RAPPORT

Onderzoek Rekenkamercommissie Informatiebeveiliging Gemeente Laarbeek

In opdracht van de Rekenkamercommissie
Secura rapport - onderzoek informatiebeveiliging Laarbeek v1.1
Versie 1.0 ref. 2019029/A&A/RK
26 februari 2019

VERTROUWELIJK

Secura B.V.
Vestdijk 59
5611 CA EINDHOVEN
Nederland

Karspeldreef 8
1101 CJ AMSTERDAM
Nederland

T +31 (0)40 23 77 990
E sales@secura.com
W secura.com

INHOUDSOPGAVE

1. BESTUURLIJKE RAPPORTAGE BEVINDINGEN OP HOOFDLIJNEN EN AANBEVELINGEN

1.1. Aanleiding en opdracht

De dienstverlening van gemeenten aan burgers en bedrijven is in hoge mate afhankelijk van geautomatiseerde informatiesystemen. Gemeenten krijgen steeds meer taken toebedeeld waar in de uitvoering intensief gebruik wordt gemaakt van informatiesystemen en daarin opgeslagen gegevens. Hierbij vervult de gemeente ook vaak taken als onderdeel van een keten van organisaties en is daarmee afhankelijk van andere organisaties en externe databases en vormt zelf ook een cruciale schakel in het realiseren van een voldoende beveiligingsniveau over de keten heen.

Dat de bedreigingen toenemen, en de kans dat deze plaatsvinden stijgt, blijkt uit recente incidenten en onderzoeken zoals die van de IBD (Informatiebeveiligingsdienst als onderdeel van de VNG) in 2018. Incidenten als ransomware incidenten, phishing aanvallen met opvolgende hacks en datalekken die publiek zijn geworden bevestigen dit. Het Nationaal Cyber Security Centrum (NCSC) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) constateren tevens een toename van cyberaanvallen op overheidsinstellingen waaronder gemeenten. Gemeenten hebben gegevens die niet in verkeerde handen mogen vallen zoals bevolkingsdata, privacygevoelige informatie van burgers, (bovenregionale) beleidsstukken, informatie over bedrijfseconomische ontwikkelingen, aanbestedingsinformatie, vertrouwelijke bedrijfsgegevens, inrichtingsinformatie over ICT beveiliging etc.
De IBD geeft daarbij aan dat risico's toenemen doordat gemeenten meer gebruik maken van Cloud oplossingen, het gebruik van moeilijker te beveiligen mobiele apparaten toestaan en steeds meer diensterlening doen met inzet van digitale informatiesystemen. Door in gemeenten gebruik te gaan maken van apparaten die, ook via internet, met elkaar communiceren zoals camera's, energievoorzieningen op wijkniveau, smart parkeermeters etc., kortgezegd: "Smart cities", zullen bedreigingen en de impact van incidenten in en rond informatiesystemen navenant toenemen.

De taken, bevoegdheden en verantwoordelijkheden van met name de colleges van b&w op het gebied van informatiebeheer en informatiebeveiliging, nemen als gevolg van deze ontwikkelingen sterk toe. In de praktijk blijkt dat, voor het kunnen realiseren en waarborgen van informatieveiligheid, deskundigheid nodig is en vanuit het college van b&w specifiek aandacht vraagt. En daarbij komt dan ook nog het effectief worden van de geactualiseerde Europese privacyregelgeving per 25 mei 2018, de AVG. Dit is complexe materie met voor burgers en gemeenten belangrijke regels en handvatten over hoe om te gaan met het verwerken van persoonsgegevens en voorzien van stevige boetebepalingen. Een forse uitdaging!

Het risico bestaat dat de gemeente onvoldoende voortvarend deze uitdagingen oppakt en te weinig werk maakt van informatieveiligheid. Hoe nu bevestigd te krijgen dat de gemeente voldoende is voorbereid op deze bedreigingen, relevante aandachtspunten helder zijn en het college van b&w voldoende handvat heeft voor het aangaan van deze uitdagingen?

De Rekenkamer Commissie heeft het initiatief genomen een onderzoek te laten uitvoeren naar de wijze waarop de betreffende colleges grip hebben op informatieveiligheid en het voldoen aan de actuele privacy regelgeving. Zij heeft daarvoor twee centrale onderzoeksvragen geformuleerd:

1. In hoeverre is de (digitale) informatiebeveiliging van de gemeenten Gemert-Bakel en Laarbeek in de praktijk op orde?
2. Zijn beide gemeenten alert en actief genoeg om de informatiebeveiliging oplossingsgericht te verbeteren en kan de raad ervan op aan dat het goed gaat?

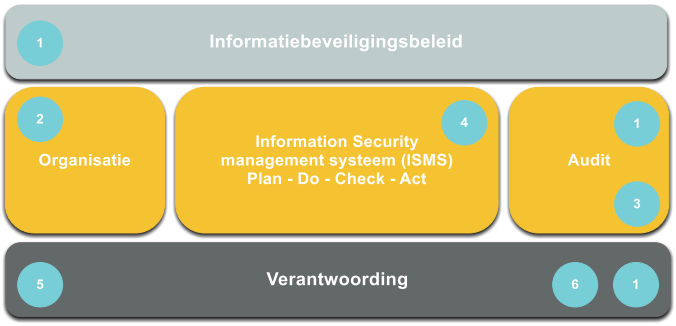
In overleg met de gemeenten is het onderzoek opgedeeld in een aantal fasen waarbij de uitkomsten van een eerdere fase bepalen wat de inhoud en aanpak van het opvolgende onderzoek zal zijn voor zover dat nog relevant is. Secura B.V. is de opdracht gegeven dit onderzoek uit te voeren. De eerste fase betreft een vooronderzoek. Dit vooronderzoek is niet gericht op het (met zekerheid) afgeven van een oordeel over de kwaliteit van de informatiebeveiliging maar heeft als doelstelling inzicht te krijgen in de wijze waarop het college van b&w een organisatie heeft ingericht, medewerkers heeft betrokken en technische en/of procedurele maatregelen heeft getroffen reeds, als onderdeel van de planning & control cyclus, ingerichte verantwoordingen en uitgevoerde audits. Oftewel de mate waarin de gemeenten nu al beschikken over een ingerichte organisatie voor het realiseren van informatieveiligheid en het kunnen voldoen aan de AVG.

Deze rapportage geeft de uitkomsten van het vooronderzoek verricht door Secura in de periode van 24 september tot en met 2 november 2018.

1.2. Aanpak

Voor dit vooronderzoek hebben wij de volgende onderzoeksvragen uitgewerkt op basis van de centrale (overkoepelende) vragen. De geformuleerde sub vragen zijn:

1. Voldoet de gemeente Laarbeek aan de ‘normen’?
2. Hoe is de organisatorische inrichting van de informatiebeveiliging?
3. Welke beveiligingschecks worden zoal uitgevoerd?
4. Welke maatregelen zijn getroffen rond back-ups?
5. Hoe vindt de opvolging plaats bij gesignaleerde tekortkomingen?
6. Hoe is de monitoring ingericht door de raad?



Figuur 1: Onderzoeksgebieden en sub vragen

Hierbij is nadrukkelijk bepaald dat er binnen het onderzoek geen technische testen plaatsvinden maar de onderzoeker enkel inventariseert welke maatregelen de gemeenten zelf hebben genomen en welk informatie over de kwaliteit van de inrichting daarvan al voorhanden is. Indien relevant hebben wij wel bij het onderzoek gevraagd om bewijsstukken die antwoorden en uitspraken staven. Ons onderzoek hebben wij uitgevoerd aan de hand van interviews met sleutelfunctionarissen, de analyse van diverse beschikbare audit rapporten en opvolging van de bevindingen opgenomen in die rapporten, het bestuderen van de diverse interne verantwoordingen en daarop gegeven opvolging en diverse vastlegging rond en in de beheerprocessen. De rapportage hebben wij opgesteld per gemeente.

