zijn. Dat wil zeggen overzicht hebben over de implementatie en risico's bewust nemen vanuit het bestuur. Men kiest daarbinnen zo veel mogelijk voor een laag ambitieniveau, vanwege de financiële situatie van de gemeenten.

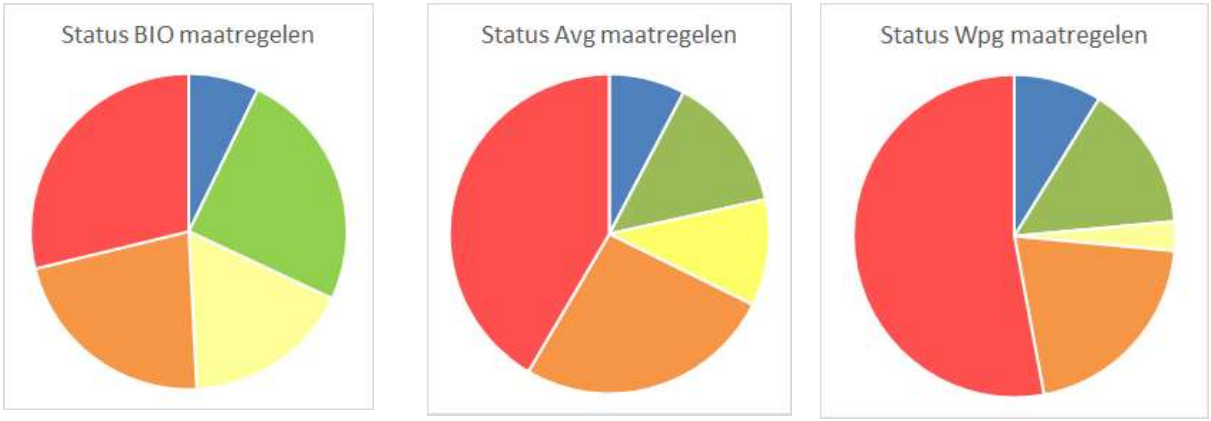
Waar staat de BAR-organisatie?

De organisatorische inrichting van informatiebeveiliging en privacy voldoet nog niet aan de ambitie van de BAR-gemeenten en de BAR-organisatie. Daarbij gaat het onder andere om:

- de inrichting en uitvoering van de plan-do-check-actcyclus;
- de verantwoordelijkheden van en samenwerking tussen centrale expertise in de stafafdelingen en de proceseigenaren, bij de uitvoering van DPIA's en de implementatie van beheersmaatregelen;
- risicoanalyses;
- rapportage en besturing.

De personele inzet, zowel centraal als decentraal, is lager dan bij qua inwonersaantal vergelijkbare gemeenten en te laag om de ambitie van de gemeenten te realiseren.

De implementatie van beheersmaatregelen van BIO en met betrekking tot de AVG en de Wpg is hieronder schematisch weergegeven. Daaruit komt naar voren dat deze implementatie nog niet voldoende is om de ambitie van de organisatie te realiseren.



Legenda status implementatie:

Aanbevelingen

Om de ambitie van de BAR-gemeenten en de BAR-organisatie te realiseren adviseren wij een programma te starten en daarin de volgende aanbevelingen te realiseren:

- Richt de governance/aanpak beter in.
- Realiseer quick wins door onder andere het:
  - inrichten van een DPIA proces;
  - inrichten van checks van processen/applicaties;
  - opstellen en communiceren van een handreiking voor medewerkers.
- Zorg voor een verdere implementatie van de BIO, de AVG en Wpg. Voor voorbeelden van de inhoudelijke aandachtspunten van de implementaties wordt verwezen naar de paragrafen over implementatie van de BIO, AVG en Wpg in hoofdstuk 3.

- Zorg voor voldoende personele inzet door structureel meer formatie toe te wijzen, decentraal rollen te benoemen en tijdelijke ondersteuning in te huren om op het gewenste niveau te komen.

Deze aanbevelingen zijn uitgewerkt in een plan van aanpak. Afhankelijk van keuzes ten aanzien van de personele inzet en de tijdshorizon waarbinnen de organisatie het ambitieniveau wil bereiken, wordt een doorlooptijd verwacht van één tot drie jaar.

H1 | Inleiding

De BAR-organisatie is een gemeenschappelijke regeling die de gezamenlijke ambtelijke organisatie vormt voor de gemeenten Barendrecht, Albrandswaard en Ridderkerk. Voor deze gemeenten zijn informatiebeveiliging en privacy van groot belang. Daarom heeft de directieraad in 2020 besloten tot het instellen van een programma Informatieveiligheid en Privacy, aangestuurd door een stuurgroep met vertegenwoordigers uit directie en management. Naar aanleiding van een rekenkameronderzoek en een onderzoek van Concerncontrol en recente calamiteiten elders in het land - zoals de ransomwareaanval bij de gemeente Hof van
Twente - is er eind 2020 een uitvoeringsplan opgesteld in opdracht van het dagelijks bestuur (DB) van de BAR-organisatie. Daarbij heeft het DB besloten in 2021 pilots te starten om op gebieden met de grootste risico's extra beveiligingsmaatregelen te nemen. Tussentijds hebben de drie verantwoordelijke bestuurders in de zomer van 2021 ook nog opdracht gegeven tot het nemen van aanvullende maatregelen om de risico's van cyberaanvallen te verkleinen. Tevens heeft het DB de opdracht aan de BAR-organisatie gegeven eind 2021 met een totaalplan te komen ten aanzien van informatieveiligheid en privacy. Daarbij is het de vraag waar de BAR-organisatie staat op het gebied van informatiebeveiliging en privacy, wat relevante ontwikkelingen zijn, wat een acceptabel niveau is en hoe daar te komen. De stuurgroep heeft daarom gevraagd om een plan van aanpak gebaseerd op een breed onderzoek.

Deze rapportage bevat antwoorden op deze vragen. In hoofdstuk 2 wordt ingegaan op het voor de BAR-organisatie acceptabele niveau en in hoofdstuk 3 wordt beschreven waar de BAR-organisatie staat op het gebied van informatiebeveiliging en privacy. In hoofdstuk 4 worden ontwikkelingen, bedreigingen en risico's beschreven in relatie tot de BAR-organisatie. Hoofdstuk 5 bevat conclusies op basis van het voorgaande en aanbevelingen om tot het door de BAR-organisatie geambieerde niveau te komen. In hoofdstuk 6 is dit uitgewerkt in een voorstel voor een plan van aanpak, dat in het vervolg nog nader gevalideerd en uitgewerkt dient te worden.

H2 | Wat is een acceptabel niveau van borging?

2.1 Kaders in wet- en regelgeving

2.1.1 De Algemene Verordening Gegevensbescherming (AVG)

De belangrijkste kaders die de Algemene Verordening Gegevensbescherming (AVG) schept ten aanzien van de inrichting en beheersing van privacy en informatiebeveiliging zijn (licht geparafraseerd) de volgende:

- passende technische en organisatorische maatregelen treffen om te kunnen waarborgen en aantonen dat wordt voldaan aan de AVG (AVG Art. 24 lid 1);
- privacybeleid (AVG Art. 24 lid 2);
- passende beveiligingsmaatregelen treffen (AVG Art. 32 lid 1), rekening houdend met de stand van de techniek, uitvoeringskosten [...] en risico's;
- de maatregelen evalueren en indien nodig actualiseren (AVG Art. 24 lid 1).

Concreet betekent dit:

- Op basis van onder andere geïnventariseerde risico's, de stand van de techniek en kosten moet worden bepaald welke maatregelen passend zijn om privacy en informatiebeveiliging te waarborgen.
- Die maatregelen moeten aantoonbaar worden geïmplementeerd.
- De maatregelen moeten worden gecontroleerd en geëvalueerd en op basis daarvan worden verbeterd.
- Een en ander wordt op basis van beleid (planmatig) gerealiseerd.

In deze eisen komt de plan-do-check-actcyclus uit het kwaliteitsmanagement naar voren:

- Plan: uitwerken en documenteren hoe de maatregelen worden geïmplementeerd ('zeggen wat je doet'). Daarbij horen beleid, richtlijnen, procedures en sjablonen. In auditterminologie gaat het hier om de 'opzet'.
- Do: implementeren van de maatregelen op een transparante, aantoonbare manier ('doen wat je zegt') over de gehele organisatie en alle informatiesystemen. Daarbij kan de diepgang variëren afhankelijk van de gevoeligheid van de gegevens. Bij het aantonen hoort het documenteren van de resultaten (de 'output') van de maatregelen. In auditterminologie gaat het hier om het 'bestaan'.
- Check:
    - Op basis van risico's, de stand van de techniek en kosten evalueren welke maatregelen passend zijn voor de organisatie en welke diepgang van implementatie passend is.
    - Per maatregel controleren/evalueren of de maatregelen (nog) goed/voldoende werken en voor alle relevante informatiesystemen zijn geïmplementeerd.
- Act: op basis van deze evaluaties verbeteren van maatregelen of extra maatregelen invoeren.

Het privacy- en informatiebeveiligingsbeleid is een voor de hand liggende plek om deze aanpak op hoofdlijnen in vast te leggen.

2.1.2 De Wet politiegegevens (Wpg)

De Wet politiegegevens (Wpg) (onder andere Wpg Art. 4a) is van toepassing op persoonsgegevens in het kader van opsporing van strafbare feiten. De AVG is daarop niet van toepassing. In de gemeentelijke context is de Wpg van toepassing op het strafrechtelijke deel van de taken van boa's.
De Wpg sluit aan bij bovenstaande aanpak van de AVG en stelt een aantal meer specifieke eisen, zoals:

- expliciete gedocumenteerde besluiten rond autorisatie;
- een DPIA (gegevensbeschermingseffectbeoordeling);
- bewaartermijnen;
- documentatie van onder andere verstrekkingen en onderzoeken;
- logging;
- interne en externe audits, waarbij niet alleen 'opzet' en 'bestaan' worden onderzocht, maar ook de 'werking'. Bij 'werking' gaat het om het vaststellen van de consequente uitvoering van een maatregel over een afgelopen periode, bijvoorbeeld door representatieve steekproeven.

Uit deze audits die zowel opzet, bestaan als werking beoordelen, komt ook voor de Wpg de noodzaak van de implementatie van een plan-do-check-actcyclus voort.

2.1.3 De Baseline Informatiebeveiliging Overheid (BIO)

De Baseline Informatiebeveiliging Overheid (BIO) is geadopteerd door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) en - namens de gemeenten - door de Vereniging van Nederlandse Gemeenten (VNG). Daarmee is dit een de facto standaard en daarmee de basis voor de passende informatiebeveiliging die op basis van de AVG is vereist.
De BIO is een baseline: een basisniveau voor informatiebeveiliging. In specifieke gevallen zullen aanvullende maatregelen passend of nodig zijn of kunnen maatregelen niet van toepassing, niet passend of in mindere mate nodig zijn. Dit is te beoordelen op basis van een expliciete risicoafweging (pas toe of leg uit, BIO paragraaf 4.2). Een dataclassificatie kan helpen om deze afweging efficiënt op hoofdlijnen te maken. Daarnaast is de DPIA een instrument om bij verwerkingen van persoonsgegevens met een hoog risico aanvullende maatregelen vast te stellen.
Een van de eisen van de BIO is de implementatie van een ISMS. Onderdeel daarvan is de bovengenoemde plan-do-check-actcyclus. Een eis die ook uit de AVG voortkomt via de eis van passende beveiliging in de AVG (AVG Art. 32 en 24 lid 1).
De BIO is onderdeel van ENSIA op basis van een zelfevaluatie. De resultaten van deze zelfevaluaties geven vaak geen betrouwbaar beeld, omdat er geen heldere criteria zijn voor het invullen van de vragenlijst. Dat is met name lastig bij gedeeltelijke implementatie van maatregelen, omdat vaak alleen 'ja' of 'nee' gekozen kan worden.

2.1.4 Overige

Naast bovenstaande algemene kaders is er specifieke regelgeving rond privacy en informatiebeveiliging voor DigiD, SUWI en basisregistraties, zoals de BRP.

Deze zijn geen onderdeel van dit brede onderzoek, mede omdat voor deze gebieden al externe audits worden uitgevoerd in het kader van ENSIA. De resultaten van deze externe audits moeten te zijner tijd wel worden meegenomen in de risicoanalyse en de keuze van beheersmaatregelen.

2.2 Ambitie van de BAR-gemeenten en de BAR-organisatie

In interviews met leden van de stuurgroep is de ambitie van de organisatie besproken. Daaruit komt het volgende naar voren:

- Men wil aantoonbaar voldoen aan wet- en regelgeving.
- Men wil in control zijn, overzicht hebben en risico's bewust nemen vanuit het bestuur.
- Men kiest daarbinnen zo veel mogelijk voor een laag ambitieniveau, vanwege de financiële situatie van de gemeenten.

Een van de geïnterviewden vergeleek het met een wielerwedstrijd: 'We willen in vergelijking met andere gemeenten zeker niet in de kopploeg zitten die tientallen minuten voor het peloton uitrijdt, maar we willen ook niet achterblijven met de bezemwagen in zicht. We willen goed meekomen in het peloton.'

H3 | Waar staat de BAR-organisatie?

3.1 Organisatorische inrichting informatiebeveiliging en privacy

3.1.1 Verantwoordelijkheden zijn decentraal belegd

In het organisatiemodel van de BAR-organisatie is de lijnorganisatie met directie, managers en teamleiders verantwoordelijk voor het integrale management van de organisatie. Dit betekent dat de managers ook voor privacy en informatiebeveiliging de verantwoordelijke zijn binnen hun afdeling en voor de processen waar zij verantwoordelijkheid voor dragen. Volgens het informatiebeveiligingsbeleid[1] zijn zij dan ook als proceseigenaren verantwoordelijk voor de implementatie en het in stand houden van beveiligingsmaatregelen en de rapportage daarover aan de CISO. Voor privacy zijn de verantwoordelijkheden niet in beleid uitgewerkt. Binnen de lijnorganisatie zijn er geen decentrale informatiebeveiligings- of privacyrollen ingericht en is er geen specialistische expertise op deze gebieden voorzien.
Naast de lijnorganisatie zijn een drietal centrale functies ingericht:

- De taken van de CISO zijn op hoofdlijnen beschreven in een functiebeschrijving met taken, zoals beleid, coördinatie, controle, communicatie en advies.
- De taken en verantwoordelijkheden van de Functionaris Gegevensbescherming (FG) en de Directieraad zijn op hoofdlijnen beschreven in een reglement.
- Over de rol van Privacy Officer (PO) is geen documentatie beschikbaar.

