Geachte leden van de raad,

De Rekenkamer Westerkwartier biedt u hierbij haar eerste onderzoeksrapport aan: een onderzoek naar de doorwerking van de aanbevelingen uit een spraakmakend onderzoek naar informatieveiligheid in het sociaal domein. In een doorwerkingsonderzoek kijk je naar de mate waarin de aanbevelingen die in een eerder onderzoek zijn gedaan daadwerkelijk zijn overgenomen en/of zijn uitgevoerd. Het onderzoek dat voor u ligt is tot stand gekomen in een bijzondere periode, waarin de samenleving getroffen is door een pandemie. Informatieveiligheid, zeker nu er veel medewerkers thuis werken, is daarmee alleen maar belangrijker geworden. De Rekenkamer is blij met de prettige samenwerking en tijdige informatievoorziening door de medewerkers van de gemeente Westerkwartier – voor ons is dit onderzoek een prettige kennismaking met de gemeentelijke organisatie geweest.

**Achtergrond**

In 2018 publiceerde de Rekenkamercommissie van de gemeenten Zuidhorn, Leek, Grootegast en Marum Informatieveiligheid een kritisch rapport over de informatieveiligheid in het sociaal domein. Het leverde aanbevelingen op over de techniek, de organisatie en de menskant van informatieveiligheid. De nieuwe Rekenkamer Westerkwartier heeft in dit eerste rapport onderzocht in hoeverre de aanbevelingen uit het onderzoek uit 2018 zijn overgenomen en uitgevoerd in het huidige beleid van de gemeente Westerkwartier over informatieveiligheid. Om dit te onderzoeken zijn documenten bestudeerd en interviews afgenomen met een aantal sleutelpersonen. In het ambtelijk wederhoor hebben de betrokken medewerkers de feitelijke bevindingen gecontroleerd op onjuistheden. Alle door hen aangegeven aandachtspunten zijn verwerkt.

Dit rapport geeft de raad inzicht in hoe de gemeentelijke organisatie de aanbevelingen uit het eerdere rapport heeft opgepakt en heeft verwerkt in beleid en werkprocessen. Het laat ook zien waar er nog een opgave ligt en biedt de raad handvatten om de voortgang in het oppakken van deze opgaven te controleren. Daarbij is het belangrijk om te benoemen dat in dit onderzoek alleen documenten zijn bestudeerd en een beperkt aantal interviews is afgenomen en dat er geen onderzoek van systemen om technisch niveau heeft plaatsgevonden. De belangrijkste inzichten uit het onderzoek zijn hieronder voor u samengevat.

**Doorwerking in beeld**

De gemeente Westerkwartier heeft de aanbevelingen rond informatieveiligheid verwerkt in het Informatiebeveiligingsbeleid, de aanpak van Privacy en een specifiek plan voor het i-Bewustzijn. Alle in het eerdere onderzoek genoemde aanbevelingen komen terug in deze plannen en beleidsdocumenten. De taken rond informatieveiligheid zijn belegd bij het team Kwaliteitszorg. Zowel bestuurlijk als ambtelijk heeft het thema veel aandacht en is er regelmatig overleg over de voortgang. Informatieveiligheid is echter een zaak van de hele organisatie. Inzicht in en verantwoordelijkheid voor processen bij alle teams en medewerkers zijn essentieel om de informatieveiligheid en privacy te kunnen bewaken**.** Juist dit blijkt een bottleneck: er is geïnvesteerd in capaciteit om alle maatregelen te kunnen uitvoeren, maar na de fusie moeten de werkprocessen opnieuw beschreven en ingericht worden, wat veel tijd en aandacht vraagt. Hoewel alle urgente aanbevelingen zijn opgepakt, zijn er veel aanbevelingen die wel zijn opgestart, maar niet zijn uitgevoerd. Hierbij kiest de organisatie voor het uitvoeren in een tempo dat past bij wat de teams en de domeinen aan kunnen: liever goed dan snel. Vanuit het team kwaliteitszorg wordt langs drie lijnen de kwaliteit en voortgang bewaakt: control, informatieveiligheid en privacy. Zodra de externe ontwikkelingen en teamontwikkeling het toelaten, worden werkprocessen beschreven en worden de criteria voor informatieveiligheid en privacy meegenomen.

**Conclusies en aanbevelingen**

Een eerste conclusie is dat er politieke urgentie is geweest rond het presenteren van de aanbevelingen, maar dat dit niet heeft geleid tot een proactieve houding bij de raad in het controleren van de aanbevelingen. Ook college en organisatie hebben de urgentie herkend en een tweede conclusie is dat het onderzoek naar informatiebeveiliging in het sociaal domein een hoge mate van doorwerking heeft gehad. Het onderzoek heeft daarmee impact gehad in beleid en organisatie, niet alleen in het sociaal domein, maar ook in de volle breedte van de organisatie van de gemeente Westerkwartier. Dat wil niet zeggen dat het proces daarmee klaar is. Een derde conclusie is dat voor de verdere implementatie van de aanbevelingen nog een aantal obstakels in de weg staat. Deze obstakels hangen samen met de taakverdeling en het format voor het beschrijven van werkprocessen, de beperkte capaciteit voor de uitvoering van de maatregelen, het niet verplichtende karakter van een aantal maatregelen en het gekozen ambitieniveau in zowel de techniek als de organisatieontwikkeling. In de rapportage zelf is deze conclusie nog verder uitgewerkt in een aantal deelaspecten. De laatste conclusie is dat de planning te ambitieus is en steeds moet worden bijgesteld. De planning lijkt daarmee niet altijd realistisch en dat maakt proactief plannen en sturen moeilijker.

De Rekenkamer adviseert de raad alert te zijn op gemelde vertragingen en actief door te vragen naar de oorzaken en aanpak daarvan. Niet alleen omdat een adequate informatieveiligheid essentieel is voor een orgaan dat zoveel gevoelige informatie bezit over inwoners, maar ook omdat het een goede graadmeter is voor de ontwikkeling van de fusieorganisatie. De Rekenkamer beveelt de raad aan het college te verzoeken de raad hierover eenmaal per jaar gericht te informeren en voldoende prioriteit en ambtelijke capaciteit te reserveren voor dit thema. Meer specifiek adviseert de Rekenkamer de raad om het college te verzoeken om een gemeentebrede systematiek te hanteren voor het ontwikkelen, beschrijven, beheren en verbeteren van werkprocessen. Het belang van adequate werkprocessen is cruciaal, niet alleen voor de informatieveiligheid, maar ook voor de kwaliteit van de in- en externe dienstverlening. Ook adviseert de Rekenkamer de raad het college te verzoeken om het grootschalige onderzoek (ook naar systemen en techniek) dat in 2018 is uitgevoerd te herhalen. Hieronder worden de belangrijkste aanbevelingen kort opgesomd:

* Wees alert op mogelijke vertragingen in de implementatie van het beleid informatieveiligheid en privacy en informeer actief naar de voortgang en de mogelijke knelpunten daarin;
* Laat je eens per jaar actief en specifiek informeren over het informatieveiligheidsbeleid;
* Vraag bij het college actief naar de aandacht voor informatieveiligheid en privacy bij het inrichten van werkprocessen, naast de inhoudelijke kwaliteit en control.
* Vraag het college te investeren in tijd en aandacht voor de uitvoering van de technische maatregelen uit het eerdere onderzoek;
* Vraag het college te streven naar BIO-niveau 3 en faciliteer in wat daarvoor nodig is in termen van formatie en techniek;
* Vraag het college zich actief in te zetten op het voorwaardelijk maken van een training privacy en informatieveiligheid voor toegang tot het systeem;
* Verzoek het college om beleid voor afstandswerken, zeker nu dat als gevolg van de COVID-maatregelen veelvuldig gebeurt;
* Verzoek het college te investeren in een herhalingsonderzoek van het door het externe bureau verrichtte onderzoek om te komen tot een 1-meting, zodra de situatie weer als normaal beschouwd kan worden.

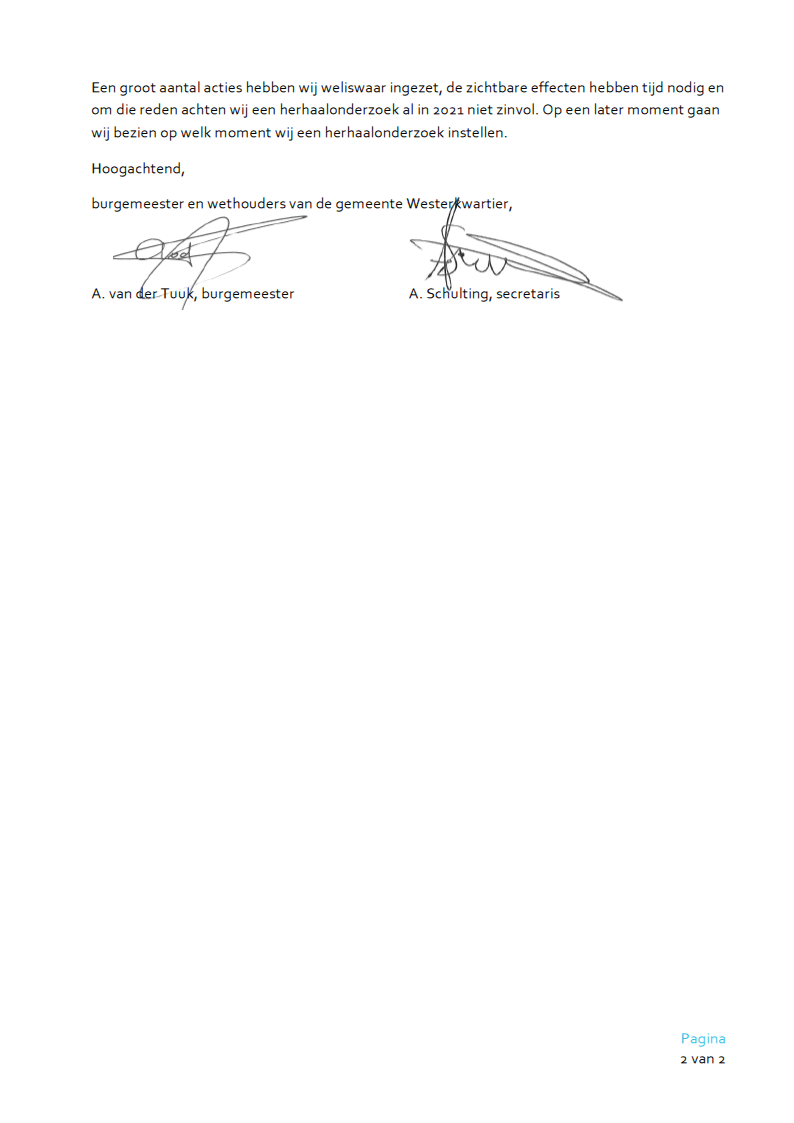
**Bestuurlijk wederhoor**

Op 30 november 2020 is het rapport aan het college verstuurd met een verzoek om een bestuurlijke reactie. Met enige vertraging vanwege het kerstreces en onzekerheid over de juiste versie, heeft de Rekenkamer op 20 januari de reactie van het college ontvangen. De Rekenkamer is blij dat het college zich herkent in de conclusies en aanbevelingen. Het college benoemt zowel de intenties rond het bewaken van de informatieveiligheid, als de documenten die de raad kan gebruiken om zich te informeren over de voortgang in de uitvoering van die intenties. De Rekenkamer heeft er begrip voor dat het college een uitgebreider onderzoek wil uitstellen, zeker gezien de huidige omstandigheden.

**Tot slot**

De Rekenkamer biedt u hierbij dit onderzoek aan. Tijdens een raadsoverleg of raadsvergadering geeft de Rekenkamer graag een toelichting op de conclusies en aanbevelingen en zijn we bereid tot een nadere uitleg en het beantwoorden van vragen over dit onderzoek.