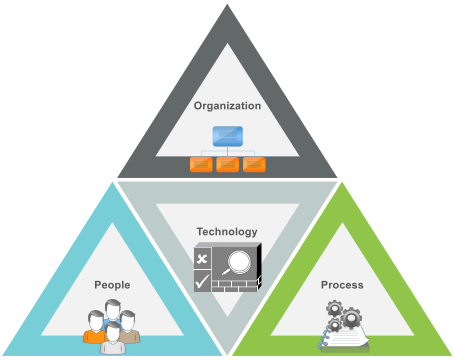
1.3. Bevindingen op hoofdlijnen

Informatiebeveiliging draagt bij aan de betrouwbaarheid (integriteit), vertrouwelijkheid en beschikbaarheid van de informatie(systemen). Betrouwbaarheid betekent dat informatie integer (juist, actueel, tijdig) moet zijn. Vertrouwelijkheid gaat dan over het enkel voor bevoegde personen

toegankelijk zijn van informatie, en de beschikbaarheid dat de informatie op de plaats en het moment aanwezig is als het nodig is. Hierbij dienen persoonsgegevens zorgvuldig, veilig, proportioneel en vertrouwelijk te worden verzameld, bewaard, beheerd en gebruikt, zodat de persoonlijke levenssfeer van inwoners wordt gerespecteerd. Inwoners moeten daarop kunnen vertrouwen, en de gemeenteraad moet voldoende inzicht hebben in de mate waarin de gemeente voldoet aan de huidige privacyregelgeving waaronder de AVG.

Voor het realiseren van informatieveiligheid is het essentieel dat (informatie)beveiligingsmaatregelen zijn getroffen op de aspecten:

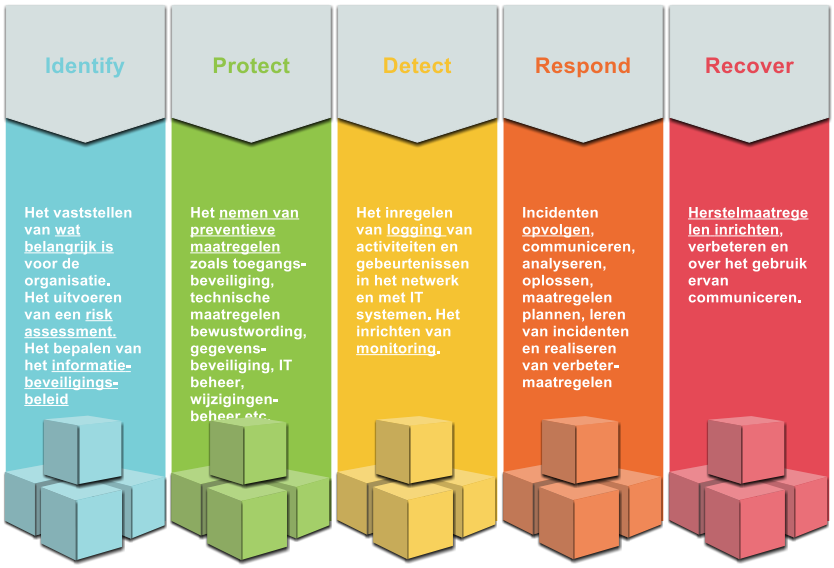
- People ((Personeel)bewustzijn van betrokken medewerkers),
- Process ((Proces) ingeregelde beveiligingsprocedures zoals toegangsbeveiliging),
- Organization ((Organisatie) verdeling van taken en bevoegdheden zoals het instellen van een beveiligingsfunctionaris en een functionaris gegevensbescherming (eis AVG)) en
- Technology ((Techniek) technische maatregelen zoals toegangssystemen, firewalls etc.). Immers



Figuur 2: Aspecten informatiebeveiliging

Immers voor de uitvoering van beveiligingsprocedures, zoals bijvoorbeeld het aanmaken van gebruikers in een systeem, dient duidelijk te zijn wie deze mogen/moeten uitvoeren, op basis van welke standaardprocedure dit dient te gebeuren, de techniek ervoor zorgt dat de bevoegdheden goed kunnen worden ingeregeld en de betrokken medewerkers de juiste handelingen doen en zich bewust zijn van het belang en de impact daarvan. Als één van deze aspecten tekortkomingen kent dan kan het bijvoorbeeld gebeuren dat onterecht een gebruiker in het systeem wordt aangemaakt of niet de juiste rechten krijgt.

De praktijk wijst uit dat het onmogelijk is alle beveiligingsincidenten uit te bannen. Het is steeds belangrijker te zijn voorbereid op eventuele incidenten. Dit vergt een alerte en voorbereide organisatie. Vrij vertaald op basis van het 'NIST Cybersecurity Framework' kan daar het volgende onderscheid in maatregelen voor worden gehanteerd:



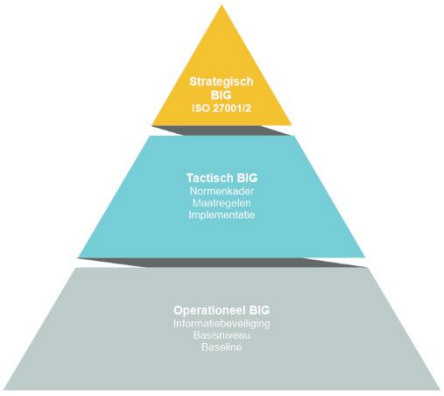
Figuur 3: Alerte organisatie op cybersecurity (vrij vertaald van NIST Cybersecurity framework v 1.1)

Wij constateren
1. dat risicomanagement nog de aandacht vraagt;
2. het beleid nog moet worden geactualiseerd voor de komende jaren;
3. daarop aansluitende maatregelen of uitwerking van bestaande maatregelen moet plaatsvinden;
4. dat op basis van de uitkomsten van een nulmeting uit 2014 de nodige verbeterslagen hebben plaatsgevonden;
5. binnen de organisatie de aandacht voor informatiebeveiliging is belegd en ook bij een incident tot en met de gemeenteraad is opgeschakeld;
6. op beleid en procedureel niveau een en ander meer in detail kan worden gestandaardiseerd en uitgewerkt.

Onderstaand hebben wij samengevat wat de belangrijkste bevindingen zijn uit het vooronderzoek bij de gemeente Laarbeek zoals deze bijdragen aan het uiteindelijk kunnen beantwoorden van de centrale onderzoeksvragen. De bevindingen per vooronderzoeksvraag zijn in het rapport verder uitgeschreven.

1.3.1. Informatiebeveiligingsbeleid

In haar informatiebeveiligingsbeleid (2014-2018) heeft de gemeente Laarbeek vastgelegd welke eisen zij stelt aan haar informatiebeveiliging. Zij heeft hiervoor gebruik gemaakt van de Baseline Informatiebeveiliging Gemeenten (BIG). De BIG is de minimumnorm voor informatiebeveiliging bij gemeenten. Het is een baseline voor het vaststellen, onderhouden en formuleren van strategische beleid (Strategische BIG), uitwerking van richtlijnen en maatregelen (Tactische BIG) en omvat diverse ondersteunende operationele producten van de IBD die daarop aansluiten.



Figuur 4: Samenhang BIG onderdelen

De gemeente Laarbeek heeft de tactische BIG als uitgangspunt gebruikt voor een nulmeting in 2014, uitgevoerd door een externe auditor, om inzicht te krijgen in de status en gewenste verbetermaatregelen.

Het informatiebeveiligingsbeleid loopt tot en met 2018, is daarmee aan vervanging toe. Aangezien de gemeente het informatiebeleid (beleid dat de eisen uitwerkt die de gemeente stelt aan haar informatievoorziening) recent heeft geactualiseerd kan nieuw informatiebeveiligingsbeleid worden bepaald.
Op basis van het nog geldende informatiebeveiligingsbeleid constateren wij dat deze nog handvatten ontbeert voor een aantal belangrijke onderdelen van informatiebeveiliging die bij de gemeente Laarbeek ook nog niet (voldoende) zijn ingericht. Wij bevelen aan deze onderdelen expliciet op te nemen in het nieuwe informatiebeveiligingsbeleid. De onderdelen die de aandacht vragen zijn:

1. Het risicomanagementproces is nog niet in het beleid opgenomen of geïmplementeerd.

   Alleen door inzicht te hebben in de risico's voor de betrouwbaarheid, beschikbaarheid en exclusiviteit van de gegevens van de gemeente, en de verwerkingen daarvan, kan de gemeente bepalen welke beveiligingsmaatregelen noodzakelijk zijn.