3.1.2 Aanpak is procesgericht

In het informatiebeveiligingsbeleid staat beschreven dat voor elk proces een dataclassificatie, DPIA[2], een BBN-toets[3] en een risicoanalyse moet plaatsvinden. Aangegeven wordt dat de proceseigenaar daarvoor verantwoordelijk is. Dit proces is niet procedureel uitgewerkt. Wel is er een DPIA-vragenlijst beschikbaar.

In de praktijk ligt de nadruk op DPIA's bij veranderingen en die verlopen stroef

In de praktijk worden DPIA's bijna alleen uitgevoerd bij veranderingen in het proces of bij aanbesteding. Bij inkoop, I-advies en initiatieven datagedreven werken wordt hier goed op gelet.
Bij innovaties en veranderingen worden informatiebeveiliging en privacy als een horde gezien omdat dit het proces vertraagt. Dat komt onder andere doordat:

- voor bijna alle verwerkingen een DPIA wordt uitgevoerd, niet alleen voor verwerkingen waarvoor dit verplicht is;
- het proces door de proceseigenaren vaak laat wordt opgestart, zodat er onvoldoende tijd is om het DPIA-proces goed te doorlopen;

[1] Informatiebeveiligingsbeleid, paragraaf 3.4.
[2] Data Protection Impact Analysis; een uitgebreide analyse van het gebruik en van persoonsgegevens, de rechtmatigheid daarvan en de risico's die dit oplevert, op basis waarvan maatregelen worden vastgesteld om risico's te verkleinen.
[3] BBN - Basisbeveiligingsniveau. De BIO onderscheidt drie basisbeveiligingsniveaus. De meeste processen van de gemeente bevinden zich op niveau 2, waarbij processpecifiek extra maatregelen nodig kunnen zijn, bijvoorbeeld in het sociaal domein of bij de boa's. Het hoogste niveau heeft betrekking op staatsgeheimen en is voor gemeenten minder relevant.

- er geen checklist is met basis-beveiligingseisen, waardoor de CISO en de PO bij elk geval intensief betrokken moeten zijn. Hun beperkte capaciteit, ook in relatie tot de omvang van de formatie (zie 3.1.5), wordt daarbij een knelpunt;
- in een aantal gevallen hogere eisen worden gesteld dan passend bij het ambitieniveau van de organisatie, bijvoorbeeld aan leveranciers. Van hen wordt een SOC 2- of ISAE 340x type 2-rapportage verlangd, terwijl dat op dit moment op veel gebieden nog niet de standaard in de markt is: leveranciers voldoen vaak alleen aan ISO 27001, wat een van de opties is in het sjabloon verwerkersovereenkomst van de VNG. De door de BAR gestelde eis aan leveranciers lijkt gemotiveerd te zijn door de onjuiste perceptie dat de implementatie en borging van maatregelen bij een ISO 27001-certificering niet getoetst zou worden. In paragraaf 8.1 van ISO 27001 wordt vereist dat de vastgestelde maatregelen worden gepland, geïmplementeerd en beheerst. In de richtlijnen voor auditoren (ISO 27006) staat dat het auditbewijsmateriaal voldoende moet zijn om te concluderen dat de beheersmaatregelen doeltreffend zijn.

De DPIA-adviezen worden onvoldoende opgepakt en zijn onvoldoende concreet voor proceseigenaren

In de DPIA-rapportages worden adviezen gegeven voor beheersmaatregelen. Deze worden in de praktijk onvoldoende opgepakt door de proceseigenaren. De indruk van geïnterviewden is dat de beveiligingsmaatregelen vaak wel als opzet of intentie worden beschreven, maar niet echt worden geïmplementeerd en geborgd.
De adviezen in de DPIA's zijn vrij algemeen, zoals het opstellen van een informatiebeveiligingsplan. Mogelijk biedt dit het lijnmanagement onvoldoende handvatten om dit te implementeren, mede gezien de beperkte expertise in de lijn.

Terugkerende DPIA-adviezen worden niet centraal gecoördineerd en/of geïmplementeerd

Een aantal in de DPIA's terugkerende adviezen zouden beter en gemakkelijker gerealiseerd kunnen worden met behulp van een organisatiebrede basis voor de processpecifieke implementatie, die afgestemd op elk proces/elke applicatie geïmplementeerd kan worden. Dat geldt bijvoorbeeld voor een indienst- en uitdienstproces, een autorisatieproces, versleuteling van gegevens en logging.
Een organisatiebrede basisimplementatie ligt niet in de lijn van de huidige aanpak van informatiebeveiliging en privacy in de organisatie. De formele verantwoordelijkheid ligt immers geheel bij de proceseigenaren van de primaire processen. Er is daarom geen afweging gemaakt welke maatregelen het beste centraal of decentraal kunnen worden gefaciliteerd, gecoördineerd en/of geïmplementeerd. In de praktijk wordt een aantal maatregelen rond ICT en huisvesting wel centraal opgepakt.

De DPIA-adviezen dekken niet de breedte van de BIO of de AVG af

De geadviseerde maatregelen dekken enkele specifieke risico's voor de onderzochte processen af, maar niet de breedte van de BIO/AVG. Daarom wordt pas een adequaat beveiligingsniveau bereikt wanneer ook de BIO/AVG volledig zijn geïmplementeerd.

DPIA-rapportages voldoen niet aan de eisen van de AVG en de toezichthouders

De DPIA-rapportages voldoen niet volledig aan de eisen van de AVG en de toezichthouders. Zo ontbreekt de systematische beschrijving van de verwerking en een beoordeling van de noodzaak en evenredigheid van de verwerking. Er is geen overzicht over de mate waarin deze beveiligingsmaatregelen door de verschillende lijnafdelingen worden toegepast.

3.1.3 Besturing

Centraal in de besturing van privacy en informatiebeveiliging staat de stuurgroep programma I&P. De stuurgroep bestaat uit vertegenwoordigingen vanuit bestuur en directie, hoofd I&A, inkoop/juridische zaken, de concerncontroller, FG en CISO. De rol van de stuurgroep is niet in het informatiebeveiligingsbeleid vastgelegd. De stuurgroep bespreekt in de praktijk de voortgang van lopende acties en opdrachten vanuit het bestuur op basis van mondelinge rapportage van de deelnemers. Nieuwe verbeterinitiatieven worden in deze stuurgroep besproken en besluitvorming voor directie en bestuur wordt voorbereid. Voorbeelden zijn:

- het uitvoeringsplan naar aanleiding van onderzoeken van concern control en de rekenkamer Ridderkerk;
- het 8-puntenplan naar aanleiding van adviezen van de IBD/NCSC.[4]

Voor deze acties zijn voorstellen gemaakt voor de besluitvorming. Ze zijn niet uitgewerkt in concrete projectplanningen met deelstappen/resultaten. Dat maakt een goede projectbeheersing lastig.
We zien dat de voorstellen deels gaan om eerste stappen naar de volledige implementatie van maatregelen. Er is geen overkoepelende roadmap voor de vervolgstappen.

Verbeteracties worden tot nu toe met name door dit soort ontwikkelingen van buiten geïnitieerd, niet op basis van een integrale risicoanalyse en/of normatieve kaders vanuit AVG, Wpg of BIO. Daardoor ontbreekt het aan overzicht en een totaalbeeld van de huidige situatie en de weg naar de toekomst. Mogelijk daardoor blijven belangrijke aandachtsgebieden, zoals bewustwording en training van medewerkers buiten het blikveld.
In het uitvoeringsplan wordt dit geassocieerd met een volwassenheidsniveau ‘informeel’ of ‘ad hoc’.

Naast de sturing door de stuurgroep acteren hoofd I&A, CISO, PO en FG in de coördinatie van informatiebeveiliging en privacy, zonder formele besturingsprocessen. Wanneer daar aanleiding voor is, worden directie en bestuur erbij betrokken en beide staan daar ook voor open.

In de besturing spelen de proceseigenaren een bescheiden rol, vooral wanneer specifieke vraagstukken naar voren komen, zoals de verstrekking van gegevens aan het bestuur. Dit ofschoon zij volgens het beleid en de besturingsfilosofie van de organisatie eigenlijk verantwoordelijk zijn. Door het ontbreken van een rapportage in meetbare doelen kunnen zij daarop niet worden aangesproken.

[4] NCSC, Handreiking Cybersecuritymaatregelen, juni 2021

Inmiddels wordt er gewerkt aan een rapportagestructuur die verder gaat dan alleen de stuurgroep, directie en bestuur. In de aangeleverde documentatie zijn rapportagelijnen, verantwoordelijkheden en taken beschreven. Waarover wordt gerapporteerd, zoals KPI en hoe dat wordt gemeten, is nog niet uitgewerkt.

3.1.4 Risicomanagement

Risicomanagement kan plaatsvinden op verschillende niveaus:

- Gemeentebreed overkoepelend: in de jaarlijkse gemeentebrede risicoanalyse in de begrotingen staat informatiebeveiliging op de vierde plaats met een bedrag van in totaal circa € 2,5 miljoen. Het gaat om een risico met een grote impact, maar de kans wordt vooralsnog klein ingeschat.
- Gemeentebreed specifiek op informatiebeveiliging: deze analyse vindt niet structureel plaats. Indirect en op deelgebieden worden risico's geïdentificeerd door bevindingen uit audits en in het kader van de analyse van het zogenoemde 8-puntenplan.
- Per proces: dit wordt incidenteel, bij veranderingen, gedaan in het kader van het DPIA-proces. Dit resulteert in adviezen. De risico's en de implementatie van de adviezen worden niet gemonitord. Er is geen overzicht over welke processen met DPIA zijn afgedekt.

3.1.5 Personele inzet

De huidige vaste formatie voor informatiebeveiliging en privacy bestaat uit:

- CISO: 1 fte
- FG: 0,2 fte (extern)
- PO: 1 fte

Voor de CISO en de Privacy Officer is een tijdelijke projectondersteuner ingezet. In de lijnorganisatie - onder verantwoordelijkheid van de proceseigenaren - is geen expertise/capaciteit opgebouwd om proceseigenaren bij de uitvoering van hun verantwoordelijkheden te ondersteunen.

Zowel in de interviews met direct betrokkenen als in de gesprekken met anderen die met hen samenwerken wordt aangegeven dat deze capaciteit niet toereikend is. Daarnaast maakt de bezetting van deze rollen door enkele personen de organisatie kwetsbaar wanneer zij afwezig zijn of vertrekken.
CISO, PO en FG ervaren de beperkte formatie als belemmerend om hun taken goed te kunnen uitvoeren. Hoewel de CISO en de PO hun best doen om ook structurele zaken op te pakken, wordt hun werk gedomineerd door ad-hoc- en operationele zaken. Medewerkers die werken aan innovaties/veranderingen zien dat hun projecten vertragen omdat ze de CISO en de PO nodig hebben voor afstemming over DPIA's et cetera.

Breder in de organisatie zien we dat capaciteit is of wordt opgebouwd op beleidsspeerpunten, zoals datagedreven werken en handhaving. Juist voor deze onderdelen is een goede ondersteuning op het gebied van privacy en informatiebeveiliging nodig.

In het uitvoeringsplan van februari 2021 wordt de volgende *extra centrale* capaciteit voorgesteld:

- ISO: 1 fte
- FG: 0,4 fte
- PO: 1 fte
- ISO/PO cluster Maatschappij: 1 fte
- tijdelijk 1 fte Business Continuity Manager

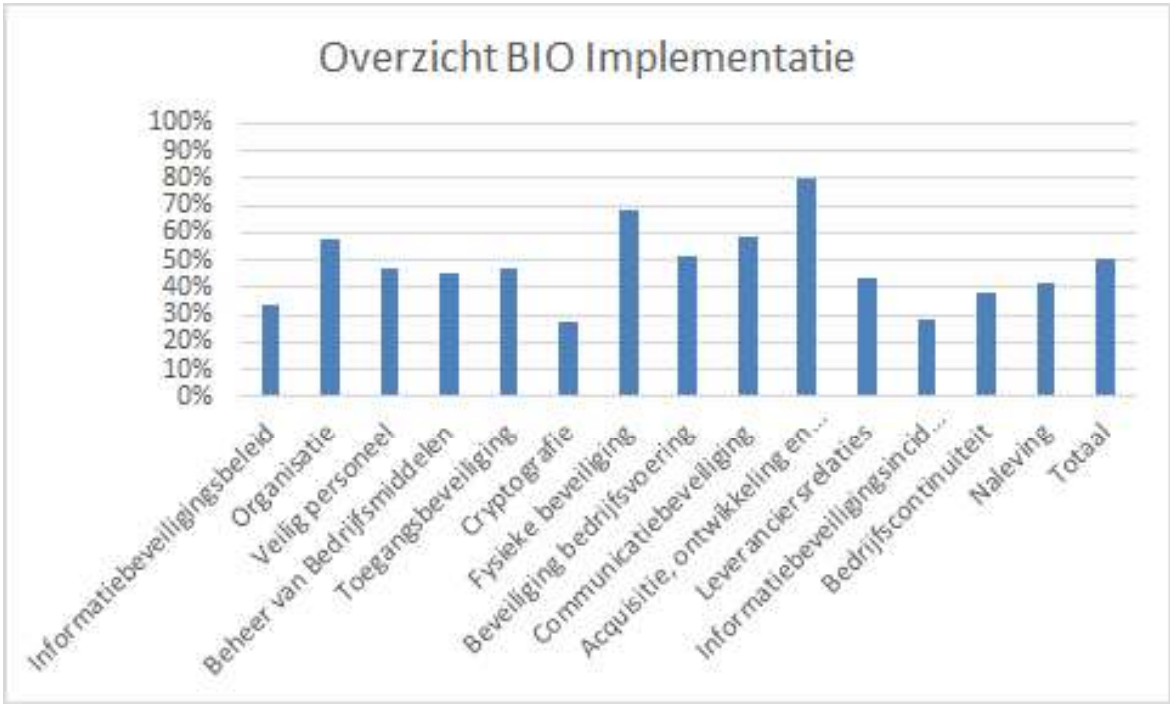
Daarmee zou de structurele capaciteit toenemen van 2,2 fte naar 5,6 fte (3,1 fte Privacy, 2,5 fte Informatiebeveiliging). Decentrale capaciteit is in het uitvoeringsplan niet voorzien. In het kader van het uitvoeringsplan is inmiddels een projectondersteuner voor de CISO en de PO aangetrokken.