**Informatieveiligheid   
werkt door**

Rapport Rekenkamer gemeente Westerkwartier



# Colofon

Rekenkamer Westerkwartier

Februari 2021

Onderzoekers: Harry van Boven (lid Rekenkamer)  
Avelien Haan (lid Rekenkamer)

Inhoudsopgave

[1 Inleiding en aanpak 1](#_Toc64754323)

[1.1 Inleiding 1](#_Toc64754324)

[1.2 Onderzoeksopzet 1](#_Toc64754325)

[1.3 Aanpak van het onderzoek 2](#_Toc64754326)

[1.4 Opbouw rapportage 3](#_Toc64754327)

[2 Politiek-bestuurlijke aandacht 4](#_Toc64754328)

[2.1 Conclusies & Aanbevelingen uit 2018 4](#_Toc64754329)

[2.2 Bestuurlijke reactie 2018 5](#_Toc64754330)

[2.3 Behandeling in de gemeenteraad 6](#_Toc64754331)

[2.4 Bevindingen 6](#_Toc64754332)

[3 Implementatie in beleid en uitvoering 8](#_Toc64754333)

[3.1 Aanpak informatieveiligheid 8](#_Toc64754334)

[3.1.1 Beleid 8](#_Toc64754335)

[3.1.2 Uitvoering 10](#_Toc64754336)

[3.1.3 Doelbereiking 12](#_Toc64754337)

[3.2 Aanpak privacy in de organisatie 13](#_Toc64754338)

[3.2.1 Beleid 13](#_Toc64754339)

[3.2.2 Uitvoering 14](#_Toc64754340)

[3.2.3 Doelbereiking 15](#_Toc64754341)

[3.3 i-Bewustzijn 16](#_Toc64754342)

[3.3.1 Beleid 16](#_Toc64754343)

[3.3.2 Uitvoering 16](#_Toc64754344)

[3.3.3 Doelbereiking 16](#_Toc64754345)

[3.4 Bevindingen 17](#_Toc64754346)

[4 Analyse doorwerking 19](#_Toc64754347)

[4.1 Aandacht in raad en organisatie 19](#_Toc64754348)

[4.2 Doorwerking in beleid 20](#_Toc64754349)

[4.3 Doorwerking in de uitvoering 21](#_Toc64754350)

[4.4 Knelpunten in de doelbereiking 21](#_Toc64754351)

[4.4.1 Gegevensbescherming en privacy 22](#_Toc64754352)

[4.4.2 i-Bewustzijn 22](#_Toc64754353)

[4.4.3 Techniek 23](#_Toc64754354)

[4.4.4 COVID-19 / afstandswerken 23](#_Toc64754355)

[4.5 Mate van doorwerking 23](#_Toc64754356)

[5 Conclusies en aanbevelingen 24](#_Toc64754357)

[5.1 Conclusies 24](#_Toc64754358)

[5.2 Aanbevelingen 26](#_Toc64754359)

[5.3 Slotopmerking 27](#_Toc64754360)

[Bijlage 1: Bestudeerde documenten 28](#_Toc64754361)

[Informatie Raad 28](#_Toc64754362)

[Documenten i-Bewustzijn 28](#_Toc64754363)

[Documenten Privacy 28](#_Toc64754364)

[Documenten Informatieveiligheid 28](#_Toc64754365)

[Documenten Integraal Veiligheidsbeleid 29](#_Toc64754366)

[Bijlage 2: Overzicht respondenten en bespreekthema’s 30](#_Toc64754367)

[Bijlage 3: Control Gemeente Westerkwartier 31](#_Toc64754368)

# Inleiding en aanpak

## Inleiding

Informatieveiligheid is een actueel en relevant thema. Met enige regelmaat worden overheden slachtoffer van hacks. Ook maken publieke organisaties zich onbedoeld schuldig aan datalekken. In haar vergadering van 16 december 2019 heeft de Rekenkamer van de gemeente Westerkwartier besloten een onderzoek uit te voeren naar de implementatie van de adviezen van het rapport over de informatieveiligheid binnen het sociaal domein. Dit rapport is in 2018 opgesteld door de toenmalige Rekenkamercommissie van de gemeenten Zuidhorn, Leek, Grootegast en Marum. De conclusies van de commissie waren pittig. De

Rekenkamer wil weten hoe het nu staat met de informatieveiligheid binnen de gemeente Westerkwartier. Dit hoofdstuk gaat in op de onderzoeksopzet, vraagstelling, aanpak van het onderzoek en opbouw van de rapportage.

## Onderzoeksopzet

De vraagstelling en opzet van het onderzoek is gebaseerd op de handreiking voor het meten van doorwerking van de NVRR (NVRR, 2018). Met de term doorwerking wordt bedoeld: de mate waarin de aanbevelingen uit de rapportage van de rekenkamercommissie invloed hebben gehad op de beslissingen van de raad en het handelen van college en ambtelijke organisatie. In de NVRR-handreiking worden meerdere niveaus van doorwerking onderscheiden en worden relevante indicatoren gegeven om te kunnen bepalen of er doorwerking is. Het normenkader dat de Rekenkamer hanteert voor het meten van de doorwerking, is op dit model gebaseerd, waarbij de nadruk ligt op de mate van doorwerking in beleid en uitvoering.

Het doel van het onderzoek is om de raad inzicht te geven in hoeverre en op welke wijze de gemeente Westerkwartier gehoor heeft gegeven aan de door de raad overgenomen aanbevelingen van het onderzoek naar informatieveiligheid in het sociaal domein. Daarbij is het interessant om te weten of de aanpak van het informatieveiligheid breder is uitgezet dan alleen binnen het sociaal domein.

De hoofdvraag van het onderzoek is:

**In hoeverre heeft de gemeente Westerkwartier opvolging gegeven aan de aanbevelingen uit het onderzoek naar informatieveiligheid in het sociaal domein?**

Om deze vraag te kunnen beantwoorden heeft de rekenkamer de volgende deelvragen opgesteld:

1. In hoeverre heeft de raad aandacht gehad voor de behandeling van het rekenkamerrapport en de opvolging van de aanbevelingen?
2. In hoeverre en op welke wijze zijn de aanbevelingen uitgewerkt in nieuw of aangepast beleid?
3. In hoeverre en op welke wijze hebben de aanbevelingen geleid tot aanpassingen in de uitvoering van het beleid?
4. In hoeverre zijn de doelen bereikt van het nieuwe beleid (wat is de mate van doelbereiking)?

Op basis van de handreiking doorwerking van de NVRR is een normenkader opgesteld, dat indicatoren geeft voor de mate waarin doorwerking heeft plaatsgevonden. De thema’s in het normenkader volgen de deelvragen uit het onderzoek.

|  |  |
| --- | --- |
| Thema | Indicatoren |
| Politiek-bestuurlijke aandacht | * het rapport is geagendeerd voor behandeling in de raad * het rapport is aan de raad/commissie gepresenteerd en met de raad besproken * de raad heeft tijd genomen voor discussie over het rapport en de daarin opgenomen aanbevelingen * de bevindingen zijn volledig gesteund door de raad * de conclusies zijn volledig overgenomen door de raad * de raad heeft door middel van vragen/moties aandacht gehad voor het rapport of nadien het onderwerp van het rapport |
| Uitwerking in beleid | * de conclusies zijn overgenomen in beleidsvoornemens en ambities tav informatieveiligheid * de aanbevelingen zijn opgenomen in nieuw/aangepast beleid * er zijn concrete doelen gesteld, met bijbehorende indicatoren voor het meten van de mate van doelbereiking |
| Uitwerking in processen | * de aanbevelingen hebben geleid tot het nemen van besluiten over het aanpassen/aanschaffen van formatie en ICT-producten * de aanbevelingen hebben geleid tot het inrichten van nieuwe werkprocessen * het thema van het rapport heeft regelmatige aandacht van college, directie en management |
| Doelbereiking | * er zijn al tijdens het onderzoek aanpassingen gedaan in beleid en uitvoering * het rapport heeft geleid tot een versnelling van het beleidsproces of de uitvoering * door het implementeren van de aanbevelingen hebben feitelijke veranderingen plaatsgevonden * de mate van doelbereiking wordt gemonitord. * de gestelde doelen worden volgens planning gehaald. |

## Aanpak van het onderzoek

Na een verkennend vooronderzoek is een beknopt doorwerkingsonderzoek uitgevoerd naar de implementatie van de aanbevelingen. De ingezette onderzoeksmethoden zijn een documentanalyse en drie interviews met sleutelpersonen rond het thema informatieveiligheid: de Corporate Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en gemeentesecretaris.

Bijlage 1 bevat de geraadpleegde verslagen van de vergaderingen waarin het rapport uit 2018 is behandeld, en de sinds 2018 opgestelde beleidsdocumenten rond privacy en informatieveiligheid. De interviews zijn voorbereid door openstaande vragen te groeperen in bespreekthema’s op basis van de documentanalyse (zie bijlage 2). De interviewverslagen zijn door de respondenten nagekeken alvorens te zijn vastgesteld.

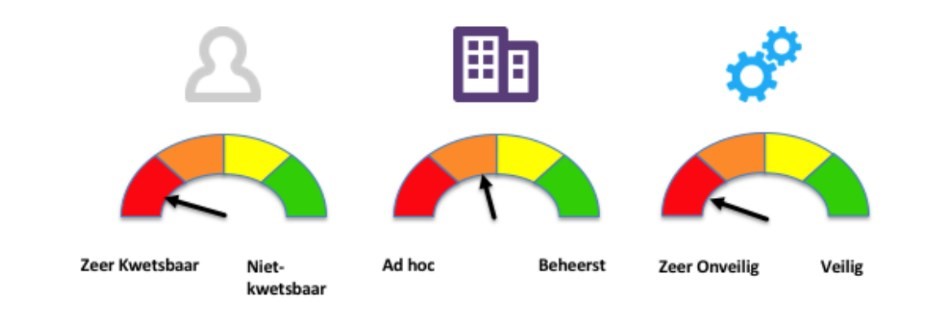
## Opbouw rapportage

De rapportage gaat eerst in op de aanbevelingen uit 2018 en de aandacht die de raad heeft gehad voor de behandeling van het rapport en het vervolgtraject. In hoofdstuk 3 staat de ontwikkeling van het beleidskader centraal en wordt de implementatie in werkprocessen beschreven. Hoofdstuk 4 analyseert de mate van doorwerking aan de hand van het gestelde kader. Het rapport sluit af met conclusies en aanbevelingen.

# Politiek-bestuurlijke aandacht

Op 22 mei 2018 kwam de ‘Rapportage Onderzoek informatieveiligheid Sociaal Domein: mens, organisatie en techniek’ uit. Hieronder staan de belangrijkste conclusies en aanbevelingen uit het onderzoek. Vervolgens bespreekt dit hoofdstuk in welke mate de raad aandacht heeft besteed aan de rapportage en de bevindingen.

## Conclusies & Aanbevelingen uit 2018

Het onderzoek uit 2018 richtte zich op de verschillende aspecten die raken aan informatieveiligheid, oftewel menselijk gedrag, de organisatie (IT Governance en beheersing) en de inrichting en werking van de techniek. De scope van het onderzoek richtte zich op de onderdelen CJG (Centrum Jeugd en Gezin) en WMO (Wet Maatschappelijke Ondersteuning). De beoordeling van mens, organisatie en techniek is door de onderzoekers als volgt gevisualiseerd: In het rapport wordt aangegeven: ‘de uit de technische onderzoek afkomstige hiaten zijn gelijk opgepakt en verbeterd waarna het continue proces van verbetering in gang is gezet’.

De hoofdconclusies luidden:

* Informatieveiligheid is nog onvoldoende verankerd in de kennis, houding en gedrag van de medewerkers. De medewerkers van CJG en WMO zijn zeer kwetsbaar voor mensgerichte aanvallen gezien het aantal medewerkers dat gebruikersnaam en wachtwoord verstrekt na een phishing praktijktest. Het niet/minder herkennen en melden van incidenten is een aandachtspunt, als ook het verifiëren van een telefonisch onderzoek.
* Op het organisatorische vlak zijn diverse maatregelen getroffen maar zijn nog niet alle maatregelen beschreven of ze zijn nog niet bij alle medewerkers bekend. Er is een nauwe samenwerking met de Functionaris Gegevensbescherming om de openstaande punten op te pakken en waar nodig te verbeteren. Daarnaast is aandacht voor privacy een natuurlijk onderdeel van het dagelijkse werk.
* Op het technische vlak dienen er diverse beheersmaatregelen genomen te worden zoals het verbeteren van patchmanagement en het uit-faseren van oude ICTcomponenten. Gezien de aangetroffen kwetsbaarheden wordt het netwerk als zeer onveilig beoordeeld’.

Als belangrijkste verbetermogelijkheden worden benoemd (2018):

1. Vul het intern reeds gestarte bewustwordingsprogramma aan met een e-learning phishing om de medewerkers het onderscheid te leren tussen een legitieme en een phishing mail. Gezien de belangrijke rol voor leidinggevenden in het veiliger werken door medewerkers, dient de leidinggevenden aanvullende ondersteuning worden geboden.
2. Het jaarlijks herhalen van de praktijktesten zoals phishing, telefonische aanval om zodoende de voortgang te monitoren. Op termijn zal ook een praktijktest mystery visits aan het onderzoek kunnen worden toegevoegd.
3. Leg de werkwijze voor het controleren van de autorisaties vast en leg daarbij de uitkomsten van een uitgevoerde controle vast.
4. Leg de werkwijze voor wijzigingen in applicaties vast waarbij minimaal wordt vastgelegd wie wijzigingen in mag dienen, wie het doorvoeren van wijzigingen mag accorderen, hoe er getest wordt en wie de doorgevoerde wijziging goedkeurt.
5. Zorg voor een eenduidige werkwijze voor het archiveren en opbergen van papieren dossiers.
6. Zorg dat de procedure voor het melden van datalekken bekend is bij alle medewerkers van het Sociaal Domein.
7. Zorg voor de uitvoering van privacy impact assessment op de processen en gegevens binnen het CJG en de WMO.
8. Het periodiek uitvoeren van beveiligingsonderzoeken op onderdelen van de gemeentelijke IT-infrastructuur om inzage te krijgen in huidige situatie en voortgang.
9. De aanbevelingen uit de technische rapportage dienen als richtlijnen voor het implementeren van een baseline-policy op basis waarvan nieuwe systemen worden beoordeeld alvorens deze in productie worden genomen om kwetsbaarheden die zijn geïdentificeerd gedurende het onderzoek in de toekomst te voorkomen.
10. Verder doorvoeren van de adviezen uit het technische rapport zoals het configuratiemanagement en hardening van het netwerk en haar doelsystemen.