   De huidige risico inschatting is gebaseerd op de uitkomsten van de nulmeting uit 2014. Er bestaat geen risicomanagement proces dat ervoor zorgt dat periodiek wordt vastgesteld welke

veranderingen in de risico's plaatsvinden en of dat aanleiding is om nieuwe maatregelen te nemen of het beleid aan te passen.
De risico's waar de gemeente mee te maken heeft zijn duidelijk anders dan 4 jaar geleden ten tijde van de nulmeting. Tevens zijn in het informatiebeleid nieuwe ontwikkelingen en gebruik van informatie aangekondigd, waar specifieke risico's voor spelen waaronder meer gebruik van Cloud toepassingen (gegevensverwerking bij derden).

Het risico bestaat dat onvoldoende maatregelen zijn getroffen voor de actuele risico's en onvoldoende inzicht bestaat in de daadwerkelijke risico's. Overigens worden deze risico's enigszins beperkt doordat de gemeente Laarbeek is aangesloten bij de Informatiebeveiligingsdienst Gemeenten (initiatief VNG (Vereniging van Nederlandse Gemeenten) en KING (Kwaliteitsinstituut Nederlandse Gemeenten)). Deze signaleert acute beveiligingsrisico's voor gemeenten en mogelijke oplossingen daarvoor en meldt deze actief bij de gemeente Laarbeek. De opvolging van belangrijke gemelde risico's en bedreigingen neemt de CISO mee in zijn kwartaalrapportage.

Wij benadrukken dat het implementeren van een risicomanagement proces de belangrijkste bouwsteen is bij het realiseren van aantoonbaar voldoende informatiebeveiliging. De opvolging (per 1 januari 2020) van de eerder genoemde BIG (minimumnorm informatiebeveiliging voor gemeenten) door de BIO (Baseline Informatiebeveiliging Overheid) betekent ook dat een op risicomanagement gebaseerde informatiebeveiliging een eis wordt.

2. Een afhankelijkheden- en kwetsbaarheden analyse ontbreekt nog.

   Het 100% veilig zijn is niet mogelijk, de gemeenten moet ook nog (gewoon) hun werk kunnen doen. Deze analyse geeft het benodigde inzicht in afhankelijkheden van informatiesystemen en kwetsbaarheden van die systemen om
   a) keuzes te maken welke risico's te accepteren en
   b) te kunnen kiezen welke maatregelen het meeste effect hebben op het verlagen van risico's.

   Door het ontbreken van de (beleid)uitgangspunten voor continuïteitsmaatregelen bestaat het risico dat teveel (kostbare) maatregelen worden geïmplementeerd of dat kritieke systemen te lang niet beschikbaar kunnen zijn. Deze analyse is ook essentieel voor het bepalen van de acties bij incidenten (response / recover) waardoor bij het ontbreken van deze analyse de gemeente minder adequaat kan optreden en daarmee systemen langer dan gewenst niet beschikbaar zijn, niet betrouwbaar werken of de vertrouwelijkheid van gegevens niet is gerealiseerd.

3. Classificatie van gegevens.

   Met de huidige ontwikkelingen en het effectief worden van de AVG (algemene verordening gegevensbescherming) is de classificatie van gegevens een steeds belangrijker hulpmiddel om de juiste maatregelen te bepalen. Bijzondere en/of gevoelige gegevens van burgers vereisen bij de verwerking zwaardere beveiligingsmaatregelen. Dit kan ook gelden voor andere gegevens zoals inrichtingsdocumenten van de beveiliging van de ICT, aanbestedingsstukken etc. De classificatie is nog beperkt uitgewerkt in het bestaande beveiligingsbeleid.

1.3.2. Organisatie

Binnen de gemeente is informatiebeveiliging organisatorisch belegd maar ook nog sterk in beweging.

Binnen het college van b&w is een aparte portefeuille informatiebeveiliging waar (min of meer) ook de verantwoordelijkheden vallen van de activiteiten rond het implementeren van maatregelen om te voldoen aan de AVG. Dit betekent dat het onderwerp op het juiste niveau is geagendeerd.

Er is een aparte verbijzonderde deeltijdtaak van een beveiligingsfunctionaris: CISO (Chief information security officer) die zich bezig houdt met de coördinatie en aansturing van de activiteiten gericht op het realiseren van het informatiebeveiligingsbeleid. Deze CISO heeft een directe verantwoordingslijn naar de portefeuillehouder (aparte taak) informatiebeveiliging in het college van b&w. Gemeente Laarbeek is bezig met het verder verbeteren van de organisatorische invulling van de informatiebeveiligingsfunctie door het rekruteren van een fulltime CISO die zij deelt met de gemeente Gemert-Bakel.

Met deze inrichting heeft de gemeente Laarbeek in de basis de operationele verantwoordelijkheid belegd in de organisatie en via de kwartaalrapportage van de CISO aan de portefeuillehouder informatiebeveiliging in het college van b&w periodieke verantwoording geborgd. Gezien de toenemende risico's is de noodzaak van een full time CISO onderkend en is de gemeente die aan het werven.

Er zijn via de gemeenschappelijke regeling (GR) Peelgemeenten 2 Functionarissen gegevensverwerking (FG's) beschikbaar gekomen die de FG rol van de CISO nu overnemen, het rekruteren van een full time CISO is nog onderhanden.

1.3.3. Het ISMS en het verbetertraject

Figuur 5: Aandachtsgebieden informatiebeveiliging

Een ISMS (Information Security management systeem) moet informatieveiligheid waarborgen door: voldoende maatregelen te plannen, te implementeren, te monitoren en continu te verbeteren.
In 2014 heeft een nulmeting plaatsgevonden door een derde partij. Naar aanleiding van de uitkomsten van deze nulmeting heeft een selectie plaatsgevonden van te implementeren verbetermaatregelen om het niveau van informatieveiligheid te verhogen.
Naar verluidt is deze selectie met de medewerkers gedaan, maar zijn de afwegingen daarbij niet vastgelegd waardoor inzicht in het geaccepteerde risico ontbreekt.

De realisatie van de geselecteerde maatregelen is nagenoeg geheel gerealiseerd (status 2e kwartaal 2018). Echter vergen diverse ontwikkelingen een heroriëntatie op de huidige status. Uit ons vooronderzoek en de analyse van de uitkomsten uit de diverse audits komen de volgende aandachtspunten naar voren voor het ISMS.

1. Uit ons vooronderzoek en de analyse van de uitkomsten uit de diverse audits komt naar voren dat de uitgangspunten en richtlijnen voor de processen toegangsbeheer, wijzigingenbeheer en incidentbeheer meer uitwerking vragen. Overigens hebben wij in november nog de nieuw opgezette uitwerking ontvangen van het toegangsbeheer, met aandacht voor de relevante onderdelen. Aandachtspunt hierin is nog de rol van samenwerkingsverbanden binnen het toegangsbeheer. De andere beheerprocessen zijn op hoofdlijnen uitgewerkt in het beleid. Overigens komt uit de diverse audits naar voren dat er wel maatregelen zijn getroffen in die processen.

Beperkte uitwerking van de eisen aan beheerprocessen en daarop aansluitende procedures brengen het risico met zich mee dat deze processen op een onvoldoende gestandaardiseerde wijze plaatsvinden en daardoor minder effectief zijn om beveiligingsrisico's het hoofd te kunnen bieden.