3.2 Implementatie van de BIO

3.2.1 Algemeen beeld

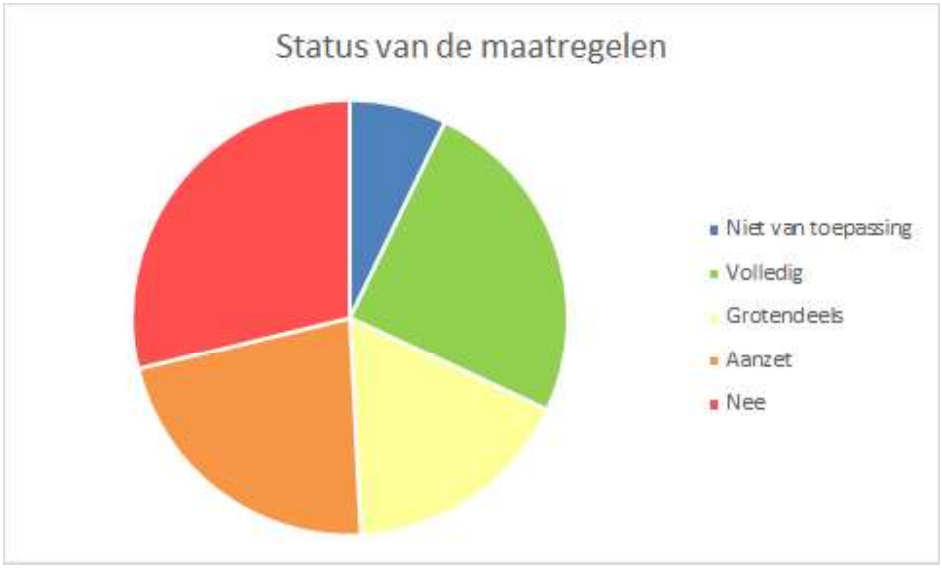
Het algemene beeld is dat de implementatie van de BIO fragmentarisch is, wat past in het beeld van ad hoc werken aan informatiebeveiliging. De aanpak lijkt pragmatisch, waarbij het documenteren van maatregelen en het borgen door een controle van de implementatie onderbelicht is. Een uitzondering daarop vormt het fysieke toegangsbeleid dat is beschreven. Dit wordt aantoonbaar uitgevoerd en periodiek gecontroleerd.
Voor een aanzienlijk deel van de overige maatregelen ontbreekt documentatie, borging en overzicht over de implementatie, bijvoorbeeld voor verschillende applicaties.

Per maatregel is de mate van implementatie gescoord (afwezig, aanzet, grotendeels, volledig). Daarbij zijn telkens tussen de 0 en 3 punten toegekend voor documentatie van de opzet, de implementatie en de borging van de beheersmaatregelen. Wanneer documentatie van de opzet of de borging ontbreken, worden er maximaal 2 punten toegekend.
Daaruit ontstaat per hoofdstuk van de BIO het volgende beeld, zie figuur 1.


Overzicht BIO Implementatie
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Informatiebeveiligingsbeleid
Organisatie
Veilig personeel
Beheer van Bedrijfsmiddelen
Toegangsbeveiliging
Cryptografie
Fysieke beveiliging
Beveiliging bedrijfsvoering
Communicatiebeveiliging
Acquisitie, ontwikkeling en ...
Leveranciersrelaties
Informatiebeveiligingsincid ...
Bedrijfscontinuiteit
Naleving
Totaal

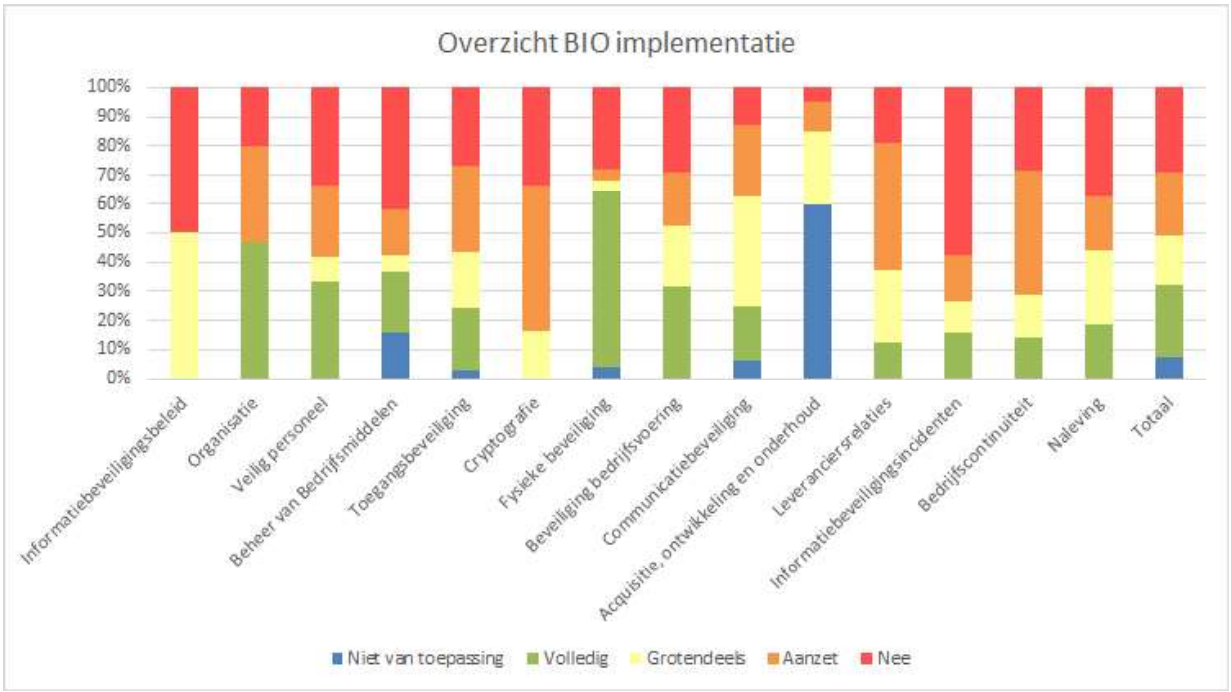
Figuur 1

Uitsplitsing naar de status van de maatregelen geeft het beeld weergegeven in figuur 2.



Figuur 2

Figuur 3 geeft de uitsplitsing van de status van de maatregelen naar de verschillende hoofdstukken weer.



Figuur 3

Dit beeld wijkt significant af van de ENSIA-zelfevaluatie. Dat komt deels omdat er voor de zelfevaluatie geen duidelijke criteria zijn voor het invullen van de vragenlijst.

Dat is met name lastig bij gedeeltelijke implementatie van maatregelen omdat vaak alleen 'ja' of 'nee' gekozen kan worden.

3.2.2 Samenvatting per onderdeel van de BIO

In deze paragraaf geven we de voornaamste aandachtspunten weer:

- **Beleid en organisatie**: Het generieke informatiebeveiligingsbeleid is redelijk volledig, maar de daarin beschreven aanpak leidt nog niet tot een goede implementatie van de BIO in de organisatie. Daarvoor is een verdere uitwerking van de plan-do-check-actcyclus en samenspel tussen centrale staf en proceseigenaren nodig.
  Specifiek informatiebeveiligingsbeleid is alleen beschikbaar voor een viertal gebieden: cryptografie, logging, wachtwoorden en cleandesk/-screen.
- **Veilig personeel**: In de indienst- en uitdienstprocessen is informatiebeveiliging redelijk goed geborgd. De bewustwording en training van medewerkers is beperkt tot een incidenteel bericht op intranet. De geïnterviewde medewerkers lijken goed doordrongen te zijn van het belang van informatiebeveiliging en privacy. Management vindt houding en gedrag belangrijk, maar het ontbreekt ze aan concrete en volledige richtlijnen. Er is geen overkoepelend document over het veilig omgaan met informatie en geen training op dat gebied. Er loopt wel een initiatief om informatiebeveiliging op te nemen in het inwerkproces voor nieuwe medewerkers.
- **Beheer van bedrijfsmiddelen**: Verschillende bedrijfsmiddelen, zoals laptops, smartphones, servers en software, zijn in verschillende systemen opgenomen. Een proces om overzicht te houden over het geheel is niet ingericht. Eigenaarschap en classificatie van informatie zijn niet structureel vastgelegd. Informatie wordt alleen in het kader van DPIA's geclassificeerd. Overige informatie is niet geclassificeerd en een totaaloverzicht ontbreekt. Criteria voor classificatie zijn niet beschikbaar.
- **Toegangsbeveiliging**: De procedure in dienst/doorstroom/uit dienst werkt goed en er is wachtwoordbeleid en een werkinstructie voor de helpdesk opgesteld. Toegangsbeleid en procedures op overige gebieden zijn niet organisatiebreed opgesteld. Er is geen overzicht over de implementatie voor de applicaties.
- **Fysieke beveiliging**: Er is een fysiek toegangsbeleid, dat in de praktijk wordt toegepast en ook borging met controles beschrijft. Tijdens een rondgang op een van de locaties zijn wel afwijkingen van het beleid en enkele verbeterpunten gesignaleerd, onder andere met betrekking tot clear desk en het afsluiten van de archiefruimte. Aandachtspunten zijn verder: de documentatie van de controles, een periodieke fysieke controle/rondgang en de documentatie van bescherming van bedreigingen van buitenaf (natuurrampen, fysieke aanvallen).
- **Technische beveiligingsmaatregelen en incidentafhandeling**: Voor enkele deelgebieden (logging, cryptografie) is beleid opgesteld en in de interviews wordt aangegeven dat een behoorlijk deel van de technische maatregelen is geïmplementeerd, bijvoorbeeld malwarescanning, beveiligingsupdate (patching), back-up en logging van de technische infrastructuur. Daarover kon echter slechts zeer beperkt documentatie worden aangeleverd en er zijn veelal geen gedocumenteerde checks op en overzichten van de uitvoering en mate van implementatie van de maatregelen. Een aantal essentiële technische maatregelen ontbreekt, zoals scheiding van netwerken. Deze zijn inmiddels gedeeltelijk opgenomen in het 8-punten-programma dat door de BAR-organisatie wordt uitgevoerd.

De procedures voor changemanagement en incidentmanagement zijn in de basis goed uitgewerkt; de beveiligingsaspecten en evaluatie daarvan ontbreken nog. Er is wel een conceptprocedure voor beveiligingsincidenten.

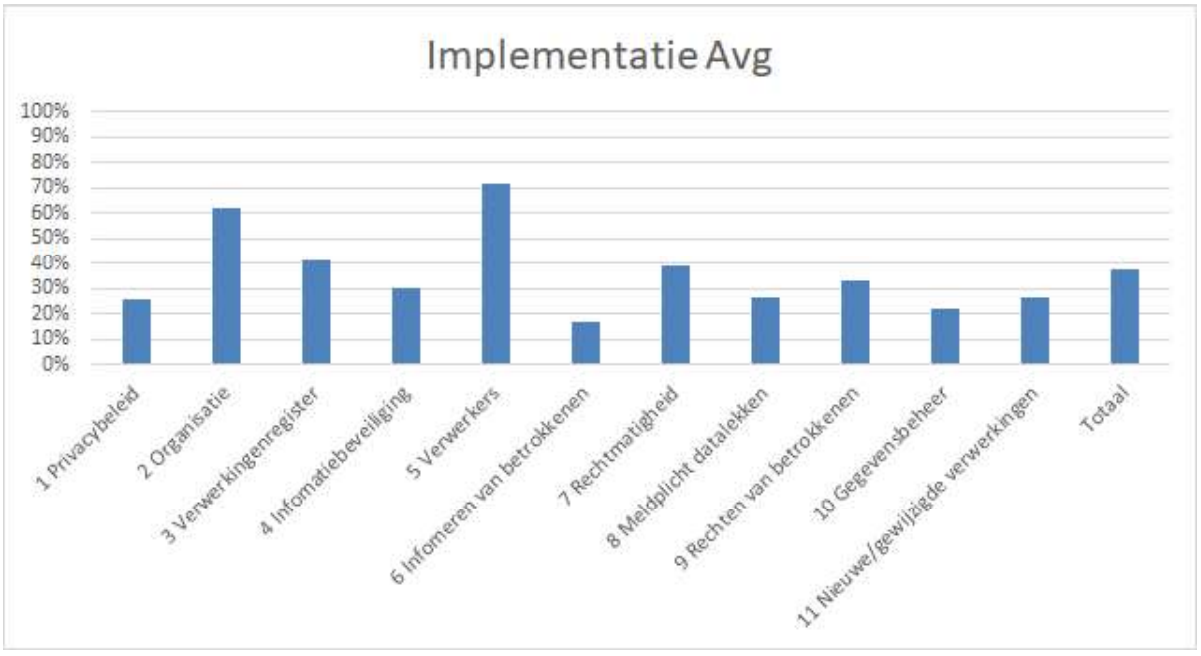
- **Aanschaf, vernieuwing en onderhoud van informatiesystemen**: Bij initiatieven wordt een DPIA uitgevoerd en worden per keer eisen gesteld aan de nieuwe of gewijzigde toepassing. Dit proces is niet beschreven en er is alleen voor cloud computing een lijst van generieke eisen aan leveranciers, diensten en applicaties. De doorlooptijd van dit proces wordt als belemmerend gezien voor de vlotte implementatie van vernieuwingen. Dat komt deels door de beperkte capaciteit van de CISO en de PO, die er intensief bij betrokken zijn.
  Voor een aantal applicaties vinden acceptatietests plaats voor het in productie nemen van nieuwe versies. Dit is niet geborgd voor alle applicaties.
  Een groot deel van de eisen van de BIO op dit gebied is niet van toepassing, omdat de organisatie geen software ontwikkelt.
- **Leveranciersrelaties**: Bij inkoop wordt rekening gehouden met informatiebeveiliging en privacy, maar dit is niet geborgd in het inkoopproces. In de praktijk gebeurt dit wel vrij consequent, doordat het ICT-budget en de -inkopen zijn gecentraliseerd via de afdeling I-advies. Voor inkopen alleen voor cloud-toepassingen zijn basisbeveiligings-eisen opgesteld, waardoor voor veel ICT-inkopen de CISO en/of PO erbij wordt betrokken.
  De afdeling I-advies voert ook het contractmanagement en licentiebeheer voor applicaties. Dat gebeurt voor de belangrijkste applicaties, zonder dat de volledigheid is geborgd. Er vinden geen periodieke leveranciersbeoordelingen plaats met daarin controle op de naleving van afspraken uit verwerkersovereenkomsten.
- **Bedrijfscontinuïteit**: Ten aanzien van de bedrijfsprocessen zijn de eisen voor de continuïteit niet vastgelegd en is er geen continuïteitsplan. Wel is er voor de IT-uitwijk een Calamiteitenplan ICT uit 2017. Daarin staat ook een jaarlijkse uitwijktest beschreven. Een verslag van een recente uitwijktest is aangeleverd.
- **Naleving**: Onafhankelijke beoordelingen van de informatiebeveiligingen vinden plaats in de volgende vormen:
  - Incidentele onderzoeken, bijvoorbeeld door concern control, de rekenkamer of het onderhavige onderzoek in opdracht van de stuurgroep.
  - Incidentele penetratietesten worden genoemd in de interviews. Een verslag van een recente vulnerability scan is aangeleverd. Dat deze periodiek worden uitgevoerd blijkt uit een dashboard met scores vanaf begin 2021.
  - Er is geen audit- en/of controleprogramma op de beheersmaatregelen uit de BIO of een programma voor penetratietesten. Wel is er periodieke scanning op kwetsbaarheden.