## Bestuurlijke reactie 2018

In de bestuurlijke reactie van 23 augustus 2018 wordt erop gewezen dat al in 2016 door een extern bureau een risicoanalyse informatieveiligheid is uitgevoerd. Aangegeven wordt dat de uitkomsten hiervan in grote lijnen overeenkomen met de uitkomsten van het onderzoek van de Rekenkamercommissie (2018). Deze uitkomsten hebben geleid tot meerdere maatregelen zoals de bevordering van bewustwording van medewerkers en ook nieuwe en aangescherpte procedures en beleid. Ook zijn per medio 2017 een CISO en een FG aangesteld. De bestuurlijke reactie op de aanbevelingen van de Rekenkamercommissies komen in grote lijnen op het volgende neer:

*Mens:* de komende jaren wordt ingezet op bewustwording van medewerkers, management en bestuur. Voor de bewustwordingstrajecten wordt structureel budget gereserveerd; deelname is verplicht. Dit traject wordt voorzien van periodieke praktijktesten zoals phishingtesten en mystery visits.

*Organisatie:* van deze aanbevelingen is een aantal al geëffectueerd of gepland. Als voorbeelden worden genoemd dat er gewerkt zal worden met (geüniformeerde) changemanagement procedures en dat er een Privacy impact assessments (PIA) op de meest kritische processen (zoals de uitvoering van de Jeugdwet en de Wet maatschappelijke ondersteuning) wordt uitgevoerd. Ook wordt een voorstel voor de inrichting van de privacy organisatie aangekondigd.

*Techniek:* na het opleveren van het technisch rapport zijn met spoed de risico's met de classificatie kritisch/hoog opgelost en is de formatie, zowel structureel als tijdelijk, uitgebreid (medewerker systeemveiligheid, security officer, tijdelijke kracht ten bate van het opstellen en implementeren van hardeningsrichtlijnen).

Voorts wordt in de bestuurlijke reactie aangegeven dat alle verbeterpunten op het gebied van informatieveiligheid en privacy worden opgenomen in de jaarplannen informatieveiligheid en privacy.

## Behandeling in de gemeenteraad

De raad is al vroeg over dit onderzoek geïnformeerd met een brief in februari 2018 en tijdens een bijeenkomst over de rapporten van de rekenkamercommissie. De rapportage is besproken in de raadsgroep Herindeling Westerkwartier van 11 oktober 2018. Daar wordt in de bespreking gememoreerd dat tijdens een eerdere informatiebijeenkomst de raadsleden geschrokken zijn van de uitkomsten. Tegelijk tonen de raadsleden zich gerustgesteld omdat de colleges volgens de bestuurlijke reactie de aanbevelingen voortvarend hebben opgepakt. Ook wordt genoemd dat het niet verwonderlijk is, dat er zaken zijn blijven liggen in het proces van de fusie. De raadsgroep neemt kennis van het eindrapport en onderschrijft de conclusies en aanbevelingen. De stuurgroep wordt verzocht uitvoering te geven aan de aanbevelingen.

Vervolgens wordt het eindrapport als ingekomen stuk voor kennisgeving aangenomen in de gemeenteraadsvergadering van 15 oktober 2018. Op de besluitenlijst staat aangegeven dat er bespreking heeft plaatsgevonden in de commissie.

De onderzoekers hebben in ibabs gezocht naar raadsvragen, moties en amendementen die over het thema informatieveiligheid gaan. In de periode na oktober 2018 zijn deze niet gevonden. Intussen is de raad wel op de hoogte gehouden in bestuursrapportages en jaarstukken en door middel van gerichte brieven (26 februari 2019 over de implementatie BIO). Begin 2020 is het integraal veiligheidsbeleid vastgesteld. Vanuit de ambtelijke organisatie werd voorgesteld om binnen het thema integriteit te kiezen voor een speerpunt: ondermijning of informatieveiligheid. De raad heeft gekozen voor ondermijning.

In april 2020 heeft de raad de jaarrapportage gegevensbescherming ontvangen. Naar aanleiding daarvan hebben enkele raadsleden gevraagd om een informatiebijeenkomst over het thema informatieveiligheid en privacy. Deze bijeenkomst is in het najaar van 2020 ingepland en gehouden.

## Bevindingen

De conclusies en aanbevelingen uit 2018 stevig zijn te noemen. Dat wordt zo herkend door raadsleden en ook door het college in de bestuurlijke reactie. De raad heeft aandacht gehad voor de rapportage voorafgaand aan publicatie en tijdens een informatiebijeenkomst over een onderzoek waarin meerdere rapportages zijn besproken. Toen het rapport uitkwam, was de raad al op de hoogte van de uitkomsten. In de raadsgroep is ook aandacht besteed aan de rapportage, waarbij alle conclusies en aanbevelingen zijn ondersteund. Het is daarna in de raad als geheel niet meer besproken. Ook heeft de raad in het vervolgtraject geen vragen meer gesteld over de voortgang, ook niet naar aanleiding van informatie daarover. Pas recentelijk heeft de raad om meer informatie gevraagd, niet zozeer naar aanleiding van het vorige onderzoek, maar eerder vanwege onbekendheid met en nieuwsgierigheid naar het thema.

|  |  |  |
| --- | --- | --- |
| Indicator | Bevinding | Oordeel |
| Het rapport is geagendeerd voor behandeling in de raad | Geagendeerd en genoemd in de notulen | Voldaan |
| Het rapport is aan de raad/commissie gepresenteerd en met de raad besproken | Er is een presentatie en commissiebehandeling geweest | Voldaan |
| De raad heeft tijd genomen voor discussie over het rapport en de daarin opgenomen aanbevelingen | Er is in de commissie een bespreking geweest, niet in de raad als geheel | Voldaan |
| De bevindingen zijn volledig gesteund door de raad | Ongewijzigd en onbesproken | Voldaan |
| De conclusies zijn volledig overgenomen door de raad | Ongewijzigd overgenomen | Voldaan |
| De raad heeft door middel van vragen/moties aandacht gehad voor het rapport of nadien het onderwerp van het rapport | Er zijn geen vragen gesteld, wel is recentelijk aandacht voor het thema gevraagd | Deels voldaan |

# Implementatie in beleid en uitvoering

Het rapport leverde aanbevelingen op gericht op mens, organisatie en techniek. Dit hoofdstuk onderzoekt op welke wijze de aanbevelingen zijn omgezet in aangepast of nieuw beleid en op welke wijze de organisatie uitvoering heeft gegeven aan de aanbevelingen.

Bij het opvragen van documenten werd duidelijk dat in drie beleidslijnen aandacht is voor de implementatie van de aanbevelingen: beleid gericht informatieveiligheid, privacy en het verbeteren van het i-Bewustzijn. De samenhang tussen de beleidsdocumenten is als volgt:

* De aanpak informatieveiligheid is gericht op het inrichten van de informatieveiligheid (met aandacht voor techniek, organisatie en processen) (paragraaf 3.1);
* De aanpak privacy is gericht op het voldoen aan de privacyregels (met aandacht voor met name processen en mensen) (paragraaf 3.2);
* De aanpak i-Bewustzijn draagt bij aan informatieveiligheid en privacy en is vooral gericht op de mens (paragraaf 3.3).

## Aanpak informatieveiligheid

In de paragrafen hieronder is de ontwikkeling in het beleid opgenomen, is beschreven op welke wijze de uitvoering is ingericht en hoe het staat met de voortgang in doelbereiking op het thema informatieveiligheid.

### Beleid

Het eerste plan waarin verwijzingen naar het onderzoekrapport uit 2018 voor komen is het Jaarplan Informatieveiligheid 2018-2019 (augustus 2018). Dit schetst een overzicht en prioritering van kwetsbaarheden. Als basis zijn gebruikt:

* het dreigingsbeeld Nederlandse gemeenten
* de risicoanalyse informatieveiligheid 2016
* het Jaarplan informatieveiligheid 2017 – 2018
* de risico’s die zijn gesignaleerd door de CIS
* de uitkomsten van het rekenkamercommissieonderzoek uit 2018

De bevindingen zijn geclusterd rond mens, processen, techniek en herindeling. Voor al die onderdelen worden maatregelen geformuleerd. In een bijlage zijn alle maatregelen uit het technisch deel van het rapport van de Rekenkamercommissie uit 2018 overgenomen. Overal in het document zijn verwijzingen naar het rekenkamerrapport zichtbaar. Een vergelijking van maatregelen uit de planning voor 2018-2019 (bijlage 1 uit het plan) laat zien dat een groot deel van de aanbevelingen is verwerkt als acties in het jaarplan. Van de aanbevelingen die in 2.1 zijn genoemd, zijn de volgende opgenomen in dit beleidsdocument:

* 1, 2 (i-Bewustzijn);
* 3 en 4 (autorisatie en changemanagement);
* 5 (archief);
* 8, 9 en 10 (technische aanbevelingen).

In 2019 is het Jaarplan Informatieveiligheid 2018-2019 herijkt, mede omdat vanaf 2020 voor de gemeenten de Baseline Informatiebeveiliging Overheid (BIO) geldt. Dit vraagt een aantal maatregelen. Dit resulteert in een gedetailleerd beeld van actiepunten omdat ook de maatregelen uit het informatiebeveiligingsplan 2018-2019, die niet (volledig) zijn uitgevoerd zijn opgenomen.

Naast het herijkte plan, is ook een beleidsdocument voor de iets langere termijn geschreven. Dit betreft het Informatiebeveiligingsbeleid 2019-2021 (versie 1, september 2019)[[1]](#footnote-2). Hieronder wordt dit kader, op basis van het vastgestelde beleid, kort beschreven. Het beleid ten aanzien van informatiebeveiliging wordt gemeentebreed bepaald. Er is dus geen specifiek beleid voor het sociaal domein. De belangrijkste uitgangspunten zijn:

* Het college van b&w is eindverantwoordelijk voor informatiebeveiliging en stelt het informatiebeveiligingsbeleid vast.
* De directie is verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid.
* De CISO rapporteert onafhankelijk over de uitvoering het informatiebeveiligingsplan aan de directie.
* De gemeente Westerkwartier beschouwt informatieveiligheid niet als een project maar als integraal onderdeel van het werkproces.
* Bij het verbeteren van informatieveiligheid wordt risicogestuurd gewerkt.
* Er wordt structureel aandacht besteed aan het verhogen van het kennis- en bewustzijnsniveau over informatiebeveiliging en het omgaan met persoonsgegevens.

Het beleidsplan benoemt strategische doelen die worden vertaald naar concrete actiepunten in een jaarlijks informatiebeveiligingsplan. Het informatiebeveiligingsbeleid treedt in werking na vaststelling door het college van burgemeester en wethouders. De CISO evalueert en beoordeelt het informatiebeveiligingsbeleid jaarlijks. Indien gewenst stelt de CISO het document bij en laat dit vaststellen door het college van burgemeester en wethouders.

Bij het opstellen, uitvoeren en managen van het informatiebeveiligingsbeleid, geldt een aantal vaste afspraken Een aantal daarvan is:

* De BIO vormt de basis voor de informatiebeveiliging evenals de bestuurlijke principes informatieveiligheid van de VNG. Bij de aanpak van informatiebeveiliging werkt de gemeente Westerkwartier met het zogeheten volwassenheidsmodel informatiebeveiliging. Het volwassenheidsmodel informatiebeveiliging bestaat uit 5 volwassenheidniveaus. Hierbij is het doel om voor alle processen in de organisatie om minimaal volwassenheidsniveau 3 te bereiken.
* De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management (directie en teamcoaches), met het college van b&w als eindverantwoordelijke.
* ‘Plan, do, check en act’ is dé cyclus om informatiebeveiliging te verbeteren. Acties worden bijgehouden en gecoördineerd in een Information security managementsysteem (ISMS).
* De CISO ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de informatieveiligheid en rapporteert hierover.
* Bij de uitvoering van het informatiebeveiligingsbeleid geldt een risico gestuurde aanpak.

Twee in de beleidsdocumenten veel voorkomende uitdrukkingen zijn BIO en ENSIA. Beide begrippen komen voort uit landelijke afspraken en verplichtingen waar alle gemeenten aan moeten voldoen. Het gaat daarmee om extern opgelegde kaders. In de tekstblokken hieronder worden deze termen nader uitgelegd.

ENSIA staat voor Eenduidige Normatiek Single Information Audit. Het landelijke project ENSIA is gestart om zorg te dragen dat gemeenten op een uniforme wijze zich verantwoorden over informatiebeveiliging. Eén van de randvoorwaarden is dat informatiebeveiliging wordt opgenomen in de planning en control cyclus en aansluit op de in ENSIA gehanteerde verantwoordingssystematiek en bijbehorende termijnen. ENSIA maakt daarbij onderscheid tussen de horizontale en de verticale verantwoording. De horizontale verantwoording bestaat uit een zelfevaluatie, een IT-audit, een verklaring van het college van b&w en een passage over informatieveiligheid in het jaarverslag. Over de informatiebeveiliging moeten gemeenten ook verantwoording afleggen richting toezichthouders (verticale verantwoording). Concerncontrol toetst in samenspraak met de CISO in dat kader of de vastgestelde beveiligingsmaatregelen worden nageleefd.