2. De gemeente Laarbeek heeft maatregelen getroffen om de beschikbaarheid van de systemen te waarborgen waaronder uitwijk en back-up systemen en procedures. Een nog uit te afhankelijkheden- en kwetsbaarheden analyse kan aangeven of deze maatregelen toereikend zijn.

   Het risico bestaat dat onvoldoende continuïteitsmaatregelen zijn getroffen.

4. De menselijk factor is belangrijk voor goed werkende beveiligingsmaatregelen. Medewerkers moeten bewust zijn van het belang van goede beveiliging en welke bijdrage zij daar dagelijks aan kunnen leveren om deze maatregelen effectief te kunnen laten zijn. Het informatiebeveiligingsbeleid benoemt de verantwoordelijkheden van medewerkers voor het beveiligingsbewust handelen. Een communicatieplan is in concept opgesteld.

   Onbewuste en onbekwame medewerkers verstoren de effectiviteit van beveiligingsmaatregelen verhogen het risico op beveiligingsincidenten. Diverse activiteiten om medewerkers bewust te krijgen en houden voor informatieveiligheid hebben in 2018 plaatsgevonden, tevens is hiervoor budget vrijgemaakt voor 2019.

5. De verantwoordelijkheid voor de kwaliteit en beveiliging van die gegevensverwerking blijft, bij uitbesteding van ICT diensten, bij de gemeente liggen. Dit vergt specifieke maatregelen vanuit de gemeente om te waarborgen dat voldoende maatregelen aantoonbaar door die leveranciers zijn getroffen. Te denken valt hierbij aan specifieke beveiligingsafspraken in de contracten, afspraken over het beheer van de geleverde service niveaus, het mogen auditen bij die derde organisatie en/of het jaarlijks verkrijgen van assurance rapporten over hun systeem van interne beheersing. In het kader van de werkzaamheden om de gemeente Laarbeek te laten voldoen aan de AVG worden momenteel ook overeenkomsten van de voor de AVG relevante leveranciers nagelopen en geactualiseerd. Dit was ten tijde van het onderzoek nog onderhanden.

   Het risico bestaat dat onvoldoende inzicht bestaat in de afspraken over en realisatie van benodigde beveiligingsmaatregelen bij leveranciers voor verwerkingen waar de gemeente Laarbeek verantwoordelijk voor is.

6. Het is van belang te kunnen signaleren als mogelijke beveiligingsincidenten zich kunnen voordoen of hebben voorgedaan (zie *Figuur 3: Alerte organisatie op cybersecurity (vrij vertaald van NIST Cybersecurity framework v 1.1))*. Een monitoring systeem en monitoring procedures vervullen daarin een belangrijke rol. Dit is nog niet uitgewerkt in het informatiebeveiligingsbeleid. Overigens heeft de gemeente Laarbeek een centraal meldpunt van (potentiële) incidenten bij de CISO (beveiligingsfunctionaris binnen de gemeente) en bestaan korte communicatielijnen tussen deze CISO en de portefeuillehouder informatiebeveiliging in het college van b&w.

1.3.4. Audits

Uit de audits DigiD assessment, Suwinet audit, jaarrekeningcontrole en de zelfevaluatie voor ENSIA (inclusief delen BAG, BGT, BRO (proefjaar), 'Waar staat je gemeente') en komen tekortkomingen naar voren die nieuw zijn en geen onderdeel vormen van de nog te implementeren openstaande verbetermaatregelen uit 2014. Overigens zijn de tekortkomingen uit de audits met hun specifieke scope en doelstellingen meegenomen in de kwartaalrapportage van de CISO en met de portefeuillehouder informatiebeveiliging besproken. De opvolging daarvan is opgepakt.

Een nulmeting door een onafhankelijke derde kan daarbij meer gewicht geven aan de uitkomsten van de zelfevaluatie als onderdeel van ENSIA. De tekortkomingen uit de DigiD assessment zijn opgevolgd en is ons in November aangetoond dat de her-assessment de normen waarin tekortkomingen waren op 'Voldoet' zijn beoordeeld.
Wel merken wij nog op dat technische beveiligingsonderzoeken zijn beperkt tot Suwinet en DigiD en de daarvoor relevante omgevingen. Technische beveiligingsonderzoeken op andere onderdelen van de ICT omgeving en systemen vinden niet plaats maar zijn wel relevant om inzicht te krijgen in eventuele risico's in de (technische) inrichting.

1.3.5. Privacy en de AVG

Binnen een gemeente vinden logischerwijs veel verwerkingen plaats van persoonsgegevens of zijn systemen gekoppeld aan centrale bestanden / registers met persoonsgegevens. De belangrijkste regels voor de verwerking van persoonsgegevens in Nederland zijn vastgelegd in de AVG. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van deze wet- en verbonden regelgeving. Uit ons onderzoek komen de volgende belangrijke bevindingen naar voren:

1. De gemeente Laarbeek beschikt nog niet over specifiek privacy beleid. Wel heeft zij een 'Privacyverklaring gemeente Laarbeek' op internet gepubliceerd met een aantal uitgangspunten. Tevens heeft zij een classificatie van verwerkingen opgesteld van 'Openbaar' tot 'Geheim' maar deze nog niet verder gedefinieerd en uitgewerkt naar de impact voor de te definiëren (beveiligings)maatregelen. Privacy beleid is nog onderhanden.

2. De implementatie van maatregelen om te voldoen aan de AVG (Algemene verordening gegevensbescherming) is onderhanden. Binnen de gemeente Laarbeek bestaat al een procedure "Protocol datalek Gemeente Laarbeek en Laarbeek". Met ondersteuning van deskundigen zijn diverse activiteiten opgestart of verder vormgegeven. De zijn samen te vatten als:
   - Opzetten en zo compleet mogelijk maken van een Register van verwerkingen;
   - Opzetten en regelen van Verwerkersovereenkomsten met verwerkers waar verwerkingen van persoonsgegeven van burgers uit de gemeente Laarbeek plaatsvinden. Indien Laarbeek van dezelfde verwerkersorganisatie gebruik maakt die dan meteen meenemen.
   - Bewustwording binnen de organisatie vergroten.

   Wij constateren dat deze activiteiten een sterk inventariserend karakter hebben waarbij de begeleidende deskundigen wel controles uitvoeren op de kwaliteit van de vastleggingen. Voor het kunnen blijven voldoen aan de AVG zijn processen nodig die nieuwe verwerkingen en veranderingen in bestaande verwerkingen tijdig (dus bij het overwegen) signaleren en ervoor zorgen dat de impact vanuit de AVG wordt bepaald.

3. De Gemeente Laarbeek heeft inzicht in welke verwerkingen een hoog risico kennen en daarmee om een verplichte, met voorgeschreven minimale eisen, DPIA (Data Protection Impact Assessment) vragen. Een DPIA geeft inzicht in de aard en het doel van de verwerking en de daarmee samenhangende risico's voor de beveiliging van persoonsgegevens op basis waarvan vervolgens maatregelen worden gedefinieerd om het risico zoveel mogelijk te beperken en vast te stellen of de verwerking wel is toegestaan. Kort gezegd is de DPIA de basis voor het, ook door de AVG verplichte, privacy by design.

4. Standaardprocedures voor het afwikkelen van het, door betrokkenen, aanspraak maken op hun rechten volgens de AVG (rectificatie, verwijderen, opvragen van verwerkingen), waren nog onderhanden ten tijde van ons onderzoek.

5. Bewustwording van medewerkers over de noodzaak van de bescherming van persoonsgegevens heeft de aandacht binnen de gemeente Laarbeek. In het bijzonder met intranet nieuwsmeldingen en kennisbijeenkomsten heeft de gemeente haar medewerkers geïnformeerd. Een communicatieplan is hiervoor niet gebruikt. In het recent aangenomen informatiebeleid is nu apart aandacht geschonken aan het belang van bewustzijn bij de medewerkers. Een communicatieplan is in opzet aanwezig.