3.3 Implementatie van de AVG

3.3.1 Algemeen beeld

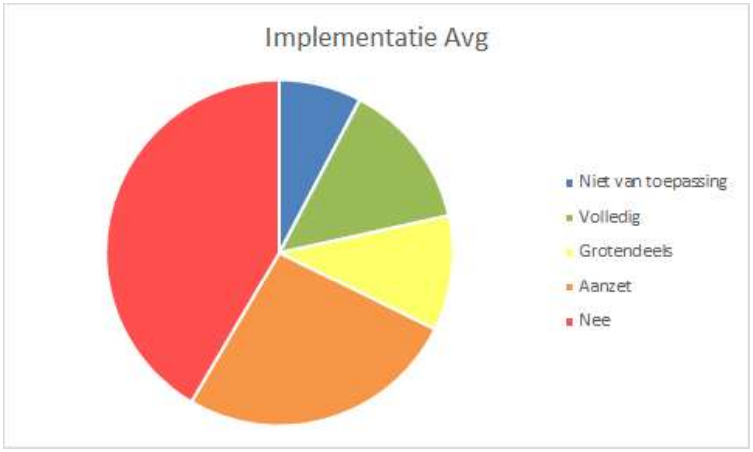
Het algemene beeld ten aanzien van de AVG is dat er op verschillende deelgebieden in het verleden implementaties zijn gestart, maar dat deze niet in de processen van de organisatie zijn geborgd en dat overzichten, zoals het verwerkingenregister, niet periodiek worden geactualiseerd. Andere aspecten zijn nog niet geadresseerd. De PO geeft aan dat zij bezig is met een inhaalslag om een aantal zaken te verbeteren.

Per beheersmaatregel in het door BMC opgestelde controlframework voor de AVG, is de mate van implementatie gescoord (afwezig, aanzet, grotendeels, volledig). Daarbij zijn telkens tussen de 0 en 3 punten toegekend voor documentatie van de opzet, de implementatie en de borging van de beheersmaatregelen. Wanneer documentatie van de opzet of de borging ontbreekt, worden maximaal 2 punten toegekend. Daaruit ontstaat per aandachtsgebied van de AVG het volgende beeld, weergegeven in figuur 4.



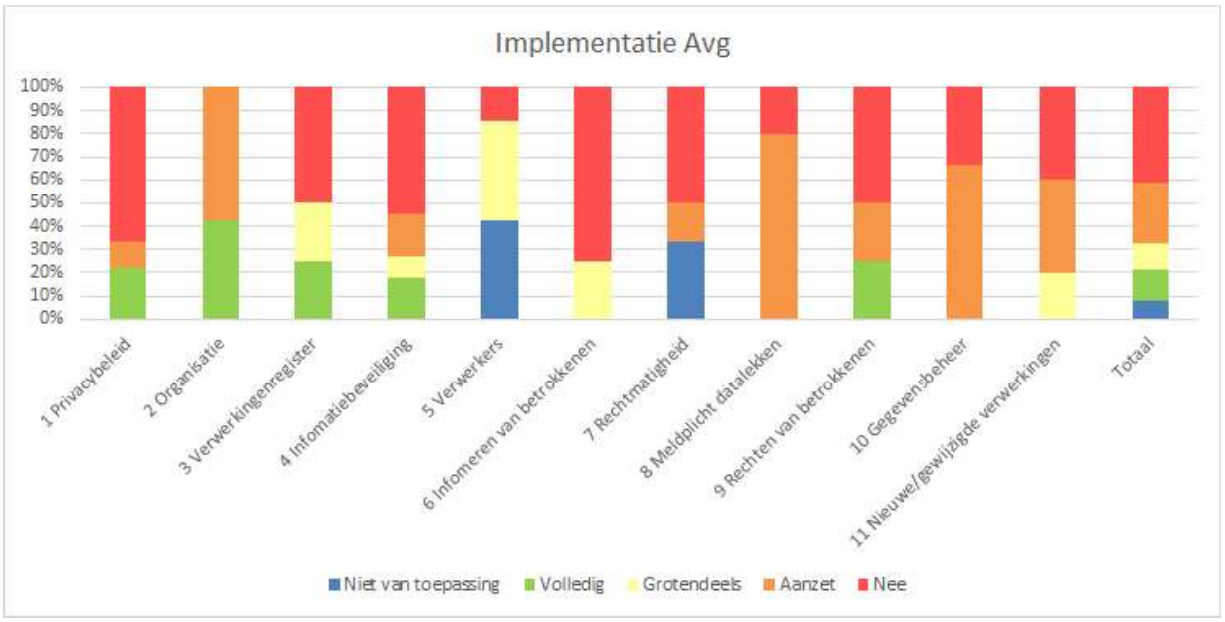
Figuur 4

Figuur 5 geeft de uitsplitsing naar de status van de maatregelen weer.



Figuur 5

Uitsplitsing van de status van de maatregelen naar de verschillende hoofdstukken geeft het volgende beeld, weergegeven in figuur 6.



Figuur 6

3.3.2 Samenvatting per aandachtsgebied

In deze paragraaf geven we de voornaamste aandachtspunten weer:

- **Privacybeleid**: Het privacybeleid richt zich met name op de verantwoordelijkheden tussen de BAR-organisatie en de deelnemende gemeenten. Omdat de BAR-organisatie met elke gemeente werkt onder gezamenlijke verantwoordelijkheid, zoals bedoeld in Art. 26 AVG, is het belangrijk om dit vast te leggen.

Dat is in het bijzonder relevant omdat gegevens van de deelnemende gemeenten in de systemen wel zodanig gescheiden moeten worden dat altijd duidelijk is wie de verantwoordelijke daarvoor is. Het beleid gaat niet in op hoe de AVG in de BAR-organisatie wordt ingericht, geimplementeerd, bewaakt en bestuurd (Plan - Do - Check - Act).

- **Organisatie**: Verantwoordelijkheden vloeien deels voort uit het besturingsmodel van de organisatie (proceseigenaren) en de AVG (FG). De samenwerking en de rol van de PO zijn niet verder uitgewerkt. De geïnterviewden uit het veld zijn zich bewust van het belang van privacy. Management vindt houding en gedrag belangrijk, maar het ontbreekt ze aan concrete richtlijnen. Er is geen overkoepelend document over hoe veilig om te gaan met informatie en geen training. Geïnterviewden geven aan dat het privacykennisniveau in een aantal afdelingen onvoldoende is.
- **Verwerkingenregister**: Er is een verwerkingenregister, maar dat is niet actueel en de juistheid en actualisering van de informatie is niet geborgd.
- **Informatiebeveiliging**: Passende informatiebeveiliging op basis van de BIO is nog niet volledig geïmplementeerd, zoals nader toegelicht in de vorige paragraaf over de BIO. Voor de AVG en de toezichthouder Autoriteit Persoonsgegevens belangrijke beveiligingsmaatregelen, zoals autorisatie en logging van gebruikersgedrag binnen applicaties, zijn niet structureel ingericht.
- **Verwerkers**: Verwerkersovereenkomsten worden afgesloten met leveranciers. De volledigheid daarvan is niet in het proces of met controles geborgd. De naleving van verwerkersovereenkomsten wordt niet gecontroleerd.
  De BAR-organisatie verwerkt voor zover bekend bij de geïnterviewden geen gegevens in opdracht van andere organisaties, waardoor deze onderdelen niet van toepassing (en dus compliant) zijn. Dit is te zijner tijd te valideren op basis van een aangevuld en geactualiseerd verwerkingenregister.
- **Informeren van betrokkenen**: Er staat een privacyverklaring op de websites van de gemeenten. Deze bevat algemene informatie, niet de specifieke informatie per verwerking die de AVG vereist. Er is geen periodieke controle of herziening van de privacyverklaring ingericht. Voor de Wmo is er op het meldingsformulier een privacyverklaring. Deze processpecifieke privacyverklaringen zijn niet organisatiebreed ingericht. Voor de medewerkers is er wel een privacyregeling personeelsinformatie (bijlage 7 van het personeelshandboek).
- **Rechtmatigheid**: De toetsing van rechtmatigheid van de verwerkingen is niet structureel ingericht. Deze komt wel aan de orde bij het uitvoeren van DPIA's bij nieuwe verwerkingen.
  De BAR-organisatie verwerkt volgens de geïnterviewden geen gegevens buiten de EU, waardoor deze onderdelen niet van toepassing (en dus compliant) zijn. Dit is te zijner tijd te valideren op basis van een aangevuld en geactualiseerd verwerkingenregister.
- **Meldplicht datalekken**: Er is een meldpunt voor datalekken op het intranet, geen procedure voor de opvolging daarvan of rapportages over datalekken. Er wordt gewerkt aan een overzicht van datalekken van de afgelopen periode.
- **Rechten van betrokkenen**: Er is een document 'intern proces bij inzageverzoek', met daarin adequate aandachtspunten bij de afhandeling van een inzageverzoek.

In dit document worden de taken in het proces niet toegewezen aan rollen of medewerkers en andere typen verzoeken blijven buiten beschouwing. De contactgegevens van de FG staan wel op de websites van de gemeenten.

- **Gegevensbeheer**: Voor een aantal applicaties, zoals het zaaksysteem, is de vernietiging van gegevens na het verstrijken van de bewaartermijn geregeld. Er is geen overzicht van de status van alle applicaties.
- **Nieuwe/gewijzigde verwerkingen**: DPIA's worden vrij consequent uitgevoerd voor nieuwe of sterk gewijzigde verwerkingen. Deze DPIA's voldoen echter niet aan de eisen van de AVG en de toelichting daarvan door de toezichthouders. Zo ontbreekt de systematische beschrijving van de verwerking en een beoordeling van de noodzaak en evenredigheid van de verwerking. Voor het uitvoeren van DPIA's is een vragenlijst beschikbaar, maar er zijn geen sjablonen voor de rapportage. Periodieke herhaling van DPIA's en de monitoring van de opvolging van acties uit de DPIA's zijn niet ingericht.

3.4 Implementatie van de Wpg

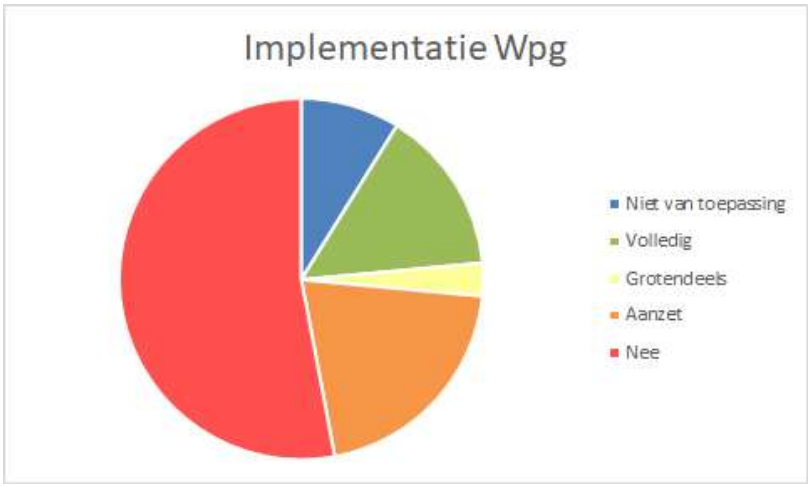
3.4.1 Algemeen beeld

Het algemene beeld is dat de nieuwe Wpg binnen de BAR-organisatie nog niet is geïmplementeerd. Voor zover de organisatie voldoet aan de Wpg is dat op basis van de werkwijze van voor de invoering van de Wpg, de algemene boa-opleiding en beroepsethiek van de boa's en de maatregelen die in het kader van de BIO en de AVG zijn vormgegeven. Ook de inzet van de applicatie CityControl draagt bij aan de compliance, omdat deze een bepaalde werkwijze afdwingt. De groei van het team maakt gedocumenteerde processen en werkafspraken belangrijker dan in het verleden. Te denken valt aan hoe om te gaan met het wisselen tussen de strafrechtelijke en de bestuursrechtelijke 'pet'.