De BIO is het normenkader voor informatiebeveiliging voor de gehele Nederlandse overheid. De BIO beschrijft de invulling van de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 voor de overheid. Een deel van de genoemde maatregelen uit de BIO zijn verplichte overheidsmaatregelen. Deze maatregelen zorgen voor een basisbeveiligingsniveau. De gemeente Westerkwartier is gehouden op deze manier werken en kiest daarin een na te streven niveau. In het Informatiebeveiligingsbeleid 2019-2020 zijn de maatregelen als aparte actie opgenomen in ‘Werkprogramma spoor 1’. De BIO gaat volgens het plan uit van een risicogestuurde aanpak waarbij de lijn vooral aan zet is. Het lijnmanagement inventariseert risico’s op al haar kritische processen en applicaties binnen haar of zijn team en neemt voldoende maatregelen neemt om deze processen en applicaties te beveiligen (focus op proces en organisatie). In eerste instantie wordt dit beperkt tot 17 kernapplicaties (werkprogramma spoor 2). In het directieadvies is te lezen dat de gemeente eind 2020 nagenoeg alle verplichte overheidsmaatregelen heeft geïmplementeerd. Echter, de verplichte overheidsmaatregel om aan te sluiten op het security operations center (SOC) van KPN wordt als separaat project beschouwd en geïmplementeerd in 2021.

### Uitvoering

De coördinatie van het verbeteren van informatiebeveiliging is belegd bij het team Kwaliteitszorg. In dit team is de CISO gepositioneerd maar ook de FG en de concerncontroller. De CISO is aanspreekpunt voor alle zaken die te maken hebben met informatiebeveiliging. De CISO bereid besluitvorming voor en ziet op de uitvoering. De CISO moet onafhankelijk kunnen opereren waarbij de CISO niet de reguliere verantwoordingsroute in de lijn hoeft te volgen. De FG is een interne toezichthouder op de verwerking van persoonsgegevenstoezichthouder en heeft een adviserende rol. Een evaluatie over de uitvoering van het informatiebeveiligingsplan en ENSIA wordt jaarlijks aan het college aangeboden.

Binnen de organisatie is de teamcoach eindverantwoordelijk is over de processen en applicaties die in het team aanwezig zijn. Het eigenaarschap van een proces of een applicatie wordt zal in de praktijk door de teamcoach worden gedelegeerd aan een medewerker uit het team. De teams, onder leiding van de teamcoach, zijn verantwoordelijk voor de integrale beveiliging van de organisatieonderdelen.

De CISO doet voorstellen over de uitvoering van het informatiebeveiligingsbeleid op basis van landelijke en Europese wet- en regelgeving en normenkaders. Ook rapporteert zij of hij gevraagd en ongevraagd over compliance aan wet- en regelgeving. De CISO rapporteert aan de teamcoach van het team Kwaliteitszorg en waar nodig rechtstreeks aan de directie. Vanuit het principe van integraal management met resultaatverantwoordelijkheid bij zelforganiserende teams) houdt concerncontrol een integrale beoordeling van de voorwaarden waaraan producten en diensten moeten voldoen. De concerncontroller is de aangewezen persoon om toe te zien op de ontwikkeling van de kaders en de toepassing en naleving ervan. Dit geldt ook voor de ontwikkeling en naleving van het informatiebeveiligingsbeleid. De concerncontroller toetst in samenspraak met de CISO of de vastgestelde beveiligingsmaatregelen worden nageleefd. De concerncontroller staat buiten het primaire proces, is onafhankelijken kan het bestuur gevraagd en ongevraagd adviseren.

Ieder proces dient een proceseigenaar te hebben. De proceseigenaar bepaalt hoe een proces verloopt, en is verantwoordelijk dat het proces aan de klantverwachtingen en bedrijfsdoelstellingen voldoet. De proceseigenaar gaat dus over de inrichting van het proces, als ook over de resultaten.

Voor iedere vakapplicatie dient in de lijnorganisatie een applicatie-eigenaar te zijn. De applicatie- eigenaar heeft de bevoegdheid te bepalen hoe de applicatie is ingericht, en de verantwoordelijkheid dat de applicatie aan de klantverwachtingen en bedrijfsdoelstellingen blijft voldoen. Degene gaat dus over de inrichting en het ontwerp van applicatie, als ook over de resultaten van de werking van de applicatie. Het proces- en applicatie eigenaarschap kan waar logisch worden toegekend aan één persoon.

De Functioneel applicatiebeheerder zorgt ervoor dat de applicatie is ingericht volgens de daarvoor gestelde eisen en richtlijnen van de applicatie-eigenaar en is verantwoordelijk voor het in stand houden van de programmatuur waarmee de functionaliteit van een applicatie wordt gerealiseerd en van de gegevensverzamelingen waarop die programmatuur bewerkingen uitvoert.

In de Werkgroep informatiebeveiliging zitten de verschillende stakeholders informatieveiligheid van zowel de gebieden van het BIO normenkader, als de deelgebieden uit de andere gemeentelijke normenkaders. De werkgroep informatiebeveiliging bestaat uit: de CISO (voorzitter), de adviseur ICT, de medewerker Systeemveiligheid ICT en de beveiligingsbeheerders.

De rol van de proceseigenaar bij risicogestuurd werken is essentieel. De proceseigenaar kent het systeem en de kwetsbaarheden van een applicatie of (werk)proces. Aan de hand van bedreigingen is de proceseigenaar het beste in staat om te beoordelen wat de kans op een beveiligingsincident is en wat daarvan de impact is op het (werk)proces.

De CISO adviseert en begeleidt proceseigenaren bij het uitvoeren van risico-inventarisaties en -analyses. De CISO is niet (eind)0verantwoordelijk voor het uitvoeren of het resultaat van risicoanalyses. Deze verantwoordelijkheid ligt altijd in de lijn, dus bij de proceseigenaar.

Het thema staat (standaard) periodiek op diverse agenda’s: om de paar weken is er overleg met de bestuurlijk portefeuillehouder, ieder kwartaal bij de directie, geregeld in de teamoverleggen. De directie geeft aan goed zicht te hebben op nieuwe risico’s door regelmatige rapportages over datalekken en andersoortige knelpunten.

### Doelbereiking

In de beleidsdocumenten wordt de voortgang in het bereiken van de gestelde doelen bijgehouden. In het Informatiebeveiligingsplan 2019-2020 is de stand van zaken per thema benoemd: mens, proces en techniek. Het thema mens krijgt als oordeel ‘groen’ (voldoende), wat in het plan volgt is toegelicht: het proces om continu te werken aan bewustwording is op orde. Er zijn in 2018 en in 2019 i-bewustwordingssessies georganiseerd en aan alle ambtenaren (in vaste dienst) wordt een e-learning i-bewustzijn aangeboden. Daarnaast is er tijd en budget gereserveerd voor het uitvoeren van interventies (phishingtest, mysteryvisit) die een bijdrage leveren aan het bewustwordingsniveau. Het e-learningtraject is niet verplicht gesteld, het resultaat hangt af mede af van het aantal deelnemende ambtenaren.

De indicator bij het onderdeel proces staat rood, wat in het plan volgt is toegelicht: de te nemen maatregelen die hieronder vallen vragen veel acties uit de teams zelf. Denk bijvoorbeeld aan het uitvoeren van een dataclassificatie op de 17 kernapplicaties, het inrichten van een systeem om de inkoopcontracten centraal te regelen of het extra beveiligen van gebouwen (locatie Leek) en het opstellen van een business continuity management (BCM) plan. Door de herindeling zijn veel taken en verantwoordelijkheden niet altijd duidelijk en uitgekristalliseerd. Ook is het eigenaarschap niet op orde. Dit maakt dat ongeveer 70 procent van de maatregelen uit het informatiebeveiligingsplan 2018-2019 op het onderdeel proces niet zijn uitgevoerd. Deze komen in het nieuwe plan opnieuw in de planning (zie Werkprogramma spoor 2: Informatiebeveiliging 17 kernapplicaties).

Op het onderdeel techniek staat de indicator op oranje. Naar aanleiding van het

Rekenkamercommissieonderzoek sociaal domein, dat in 2018 is uitgevoerd, heeft het team

Automatisering veel verbeterd. De capaciteit is structureel uitgebreid (aanstelling Medewerker Systeemveiligheid) en essentiële processen om de beveiliging te verbeteren zijn ingericht (logging, monitoring, patching). Echter, niet alle aanbevelingen van het technisch rapport van de Rekenkamercommissie over de interne staat van het netwerk zijn opgelost. Ook moet er nog een verbeterslag gemaakt worden in het opstellen van beleid, protocollen en (werk)procedures. Veel van deze zaken zijn nu opgenomen als verplichte overheidsmaatregelen in de BIO. Het doorvoeren van de technische aanbevelingen van de Rekenkamercommissie komt daarom als één actiepunt terug in dit informatiebeveiligingsplan.

In het voorjaar van 2020 is er een update gegeven van de voortgang van de implementatie van de technische maatregelen uit het rekenkamerrapport (juni 2020). Daaruit blijkt dat nog steeds een aantal maatregelen niet zijn opgelost. Vanuit de technische invalshoek is een aantal, op zich losstaande, bijzonderheden naar voren gekomen:

* Verbetering van backupsystemen en -procedures (onder andere in verband met risico gijzelsoftware).
* Er dient een business-continuityplan te worden opgesteld (er is een stageopdracht uitgezet om dit op te stellen op basis van maatwerk voor Westerkwartier; vraag is of dit gezien de COVID-19-maatregelen binnen afzienbare tijd tot resultaat leidt).
* Compartimentering door firewalls binnen de gemeentelijke systemen is van onvoldoende niveau.
* Aansluiting SOC op KPN wordt volgens planning in 2021 gerealiseerd; gevolg is dat er momenteel niet 24/7 wordt gescand op risico’s.
* Changemanagementprocedures dienen te worden aangepast (bijvoorbeeld ten aanzien van het proces ‘uitdiensttreding personeel’).

In de rapportage Informatieveiligheid 2020 Q1 en Q2 wordt de voortgang aangeduid als gestaag vorderend. De COVID-19 situatie zorgt voor een vertraging in het uitvoeren van risicoanalyses. Uit de interviews kwam (unaniem) het belang van adequate werkprocessen aan de orde. Dit belang hangt samen met de kwaliteit van de processen en de in- en externe dienstverlening, en in samenhang hiermee de informatieveiligheid. Vanwege de fusie worden alle processen opnieuw beschreven; dit traject wordt centraal geprioriteerd door de directie waarbij informatieveiligheid slechts één van de criteria voor prioritering is (een ander criterium is de toekomstvastheid). Vanuit het oogpunt van informatieveiligheid zou het goed zijn als de processen snel en goed beschreven zijn. Vanuit de directie wordt bewust de keuze gemaakt om aan te sluiten bij het tempo van teams, domeinen of de relevante processen. Ieder team/domein heeft de ruimte gekregen om dit op de eigen manier en afhankelijk van de omstandigheden te beschrijven. De gemeentesecretaris gaf in het interview aan, dat het wel haar voornemen is, om hierop steviger te sturen, zodat de processen op een meer gelijke wijze in beeld worden gebracht.

## Aanpak privacy in de organisatie

### Beleid

Het beleid over de aanpak van Privacy is terug te vinden in het jaarplan privacy dat is opgesteld in april 2018. De focus van dit plan is het voldoen aan de eisen die de Algemene Verordening Gegevensbescherming (AVG) stelt. De te nemen maatregelen zijn ingedeeld in de thema’s: Mens, Informatie/Verantwoordingsplicht, Organisatie/Processen en Techniek. In het plan is een planning te vinden met maatregelen die op basis van het plan genomen worden. In het jaarplan privacy wordt niet verwezen naar het rekenkamerrapport uit 2018. Wel wordt duidelijk dat het plan is gebaseerd op de risicoanalyse die eerder vanuit de organisatie was uitgevoerd. In de bestuurlijke reactie verwijst het college ook naar een aantal van de maatregelen die op basis van het jaarplan privacy al is ingezet. Er is ook een duidelijk verband tussen de aanbevelingen uit het rekenkamerrapport en de maatregelen uit het jaarplan privacy. Van de aanbevelingen die in 2.1 zijn opgenomen zijn de volgende aanbevelingen onderdeel van dit beleidsdocument:

* 1, 2 (i-Bewustzijn);
* 6 (melden datalekken);
* 7 (PIA uitvoeren).