1.3.6. De opvolging en verantwoording

Over de kwaliteit van de informatiebeveiliging en de voortgang in de realisatie van de verbetermaatregelen rapporteert de CISO per kwartaal aan de portefeuillehouder informatiebeveiliging, die deze ook inbrengt in het college overleg. Deze kwartaalrapportage behandelt niet enkel de voortgang op de implementatie van de verbetermaatregelen uit de eerdere nulmeting maar gaat ook in op andere relevante zaken zoals:

a. Door IBD gesignaleerde bedreigingen en de wijze waarop de CISO hiermee is omgegaan of actie vraagt van het college van b&w.
b. De status rond de implementatie van maatregelen om voldoende compliant te zijn aan de AVG.
c. Aanvullende verbetermaatregelen die naar voren zijn gekomen bij de implementatie van verbetermaatregelen uit de nulmeting.
d. Uitkomsten en opvolging van eventuele tekortkomingen uit audits (DigiD, Suwinet, ENSIA).

Deze kwartaalrapportage wordt nog niet actief gedeeld met de Raad maar zou de raad wel een groter inzicht kunnen geven in de huidige status van informatiebeveiliging. Mogelijk kan een samenvatting van de kwartaalrapportage een overweging zijn om niet te gedetailleerde beveiligingsgevoelige informatie in openbare stukken naar voren te laten komen.

Aan de hand van een eerder beveiligingsincident hebben wij kunnen vaststellen op welke wijze de CISO, in samenspraak met de portefeuillehouder, buiten de reguliere verantwoordingsmomenten heeft geacteerd waardoor het college van b&w in actie kon komen en de raad daarin kon informeren en betrekken via een RIB (Raad Informatie Brief).

Rapportage over de voortgang in de realisatie van maatregelen om te voldoen aan de AVG eisen vindt op hoofdlijnen plaats via de kwartaalrapportage informatiebeveiliging van de CISO aan de portefeuillehouder informatiebeveiliging van het college b&w. De verantwoording betreft een statusoverzicht per onderwerp en geen detailgegevens.

Het is belangrijk dat het college van b&w meer inhoudelijk inzicht heeft in:

- welke verwerkingen plaatsvinden;
- de registraties daarvan juist zijn;
- bij verwerkingen door derden de benodigde verwerkersovereenkomsten zijn afgesloten;
- de hoog risico verwerkingen in beeld zijn en een juiste DPIA hebben ondergaan;
- en dat is vastgelegd dat er voldoende maatregelen zij getroffen volgens de eisen van de AVG.

Voor de gemeenteraad is het van belang inzicht te krijgen in de huidige status en de voortgang in het proces om volledig compliant te zijn aan de AVG.

1.4. Aanbevelingen

Op grond van onze bevindingen hebben wij de volgende aanbevelingen voor de gemeente Laarbeek:

1. Wij adviseren de gemeente nadrukkelijk een afhankelijkheden- en kwetsbaarheden analyse uit te voeren om vast te stellen welke systemen kritiek zijn en specifieke beveiligingsmaatregelen vergen om de beschikbaarheid, betrouwbaarheid en vertrouwelijkheid te kunnen garanderen. Dit is tevens

noodzakelijk voor het kunnen formuleren van adequaat informatiebeveiligingsbeleid. Met de uitkomsten van de analyse, en het geformuleerde beleid in de hand, kan de gemeente ook haar huidige continuïteitsmaatregelen evalueren in relatie tot de beschikbaarheidseisen.

2. Richt een risicomanagementproces in voor het identificeren, analyseren en evalueren van risico's en voor het bepalen van de risicohouding: accepteren of maatregelen treffen. Dit dient een continu proces te zijn. Maak hierbij o.a. gebruik van de best practices van de IBD en andere gemeenten, betrek hierin ook de eisen uit de BIO (Baseline informatiebeveiliging overheid) die als opvolger van de BIG de minimumnorm voor de komende jaren zal zijn.

3. Het op zeer korte termijn vastleggen van informatiebeveiligingsbeleid dat is geactualiseerd op het nieuwe informatiebeleid en uit te voeren risicoanalyse. Neem daarin de aandachtspunten uit dit vooronderzoek mee.

4. Laat een nieuwe nulmeting informatiebeveiliging uitvoeren aan de hand van het nieuwe beleid om vast te stellen welke risico's en aandachtspunten aanwezig zijn. Stel daaropvolgend een goed implementatieplan op en leg de overwegingen rond de selectie van te nemen maatregelen vast.

5. Leg procedures rond kritieke beheertaken als wijzigingenbeheer, toegangsbeheer en incidentenbeheer vast. Overweeg de uitvoering van periodieke audits op de werking van deze beheersmaatregelen. Deels kan hier gebruik worden gemaakt van de uitkomsten van de audit voor de jaarrekeningcontrole en de DigiD assessment.

6. Completeer de bewerkersovereenkomsten met leveranciers en besteedt daarbij aandacht aan de mogelijkheid onderzoeken te doen bij de leveranciers, of beter nog: het ontvangen van (onafhankelijke) Assurance rapporten over de kwaliteit van beveiligingsmaatregelen bij die leveranciers (opzet, bestaan en werking).

7. Tevens adviseren wij de portefeuillehouder, in samenwerking met de CISO, meer inhoudelijk een beeld te vormen van de huidige status van de implementatie van de AVG maatregelen. Mogelijk dat een nulmeting AVG hierbij een goede eerste aanzet kan zijn.

2. INLEIDING

2.1. Informatieveiligheid en gemeenten

Informatieveiligheid en het voldoen aan de eisen van de AVG (Algemene Verordening Gegevensverwerking) staan hoog op de agenda van gemeenten. Gemeenten hebben een groot aantal wettelijke taken te verrichten waar enerzijds in toenemende mate automatisering bij wordt ingezet en anderzijds veel gegevens van burgers worden verwerkt. Automatisering helpt gemeenten om hun dienstverlening efficiënt en effectief in te richten.

De verregaande digitalisering van de informatie introduceert nieuwe bedreigingen dat deze informatie niet betrouwbaar blijkt, niet op het juiste moment beschikbaar is en toegankelijk is voor onbevoegde gebruikers. Om de informatie betrouwbaar, beschikbaar en exclusief te krijgen zijn specifieke informatiebeveiligingsmaatregelen noodzakelijk. Begin 2018 heeft de IBD (Informatiebeveiligingsdienst), als de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en onderdeel van de Vereniging Nederlandse Gemeenten, een onderzoek gedaan naar het 'Dreigingsbeeld informatiebeveiliging gemeenten 2018[1]'. Het risicobeeld dat de IBD heeft samengesteld op basis van dit onderzoek stelt bestuurders in staat om in afstemming met de gemeenteraad, het management en de informatiebeveiligers prioriteiten te stellen en bewust risico's te mitigeren of juist te nemen. Daarbij levert het dreigingsbeeld inzichten voor het opstellen van een strategie en aanpak van informatiebeveiliging. Het onderzoek vat de belangrijkste bedreigingen samen als:

1. Mensen maken fouten;
2. Gemeenten zijn, net als alle organisaties, kwetsbaar;
3. Dreigingen liggen ook (vlak) buiten de eigen organisatie;
4. De waan van de dag bepaalt de agenda;
5. We weten niet wat we niet weten.

De impact van een beveiligingsincident kan heel groot zijn. Gemeenten werken met persoonlijke en vertrouwelijke gegevens en zijn sterk afhankelijkheid voor hun dienstverlening van geautomatiseerde systemen. Als deze niet betrouwbaar werken, of uitvallen, dan heeft dat direct effect op de kwaliteit van de dienstverlening aan burgers, bedrijven en andere organisaties en dat raakt het maatschappelijk verkeer. Los van het feit dat het maatschappelijk verkeer van de overheid, en dus ook gemeenten, verwacht dat zij een voorbeeldfunctie is voor hoe veilig om te gaan met gegevens van haar burgers, introduceert de AVG ook een zwaardere boeteregeling bij het niet naleven van de AVG. Beveiligingsincidenten kunnen daardoor ook leiden tot forse financiële boetes.