Per beheersmaatregel in het door BMC opgestelde controlframework voor de Wpg is de mate van implementatie gescoord (afwezig, aanzet, grotendeels, volledig). Daarbij zijn telkens tussen de 0 en 3 punten toegekend voor documentatie van de opzet, de implementatie en de borging van de beheersmaatregelen. Wanneer documentatie van de opzet of de borging ontbreekt, worden er maximaal 2 punten toegekend. Daaruit ontstaat per aandachtsgebied van de Wpg het volgende beeld, weergegeven in figuur 7.

Figuur 7

Uitsplitsing naar de status van de maatregelen geeft het volgende beeld, zie figuur 8.



Figuur 8

Figuur 9 geeft de uitsplitsing weer van de status van de maatregelen naar de verschillende hoofdstukken.

Figuur 9

3.4.2 Samenvatting per aandachtsgebied

In deze paragraaf geven we de voornaamste aandachtspunten weer, voor zover deze aanvullend zijn op de punten genoemd bij de AVG:

- **Beleid en organisatie**: Er is op het gebied van de Wpg geen beleid of organisatie beschreven. Wel is er een FG benoemd.
  Er zijn geen handreikingen of gedragsregels voor boa's opgesteld, maar wel informele werkafspraken.
- **Verwerkingenregister en documentatieplicht**: Er is een verwerking opgenomen in het AVG-verwerkingenregister, maar deze bevat onjuistheden. De vanuit Wpg Art. 32 verplichte documentatie is niet ingericht.
- **Informatiebeveiliging**: Aanvullende maatregelen ten opzichte van BIO en AVG zijn niet ingericht.
- **Verwerkers**: Het betreft alleen de verwerkersovereenkomst met Sigmax ten aanzien van CityControl. Deze is aanwezig en adequaat. De naleving van de verwerkersovereenkomst door Sigmax wordt niet periodiek vastgesteld.
- **Rechtmatigheid**: Geautomatiseerde vergelijking en combinatie van gegevens vindt volgens de geïnterviewden niet plaats. Er zijn geen procedures om de rechtmatigheid van ter beschikkingstelling of verstrekking te waarborgen en te documenteren.
- **Meldplicht datalekken**: Zie paragraaf onder AVG.
- **Rechten van betrokkenen**: De beschikbare procedure voor het afhandelen van verzoeken gaat niet in op de Wpg. Het informeren van betrokkenen over de verwerking van politiegegevens is niet ingericht en niet opgenomen in de privacyverklaring op de websites van de gemeenten. De contactgegevens van de FG staan wel op de websites van de gemeenten.

- **Gegevensbeheer**: Aangenomen wordt dat dit via de applicatie CityControl is ingeregeld. Dit is niet bevestigd. Het is niet duidelijk in hoeverre politiegegevens worden verwerkt buiten CityControl.
- **Nieuwe of gewijzigde verwerkingen**: De voor de verwerking van politiegegevens verplichte DPIA is nog niet uitgevoerd. Zie verder de paragraaf hierover onder AVG.

H4 | Ontwikkelingen, bedreigingen en risico's

De risico's rond informatiebeveiliging en privacy voor de BAR-gemeenten nemen toe en zullen blijven toenemen tegen de achtergrond van de ontwikkelingen die we in de volgende paragrafen beschrijven.
Door informatiebeveiligings- en privacyincidenten/datalekken ontstaat schade voor de gemeente en haar inwoners in verschillende vormen (zie ook Dreigingsbeeld informatiebeveiliging IBD 2021):

- het niet beschikbaar zijn van de gemeentelijke dienstverlening;
- imagoschade en vertrouwen in de gemeente en de politiek;
- privacyschade voor inwoners en medewerkers;
- financiële schade voor herstelwerkzaamheden, schadevergoedingen en eventuele boetes;
- schade aan democratische processen.

Met het oog op het onderstaande zien we voor de BAR-organisatie steeds hogere risico's:

- door gemeentelijke ontwikkelingen; het gaat hier met name om vertrouwelijkheid van gegevens en een juiste toepassing van de privacywetgeving;
- door cybercriminaliteit en statelijke actoren; het gaat hier met name om beschikbaarheid en vertrouwelijkheid van informatie.

Deze risico's komen boven op of versterken al langer bestaande risico's zoals onveilig gedrag van gebruikers of natuurrampen.

4.1 Ontwikkelingen bij gemeenten

Met een blik op de toekomst zien we de volgende interne ontwikkelingen voor gemeenten:

- De voortgaande digitalisering van werkprocessen.
- Werken op afstand betekent minder grip op de fysieke en technische omgeving waarin het werk - ook met (zeer) gevoelige gegevens - wordt gedaan.
- Beweging naar datagedreven werken en mogelijk 'big data', waardoor gegevens worden gekopieerd naar aparte omgevingen (data warehouses of data lakes) en gegevens worden gecombineerd. We zien in het algemeen dat medewerkers zich vaak niet bewust zijn van de risico's van datagedreven werken.
- De toenemende burgerparticipatie, zoals vanuit de Omgevingswet.
- Gemeenten spelen een steeds grotere rol in samenwerking, zowel in de zorg als in het veiligheidsdomein, waarbij zeer gevoelige gegevens worden verwerkt.

4.2 Technologische ontwikkelingen

Ten aanzien van technologische ontwikkelingen zien we het volgende:

- Gemakkelijker gebruik van ICT-diensten uit het internet/de cloud zonder tussenkomst van de IT-afdeling en soms zelfs zonder directe betaling. Dit kan leiden tot zogenoemde 'shadow IT': informatie die wordt verwerkt buiten het blikveld van de organisatie.
  Eenvoudige voorbeelden zijn het gebruik van WhatsApp of WeTransfer.

- Toename van Internet of Things, waarbij met het internet verbonden apparaten, deels ongemerkt, de organisatie binnenkomen. Een voorbeeld zijn bluetooth-bakens voor het vaststellen van het gebruik van bureaus.
- Ruime beschikbaarheid van technologie waarmee mensen gevolgd of opgenomen kunnen worden: camera's (bodycams), automatische kentekenherkenning, wifitracking et cetera.
- Een blijvende stroom van kwetsbaarheden in software, zowel op servers, als op pc's als op smartphones, die vaak al snel worden uitgebuit door aanvallers.
- Het internet wordt zowel door kwaadwillende actoren als door organisaties met goede intenties voortdurend afgezocht naar apparatuur die kwetsbaar is en dus gebruikt kan worden om in te dringen in de organisatie.
- Aanvallen vinden toenemend plaats via leveranciers, zeker wanneer de organisatie zelf goed beveiligd is. Leveranciersmanagement en de beveiliging van leveranciers is dus in toenemende mate van belang.
- Door de toepassing van cloud-computing wordt de beveiliging van gegevens mogelijk beter, maar de impact van een internetverstoring of een verstoring bij een leverancier wordt groter.

4.3 Ontwikkelingen en bedreigingen door cybercriminaliteit

Cybercriminelen werken niet langer individueel, maar er is een hoge mate van commerciële samenwerking tussen partijen die zich hebben gespecialiseerd in verschillende stappen van een aanval. Bij ransomwareaanvallen bijvoorbeeld zijn het vaak verschillende partijen die:

a) de eerste toegang tot een intern netwerk verkrijgen;
b) het netwerk in kaart brengen en brede toegang krijgen;
c) de ransomware installeren;
d) het losgeld opeisen.

Deze verspreide activiteiten, die vaak vanuit verschillende landen buiten Nederland en de EU worden uitgevoerd, maken opsporing en vervolging moeilijk, zeker wanneer buitenlandse overheden de criminelen de hand boven het hoofd houden.
Een nieuwe ontwikkeling is dat (zeer) vertrouwelijke gegevens worden gepubliceerd als de organisatie weigert het losgeld te betalen. Een krachtig extra dwangmiddel als we bedenken wat het voor inwoners en voor de gemeente zou betekenen wanneer bijvoorbeeld Jeugdwetdossiers op straat zouden komen te liggen of informatie rond ondermijning en drugscriminaliteit.
In het Cybersecuritybeeld 2021, uitgegeven door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), wordt aangegeven dat cyberaanvallen het zenuwstelsel van de maatschappij aantasten en dat de weerbaarheid nog niet voldoende is. Kleinere organisaties hebben vaak niet de expertise en de middelen om de weerbaarheid naar een hoger plan te tillen. Daarnaast gebruiken cybercriminelen actuele gebeurtenissen, zoals de coronapandemie en thuiswerken, in hun campagnes om medewerkers te verleiden al dan niet bewust wachtwoorden prijs te geven of malware te installeren.

4.4 Ontwikkelingen en bedreigingen door statelijke actoren

Andere landen gebruiken steeds vaker digitale middelen voor spionage, aanvallen en het ondermijnen van het vertrouwen in de overheid, democratie en de rechtsorde.
Dat gebeurt via sociale media, maar ook door het gedogen van of mogelijk ook samen te werken met criminele organisaties die aanvallen uitvoeren in Nederland en bij haar bondgenoten. Gemeenten zijn een mogelijk doelwit, met name voor aanvallen op de Nederlandse samenleving en de ondermijning van het vertrouwen in de overheid.

4.5 Ontwikkelingen in de maatschappij en toezicht

De aandacht voor privacy en beveiliging van gegevens bij burgers en daarmee ook de gemeenteraad neemt toe. De veiligheid van het stemproces staat zowel in Nederland als in andere landen ter discussie. Dat gebeurt in het buitenland weliswaar deels op basis van desinformatie, maar ook die heeft grote effecten op het democratische proces. Dit is van bijzonder belang voor gemeenten, die immers in Nederland een grote rol hebben bij de organisatie van verkiezingen.
Waar de Autoriteit Persoonsgegevens aanvankelijk een pedagogische aanpak hanteerde door middel van informeren en waarschuwen, worden nu steeds vaker (grote) boetes opgelegd, ook bij gemeenten. De boete voor de gemeente Enschede naar aanleiding van wifitracking is daarvan een voorbeeld.

4.6 Kwetsbaarheid van gemeenten

Gemeenten zijn kwetsbaar voor de bovengenoemde ontwikkelingen en bedreigingen en de daaruit voortkomende risico's, omdat:

- de weerbaarheid van gemeenten nog niet voldoende is. Veel gemeenten voldoen nog niet aan de basismaatregelen, zoals die door de NCSC zijn gecommuniceerd en door de BAR-organisatie in het kader van het 8-puntenplan worden geïmplementeerd;
- de kans om een indringer vroegtijdig te herkennen klein is zonder een Security Operations Center. Dat is bij veel gemeenten, waaronder de BAR-organisatie, nog niet (volledig) geïmplementeerd;
- cybercriminelen pragmatisch zijn: zij vallen het liefst organisaties aan die hun beveiliging minder op orde hebben;
- kennis en ervaring bij gemeenten beperkt is, zowel in capaciteit als qua diepgang.

Aan de ransomwareaanvallen op de gemeente Lochem en de gemeente Hof van Twente zien we dat gemeenten wel degelijk de aandacht hebben van criminele actoren.

H5 | Conclusies en aanbevelingen

5.1 Conclusies

Op basis van de bevindingen, zoals die zijn uitgewerkt in de voorgaande hoofdstukken, trekken we - samengevat - de volgende conclusies.

5.1.1 Ontwikkelingen in risico's en bedreigingen

De risico's en bedreigingen ten aanzien van informatiebeveiliging en privacy worden voor de BAR-gemeenten en de BAR-organisatie groter door:

- voortschrijdende digitalisering, datagedreven werken en samenwerking met andere organisaties;
- laagdrempeliger inzet van technologie, zoals clouddiensten en Internet of Things, die zich mogelijk buiten het blikveld van de CISO en/of de PO voltrekt;
- een blijvende stroom van kwetsbaarheden in software;
- toegang tot gegevens via en afhankelijk van leveranciers en intranet, beide mogelijke aanvalsroutes voor kwaadwillenden;
- toenemende activiteit van buitenlandse overheden ('statelijke actoren') en cybercriminelen, al dan niet gedoogd door die overheden;

Een relevante ontwikkeling is daarnaast: een toenemend bewustzijn in de samenleving en handhaving door toezichthouders.

De BAR-gemeenten en de BAR-organisatie zijn net als andere gemeenten kwetsbaar, omdat de weerbaarheid nog niet voldoende is, zoals onder andere blijkt uit de beperkte implementatie van BIO, AVG en Wpg.

5.1.2 Ambitie - wat is een acceptabel niveau?

De BAR-gemeenten en de BAR-organisatie willen *aantoonbaar* voldoen aan wet- en regelgeving. Dit betekent de implementatie van een plan-do-check-actcyclus:

- Plan: Opschrijven hoe de organisatie ervoor zorgt dat aan wet- en regelgeving wordt voldaan, bijvoorbeeld met beleid, richtlijnen, procedures en sjablonen. Het gaat hier onder andere om beveiligingsmaatregelen uit de BIO en de vertaling van de eisen uit de AVG en Wpg in organisatorische en technische maatregelen.
- Do: Aantoonbaar implementeren van de maatregelen over de gehele organisatie en alle informatiesystemen, met een diepgang die afgestemd is op de gevoeligheid van de gegevens. Bij het aantonen hoort het documenteren van de resultaten (de 'output') van de maatregelen.
- Check: Controleren of de maatregelen inderdaad voldoende worden uitgevoerd en of zij nog voldoende zijn tegen de achtergrond van ontwikkelingen en risico's. Voor deelgebieden zoals de Wpg, SUWI, DigID et cetera gebeurt dit (ook) in het kader van verplichte in- en/of externe audits.
- Act: Op basis van deze controle verbeteren van (de implementatie van) maatregelen of invoeren van extra maatregelen.

Daarnaast wil men 'in control' zijn, dat wil zeggen: overzicht hebben over de implementatie en risico's bewust nemen vanuit het bestuur. Men kiest daarbinnen zo veel mogelijk voor een laag ambitieniveau, vanwege de financiële situatie van de gemeenten.