In het voorjaar van 2019 werd een eerste PIA (Privacy Impact Assessment) in het sociaal domein uitgevoerd, zoals was aanbevolen in het rekenkamerrapport uit 2018. De DPIA is uitgevoerd om vroegtijdig inzicht te krijgen in de belangrijkste privacyrisico’s zodat met de inrichting van de processen daarmee rekening gehouden kan worden. Dat leidt tot een overzicht aan maatregelen (maatregelen en acties DPIA 18 augustus 2019). Een aantal aanbevelingen overstijgt het sociaal domein. Zij hebben betrekking op technische of organisatorische maatregelen die onderdeel zijn van de implementatie van beveiligingsmaatregelen vanuit de BIG/BIO, de inrichting van het functioneel beheer en de inrichting van de privacyorganisatie. Het gaat daarbij om de volgende aanbevelingen: toezien op het volgen van e-learning informatieveiligheid en privacy, aanbieden van cursussen gebruik MS-office, verbeteren van patching/hardening, invoeren van wijzigingsbeheer op applicatieniveau, monitoren naleving Service Level Agreements, opstellen en beheren van register van verwerkingen, aanstellen van privacy officer / privacybeheerder, en fysieke beveiliging van de locatie Leek. Dit leidt tot twee overzichten:

* de maatregelen uit het jaarplan Privacy
  + Overzicht maart 2020
* de maatregelen naar aanleiding van de DPIA Sociaal Domein
  + Overzicht december 2019
  + Overzicht juni 2020

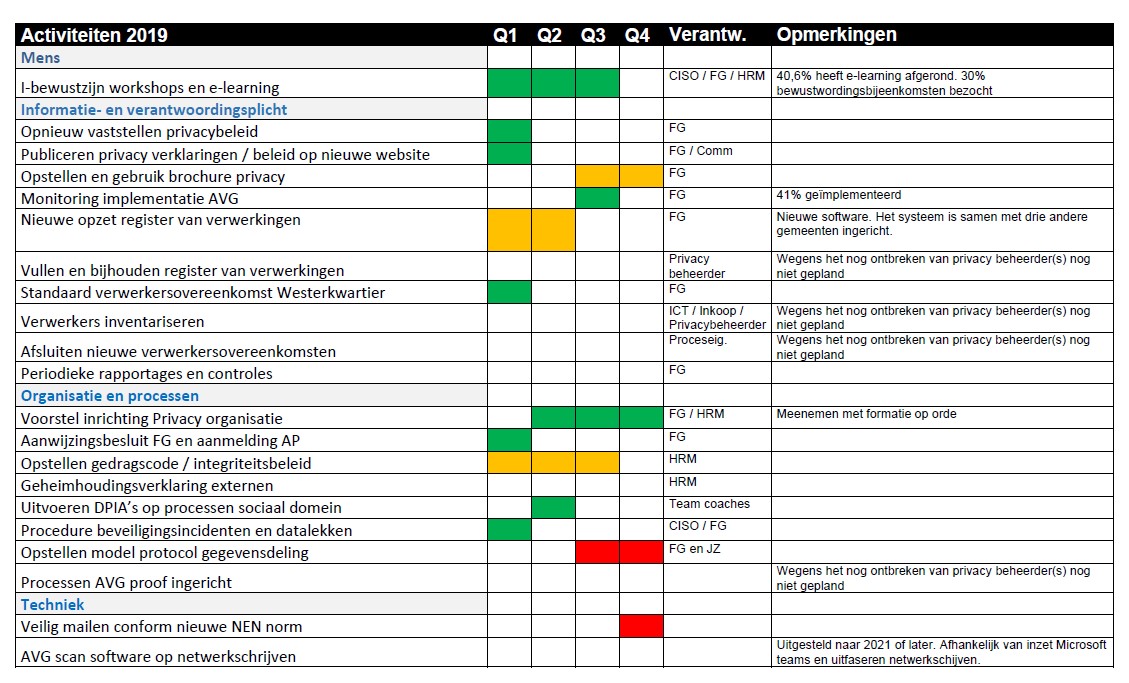
Daarnaast krijgt de raad in april 2020 de jaarrapportage gegevensbescherming 2019, met daarin een aantal aanbevelingen van de FG als functionaris voor de raad. In de rapportage Informatieveiligheid en Privacy over de eerste helft van 2020 is aandacht voor de voortgang van de maatregelen op het gebied van privacy.

### Uitvoering

De FG is gepositioneerd in het team Kwaliteitszorg. Vanuit een onafhankelijke positie houdt de FGintern toezicht op de manier waarop door de gemeente wordt omgegaan met persoonsgegevens. De FG is verantwoordelijk voor het structureel toetsen van de implementatie, de uitvoering van de wettelijke eisen en de gemeentelijke regels op het gebied van privacy, en is contactpersoon voor de Autoriteit Persoonsgegevens. De teams binnen de gemeente hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens.

De Privacybeheerder heeft een uitvoerende rol. Hij of zij voert Privacy Impact Assessments (PIA’s) uit, neemt het voortouw bij de uitvoering van maatregelen om processen en applicaties aan de AVG te laten voldoen, meldt verwerkingen van persoonsgegevens aan de FG ten behoeve van het register van verwerkingen en fungeert als eerste aanspreekpunt op gebied van privacy binnen het team. De Privacybeheerder speelt een belangrijke rol op de werkvloer en heeft intensief contact met de FG. Recent is besloten tot het aannemen van een privacybeheerder, die het register van verwerkingen gaat opstellen. Dit besluit is in juni 2020 genomen door de directie.

### Doelbereiking

De acties en maatregelen naar aanleiding van het jaarplan Privacy en de DPIA Sociaal Domein worden bijgehouden. Hieronder is het overzicht opgenomen zoals dat in maart 2020 aan de raad is verstuurd over de maatregelen bij het jaarplan privacy.

De PIA-actielijst zou in 2019 zijn afgerond maar dat is niet gerealiseerd. Inmiddels is er een nieuwe actielijst opgesteld. Er is nog geen planning voor de overige zaken want dat hangt af van het moment van de komst van de privacybeheerder. Hij of zij gaat eerst het register verwerkingen op orde brengen, dan de verwerkersovereenkomsten checken om daarna de PIA’s te doen op nieuwe verwerkingen of applicaties. Daarna is het voornemen om eens per drie jaar PIA’s uit te voeren voor verschillende processen. In de rapportage Informatieveiligheid 2020 Q1 en Q2 wordt aangegeven dat er vertraging is ontstaan door COVID-19. Er worden kleinere stappen gezet dan gepland. De vertraging is volgens dit bericht te wijten aan de nog niet aangestelde privacybeheerder.

In de interviews is gevraagd naar de mate van doelbereiking van de maatregelen. Daaruit komt naar voren dat er voor het voldoen aan alle maatregelen een aantal obstakels is. Zo voldoe je sneller aan de maatregelen privacy als de BIO is geïmplementeerd, wat nog niet het geval is. Dat heeft daarmee ook impact op het bereiken van doelen rond privacy. Daarnaast is nog geen privacybeheerder aangesteld, waardoor de basis ‘het beschrijven en bijhouden van de registers’ nog niet op orde is. Dat nog niet alle maatregelen volgens planning worden behaald is geen reden om ontevreden te zijn. De FG heeft in beeld waar de mogelijke risico’s zitten. Omdat privacy sterk gerelateerd is aan menselijk gedrag, is het zinvol om rekening te houden met het tempo van de diverse teams: de mate van bewustzijn en de grip op de te beschrijven processen. Door de regelmatige metingen is er goed zicht op de ontwikkeling van het bewustzijn rond privacy.

## i-Bewustzijn

### Beleid

Zowel in de beleidsdocumenten en jaarplannen voor Informatieveiligheid als Privacy wordt verwezen naar i-Bewustzijn als belangrijkste aanpak voor de mensfactor in het beleid. De aanpak van i-Bewustzijn is opgestart naar aanleiding van een risico-inventarisatie die in 2017 is uitgevoerd. De gemeente is al enige tijd aan de slag met informatieveiligheid en het

(informatie)Bewust handelen van de medewerkers binnen de organisatie. Hiervoor heeft de gemeente het concept van de leercirkel ingezet waarbij gewerkt wordt aan permanente verbetering van het i-Bewustzijn in de organisatie. Dit is gedaan met behulp van een subsidie.

### Uitvoering

In maart-april 2019 is een 0-meting uitgevoerd, op basis waarvan een i-Bewustzijnsplan is opgesteld (mei 2019). In dit plan komt naar voren dat mensen informatieveiligheid een belangrijk thema vinden, maar dat het gedrag hier niet mee correspondeert.

Nadat een e-learning is ingezet en workshops zijn georganiseerd is het traject geëvalueerd en is een vervolgadvies gegeven (september 2019). Het blijkt dat maar een klein deel van de mensen heeft deelgenomen aan de e-learnings en workshops. Het advies is om de cyclus te herhalen, het onderdeel te maken van het introductieprogramma en met het MT het gesprek aan te gaan over het verplichten van het behalen van de certificering.

In het voorjaar van 2020 is daarover een advies gegeven aan de directie met het verzoek te besluiten het aanbod aan e-learnings uit te breiden en deelname verplicht te maken voor toegang tot het netwerk.

### Doelbereiking

Het onderdeel i-Bewustzijn is een maatregel in zowel de plannen rond Informatieveiligheid als Privacy. In de voortgang van de maatregelen kleurt dit onderdeel steevast groen. De evaluatie van het ingezette instrument laat echter zien dat de instrumenten wel zijn ingezet, maar dat daarvan nog niet voldoende gebruik wordt gemaakt. De indicator staat op groen, omdat de acties om het bewustzijn te verhogen maximaal worden ingezet. De maatstaf is niet of iedere medewerker informatiebewust is, 100% bewustzijn is onmogelijk. Het is een continu proces en daarom heeft de organisatie er blijvend aandacht voor. Zolang de inzet daarop wordt gedaan, is de indicator groen.

Uit de interviews blijkt dat het bewustzijn bij de bestuurlijk portefeuillehouder, directieteam en teamleiders groot wordt geacht. Er is geen helder beeld over de mate van bewustzijn bij de medewerkers; wel wordt aangegeven dat de indruk bestaat dat het bewustzijn groeit. Dit zou onder andere blijken uit de toename van het aantal interne meldingen. Inmiddels zijn de trainingen verplicht en komt er naast bewustzijnstrainingen ook een verplicht certificaat dat iedere medewerker moet behalen om toegang te krijgen tot de gemeentelijke systemen (dit is nog wel onderwerp van overleg met de Ondernemingsraad). De bewustzijnsmaatregelen gelden niet alleen voor het sociaal domein, maar organisatiebreed. Omdat het in het sociaal domein privacy een grotere rol speelt is het bewustzijn in dat team wel verder ontwikkeld. Voor het overige heeft ieder team, domein of proces een eigen tempo dat past bij de specifieke situatie van dat team, domein of proces.

## Bevindingen

Het geheel aan maatregelen dat op basis van het rapport van de Rekenkamercommissie is voorgesteld, komt terug in verschillende plannen en documenten. Centraal daarin staan het Informatiebeveiligings- en Privacybeleid. Het beleid rond i-Bewustzijn draagt aan beide beleidsdocumenten bij. Het beleid rond Privacy is het eerst opgesteld, daarin is niet expliciet verwezen naar de aanbevelingen uit het rapport van de Rekenkamercommissie. Het beleid Informatieveiligheid is daarentegen opgesteld mede op basis van de aanbevelingen uit het rapport en met name de specifieke aanbevelingen worden integraal gemonitord. Er zijn meerdere lijsten met maatregelen die gemonitord worden:

* De maatregelen uit het jaarplan Privacy
* De maatregelen naar aanleidingen van de DPIA sociaal domein
* De maatregelen uit het jaarplan informatieveiligheid
  + Aangevuld met de technische maatregelen uit het rapport van de Rekenkamercommissie
  + Aangevuld met de maatregelen BIO
  + Aangevuld met maatregelen ENSIA

De maatregelen lijken wellicht onoverzichtelijk, maar zijn aanvullend en soms ook voorwaardelijk aan elkaar. De raad wordt geïnformeerd over de voortgang van de maatregelen.

|  |  |  |
| --- | --- | --- |
| Indicator | Bevinding | Oordeel |
| De conclusies zijn overgenomen in beleidsvoornemens en ambities tav informatieveiligheid | In het Informatieveiligheidbeleid worden de conclusies gebruikt als basis voor de maatregelen. De technische conclusies vormen een apart document waarvan de voortgang wordt bijgehouden. | Voldaan |
| De aanbevelingen zijn opgenomen in nieuw/aangepast beleid | De beleidsdocumenten  Informatieveiligheid en Privacy samen dekken alle aanbevelingen af. | Voldaan |
| Er zijn concrete doelen gesteld, met bijbehorende indicatoren voor het meten van de mate van doelbereiking | Er zijn concrete maatregelen geformuleerd, waarvan de voortgang wordt bijgehouden. Dit heeft meer het karakter van een planning. | Voldaan |

De maatregelen worden uitgevoerd. Het rapport van de Rekenkamercommissie heeft geleid tot meer aandacht voor het onderwerp bij directie, portefeuillehouder en medewerkers met een specifieke taak (medewerker systeemveiligheid en recent het besluit tot de aanstelling van een privacybeheerder). De technische maatregelen zijn mede gekoppeld aan de maatregelen rond BIO en ENSIA en het SOC van KPN. Daarnaast dient een keuze gemaakt te worden voor een ISMS/PMS. De gemeente Westerkwartier heeft de verschillende vormen van control binnen het team kwaliteitszorg: interne control, informatieveiligheid en privacy. Het overzicht is er, echter nog niet alle posities in het model van de 3 lines of defence zijn ingevuld.