Wat beveiligingsonderzoeken en recente beveiligingsincidenten ons leren is dat het nagenoeg onmogelijk is een organisatie 100% te beveiligen tegen de steeds maar toenemende en ook veranderende bedreigingen. Het inrichten van informatiebeveiliging betekent keuzes maken en ook accepteren dat zich incidenten kunnen voordoen. Daarmee is het van het grootste belang inzicht te hebben in de (ontwikkeling van) de risico's en processen te hebben ingericht die waarborgen dat tijdig de juiste actie op een eventueel incident wordt genomen.

[1] "Dreigingsbeeld informatiebeveiliging gemeenten 2018"; IBD; 2018

2.2. Informatiebeveiliging handvatten

De rijksoverheid en de VNG zien het belang van een goed niveau van informatiebeveiliging bij gemeenten. Daarvoor zijn al diverse gezamenlijke initiatieven genomen. De al genoemde IBD is daarbij een belangrijk initiatief en als collectieve voorziening in 2013 opgericht door en voor alle Nederlandse gemeenten, om hen te ondersteunen bij het verbeteren van de informatiebeveiliging. De IBD is ook actief met het signaleren van (nieuwe) bedreigingen en het geven van adviezen over hoe deze het hoofd te bieden. De gemeente Laarbeek maakt ook gebruik van deze dienst.
Het belangrijkste initiatief vanuit de IBD betreft de ontwikkeling van de Baseline Informatiebeveiliging Gemeenten (BIG) die bestaat uit een strategische baseline en een tactische baseline. De IBD heeft ter ondersteuning van de implementatie van informatiebeveiliging aan de hand van het tactische deel van de BIG een groot aantal operationele producten ontwikkeld en beschikbaar gemaakt voor de gemeenten. Dit zijn zeer praktische handvatten die gemeenten helpen bij het snel op orde brengen en houden van informatiebeveiliging.
De laatste versie van de BIG is van juni 2016 (versie 1.02). Overigens zal de BIG op korte termijn worden vervangen door de Baseline Informatiebeveiliging Overheid (BIO). De BIO verschilt op een aantal punten van de BIG. De grootste verschillen zijn:

- Minder maatregelen;
- Meer aandacht voor risicomanagement;
- Onderscheid in drie BBN's (Basisbeveiligingsniveaus) met voor ieder BBN een aantal relevante beheersmaatregelen, verplichte maatregelen en gewenst verantwoordings- en toezicht structuur;
- Toewijzen van maatregelen op eindverantwoordelijke;

De status is dat de BIO per 1 januari 2019 gaat gelden waarbij 2019 nog een overgangsjaar is en de BIO per 1 januari 2020 de BIG vervangt. De introductie heeft ook impact op een ander initiatief in de gemeentesector: ENSIA (Eenduidige Normatiek Single Information Audit). Deze had tot doel om in de plaats van de vele audits die, uit hoofde van wet- en regelgeving, jaarlijks moeten plaatsvinden bij gemeenten één alomvattende audit te laten verrichten. ENSIA is ingegaan per 2017. Een belangrijk facet van de ENSIA is dat deze benadrukt dat de verantwoordelijkheid voor een voldoende beveiligingsniveau nadrukkelijk bij de gemeenten zelf ligt. Dit is kracht bij gezet door het college zich jaarlijks, met een 'In Control' verklaring, zich te laten verantwoorden over het niveau van informatiebeveiliging. Deze verantwoording is dan het object van onderzoek voor de 'ENSIA audit' door een onafhankelijke en deskundige auditor.
Het college van de Gemeente Laarbeek heeft ook zo'n 'In Control' verklaring in de vorm van een Collegeverklaring afgegeven en door een (ENSIA) auditor laten toetsen. In beginsel betreft de scope van de College verklaring de implementatie van informatiebeveiliging volgens minimaal de BIG. Voor de overgangsjaren is dit nog ingeperkt tot de Suwinet audit normen en de normen van de DigiD assessment. Met de introductie van de BIO zal de BIG niet meer als minimum niveau gelden maar zal dit het BBN zijn volgens de BIO. Het is raadzaam voor gemeenten inzicht te krijgen in hun status informatiebeveiliging volgens de BIO om na de overgangsjaren ook direct aantoonbaar te voldoen aan het van toepassing zijnde BBN.

1. Bepalen van het BBN (Basis beveiligingsniveau);
2. Uitvoeren van een Fit Gap analyse;
3. Uitvoeren van een nulmeting (het onderzoek naar het daadwerkelijk geïmplementeerd zijn van maatregelen).

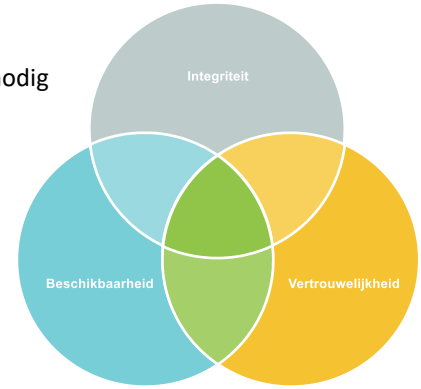
De nulmeting geeft dan weer een goed handvat voor het vaststellen van de te realiseren verbeterpunten en het bewaken van de opvolging daarvan, zodat de college verklaring over de status van informatiebeveiliging eenvoudig is op te stellen en te onderbouwen.

2.3. Aspecten informatiebeveiliging

Samenvattend betekent dit dat gemeenten alert moeten zijn, de juiste prioriteiten moeten stellen en naast preventieve maatregelen ook zich hebben voorbereid op het snel en adequaat kunnen opvolgen van beveiligingsincidenten. Het management, het college en de raad moeten daarin een voorbeeldfunctie vertolken en de trekker- en sturende rol vervullen.

Vanuit de BIG als sectorspecifieke implementatie handvat voor informatiebeveiliging zijn 3 kwaliteitscriteria gedefinieerd (conform ISO 27001 normen) die relevant zijn, vaak afgekort als 'BIV'. Samengevat:

- *Beschikbaarheid*: de mate waarin een informatiesysteem in een organisatie aanwezig is op het moment dat de organisatie deze nodig heeft;
- *Integriteit (of betrouwbaarheid)*: de mate waarin informatie juist en volledig is.
- *Vertrouwelijkheid (of exclusiviteit)*: de mate waarin de toegang tot, en de kennisname van, een informatiesysteem en de informatie daarin is beperkt tot een gedefinieerde groep gerechtigden;

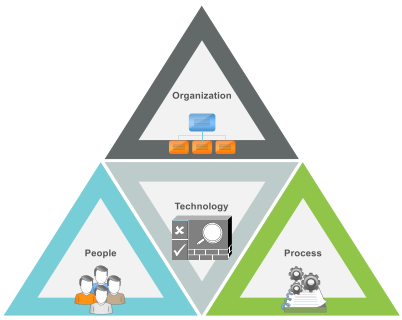


Figuur 6: Kwaliteitscriteria

Informatiebeveiliging is dan het treffen en onderhouden van een samenhangend stelsel van maatregelen om deze kwaliteitsaspecten van de informatievoorziening te garanderen.

Bij het realiseren van voldoende informatieveiligheid door het treffen van informatiebeveiligingsmaatregelen komen verschillende aspecten naar voren die in hun onderlinge samenhang bepalen wat de effectiviteit van die informatiebeveiliging is. Bijvoorbeeld het signaleren van potentiële datalekken vergt dat er technische maatregelen zijn om bijzonder gedrag of dataverkeer signaleert en filter, in de organisatie verbijzonderde functies bestaan die als taak hebben de signalering op te volgen volgens een standaard proces met benodigde vastleggingen. De uitvoerende medewerker zal zich bewust moeten zijn van de relevantie van de signalen en de mogelijke impact die dat kan hebben op de gemeente en zorgvuldig en alert handelen.