5.1.3 Organisatorische inrichting

De organisatorische inrichting is voor informatiebeveiliging beschreven in het informatiebeveiligingsbeleid. In het privacybeleid is de verhouding tussen de BAR-gemeenten en de BAR-organisatie uitgewerkt.
De praktijk voldoet nog niet aan de ambitie van de BAR-gemeenten en de BAR-organisatie:

- De plan-do-check-actcyclus die wordt genoemd in het informatiebeveiligingsbeleid is niet uitgewerkt in praktische handvatten/procedures en wordt onvoldoende uitgevoerd. Voor privacy is deze aanpak in het privacybeleid nog niet benoemd.
- De verantwoordelijkheden van en samenwerking tussen centrale expertise in de stafafdelingen en de proceseigenaren zijn onvoldoende uitgewerkt (en geïmplementeerd).
- Proces-/applicatiegerichte toetsen op beveiliging en privacy worden bij vernieuwing uitgevoerd, maar verlopen stroef en dekken niet alle eisen uit BIO, AVG en Wpg af. De toets is niet procedureel uitgewerkt en handvatten, zoals een lijst met generieke beveiligings- en privacyeisen, zijn nog niet opgesteld.
- In de risicoanalyse bij de begroting wordt informatiebeveiliging meegenomen. Er is ook een incidentele analyse van risico's geweest naar aanleiding van incidenten elders in het land, leidend tot een 8-puntenverbeterprogramma. Er zijn nog geen jaarlijkse organisatiebrede analyses van concrete beveiligings- en privacyrisico's met afweging, vaststelling en bewaking van mitigerende maatregelen.
- Voor de besturing van informatiebeveiliging en privacy is een brede stuurgroep opgericht. Deze bestuurt lopende en nieuwe verbeteracties naar aanleiding van externe ontwikkelingen, zoals incidenten en onderzoeken van concerncontrol en de rekenkamer. Deze verbeteracties worden vrij informeel bestuurd, zonder projectplannen en met mondelinge rapportage aan de stuurgroep.
- Er wordt wel gewerkt aan een rapportagestructuur, maar er is op dit moment nog geen overzicht van de mate waarin de organisatie en/of specifieke processen voldoen aan BIO, AVG en Wpg. Daarom zijn verantwoordelijken, zoals proceseigenaren, daar niet op aanspreekbaar en kan de stuurgroep daar niet op sturen.
- De personele inzet, zowel centraal als decentraal, is lager dan bij qua inwonersaantal vergelijkbare gemeenten (2,2 fte bij BAR-organisatie vs. circa 7 fte bij gemeentelijke organisaties met een vergelijkbaar aantal inwoners; zie voor nadere toelichting de aanbevelingen) en te laag om de ambitie van de gemeenten te realiseren.

5.1.4 Implementatie van BIO, AVG en Wpg

Ten aanzien van de implementatie van de BIO, de AVG en de Wpg concluderen we:

- De BIO is slechts gedeeltelijk geïmplementeerd; met name documentatie en borging is onderbelicht. Daarmee voldoet de huidige implementatie niet aan de ambitie van de organisatie.

- Voor de implementatie van de AVG zijn in het verleden implementaties gestart op deelgebieden, maar deze zijn niet geborgd in de processen van de organisatie en niet periodiek geactualiseerd. Daarmee voldoet de huidige implementatie niet aan de ambitie van de organisatie.
- De Wpg is binnen de BAR-organisatie nog niet systematisch geïmplementeerd. De organisatie voldoet op deelaspecten op basis van het gebruik van CityControl, de algemene boa-opleiding en de beroepsethiek van de boa's en de maatregelen die in het kader van de BIO en de AVG zijn vormgegeven. Daarmee voldoet de huidige implementatie niet aan de ambitie van de organisatie.

5.2 Aanbevelingen

Om de ambitie van de BAR-gemeenten en de BAR-organisatie te realiseren adviseren wij om een programma te starten. Daarbij doen wij de volgende aanbevelingen:

5.2.1 Richt de governance/aanpak beter in

Richt de governance/aanpak van informatiebeveiliging en privacy beter in, zodanig dat:

A. de verantwoordelijkheid voor generieke beveiligingsmaatregelen centraal is belegd bij afdelingen, zoals HR, Facilities, IT, CISO of PO;
B. de verantwoordelijkheid voor proces-/applicatiespecifieke beveiligingsmaatregelen is belegd bij proces-/applicatie-eigenaren;
C. de proces-/applicatie-eigenaren worden gefaciliteerd met een centrale basis voor de implementatie, zoals bijvoorbeeld processen, procedures, sjablonen en checklists;
D. de plan-do-check-actcyclus zowel voor informatiebeveiliging als privacy wordt beschreven:
    a. organisatiebreed met jaarlijkse risicoanalyses, verbeter- en operationele plannen en de bewaking van de uitvoering in de stuurgroep;
    b. op maatregelniveau met documentatie van opzet, implementatie en de gedocumenteerde uitvoering van checks (borging) en verbeteracties;
E. de 'Three lines of defense' worden toegepast waarin:
    a. binnen de afdelingen/teams zelf de checks op veilig en privacyconform werken worden toegepast, zoals de uitvoering van beheersmaatregelen;
    b. de centrale staf (CISO en PO) overzicht houdt, bewaakt, adviseert en faciliteert;
    c. concerncontrol en/of de FG het totaal periodiek toetst door middel van een interne audit. Daarbij kunnen de aandachtspunten jaarlijks worden bepaald. Voor de Wpg en ENSIA komen daar aanvullend externe audits bij;
F. voor de stuurgroep inzichtelijk is in hoeverre de verantwoordelijken hun taken uitvoeren op basis van meetbare criteria, zodat zij daarop door de stuurgroep en/of de directie aangesproken kunnen worden. Geadviseerd wordt om dat mee te nemen bij de nadere invulling van de rapportagestructuur die in ontwikkeling is.

Leg de governance/aanpak vast in het informatiebeveiligingsbeleid en het privacybeleid.

5.2.2 Realiseer quick wins

Realiseer quick wins door:

Scoping en inrichting van een DPIA-proces

1. **Voer alleen een DPIA uit wanneer dit verplicht is** en ontwikkel daarvoor een aanpak die borgt dat de DPIA-rapportage voldoet aan de eisen van de AVG/Wpg en de richtlijnen van de toezichthouders.
2. **Richt het DPIA-proces in**, inclusief de rol die proceseigenaren, I-adviseurs, CISO, PO en FG daarin dienen te spelen. Onderdeel van het DPIA-proces is besluitvorming door de stuurgroep bij onenigheid over te treffen maatregelen op aanvraag van de proceseigenaar en met advies van de CISO, PO en/of FG. Stel voor de proceseigenaren een toolkit samen die hen ondersteunt bij het uitvoeren van de DPIA conform de eisen van de wet en de richtlijnen van toezichthouders. Dat kan door de huidige vragenlijst aan te vullen met een procedure/aanpak en sjablonen, bijvoorbeeld voor de rapportage. Stel het proces vast in de stuurgroep en/of de directie.

Inrichting van checks op processen/applicaties

1. **Stel basiseisen op aan processen/applicaties** (inclusief bijbehorende leveranciers). Deze basiseisen omvatten ten minste zowel privacy- als informatiebeveiligingseisen en mogelijk eisen vanuit de architectuur. Daarbij kunnen de basiseisen afhankelijk zijn van de classificatie van de gegevens (zie ook 5.2.3 onder a). Stel deze eisen vast in de stuurgroep en/of de directie. Deze kan daarbij waarborgen dat de eisen in lijn zijn met de ambitie van de organisatie.
2. **Controleer periodiek en bij grote wijzigingen per proces/applicatie of deze voldoen aan de basiseisen.** Richt deze check procesmatig in onder centrale coördinatie en maak deze ook onderdeel van een vernieuwings-/projectenproces. Daarbij kan de frequentie van de periodieke controle afhankelijk zijn van de classificatie van de gegevens.
   Onderdeel van het checkproces is het (al of niet tijdelijk) door de stuurgroep toestaan van afwijkingen van de basiseisen op aanvraag van de proceseigenaar en met advies van de CISO, PO en/of FG.
   De controle zou zo veel mogelijk door proces-/applicatie-eigenaren met de I-adviseur uitgevoerd moeten worden, waarbij CISO en/of PO betrokken zijn wanneer niet aan de basiseisen kan worden voldaan en/of aanvullende maatregelen nodig zijn.
   Stel het proces vast in de stuurgroep en/of de directie.

Het opstellen van gedragsregels/handreiking voor medewerkers

Met het opstellen en communiceren van gedragsregels/handreiking voor medewerkers over veilig omgaan met informatie worden circa 50 maatregelen uit de BIO afgedekt of geraakt.

Overige te realiseren quick wins

- formaliseren van de autorisatieprocedure;
- borgen van de fysieke beveiliging door periodieke rondgangen door de gebouwen;
- toevoegen van informatiebeveiliging in de change procedure;
- afronden van de incident response procedure, die nu nog in concept is aangeleverd;

- verder uitwerken van procedures voor datalekken en verzoeken van betrokkenen;
- opnemen van de verwerking van politiegegevens in de privacyverklaring op de website.

5.2.3 Zorg voor verdere implementatie van BIO, AVG en Wpg

Hier gaat het om de verdere en volledige implementatie van de BIO, de AVG en Wpg, afgestemd op de ambitie van de organisatie. Daaronder valt onder andere:

a. het zorgen voor overzicht en classificatie van gegevens. Voor het dataclassificatie-schema kan het sjabloon van de IBD als basis worden gebruikt, met aanpassingen aan de omvang van de BAR-organisatie en aanscherping van criteria, met name bij de classificatie op beschikbaarheid;
b. het kiezen van een raamwerk voor beheersmaatregelen voor de AVG en Wpg, zoals die van NOREA, de VNG of van BMC. De BIO is zelf al een raamwerk met beheersmaatregelen;
c. het bepalen van verantwoordelijkheden per beheersmaatregel;
d. het documenteren van opzet, bestaan en borging van beheersmaatregelen uitgaande van de huidige situatie. Voor een aanzienlijk deel van BIO-maatregelen kan door documentatie en borging met beperkte inspanning een vrij grote verbetering van de implementatie en beheersing worden bereikt;
e. het vaststellen van GAP's ten opzichte van de ambitie van de BAR-organisatie;
f. het opstellen en uitvoeren van een jaarlijks bij te stellen implementatieplan, waaronder de basis voor de implementatie van proces-/applicatiespecifieke maatregelen.

Bij de implementatie van de beheersmaatregelen kunnen keuzes worden gemaakt ten aanzien van diepgang van de implementatie, bijvoorbeeld afhankelijk van de classificatie van de verwerkte gegevens. Afhankelijk van deze keuzes zullen er voor de verdere implementatie hogere of lagere structurele kosten ontstaan, bijvoorbeeld voor software of diensten van leveranciers. Deze zullen te zijner tijd ter besluitvorming voorgelegd moeten worden.
Voor voorbeelden van de inhoudelijke aandachtspunten van de implementaties wordt verwezen naar de paragrafen over implementatie van de BIO, AVG en Wpg in hoofdstuk 3.
Het implementatietraject is in het volgende hoofdstuk 'Plan van aanpak' nader uitgewerkt.
We bevelen aan om de lopende initiatieven, zoals het 8-puntenplan, daarin op te nemen.

5.2.4 Zorg voor voldoende personele inzet

Zorg voor voldoende personele inzet, zowel structureel als tijdelijk, zowel centraal als decentraal:

- Structurele decentrale inzet
  In de BAR-organisatie wordt integraal management toegepast, waarbij managers en teamleiders ook verantwoordelijk zijn voor inhoud, werkprocessen, HR, financiën et cetera en ook voor de informatiebeveiliging en privacy in hun afdeling of team. Om die verantwoordelijkheid goed te kunnen nemen heeft de manager/teamleider zowel qua capaciteit als qua kennis/vaardigheden in vergelijkbare organisaties ondersteuning vanuit eigen afdeling/team.

Aanbevolen wordt om zulke **decentrale informatiebeveiligings- en privacyrollen in te richten**. Daarbij kunnen informatiebeveiliging en privacy worden gecombineerd. De tijdsbesteding van de rol zal afhankelijk zijn van de hoeveelheid en aard van de gegevens die binnen een afdeling of team worden verwerkt. Afhankelijk van de tijdsinzet kan de rol op afdelings- of teamniveau worden ingevuld. Bijvoorbeeld voor Financiën op afdelingsniveau en voor het Sociaal Domein op teamniveau.
De rol kan worden gecombineerd met een proces- of kwaliteitsfunctionaris op afdelingen die deze rol kennen.
De taken van deze rol kunnen bijvoorbeeld zijn:

- contactpersoon voor CISO, PO en FG;
- ondersteunen van de proceseigenaar bij diens taken door het:
  - veilig en privacyconform inrichten van de werkprocessen;
  - coördineren van het invoeren en onderhouden van proces-/ applicatiespecifieke beheersmaatregelen;
  - uitvoeren/begeleiden van checks van processen/applicaties;
  - uitvoeren van DPIA's begeleid door I-adviseurs, CISO en PO;
- signaleren van issues aan de proceseigenaar, CISO of PO.

Keuzes zijn mogelijk in de omvang van het takenpakket in samenhang met de centraal beschikbare personele capaciteit.