Op de verschillende niveaus is regelmatig overleg over het onderwerp. Het beeld dat uit de interviews naar voren komt is dat CISO en FG goed op elkaar zijn ingespeeld. Ze weten zich goed gezien en gehoord door management, directie en portefeuillehouder. Alle partijen zijn het eens dat op dit moment het beschrijven van de processen in de teams een knelpunt is in de uitvoering. Daar valt nog winst te behalen.

|  |  |  |
| --- | --- | --- |
| Indicator | Bevinding | Oordeel |
| De aanbevelingen hebben geleid tot het nemen van besluiten over het aanpassen/aanschaffen van formatie en ICT-producten | Ja, zowel voor informatieveiligheid als voor privacy is een uitbreiding formatie gerealiseerd om aan de maatregelen te kunnen werken. | Voldaan |
| De aanbevelingen hebben geleid tot het inrichten van nieuwe werkprocessen | Dat is wel de bedoeling, maar blijkt ook het cruciale zwakke punt | Deels voldaan |
| Het thema van het rapport heeft regelmatige aandacht van college, directie en management | Er is regelmatig overleg over dit onderwerp op alle niveaus. | Voldaan |

Naast de maatregelen in beleid en de uitvoering in de praktijk, is ook gekeken naar de mate van doelbereiking van de aanbevelingen. De technische aanbevelingen zijn al tijdens de afronding van de rapportage van de Rekenkamercommissie opgepakt. Daarnaast blijkt uit de interviews dat het rapport en de urgente toon voor een versnelling in de aanpak hebben gezorgd. Hoewel de maatregelen allemaal concreet zijn benoemd, blijkt uit de staatjes waarin de voortgang wordt bijgehouden, dat een aantal maatregelen niet volgens planning is uitgevoerd. De bottleneck daarin is het beschrijven van de verschillende werkprocessen. Daarnaast zijn de nog aan te passen technische maatregelen (zoals aansluiting op het SOC), de beperkte capaciteit die binnenkort wordt uitgebreid en COVID-19 verklaringen voor de vertragingen in de uitvoering.

|  |  |  |
| --- | --- | --- |
| Indicator | Bevinding | Oordeel |
| Er zijn al tijdens het onderzoek aanpassingen gedaan in beleid en uitvoering | De technische maatregelen met het  risico levels critical en high zijn direct opgepakt en in uitvoering gebracht. | Voldaan |
| Het rapport heeft geleid tot een versnelling van het beleidsproces of de uitvoering | In de interviews wordt aangegeven dat het dit effect heeft gehad | Voldaan |
| Door het implementeren van de aanbevelingen hebben feitelijke veranderingen plaatsgevonden | Het instellen van functies, aannemen van mensen, aanpassen van systemen | Voldaan |
| De mate van doelbereiking wordt gemonitord | De door de organisatie gestelde doelen worden gemonitord, daarin zijn ook de maatregelen zoals voorgesteld door de Rekenkamercommissie opgenomen. | Voldaan |
| De gestelde doelen worden volgens planning gehaald | Er is vertraging in het nemen van de maatregelen, onder andere door het nog niet volledig implementeren van de technische maatregelen, beperkte capaciteit en het aansluiten op de draagkracht van de teams. | Niet voldaan |

# Analyse doorwerking

De centrale vraag luidt in welke mate er sprake is van doorwerking van aanbevelingen van de Rekenkamercommissie. Daarbij is op voorhand geconstateerd dat er twee bijzondere aspecten een rol spelen. Om te beginnen is sprake is van een gefuseerde organisatie en daarnaast rijst de vraag in hoeverre de adviezen een breder terrein beslaan dan alleen het sociaal domein.

De analyse bespreekt eerst in welke mate er sprake is van doorwerking op het niveau van politiek-bestuurlijke aandacht. Vervolgens bespreekt de analyse in welke mate de aanbevelingen zijn opgenomen in beleid en uitvoering en hoe het staat met de doelbereiking. Uit de analyse komt een aantal knelpunten naar voren, die aan het einde van dit hoofdstuk worden besproken.

## Aandacht in raad en organisatie

Nadat de rapportage van de Rekenkamercommissie (2018) aan de raadscommissie is aangeboden heeft de raadscommissie aangegeven geschrokken te zijn van de uitkomsten en dit te zien als 0-meting die herhaald moet worden. Het college werd verzocht alle aanbevelingen over te nemen. De raadscommissie neemt zich voor om dit actief te blijven volgen. In de raadsvergadering zelf wordt er nadien niet meer over gesproken en zijn er door raadsleden geen vragen meer gesteld over dit onderwerp. Vervolgens is de gemeenteraad over het onderwerp geïnformeerd via (nieuwe) beleidsdocumenten over informatieveiligheid, bestuursrapportages en jaarstukken. Ook naar aanleiding hiervan zijn geen vragen gesteld over informatieveiligheid. In het integraal veiligheidsbeleid wordt rond dit thema aan de gemeenteraad gevraagd bij het veld integriteit en veiligheid aandacht te geven aan informatieveiligheid of ondermijning, de raad kiest dan voor ondermijning.

De rapportage van de Rekenkamercommissie (2018) heeft geleid tot urgentie bij het bestuur en de organisatie. De aandacht voor dit thema is nu organisatiebreed en beperkt zich niet tot het sociaal domein, waar het onderzoek over ging. Eerst ontstond er binnen de organisatie een negatief sentiment. Op verzoek van het onderzoeksbureau werd de firewall voorafgaande aan de testen uitgezet. Daarmee werd een te negatief beeld opgeroepen hetgeen de betreffende ICT-medewerkers zich eerst sterk aantrokken. Uiteindelijk draaide dit bij omdat de rapportage van de Rekenkamercommissie leidde tot interne aandacht en middelen ten behoeve van de informatiebeveiliging, onder andere door het aantrekken van een nieuwe medewerker systeemveiligheid. In de planvorming en verantwoording zijn de aanbevelingen vanuit de Rekenkamercommissie (2018) meegenomen. De urgente technische risico’s zijn direct na het verschijnen van de rapportage opgepakt.

De versterking van de informatieveiligheid en de opbouw van de nieuwe fusieorganisatie maakte dat hard geprioriteerd moest worden binnen de ambtelijke capaciteit. Maar informatiebeveiliging kon ook direct mee worden genomen in de opbouw van de nieuwe organisatie, onder andere bij het (her)inrichten van werkprocessen. Zowel binnen het directieteam als bij de bestuurlijk portefeuillehouder is er serieuze aandacht voor informatieveiligheid. Het thema staat standaard periodiek op diverse agenda’s: om de paar weken is er overleg met de bestuurlijk portefeuillehouder, ieder kwartaal bij de directie, geregeld in de teamoverleggen en in het najaar van 2020is er een informatieavond voor de gemeenteraad. De directie geeft aan goed zicht te hebben op nieuwe risico’s door regelmatige rapportages over datalekken en andersoortige knelpunten.

## Doorwerking in beleid

Het huidige beleid is gebaseerd op het Informatiebeveiligingsbeleid 2019-2021. In dit beleid worden uitgangspunten, doelen en kaders aangegeven. Ook de verantwoordelijkheden, taken en bevoegdheden zijn beschreven. Uit de interviews is gebleken dat het beleidskader niet ter discussie staat en een werkbaar kader vormt voor informatieveiligheid van de gemeente. Dit geheel biedt naar de mening van de geïnterviewden voldoende interne checks and balances. Zo functioneert het team kwaliteitszorg onafhankelijk van de overige teams met een directe lijn naar de directie. In het beleid wordt aangegeven dat het doel is om voor alle processen in de organisatie minimaal volwassenheidsniveau 3 te bereiken. De knelpunten van de werkprocessen, ook in relatie tot de onvoldoende mate van onderlinge afstemming van applicaties en processen, staan doorgroei naar dit niveau in de weg. Een hoger BIO-niveau zou een betere prestatie ten aanzien van privacy-aspecten betekenen.

Het privacybeleid is gebaseerd op het jaarplan privacy. In eerdere versies is gesproken over jaarplannen en een specifiek communicatieplan voor privacy, maar in de interviews blijkt dat dat onnodig wordt gevonden. De maatregelen worden regelmatig bijgehouden, maar het is niet de bedoeling om onnodig plannen te schrijven. De FG communiceert ten tijde van de informatiemomenten over informatieveiligheid. De maatregelen en randvoorwaarden zijn dermate verweven, dat dat een verstandige keuze lijkt.

Een bestudering van de aanbevelingen uit het rapport van de Rekenkamercommissie en de maatregelen in de beleidsdocumenten laat zien dat alle aanbevelingen worden afgedekt door de maatregelen. Het niveau waarop de maatregelen zijn geformuleerd verschilt. Het werken met de verschillende lijsten aanbevelingen, maakt het niet eenvoudig de aanbevelingen kritisch te volgen.

## Doorwerking in de uitvoering

In de interviews geven CISO en FG aan dat het rapport van de Rekenkamercommissie gezorgd heeft voor meer aandacht, meer personeel en een versnelling in de uitvoering van de opgestarte processen. Uit de interviews kwam unaniem het belang van adequate werkprocessen aan de orde. Dit belang hangt samen met de kwaliteit van de processen en dus die van de in- en externe dienstverlening en productie, en in samenhang hiermee de informatieveiligheid. Vanwege het fusieproces worden alle processen opnieuw beschreven. Dit traject wordt centraal geprioriteerd door de directie waarbij informatieveiligheid slechts één van de criteria voor prioritering is. De teamleiders zijn individueel verantwoordelijk voor de beschrijving en het onderhoud van één of meer processen en moeten er zorg voor dragen dat een proces voldoet aan de eisen rond informatieveiligheid, privacy en interne controle. Uit de interviews bleek dat, ondanks de heldere beschrijving van taken en bevoegdheden in het beleid, dit in de praktijk niet voor iedereen even helder is. Dit betreft bijvoorbeeld de aansturingslijnen en rollen.

Vanuit de optiek van informatieveiligheid is het gegeven, dat tot nu toe niet volledig wordt geprioriteerd op basis van informatieveiligheid en privacy, te zien als een zwakke schakel. Daar komt bij dat de 17 teamleiders (34 teams) zelf bepalen op welke wijze het proces beschreven wordt. Alle methodieken zijn toegestaan waarbij wel de algemene centrale interne randvoorwaarden gelden zoals op het terrein van financiën en control. De medewerker die belast is met het (meer) op één lijn krijgen van de beschrijvingsmethodiek is langdurig uitgevallen en niet vervangen. Overigens geeft de directie aan zelf bij te sturen waar nodig (langs de lijnen van teams, domeinen en processen) en inmiddels op zoek te zijn naar een oplossing. Daarenboven geeft zij aan dat informatieveiligheid in 2021 een organisatiebrede prioriteit wordt en gezien wordt als basis voor het inrichten van processen en functioneel beheer.

Vanuit de bestudeerde documenten en gehouden interviews valt het taalverschil tussen informatieveiligheid en privacy op. Dit wordt onder meer verklaard door verschillen tussen de BIO en AVG inclusief de verschillende wijzen van monitoring en beoordeling. De toekomstige keuze voor een definitief ISMS/PMS draagt bij aan een oplossing. De samenwerking tussen de sleutelpersonen is goed (de CISO en FG werken samen binnen team Kwaliteitszorg). Ook is er een goede samenwerking met team Juridische Zaken. De aanbevelingen hebben voor een groot deel hun beslag gekregen in de uitvoering, ook al zijn vertragingen ontstaan in de voortgang. Het is duidelijk waar deze vertraging is en er wordt bewust geprioriteerd in aansluiting op de ontwikkelingen binnen de teams, domeinen en processen. Er is daarnaast een helder risicobewustzijn, waardoor betrokkenen tevreden zijn over de voortgang.

## Knelpunten in de doelbereiking

In het verkennen van de mate waarin de aanbevelingen zijn uitgevoerd, is een aantal knelpunten in beeld gekomen. Deze worden hieronder besproken.

### Gegevensbescherming en privacy

Privacy is breder dan informatiebeveiliging en heeft, naast een systeemkant, nadrukkelijk een relatie met de menskant. De AVG is daarbij geen doel op zich. Maar dienstverlening vindt plaats binnen de kaders van de AVG. Inmiddels is het de bedoeling dat er een privacybeheerder wordt aangesteld waardoor de functionaris gegevensbescherming meer de rol van ‘onafhankelijk toezichthouder’ op zich kan nemen en veel uitvoeringszaken aan de beheerder kan overlaten, zoals het bijhouden van het register verwerkingen en de uitvoering van PIA’s. Vanuit een breder afwegingskader kan dit voornemen nog veranderen, echter de directie geeft aan in dat geval te zoeken naar een oplossing.

Het belang van de aanstelling van een privacybeheerder voor de privacyorganisatie is groot: omdat dit essentieel is voor de eerste ‘line of defence’ (tweede lijn is de interne toezichthouder (FG) en derde de Autoriteit Persoonsgegevens). Deze eerste lijn is het meest kwetsbaar want dat raakt het werk van de proceseigenaren en de kwaliteit van de processen. Teamleiders zijn verantwoordelijk maar in de praktijk zijn zij niet degenen die zicht hebben op hoe applicaties en systemen worden gebruikt en aansluiten op het proces. Idealiter zijn de processen in beeld en is voor ieder proces iemand aanspreekbaar op de aansluiting van de applicaties en systemen.

De PIA-actielijst zou in 2019 zijn afgerond maar dat is niet gerealiseerd. Inmiddels is er een nieuwe actielijst opgesteld. Er is nog geen planning voor de overige zaken want dat hangt af van het moment van de komst van de privacybeheerder. Die gaat eerst het register verwerkingen op orde brengen, dan de verwerkersovereenkomsten checken om daarna de PIA’s te doen op nieuwe verwerkingen of applicaties. Als die basis staat, dan is het voornemen om eens per drie jaar PIA’s uit te voeren.