Wij vatten deze aspecten samen als het PPOT model. PPOT staat voor de aspecten:



Figuur 7: Aspecten informatiebeveiliging

People: De mensfactor is zeer bepalend voor het realiseren van informatiebeveiliging omdat die vaak is betrokken bij de gegevensverwerking en een rol speelt bij het uitvoeren van beveiligingsmaatregelen.

Process: Het standaardiseren van processen en daarin verbijzonderen van beveiligingsmaatregelen geeft een grotere zekerheid over het daadwerkelijk op de juiste wijze toepassen en uitvoeren van beveiligingsmaatregelen.

Organization: Delegatie van bevoegdheden (waaronder het realiseren van beveiliging technische functiescheidingen) en met expliciete aandacht voor de bevoegdheden en verantwoordelijkheden rond de gegevensverwerking en beveiligingsfuncties

Technology: Technische maatregelen gericht op het beveiligen van de informatiesystemen, de communicatie en de data die in de informatiesystemen is opgenomen.

Vorenstaande aandachtsgebieden hebben wij in onze onderzoekaanpak opgenomen.

2.4. Leeswijzer

In hoofdstuk 1 hebben wij de uitkomsten van ons onderzoek samengevat. Voor een toelichting op informatieveiligheidsaspecten bij de beide gemeenten en de uitgangspunten voor het realiseren van informatiebeveiligingsmaatregelen hebben wij ter inleiding hoofdstuk 2 gebruikt. De opdracht waarmee wij aan de slag zijn gegaan hebben wij uitgeschreven in hoofdstuk 3 en de daarbij gevolgde aanpak toegelicht in hoofdstuk 4.

In de opvolgende hoofdstukken behandelen wij per hoofdstuk een onderzoeksvraag ter verdieping van de in hoofdstuk 1 opgenomen samenvatting. In de bijlage hebben wij een overzicht van de gebruikte afkortingen en termen opgenomen met een toelichting daarop.

3. OPDRACHT

De Rekenkamercommissie van Gemert-Bakel en Laarbeek wil graag inzicht krijgen in de wijze waarop de beide gemeenten omgaan met informatiebeveiliging. Zij heeft hiervoor een opdracht gegeven aan Secura B.V. om onderzoek te doen naar de status van de informatiebeveiliging en hoe de gemeenten daarmee omgaan. Voor dat onderzoek dient Secura B.V. zich te baseren op de reeds voorhanden documentatie en uitgevoerde technische en overige onderzoeken bij de gemeenten. Het betreft onderzoeksvragen die niet zijn gericht op het krijgen van een oordeel met enige mate van zekerheid maar om inzichtelijk te krijgen wat de belangrijkste aandachtspunten zijn bij de gemeenten en op welke wijze de gemeenten grip houden op informatiebeveiliging en in staat zijn daar alert in te acteren.

De 2 centrale onderzoeksvragen in het onderzoek zijn:

3. In hoeverre is de (digitale) informatiebeveiliging van de gemeenten Gemert-Bakel en Laarbeek in de praktijk op orde?
4. Zijn beide gemeenten alert en actief genoeg om de informatiebeveiliging oplossingsgericht te verbeteren en kan de raad ervan op aan dat het goed gaat?

Afgesproken is dat Secura B.V eerst start met een vooronderzoek. Dit vooronderzoek heeft als doelstelling inzicht te krijgen in de reeds, als onderdeel van de planning & control cyclus, ingerichte verantwoordingen en uitgevoerde audits. Het beeld uit die audits en verantwoordingen kan een eerste indruk geven van de kwaliteit van de informatiebeveiliging en de mate waarin deze is geborgd binnen de organisatie van de gemeenten.

Voor het vooronderzoek zijn de volgende onderzoeksvragen uitgewerkt op basis van de centrale (overkoepelende) vragen. Hierbij is nadrukkelijk bepaald dat er binnen het onderzoek geen technische testen plaatsvinden maar de onderzoeker enkel inventariseert welke maatregelen de gemeenten zelf hebben genomen en welk informatie over de kwaliteit van de inrichting daarvan al voorhanden is.

1. Voldoen de gemeenten aan de ‘normen’?
2. Hoe is de organisatorische inrichting van de informatiebeveiliging?
3. Welke beveiligingschecks worden zoal uitgevoerd?
4. Welke maatregelen zijn getroffen rond back-ups?
5. Hoe vindt de opvolging plaats bij gesignaleerde tekortkomingen?
6. Hoe is de monitoring ingericht door de raad?

Voor vraag 6 is uitvraag gedaan naar de wijze van informeren van de raad, maar heeft geen interview plaatsgevonden met een raadslid. In aanvulling op deze onderzoeksvragen voor het vooronderzoek zijn nog een aantal sub vragen over de compliance aan de AVG regelgeving in scope genomen:

1. Bestaat inzicht in de verwerkingen van persoonsgegevens?
2. Zijn er standaardprocedures rond datalekken, rechten van betrokkenen?
3. In hoeverre is rekening gehouden met de vereisten uit de AVG?

Immers met het effectief afdwingbaar worden van de AVG per 25 mei 2018 hebben gemeenten daar wie nieuwe uitdagingen bij gekregen en zijn daar ook de nodige acties in onderhanden. Een basisinzicht waar de beide gemeenten daarin nu staan is van belang voor het inschatten van een compliance risico.

4. UITGEVOERDE WERKZAAMHEDEN

In ons onderzoek hebben wij de voorgestelde aanpak gevolgd. Bij aanvang hebben wij, ten behoeve van het soepel verlopen van de audit en op verzoek van de betrokkenen, een bijdrage geleverd aan het juist informeren van de betrokkenen over het doel en de aanpak van het onderzoek. Op hoofdlijnen hebben wij de volgende werkzaamheden verricht:

1. Voorbereidingsfase;
2. Informeren en voorbereiden betrokkenen;
3. Analyse risicomanagement;
4. Analyse audits;
5. Analyse verantwoordingsproces;
6. Rapportage.

Stap 1: Voorbereidingsfase
In de voorbereidende fase hebben wij een lijst opgesteld van gewenste / verwachte documenten en initieel geanalyseerd op aandachtspunten en het verkrijgen van een eerste beeld met:

1) Het huidige informatiebeveiligingsbeleid van de gemeenten;
2) De verantwoordingen over informatiebeveiliging;
3) De laatste op raad en college niveau behandelde stukken rond informatiebeveiliging;
4) De huidige (organisatorische) inrichting van de informatiebeveiliging en het informatielandschap opgevraagd en doorgenomen.

Hiermee kregen wij inzicht in de wijze waarop de gemeenten omgaan met informatiebeveiliging en de verwerkingen van persoonsgegevens conform de komende regelgeving AVG. Vervolgens hebben wij bepaald welke functionarissen wij in ons onderzoek wilden interviewen. Aangezien de gemeente Gemert-Bakel binnen het intergemeentelijk team IV de trekker is voor de ICT en de informatiebeveiliging hebben wij ook functionarissen van de gemeente Gemert-Bakel geïnterviewd. Dit betroffen:

Functionaris
• Manager KCI
• CISO / FG / ENSIA coördinator
• Beleidsmedewerker Informatievoorziening intergemeentelijk team informatievoorziening
• Manager Dienstverlening & Informatie
• Privacy deskundige
• Portefeuillehouder informatiebeveiliging college b&w

Stap 2: Analyse Risk management
In stap twee hebben wij kennis genomen van de plaats van risicomanagement (betreffende informatieveiligheid) binnen de gemeente Laarbeek. Voor het vaststellen van de inhoudelijk uitgevoerde risicoanalyses door de gemeente Laarbeek hebben wij vooral gebruik gemaakt van een nulmeting uit 2014 op basis van de 1e versie van de BIG dat voor de gemeente Laarbeek de basis is geweest voor het verbetertraject. Aan de hand van periodieke rapportages uit 2018 is een indruk verkregen over de wijze waarop de gemeente omgaat met veranderingen in de risico's.