- Structurele centrale inzet

Om de ambitie van de organisatie te realiseren is er structureel meer centrale inzet nodig dan de huidige 2,2 fte.
We zien verschillende opties die gekozen kunnen worden in samenhang met het tempo waarmee de organisatie het ambitieniveau wil bereiken en de beschikbare decentrale inzet en de ondersteuning door de I-adviseurs.
Deze opties zijn tot stand gekomen door de personele capaciteit bij enkele qua omvang vergelijkbare gemeenten en het uitvoeringsplan (minimale optie) te beschouwen en dat te combineren met onze professionele inschatting.
Op basis daarvan komen we tot de volgende opties om de ambitie van de organisatie te realiseren:

- Optie 'niveau gemeentelijke organisaties met een vergelijkbaar aantal inwoners': 7 fte, bijvoorbeeld:
  - (C)ISO tactisch/strategisch: 1 fte
  - (C)ISO operationeel/technisch: 1 fte
  - PO tactisch/strategisch: 1 fte
  - PO operationeel generiek: 1 fte
  - ISO/PO operationeel cluster Maatschappij en Veiligheid: 1 fte
  - FG: 1 fte
  - ISO/PO ENSIA-coördinatie en projecten: 1 fte

  Uitgaande van gemiddelde kosten van € 90.000,— per fte op het gewenste niveau, betekent deze optie extra structurele kosten van € 432.000,— per jaar voor 4,8 fte extra.
- Optimale optie: 10 fte, bijvoorbeeld:
  - (C)ISO tactisch/strategisch: 1 fte

- (C)ISO operationeel: 1 fte
- ISO technisch: 1 fte
- PO tactisch/strategisch: 1 fte
- PO operationeel generiek: 1 fte
- ISO/PO operationeel cluster Maatschappij: 1 fte
- ISO/PO operationeel cluster Veiligheid: 1 fte
- FG: 1 fte
- ISO/PO ENSIA-coördinatie en projecten: 1 fte
- ISO/PO projecten: 1 fte

Uitgaande van gemiddelde kosten van € 90.000,— per fte op het gewenste niveau, betekent deze optie extra structurele kosten van € 702.000,— per jaar voor 7,8 fte extra.

Ter vergelijking geven we hieronder nog twee andere scenario's weer:

- Voorstel uit het Uitvoeringsplan: 5,6 fte gespecialiseerde capaciteit:
  - Bestaand
    - CISO: 1 fte
    - PO: 1 fte
    - FG: 0,2 fte
  - Aanvullend
    - ISO 1 fte
    - PO: 1 fte
    - ISO/PO Maatschappij: 1 fte
    - FG: 0,4 fte

  Uitgaande van gemiddelde kosten van € 90.000,— per fte op het gewenste niveau, betekent deze optie extra structurele kosten van € 306.000,— per jaar voor 3,4 fte extra.
- 'Drie afzonderlijke gemeenten', dat wil zeggen: de formatie die drie vergelijkbare gemeenten nodig zouden hebben zonder ambtelijke fusieorganisatie: 11,5 fte centrale capaciteit (4,5 fte voor de twee grotere gemeenten, 2,5 fte voor de kleinere gemeenten), bijvoorbeeld:
  - (C)ISO 2,5 fte per grotere, 1 fte per kleinere gemeente: 6 fte
  - FG/PO 2 fte per grotere, 1,5 fte per kleinere gemeente: 5,5 fte

  Uitgaande van gemiddelde kosten van € 90.000,— per fte op het gewenste niveau, betekent deze hypothetische optie extra structurele kosten van € 837.000,— per jaar voor 9,3 fte extra.

Bij de invulling van de capaciteit is het van belang dat de aanvullend te benoemen medewerkers complementair zijn aan de huidige medewerkers als het bijvoorbeeld gaat om operationele versus tactisch/strategische focus en technische en/of bedrijfskundige kennis en ervaring. Daarbij is in ieder geval aandacht nodig voor kennis op het gebied van de Wpg of training op dat gebied.

- Tijdelijke inzet

  Voor het uitvoeren van de bovenstaande aanbevelingen om de ambitie van de BAR-gemeenten en de BAR-organisatie te realiseren, zal tijdelijk extra capaciteit nodig zijn.

De omvang daarvan is afhankelijk van:

- de snelheid waarmee structurele capaciteit beschikbaar komt en (met name decentraal) toegerust is;
- de tijdshorizon waarbinnen de organisatie het ambitieniveau wil bereiken;
- de uitwerking van de ambitie op maatregelniveau. Hierin zijn immers nog keuzes mogelijk.

Een voorlopige raming van de kosten voor het programma-/verandermanagement en programmaondersteuning in 2022 bedraagt circa € 150.000,—. Dat is exclusief capaciteit voor het vrijspelen van interne medewerkers voor de implementatie van de verandering.

H6 | Plan van aanpak

In dit plan van aanpak wordt een voorstel gedaan voor de implementatie van de aanbevelingen wanneer deze door de opdrachtgever worden overgenomen. Dit is per aanbeveling uitgewerkt met de volgende uitgangspunten:

- Start per 1 januari 2022, uitgaande van besluitvorming in 2021.
- Inrichting van een programma met extern advies en ondersteuning om alle activiteiten te coördineren en inhoudelijk te begeleiden en te ondersteunen.
- Afhankelijk van keuzes ten aanzien van de personele inzet en de tijdshorizon waarbinnen de organisatie het ambitieniveau wil bereiken, wordt een doorlooptijd verwacht van één tot drie jaar. In dit plan van aanpak is de planning alleen voor 2022 nader uitgewerkt.
- De hier gegeven planning is indicatief en moet met de betrokkenen, in het bijzonder de CISO en de PO, worden gevalideerd en verder uitgewerkt. Als startpunt is uitgegaan van ambitieuze tijdslijnen.
- Het gaat niet alleen om een implementatie, maar ook om een veranderopgave.

6.1 Aanpak programmacoördinatie

Om alle activiteiten te coördineren, veranderkundig en inhoudelijk te begeleiden en te ondersteunen wordt een programma ingericht. Daarbij wordt gebruikgemaakt van externe advisering en ondersteuning om expertise en capaciteit in de eigen organisatie aan te vullen. Bij voorkeur wordt gebruikgemaakt van sjablonen en ervaring van de externe adviseurs om snel resultaten te boeken en medewerkers van de BAR-organisatie mee te nemen in elders ontwikkelde best practices.

Gedacht kan worden aan:

- een ervaren programma-/verandermanager/adviseur met inhoudelijke expertise en ervaring op de aandachtsgebieden met een inzet van gemiddeld 16-20 uur per week flexibel verdeeld over de hele week;
- aangevuld met een programmaondersteuner voor enkele dagen per week.

Het programma start met de organisatie van één of meerdere kick-offbijeenkomsten met werkgroepen per stream, waarin werkafspraken worden gemaakt en de planning voor de streams met CISO, PO en andere betrokkenen verder wordt uitgewerkt.
We onderscheiden daarbij de volgende zes streams:

- stream 1: governance/aanpak;
- stream 2: DPIA en proces-/applicatiespecifieke checks;
- stream 3.1: verder implementeren BIO;
- stream 3.2: verder implementeren AVG;
- stream 3.3: verder implementeren Wpg;
- stream 4: personele inzet.

Lid van de werkgroepen zijn naast CISO en PO de uitvoerenden in de verschillende activiteiten, zoals proceseigenaren en/of decentrale ondersteuning en overige medewerkers, waaronder die bij IT. Mogelijk is de FG bij een aantal streams betrokken, maar deze kan gezien zijn rol alleen een adviserende (en geen uitvoerende) rol spelen.
Na de start wordt vanuit het programma expertise ingebracht, gecoördineerd en ondersteund. Ook worden de veranderkundige aspecten vanuit het programma bewaakt. Er wordt periodiek schriftelijk gerapporteerd aan de stuurgroep over de voortgang en eventuele knelpunten. De programmaondersteuning kan in de loop van de tijd worden overgedragen aan de nieuw te werven structurele capaciteit.

Hieronder is een eerste voorstel voor de planning van de stappen weergegeven:

	Activiteit	jan-22	feb-22	mrt-22	apr-22	mei-22	jun-22	jul-22	aug-22	sep-22	okt-22	nov-22	dec-22
	0 Programmacoördinatie												
1	Werven en samenstellen programmacoördinatie												
2	Samenstellen van werkgroepen per stream												
3	Kick-off bijeenkomsten met de streams												
4	Programmacoördinatie												
5	Advisering												
6	Ondersteuning												

6.2 Aanpak governance/aanpak informatiebeveiliging en privacy

Voor de inrichting van governance zien we de volgende stappen:

1) Uitwerken van een governancemodel in aan te passen of op te stellen concepten voor informatiebeveiligingsbeleid en privacybeleid op basis van de aanbevelingen in dit rapport.
2) Afstemming in de werkgroep en met leden van de stuurgroep, waaronder CISO, PO en FG.
3) Formele besluitvorming in stuurgroep en directie.
4) Eerstmaals uitvoeren van de organisatiebrede cyclus onder begeleiding van het programma.

Hieronder is een eerste voorstel voor de planning van de stappen weergegeven:

	Activiteit	jan-22	feb-22	mrt-22	apr-22	mei-22	jun-22	jul-22	aug-22	sep-22	okt-22	nov-22	dec-22
	1 Governane/aanpak IB en Privacy												
1	Uitwerken governancemodel in beleid												
2	Afstemming met stuurgroep												
3	Formele besluitvorming												
4	Eerstmalig uitvoeren van de cyclus												

6.3 Realiseren quick wins

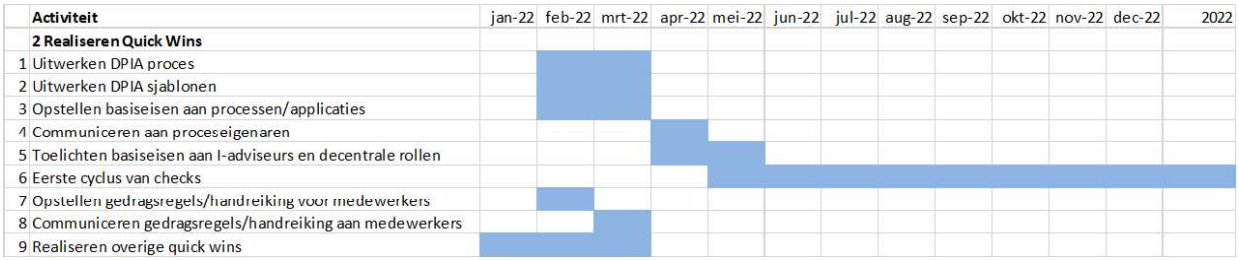
Voor de inrichting van het DPIA-proces en de proces-/applicatiespecifieke checks worden de volgende stappen voorzien:

- inrichten DPIA-proces:
    1) uitwerken en afstemmen van een DPIA-proces/-procedure;
    2) uitwerken en afstemmen van sjablonen voor de DPIA;
- inrichten van checks van processen/applicaties:

1) opstellen basiseisen aan processen/applicaties (inclusief bijbehorende leveranciers):
    a) NB Deze kunnen worden aangevuld naarmate BIO, AVG en Wpg verder zijn geïmplementeerd.
2) communiceren van de nieuwe aanpak naar de proceseigenaren:
    a) NB Afhankelijkheid: na besluitvorming over het beleid.
3) toelichten van de basiseisen, checks en DPIA-proces aan de I-adviseurs en de decentrale informatiebeveiligings-/privacyrollen, eveneens startschot voor de nieuwe werkwijze:
    a) NB Afhankelijkheid: benoeming van decentrale informatiebeveiligings-/privacyrollen.
4) eerste cyclus van checks van processen/applicaties met de basiseisen:
    a) NB Prioriteit op basis van de classificatie van gegevens;
    b) NB Afhankelijkheid: inventarisatie en classificatie van gegevensverzamelingen.

- Gedragsregels/handreiking:
    1) opstellen gedragsregels/handreiking voor medewerkers, waar mogelijk gebruikmakend van een sjabloon waarin de relevante BIO-maatregelen zijn verwerkt;
    2) communiceren gedragsregels/handreiking aan medewerkers.
- Realiseren overige quick wins.

Hieronder is een eerste voorstel voor de planning van de stappen weergegeven:



6.4 Aanpak verdere implementatie BIO, AVG en Wpg

Voor de verdere implementatie worden voor de BIO, de AVG en de Wpg parallel een aantal stappen uitgevoerd. Bij elke hoofdstap geven we aan in hoeverre deze voor BIO, AVG en Wpg relevant is. De uitvoering van de stappen kan deels overlappen, zoals in de planning is weergegeven. Sommige stappen, zoals documentatie van beheersmaatregelen, kunnen mogelijk eerder worden gestart.

1) Overzicht en classificatie van gegevens (BIO en ondersteunend voor AVG en Wpg):
    a) Inventariseer alle gegevensverzamelingen, zoals applicaties, databases en netwerkschijven.
    b) Voer een volledigheidscontrole uit met het verwerkingenregister.
    c) Stel een dataclassificatieschema vast ten aanzien van vertrouwelijkheid, integriteit en beschikbaarheid. Zorg dat dit bekend is bij iedereen die daarmee werkt.

d) Classificeer de geïnventariseerde gegevensverzamelingen.
e) Gebruik de classificatie bij het bepalen van de gewenste diepgang van de implementatie voor proces-/applicatiespecifieke beheersmaatregelen.

2) Kies voor AVG en Wpg een raamwerk voor beheersmaatregelen (AVG en Wpg; de BIO bestaat al uit 250 beheersmaatregelen voor informatiebeveiliging):
   a) Voor de AVG kan het VNG-framework worden gebruikt met 183 beheersmaatregelen of een ander framework, zoals dat van BMC met 65 beheersmaatregelen dat voor dit brede onderzoek is gebruikt.
   b) Voor de Wpg kunnen de 31 beheersmaatregelen uit de 'NOREA-Handreiking Privacy Audit Wpg voor boa's' of een ander framework, zoals dat van BMC met 68 beheersmaatregelen dat voor dit brede onderzoek is gebruikt.
3) Bepaal per maatregel wie verantwoordelijk is voor de implementatie (BIO, AVG en Wpg):
   a) Beleg de verantwoordelijkheid voor generieke maatregelen centraal bij HR, Facilities, IT, CISO of PO.
   b) Beleg de verantwoordelijkheid voor proces-/applicatiespecifieke maatregelen. Stel per proces-/applicatie vast wie de proces-/applicatie-eigenaar is.
   c) Stel voor proces-/applicatiespecifieke maatregelen vast wie verantwoordelijk is voor de centrale basis voor de implementatie. Enkele voorbeelden zijn:
      - beleid en procedures voor toegang tot IT-systemen;
      - gedragsregels/handreiking voor medewerkers over het veilig omgaan met informatie;
      - loggingbeleid en -tooling waarop de applicaties aangesloten kunnen worden;
      - incidentproces waarop de gebruikers en beheerders van applicaties kunnen aansluiten;
      - overkoepelend business continuity- en uitwijkplan.
4) Documenteer per maatregel op basis van de huidige situatie (BIO, AVG en Wpg):
   a) Plan: Documenteer hoe de maatregelen voor de BAR-organisatie zijn uitgewerkt ('zeggen wat je doet'). Daarbij horen ook afwegingen om maatregelen met meer of minder diepgang toe te passen afhankelijk van de classificatie van de gegevens. Bij deze documentatie horen beleid, richtlijnen, procedures en sjablonen. In auditterminologie gaat het hier om de 'opzet'.
   b) Do: Documenteer de implementatie van de maatregelen op een transparante, aantoonbare manier ('doen wat je zegt'). Stel daarbij vast in hoeverre de maatregel over de gehele organisatie en alle informatiesystemen wordt uitgevoerd. Bij het aantonen hoort het documenteren van de resultaten (de 'output') van de maatregelen, bijvoorbeeld een incidentregister of een lijst met verwerkersovereenkomsten. In auditterminologie gaat het hier om het 'bestaan'.
   c) Check: Documenteer in hoeverre er periodieke checks zijn op de volledige en correcte implementatie conform de gekozen opzet. Daarbij kan de intensiteit van de controles worden afgestemd op de classificatie van de gegevens. We spreken hier van 'borging' van de implementatie.