### i-Bewustzijn

Uit de interviews blijkt dat het bewustzijn bij de bestuurlijk portefeuillehouder, directieteam en teamleiders groot is. Er is geen helder beeld over de mate van bewustzijn bij de medewerkers op directieniveau, dat inzicht is er wel bij de teamleiders en het team kwaliteitszorg. Wel wordt aangegeven dat de indruk is dat het bewustzijn groeit, dit blijkt bijvoorbeeld uit de toename van het aantal interne meldingen. Hoewel de bestuurlijke reactie op het rapport van de Rekenkamercommissie sprak over het verplicht stellen van de cursussen, zijn deze in 2019 in de eerste instantie niet verplicht gesteld. Pas recent, na de evaluatie van de eerste leercyclus en naar aanleiding van de rapportage over het eerste half jaar van 2020 is besloten om naast bewustzijnstrainingen ook een certificaat verplicht te stellen, dat iedere medewerker moet behalen om toegang te krijgen tot de gemeentelijke systemen (dit is nog wel onderwerp van overleg met de Ondernemingsraad).

De bewustzijnsmaatregelen gelden niet alleen voor het sociaal domein, maar organisatiebreed. Omdat het in het sociaal domein privacy een grotere rol speelt is het bewustzijn daar wel verder ontwikkeld. Voor het overige heeft ieder team een eigen tempo dat past bij de specifieke situatie van dat team.

### Techniek

De technische risico’s level Critical en high zijn direct na het verschijnen van de rapportage van de Rekenkamercommissie (2018) aangepakt. Uit de interviews komt naar voren dat de technische beveiliging inmiddels op orde is, maar dat vooral bij ‘mens’ en ‘proces’ de nodige actiepunten open staan. Vanuit de technische invalshoek is een aantal, op zich losstaande, bijzonderheden naar voren gekomen:

* Verbetering van backupsystemen en -procedures (o.a. in verband met risico gijzelsoftware).
* Er dient een business-continuityplan te worden opgesteld (er is een stageopdracht uitgezet om dit te laten opstellen op basis van maatwerk voor Westerkwartier. De vraag is of dit gezien de COVID-19-maatregelen binnen afzienbare tijd tot resultaat leidt).
* Compartimentering middels firewalls binnen de gemeentelijke systemen is van onvoldoende niveau.
* Aansluiting SOC op KPN wordt volgens planning (pas) in 2021 gerealiseerd. Het gevolg is dat er momenteel niet 24/7 wordt gescand op risico’s.
* Changemanagementprocedures dienen te worden aangepast (bijvoorbeeld ten aanzien van het proces ‘uitdiensttreding personeel’). De bestuurlijke reactie geeft aan dat er changemanagement procedures worden opgesteld.

In het informatiebeveiligingsplan zijn de door de Rekenkamercommissie benoemde technische acties opgenomen als één actiepunt, maar ze worden op een aparte lijst bijgehouden. De voortgang daarin is medebepalend of het mogelijk zal zijn om voor BIO een hoger niveau te kunnen halen.

### COVID-19 / afstandswerken

De situatie en maatregelen die samenhangen met COVID-19 hebben effect op aspecten van informatiebeveiliging. Enerzijds geldt dit voor de planning, voorbeelden zijn het risicogestuurd werken volgens de BIO en de uitvoering van mystery-visits. Anderzijds voor de nieuwe bedrijfsvoeringssituatie waarbij grootschalig op afstand wordt gewerkt terwijl het actiepunt ‘opstellen telewerkbeleid (HRM) inclusief aandacht voor de risico’s met betrekking tot thuiswerken’ volgens planning pas gereed zijn nadat de COVID-maatregelen van kracht waren (zie openstaande maatregelen informatiebeveiligingsplan 2018-2019).

## Mate van doorwerking

Het beeld is dat het onderzoek naar informatiebeveiliging in het sociaal domein een hoge mate van doorwerking heeft gehad: niet alleen in de volle breedte van de organisatie van de gemeente Westerkwartier, maar ook in termen van effect en impact op beleid en organisatie. Dat wil echter niet zeggen dat het proces daarmee klaar is. Er zijn duidelijke obstakels in de verdere implementatie van de aanbevelingen, die samenhangen met de ontwikkeling van teams, domeinen en processen, waarin na de gemeentelijke fusie alle werkprocessen opnieuw ingericht moeten worden. De betrokkenen zijn zich bewust van de obstakels en de mogelijke risico’s die de organisatie hierdoor loopt.

# Conclusies en aanbevelingen

Toen de Rekenkamer Westerkwartier startte met een verkenning van het onderwerp informatieveiligheid, speelde de vraag of er een doorwerkingsonderzoek gedaan zou moeten worden, of wellicht een nieuw onderzoek, uitgebreid naar de hele organisatie. Na de eerste interviews en het bestuderen van de beleidsdocumenten is besloten om te kiezen voor een doorwerkingsonderzoek.

De conclusie is dat sprake is van doorwerking, zowel in beleid als uitvoering. Maar de klus is nog niet klaar. Er zijn maatregelen nog niet uitgevoerd en obstakels te overwinnen. Het is dus zaak om kritisch te blijven op de voortgang van de uitvoering en op termijn een 1 en 2 meting te doen om daadwerkelijk effect te kunnen aantonen.

In de volgende paragrafen worden de conclusies van het onderzoek getrokken en een aantal aanbevelingen gedaan.

## Conclusies

Hoewel het rapport destijds goed is ontvangen, heeft het thema informatieveiligheid weinig actieve aandacht van de gemeenteraad. De rapportage van de Rekenkamercommissie (2018) was dusdanig urgent van aard dat een de gemeenteraad een proactieve rol had kunnen kiezen. Wel is recent door één van de partijen een raadsoverleg over dit thema aangevraagd. Dat vindt na het zomerreces plaats. Overigens geldt als kanttekening dat de ontwikkelingen op dit terrein meestal niet snel gaan. De gemeenteraad moet één keer per jaar actief worden geïnformeerd, uiteraard met uitzondering van eventuele incidenten. **Een eerste conclusie is: er is politiek-bestuurlijke aandacht voor de aanbevelingen geweest, maar de raad heeft geen proactieve rol gekozen naar aanleiding van de eerder geconstateerde urgentie van het implementeren van de aanbevelingen.**

De organisatie, inclusief de bestuurlijk portefeuillehouder, heeft de rapportage van de Rekenkamercommissie (2018) serieus genomen. De capaciteit is aangepast (maar is nog niet volledig op niveau), urgente risico’s zijn opgepakt en de bevindingen zijn verwerkt in planvorming. De directie geeft aan goed zicht te hebben op nieuwe risico’s door regelmatige rapportages over datalekken en andersoortige incidenten/knelpunten. Over de voortgang in de plannen wordt regelmatig gerapporteerd. **Een tweede conclusie is: de aanbevelingen hebben hun weg gevonden in het beleid en in de uitvoering van het beleid.**

Het huidige beleid is gebaseerd op het Informatiebeveiligingsbeleid 2019-2021 (september

2019) dat uitgangspunten, doelen, verantwoordelijkheden, taken en bevoegdheden (inclusief checks and balances) adequaat beschrijft. Dit beleid vormt een werkbaar kader voor informatieveiligheid van de gemeente. In het beleid wordt aangegeven dat het doel is om voor alle processen in de organisatie minimaal volwassenheidsniveau 3 te bereiken. Knelpunten ten aanzien van de werkprocessen staan doorgroei naar dit niveau in de weg. Het belang van adequate werkprocessen is dan ook cruciaal, niet alleen voor de kwaliteit van de in- en externe dienstverlening, maar ook voor informatieveiligheid. Er zijn intern, vanuit de optiek van informatiebeveiliging, zorgen over de tijd- en tempofactoren, de aansturing en uitvoering alsmede de kwaliteit van de procesbeschrijvingen zelf (dit laatste hangt in alk geval samen met het ontbreken van een centrale methodiek en format). Er bestaat zorg over de aansluiting van de onderscheiden werkprocessen. Het is van belang te komen tot adequate procesontwikkeling en -beheer en deze opnieuw te bezien en waar mogelijk te verbeteren. Een dergelijke verbetering leidt tot betere kwaliteit van alle geledingen van de organisatie en de samenhang daartussen. Daarnaast wordt geadviseerd om intern de gegroeide praktijk van rollen, taken en verantwoordelijkheden ten aanzien van de processen tegen het licht te houden. De directie geeft aan dat informatieveiligheid in 2021 een organisatiebrede prioriteit wordt. Het thema wordt basis voor het inrichten van processen en functioneel beheer. Dit zal beslag moeten krijgen in de planvorming voor 2021. **Een derde conclusie is: voor de implementatie van de aanbevelingen staat een aantal obstakels in de weg. Deze obstakels hangen samen met de taakverdeling en het format voor het beschrijven van werkprocessen, de beperkte capaciteit voor de uitvoering van de maatregelen, het niet verplichtende karakter van een aantal maatregelen en het gekozen ambitieniveau in zowel de techniek als de organisatieontwikkeling.**

* Het belang van de aanstelling van een privacybeheerder voor de privacyorganisatie is groot, omdat dit essentieel is voor de eerste ‘line of defence’. Deze lijn is het meest kwetsbaar want dat raakt het werk van de proceseigenaren en de kwaliteit van de processen. Zodra er zicht is op de aanstelling van een privacybeheerder kan er een planning van werkzaamheden worden gemaakt (register verwerkingen op orde brengen, dan de verwerkersovereenkomsten checken om daarna de PIA’s te doen op nieuwe verwerkingen of applicaties).
* Op het vlak van ‘bewustzijn’ wordt in de plannings- en verantwoordingsdocumentatie (inmiddels) ‘groen’ gescoord. Achterliggende reden is dat er trainingen plaatsvinden; dit zegt echter weinig over het effect. Positief is dat de bewustzijnstrainingen voor medewerkers alsnog verplicht zijn gesteld en dat er een systeem van verplichte certificering komt voor toegang tot het gemeentelijk netwerk. Geadviseerd wordt om individuele medewerkers periodiek te trainen en te certificeren.
* Vanuit de technische invalshoek is een aantal aandachtspunten naar voren gekomen op de volgende terreinen: backupsystemen en -procedures, businesscontinuityplan, compartimentering binnen de gemeentelijke systemen, aansluiting SOC op KPN en changemanagementprocedures. Deze onderdelen zijn cruciaal om verder te komen in het volwassenheidsniveau van informatieveiligheid. Dit terwijl de planning van deze actiepunten voorlopig nog niet gehaald is.
* De balans tussen de versterking van de informatieveiligheid en de opbouw van de nieuwe fusieorganisatie is niet altijd even eenvoudig, ook al omdat veel focus op en versnelling van informatiebeveiliging onvoldoende kan landen bij management en medewerkers waardoor er een papieren werkelijkheid ontstaat, terwijl de menskant, bewustwording en gedrag, van wezenlijk belang is. Het directieteam heeft hierin een belangrijke rol, hetgeen in de interviews wordt bevestigd. Het aanpassen van de ambities op de ontwikkeling in de teams lijkt verstandig, maar levert ook risico’s op.

**Een laatste conclusie is dat de planning ambitieus is en steeds moet worden bijgesteld. De planning lijkt daarmee niet altijd realistisch en dat maakt proactief plannen en sturen moeilijker.** Dit verdient extra aandacht nu de situatie en maatregelen die samenhangen met COVID-19 ertoe leiden dat de (jaar)planning op deze punten moet worden herzien. Zeker voor wat betreft het (grootschalig) afstandswerken dient het beleid (bij voorrang) te worden opgesteld en geïmplementeerd.

## Aanbevelingen

1. Informatieveiligheid lijkt technisch en niet direct relevant, maar een adequaat niveau van informatieveiligheid is een essentiële verantwoordelijkheid van overheidsorganisaties. Nu de voortgang hierin samenhangt met de teamontwikkeling en randvoorwaardelijk is voor het voldoen aan privacy beleid, verdient het de aandacht van de raad. Raad, wees daarom alert op mogelijke vertragingen en informeer actief naar de voortgang van de implementatie en de mogelijke knelpunten daarin.
2. Verzoek het college om de gemeenteraad één keer per jaar actief specifiek te informeren over de stand van zaken ten aanzien van informatieveiligheid (naast de reguliere P&C-cyclus en met uitzondering van incidenten).
3. Verzoek het college om uit te spreken dat informatieveiligheid een organisatiebrede prioriteit is in de planvorming voor 2021 en verder (het directieteam is dit voornemens te doen).
4. Het belang van adequate werkprocessen is cruciaal, niet alleen voor de informatieveiligheid, maar ook voor de kwaliteit van de in- en externe dienstverlening. De rekenkamer beveel de raad aan het college te verzoeken bij de inrichting van werkprocessen aandacht te hebben voor de volgende aspecten:
   1. Overweeg om te komen tot een adequate gemeentebrede systematiek voor de ontwikkeling, beschrijving, beheer en verbetering van processen.
   2. Beschouw informatieveiligheid inclusief privacy als belangrijke aspecten bij de organisatiebrede prioritering van de ontwikkeling van processen.
   3. Houd de gegroeide praktijk van rollen, taken, verantwoordelijkheden e.d. ten aanzien van de processen (zie het beleidsplan) nog eens tegen het licht.
   4. Zorg voor een voldoende stevige ambtelijke bezetting opdat de verbeterpunten voortgang houden.
5. Verzoek het college om gedetailleerd in beeld te brengen wat nodig is om toe te groeien naar BIO-niveau 3 en zet dit om in een concrete planning (en neem dit mee in de planvorming voor 2021 of controleer of dat inmiddels al is gedaan).
6. Verzoek het college om zorg te dragen voor formatieruimte zodat een privacybeheerder op niet al te lange termijn kan worden aangesteld of controleer of dat inmiddels al is gedaan.
7. Verzoek het college om te voorzien in een periodieke training/certificering van individuele medewerkers en maak deze training verplicht voor toegang tot het systeem (zoals de directie voornemens is) of controleer of dat inmiddels al is gedaan.
8. Vanuit de technische invalshoek is een aantal aandachtspunten naar voren gekomen; verzoek het college om op korte termijn specifiek aandacht te besteden aan deze punten en deze punten te prioriteren (of controleer of dat inmiddels al is gedaan).
9. Verzoek het college om het beleid voor het (grootschalig) afstandswerken, als gevolg van de COVID-19 maatregelen, bij voorrang op te stellen en te implementeren (of controleer of dat inmiddels is gedaan).
10. Verzoek het college om te investeren in een herhalingsonderzoek van het door het externe bureau verrichtte onderzoek voor het rapport van de Rekenkamercommissie uit 2018. Plan dit als de situatie genormaliseerd is en beschouw dit als een 1-meting om daarmee de daadwerkelijke effecten op mensen, organisatie en techniek in beeld te brengen.
11. De rekenkamer beveelt de raad aan om met enige regelmaat te controleren of hoge mate van betrokkenheid bij college en organisatie bij dit thema nog steeds aanwezig is.

## Slotopmerking

Voorliggend doorwerkingsonderzoek is gebaseerd op bestudering van actuele documenten en een beperkt aantal interviews. Dit levert het beeld op zoals in deze rapportage weergegeven, echter met nadruk wijst de Rekenkamer erop dat er geen diepere analyse, zoals een onderzoek van systemen op technisch niveau, heeft plaatsgevonden.

# Bijlage 1: Bestudeerde documenten

NVRR (april 2018*), Handreiking meten van doorwerking rekenkamerproducten.* NVRR: te raadplegen op: https://wiki.nvrr.nl/download/?id=81746.

## Informatie Raad

Raad Westerkwartier. *Brief informatie 0-meting*. 8 februari 2018

Raad Westerkwartier. *Verslag raadscommissie herindeling.* 11 oktober 2018.

Raad Westerkwartier. *Besluitenlijst vergadering*. 15 oktober 2018.

Raad Westerkwartier. *Brief informatieveiligheid c.q. implementatie BIO.* 26 februari 2019.

## Documenten i-Bewustzijn

Zeeland, van, I. (2019, april). *Nulmeting iBewustzijn* (Rapport). Nijmegen: SEP, partners in leren. Inclusief bijbehorende infographic.

Zeeland, van, I. (2019, mei). *iBewustzijnplan* (Plan). Nijmegen: SEP, partners in leren. Zeeland, van, I. (2019, sept). *Evaluatie – iBewustzijn.* (Presentatie). Nijmegen: SEP, partners in leren.

Zeeland, van, I. (2019, sept). *Evaluatie-advies borging iBewustzijn gemeente Westerkwartier* (Adviesrapport). Nijmegen: SEP, partners in leren.

Pilon, Louise. (2020). *Memo e-learning informatieveiligheid en privacy* (Advies: zaaknummer 196933514). Grootegast: gemeente Westerkwartier.

Pilon, Louise. (2020, 17 juni). *Besluit* *e-learning informatieveiligheid en privacy* (DO Besluit). Grootegast: gemeente Westerkwartier.

## Documenten Privacy

Pilon, Louise. (2018, 12 april). *Jaarplan Privacy 2018* (Jaarplan). Grootegast: gemeenten Grootegast, Leek, Marum, Zuidhorn.

Sturkenboom, E., Akay, M.T., IJpelaar, R. (2019, 29 juli). *Rapportage Quick DPIA Westerkwartier juni 2019* (Presentatie). Vlijmen: BKBO.

Pilon, Louise. (2019, 18 augustus). *Memo maatregelen/acties n.a.v. DPIA* (Memo).

Grootegast: gemeente Westerkwartier.

Pilon, Louise. (2019, december). *Voortgang maatregelen/acties n.a.v. DPIA* (Overzicht).

Grootegast: gemeente Westerkwartier.

Pilon, Louise. (2020, maart). *Voortgang implementatie AVG* (Overzicht). Grootegast:

gemeente Westerkwartier.

Pilon, Louise. (2020, 9 april). *Jaarrapportage Gegevensbescherming 2019* (Rapport:

zaaknummer 196929891). Grootegast: gemeente Westerkwartier.

Pilon, Louise. (2020, juni). *Voortgang maatregelen/acties n.a.v. DPIA* (Overzicht).

Grootegast: gemeente Westerkwartier.

Pilon, Louise. (2020, 10 juni). *Q1 en Q2 2020 rapportage informatieveiligheid en privacy* (DO Besluit). Grootegast: gemeente Westerkwartier.

## Documenten Informatieveiligheid

Latifi, K., Compaan, P. (2018, 8 januari). *Infrastructure assessmenrt IT-infrastructure of Gemeente Westerkwartier* (Rapport, 0-meting, vertrouwelijk). Haarlem: ITsec Security Services BV.

Westerhof, M.D. (2018, augustus). *Jaarplan informatieveiligheid 2018-2019*

*Westerkwartiergemeenten* (Plan, vertrouwelijk). Grootegast: gemeenten Grootegast, Leek, Marum, Zuidhorn.

Westerhof, M.D. (2019). *DO advies Implementatie Baseline Overheid* (BIO) (Advies:

zaaknummer 19699598). Grootegast: gemeente Westerkwartier.

Westerhof, M.D. (2019, september). *Informatiebeveiligingsplan 2019-2020* (Plan).

Grootegast: gemeente Westerkwartier.

Westerhof, M.D. (2019, september). *Informatiebeveiligingsbeleid 2019-2021* (Beleid).

Grootegast: gemeente Westerkwartier.

Westerhof, M.D. (2020, februari). *GAP-analyse BIO gemeente Westerkwartier* (Analyse).

Grootegast: gemeente Westerkwartier.

Westerhof, M.D. (2019, november). *Verbeterplan ENSIA* (Advies aan het college: zaaknummer 196922538). Grootegast: gemeente Westerkwartier.

Westerhof, M.D. (2020, april). *ENSIA 2019-2020* (Collegevoorstel: zaaknummer 196922538). Grootegast: gemeente Westerkwartier.

Tuuk, van der A. (2020, juni). *ENSIA 2020* (Raadsvoorstel: zaaknummer 196922538, inclusief bijlagen). Grootegast: gemeente Westerkwartier.

Tuuk, van der A. (2020, juni). *ENSIA 2020, geheimhouding* (Raadsvoorstel: zaaknummer 196922538). Grootegast: gemeente Westerkwartier.

Westerhof, M.D. (2020, juni). *Oplossen technische bevindingen rekenkamerrapport informatieveiligheid* (Overzicht). Grootegast: gemeente Westerkwartier.

Pilon, L. (2020, januari). *Drie lijnen van control* (Overzicht). Grootegast: gemeente Westerkwartier.

## Documenten Integraal Veiligheidsbeleid

Gemeente Westerkwartier. (2019, 5 december) *Sfeerverslag ophalen input IVB* (Rapport).

Grootegast: Auteur.

Gemeente Westerkwartier. (2019, z.d.). *Integrale Veiligheidsanalyse* (Rapport). Grootegast:

Auteur.

Gemeente Westerkwartier. (2019, z.d.). *Integraal Veiligheidsbeleid 2020-2023* (Beleidsvoorstel). Grootegast: Auteur.

Tuuk, van der A. (2019, 11 december). *Vaststellen integraal veiligheidsbeleid 2020-2023* (Raadsvoorstel: zaaknummer 19693259). Grootegast: gemeente Westerkwartier. Tuuk, van der A. (2020, 22 januari). *Vaststellen integraal veiligheidsbeleid 2020-2023* (Raadsvoorstel: zaaknummer 19693259). Grootegast: gemeente Westerkwartier.

Gemeente Westerkwartier. (2019, z.d.). *Integraal Veiligheidsbeleid 2020-2023* (Beleid). Grootegast: Auteur.

# Bijlage 2: Overzicht respondenten en bespreekthema’s

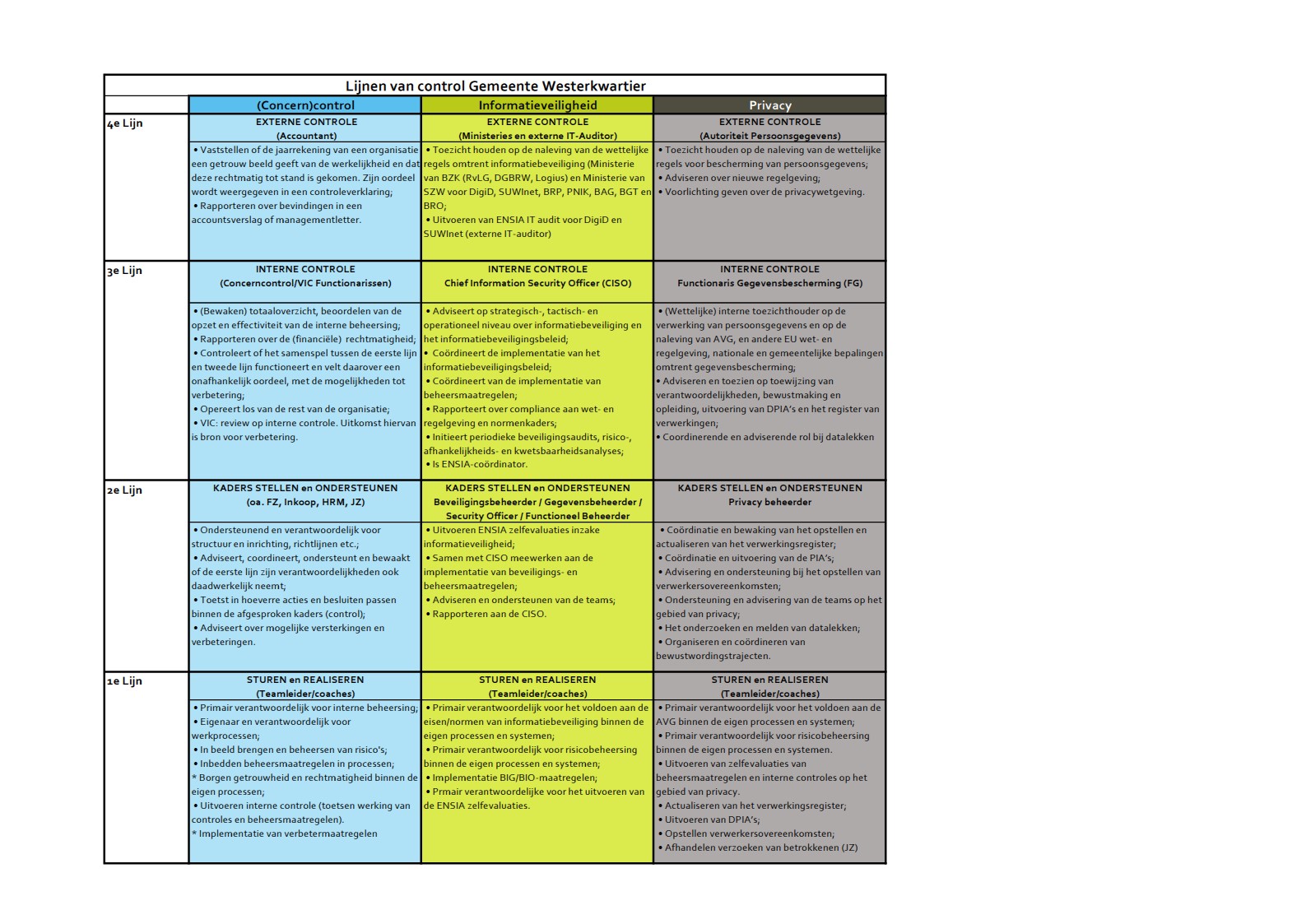
Voor dit onderzoek zijn drie interviews afgenomen met:

1. Astrid Schulting, gemeentesecretaris
2. Louise Pilon, functionaris gegevensbescherming/FG
3. Melcher Westerhof, functionaris informatieveiligheid/CISO

De semi-gestructureerde interviews zijn ingericht aan de hand van gespreksthema’s waarbij bij ieder thema een aantal subvragen is geformuleerd. Thema’s:

* Algemene vragen over functie, positionering en bekendheid met het onderwerp;
* Herkenbaarheid van het onderzoek en het thema in de organisatie;
* Informatieveiligheid, budget, maatregelen en ontwikkeling in planvorming;
* Voortgang technische aanbevelingen, voortgang, risico’s en koppeling BIO en ENSIA;
* i-Bewustzijn, voortgang maatregelen en implementatie aanbevelingen uit de evaluatie;
* Privacy, plannen en voortgang, koppeling met informatieveiligheid;
* Tempo en voortgang van de maatregelen;
* Organisatieontwikkeling en aandacht voor informatieveiligheid daarin.

# Bijlage 3: Control Gemeente Westerkwartier



1. NB het Informatiebeveiligingsplan 2019-2020 en Informatiebeveiligingsbeleid 2019-2021 zijn gelijktijdig verschenen. [↑](#footnote-ref-2)