5) Risicoanalyse: Maak een organisatiebrede risicoanalyse met concrete beveiligings- en privacyrisico's en leg deze ter goedkeuring voor aan de stuurgroep. (BIO en ondersteunend aan AVG en Wpg)
6) GAP-analyse: Stel vast welke GAP's er nog zijn tegen de achtergrond van de ambitie van de organisatie, risico's en de classificatie van de gegevens. Leg deze ter besluitvorming voor aan de stuurgroep. (BIO, AVG en Wpg)
7) Stel een implementatieplan op en voer dat uit om de GAP's op te lossen met prioritering op basis van risico, waarbij de classificatie van de gegevens de basis is bij de uitrol van proces-/applicatiespecifieke maatregelen. In dit plan zijn per maatregel of groep van maatregelen verantwoordelijken en tijdslijnen benoemd, voor eind- en tussenresultaten. Met de implementatie van bijvoorbeeld toegangsbeleid of gedragsregels worden immers in één keer meerdere maatregelen uit de BIO, AVG en/of Wpg afgedekt. (BIO, AVG en Wpg)
8) Richt parallel aan de uitvoering van het implementatieplan een proces in om corrigerende acties die voortvloeien uit de checks te registreren, toe te wijzen aan actiehouders en te bewaken. (BIO, AVG en Wpg)
9) Rapporteer schriftelijk over de voortgang van de implementatie en corrigerende acties op basis van behaalde resultaten en KPI's. (BIO, AVG en Wpg)

Voor voorbeelden van de inhoudelijke aandachtspunten van de implementaties wordt verwezen naar de paragrafen over implementatie van de BIO, AVG en Wpg in hoofdstuk 3.

Hieronder is een eerste voorstel voor de planning van de stappen weergegeven:

6.5 Aanpak personele inzet

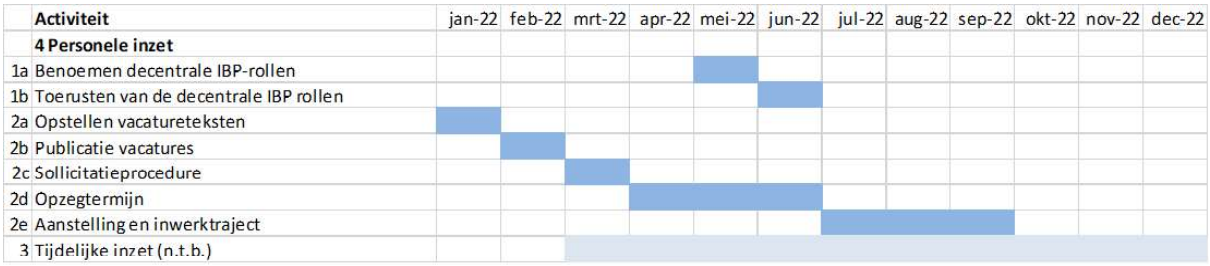
Met de volgende stappen kan de personele capaciteit op niveau worden gebracht:

1) Structurele decentrale inzet:
    a) Het benoemen van medewerkers op de decentrale IBP-rollen onder verantwoordelijkheid van de proceseigenaren. Deze stap kan worden genomen na besluitvorming over de governance, het overzicht over de gegevensverzamelingen en het vastleggen van de verantwoordelijkheden voor processen/applicaties. De proceseigenaren vullen deze rollen vervolgens in onder coördinatie van het programma.

b) Het toerusten van de IBP-rollen in een aantal workshops van circa een halve dag. Daarin komen de taken van de rol, de DPIA en de basiseisen voor processen/applicaties aan de orde.
In sommige gevallen is er mogelijk een uitgebreidere training nodig, bijvoorbeeld op het gebied van de Wpg.

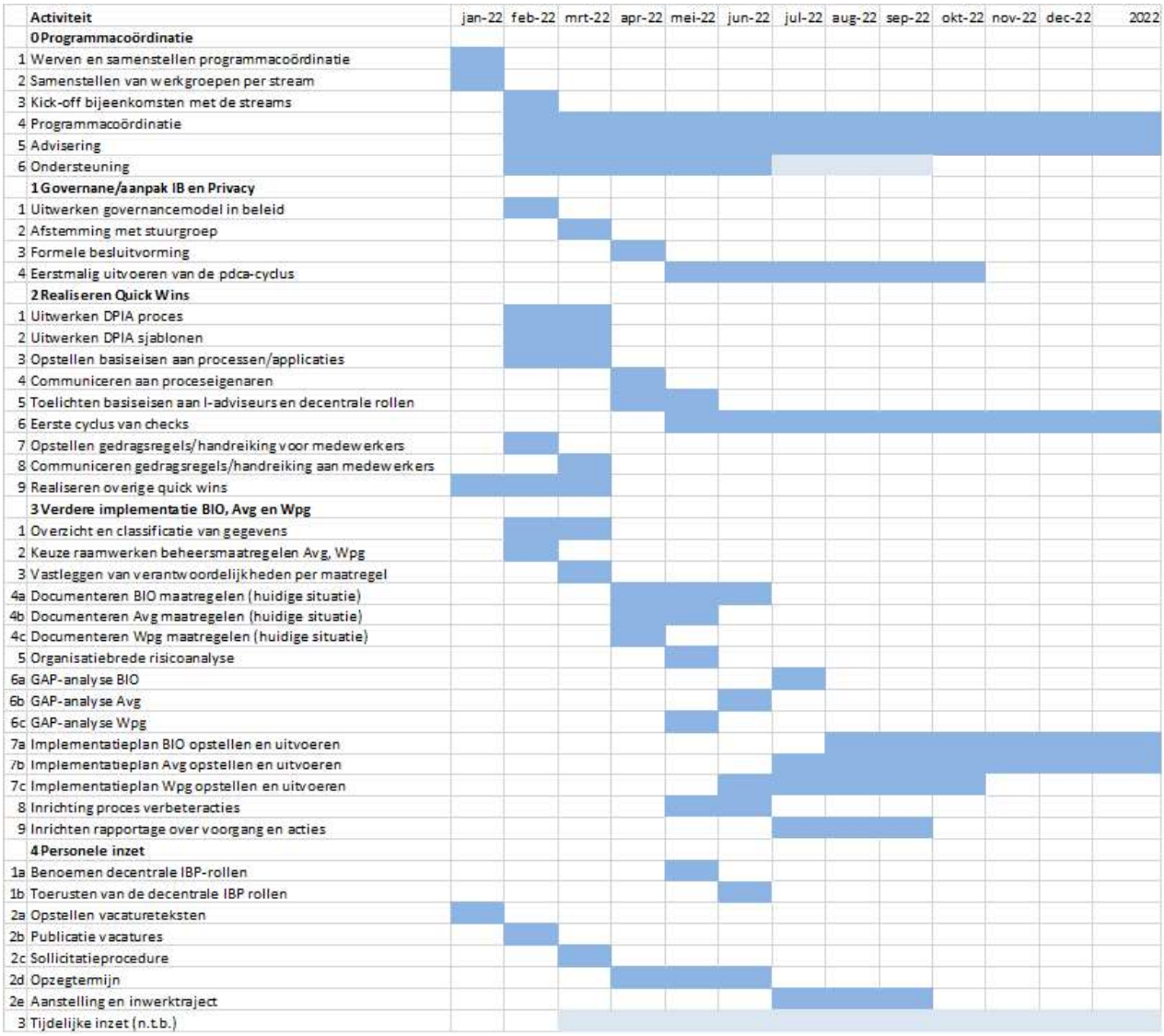
2) Structurele centrale inzet:
   a) opstellen vacatureteksten;
   b) publicatie vacatures;
   c) sollicitatieprocedure;
   d) opzegtermijn;
   e) aanstelling en inwerktraject.
3) Tijdelijke inzet
   De tijdelijke inzet bestaat gedeeltelijk uit de programmaorganisatie. Daarnaast is er mogelijk inzet nodig om medewerkers vrij te maken om bij te dragen aan het programma of voor de implementatie van maatregelen, bijvoorbeeld waar technische implementatiekennis nodig is. Dit is nader te bepalen bij de uitwerking van de planning in de werkgroepen.

Hieronder is een eerste voorstel voor de planning van de stappen weergegeven:



6.6 Overzicht van de planning

In het volgende overzicht is een eerste voorstel voor een planning met daarin alle streams weergegeven.


Activiteit
jan-22
feb-22
mrt-22
apr-22
mei-22
jun-22
jul-22
aug-22
sep-22
okt-22
nov-22
dec-22
2022
0 Programmacoördinatie
1 Werven en samenstellen programmacoördinatie
2 Samenstellen van werkgroepen per stream
3 Kick-off bijeenkomsten met de streams
4 Programmacoördinatie
5 Advisering
6 Ondersteuning
1 Governane/aanpak IB en Privacy
1 Uitwerken governancemodel in beleid
2 Afstemming met stuurgroep
3 Formele besluitvorming
4 Eerstmalig uitvoeren van de pdca-cyclus
2 Realiseren Quick Wins
1 Uitwerken DPIA proces
2 Uitwerken DPIA sjablonen
3 Opstellen basiseisen aan processen/applicaties
4 Communiceren aan proceseigenaren
5 Toelichten basiseisen aan I-adviseurs en decentrale rollen
6 Eerste cyclus van checks
7 Opstellen gedragsregels/handreiking voor medewerkers
8 Communiceren gedragsregels/handreiking aan medewerkers
9 Realiseren overige quick wins
3 Verdere implementatie BIO, Avg en Wpg
1 Overzicht en classificatie van gegevens
2 Keuze raamwerken beheersmaatregelen Avg, Wpg
3 Vastleggen van verantwoordelijkheden per maatregel
4a Documenteren BIO maatregelen (huidige situatie)
4b Documenteren Avg maatregelen (huidige situatie)
4c Documenteren Wpg maatregelen (huidige situatie)
5 Organisatiebrede risicoanalyse
6a GAP-analyse BIO
6b GAP-analyse Avg
6c GAP-analyse Wpg
7a Implementatieplan BIO opstellen en uitvoeren
7b Implementatieplan Avg opstellen en uitvoeren
7c Implementatieplan Wpg opstellen en uitvoeren
8 Inrichting proces verbeteracties
9 Inrichten rapportage over voorgang en acties
4 Personele inzet
1a Benoemen decentrale IBP-rollen
1b Toerusten van de decentrale IBP rollen
2a Opstellen vacatureteksten
2b Publicatie vacatures
2c Sollicitatieprocedure
2d Opzegtermijn
2e Aanstelling en inwerktraject
3 Tijdelijke inzet (n.t.b.)

H7 | Verantwoording

Deze rapportage is gebaseerd op door de BAR-organisatie aangeleverde documenten en ruim twintig interviews met onder andere een wethouder, een directielid, de FG, de PO, de CISO, het management en enkele medewerkers I&A en Facilitair en medewerkers uit het primaire proces, met name uit het Sociaal Domein. Daarnaast is in het kader van het onderzoek een van de locaties van de BAR-organisatie bezocht.
Omdat gebruikers en beheerders van slechts enkele applicaties zijn gesproken, zijn de resultaten mogelijk niet representatief voor alle applicaties. Er zijn daarvoor immers geen uniforme werkwijzen beschreven en geborgd. Bij de waardering van de implementatie is daar rekening mee gehouden.
Niet alle gevraagde documentatie is aangeleverd, ook niet wanneer in interviews werd aangegeven dat deze documentatie aanwezig zou zijn. Wij hebben aangenomen dat de desbetreffende documentatie niet aanwezig is.

Naar aanleiding van een concepttussenrapportage zijn in overleg met de gedelegeerd opdrachtgever opmerkingen van twee leden van de stuurgroep, de CISO en de PO verwerkt in de hoofdstukken 2, 3 en 4.

Bij het assessment van de implementatie van BIO, AVG en Wpg is door een onafhankelijke adviseur onderzocht of beheersmaatregelen zijn beschreven, welk inzicht er is in de volledige implementatie en - aan de hand van voorbeelden - of ze worden uitgevoerd (in audit-terminologie: opzet en bestaan).
Daarmee is het assessment geen volledige audit waarin de werking van de maatregelen over alle bedrijfsprocessen/applicaties wordt gecontroleerd (in auditterminologie: geen onderzoek over de werking).

BMC

Databankweg 26D
3821 AL Amersfoort

Postbus 490
3800 AL Amersfoort

(033) 496 52 00
info@bmc.nl
www.bmc.nl

KvK BMC Advies 32078667
IBAN NL91ABNA0504035754
BTW NL80.86.63.598 B.01

Colofon

29 november 2021

Classificatie : Vertrouwelijk

Naam adviseur : ir. Julius Duijts CMC CISSP CIPP/E

Projectnummer : PO022465

Kijk voor meer info op onze website: bmc.nl