Stap 3: Analyse Audits
In deze stap hebben wij kennis genomen van de ontvangen auditrapportages van de gemeente Laarbeek. De belangrijkste bevindingen en de opvolging daarvan door de gemeente hebben wij geanalyseerd.

Stap 4: Analyse verantwoordingsproces
Wij hebben kennis genomen van de verantwoordingsrapportages van de security officer (CISO) en de wijze waarop de verantwoording over de voortgang van het AVG compliant worden daarin plaatsvindt. Hierin hebben wij ook aandacht geschonken aan de wijze van opvolgen van de bevindingen uit de diverse audits waaronder de Suwinet audit en de Digid assessment. In het bijzonder hebben wij hierbij ook een interview afgenomen met de portefeuillehouder van informatiebeveiliging binnen het college en onderzoek gedaan naar de wijze waarop de raad is betrokken. Uiteindelijk hebben wij geen raadslid meer geïnterviewd.

Bovenstaande werkzaamheden zijn uitgevoerd in de periode van 24 september 2018 tot en met 2 november 2018, inclusief de periode van het ontvangen van nagestuurde bewijsstukken.

Stap 5: Rapportage
Het vooronderzoek hebben wij afgerond met deze rapportage waarbij wij de relevante uitkomsten van het onderzoek per (voor)onderzoeksvraag samenvatten. Tevens gaan wij in op het informatielandschap. Voor de relevante bevindingen houden wij aandacht voor de onderscheiden aspecten van PPOT voor het kunnen realiseren van effectieve informatiebeveiliging.

5. ONDERZOEKSVRAGEN

5.1. Inleiding

Zoals aangegeven zijn, voor het vooronderzoek, de centrale onderzoeksvragen uitgewerkt in 6 detailvragen. Aan de hand van deze detailvragen hebben wij het vooronderzoek verricht en de bevindingen verzameld. Het betreft de volgende 6 vragen:

1. Voldoet de gemeente Laarbeek aan de 'normen'?
2. Hoe is de organisatorische inrichting van de informatiebeveiliging?
3. Welke beveiligingschecks worden zoal uitgevoerd?
4. Welke maatregelen zijn getroffen rond back-ups?
5. Hoe vindt de opvolging plaats bij gesignaleerde tekortkomingen?
6. Hoe is de monitoring ingericht door de raad?

Ons onderzoek hebben wij uitgevoerd aan de hand van interviews met sleutelfunctionarissen, de analyse van diverse beschikbare audit rapporten en opvolging, het bestuderen van de diverse interne verantwoordingen en daarop gegeven opvolging en diverse vastlegging rond en in de beheerprocessen.

In de volgende paragrafen beschrijven wij onze bevindingen per onderscheiden vooronderzoeksvraag.

5.2. Voldoet de gemeente Laarbeek aan de 'normen'?

In ons onderzoek hebben wij vastgesteld dat de gemeente Laarbeek voor haar beleid gebruik heeft gemaakt van de tactische baseline informatiebeveiliging gemeenten (tactische BIG)van het IBD. In het op 8 oktober 2013 vastgelegde informatiebeveiligingsbeleid heeft de gemeente Laarbeek uitgewerkt welke uitgangspunten en visie zij over informatiebeveiliging heeft voor de periode van 2014 - 2018. Door gebruik te maken van de tactische BIG bestaat zoveel mogelijk aansluiting met de in wet- en regelgeving opgenomen eisen aan informatiebeveiliging bij gemeenten.

In 2014 heeft een nulmeting plaatsgevonden aan de hand van het BIG normenkader. Dit heeft het college inzicht gegeven in de toen bestaande status van informatieveiligheid. Daar waar de maatregelen nog ontbraken heeft een risico inschatting plaatsgevonden. Naar verluidt is deze uitgevoerd door de proceseigenaar in samenspraak met de (externe) audit organisatie. De uitkomsten van de risico analyse zijn vastgelegd, de onderbouwing ervan niet. Op basis van de risico inschatting is een maatregelverbeterplan opgesteld. Hierin zijn 39 normen geselecteerd die volgens de risico inschatting de meeste aandacht vroegen. Per ultimo Q2 (laatste in ons onderzoek betrokken verantwoordingsrapportage van de CISO) staan er nog actiepunten uit voor 4 normen (3 met een medium risico aanduiding en 1 met een laag risico aanduiding.

De volgende aandachtspunten zijn naar voren gekomen waardoor het risico bestaat dat de gemeente Laarbeek nog niet voldoet aan de 'normen'.

- [Organisatie] Doordat het informatiebeveiligingsbeleid is gebaseerd op enkel de tactische BIG heeft het strategische aspect, zoals bijvoorbeeld uitgewerkt in de strategische BIG van het IBD, minder aandacht gekregen.

- [Organisatie] Het betreft een gezamenlijk beleid voor de gemeenten Gemert-Bakel en Laarbeek. In dit beleid is verder niet ingegaan op het verdelen van verantwoordelijkheden tussen de gemeenten en hoe men daarbij omgaat met de toegang en het gebruik van elkaars informatie.

- [Organisatie] Een nieuw informatiebeveiligingsbeleid voor de periode na 2018 is nog onderhanden. Bij de gemeente Laarbeek is nieuw informatiebeleid voor de jaren 2018 – 2020 bekrachtigd. Hierin zijn nieuwe ontwikkelingen voorzien voor de interne ICT die ook aanpassingen vergen in het informatiebeveiligingsbeleid (Cloudservices / BYOD). Daar is apart in het informatiebeleid aandacht aan geschonken.

- [Organisatie] Er is geen afhankelijkheden en kwetsbaarheden analyse uitgevoerd en vastgelegd waarin de gemeente heeft vastgesteld wat de beschikbaarheid eisen zijn aan de informatievoorziening waaronder de maximale uitvaltijden. Dit is een belangrijk handvat voor het bepalen van de juiste continuïteitsmaatregelen waaronder back-up.

- [Organisatie] De in het beleid opgenomen classificatie van gegevens in 3 categorieën (openbaar, intern en vertrouwelijk) is niet verder uitgewerkt zoals o.a. in de wijze van rubricering, door welke functionarissen vast te stellen, het labelen, het onderhouden van het overzicht van geclassificeerde informatie en de eisen aan de te nemen maatregelen per classificatie (waaronder de toegang).

- [Personeel] In het beleid is aangegeven dat elke ambtenaar afzonderlijk verantwoordelijkheid draagt voor de wijze waarop hij/zij omgaat met informatie met bewustwording van kansen en risico's van nieuwe technologieën. Dit is niet verder uitgewerkt met handvatten voor de ambtenaar anders dan do's en don'ts in een 11 puntenlijst. De benodigde communicatie naar de betrokkenen over hun rol in het realiseren van de informatiebeveiliging is binnen het informatiebeveiligingsbeleid verder niet uitgewerkt dan dat dit als taak is geformuleerd voor de individuele ambtenaar en het managementteam en de afdelings- pijlerhoofden. Een communicatieplan gericht op het bewust maken en houden van medewerkers met aandacht voor het positief beïnvloeden van gedrag, houding en kennis aspecten is in concept opgesteld . Overigens zijn er binnen de gemeente Laarbeek wel activiteiten ontplooid gericht op het meer bewust maken van medewerkers van het belang van informatiebeveiliging en privacybescherming in de vorm van kennisbijeenkomsten en informatie via o.a. intranet en zijn er plannen daar een vervolg aan te geven in de komende jaren.

- [Proces] Het beleid geeft geen uitwerking aan een proces van periodieke evaluatie om vast te stellen of het beleid nog steeds voldoende invulling geeft aan de veranderende omgeving wat betreft risico's en aanpassingen in de regelgeving. Het beleid is niet tussentijds aangepast op de wijzigingen in de BIG per 2015 en 2016. In het bijzonder vragen wij hierbij ook aandacht voor het steeds meer inzetten van Cloudservices waarvoor specifieke maatregelen vanuit de gemeente Laarbeek noodzakelijk zijn. Wij tekenen wel aan dat:

    - actief gebruik wordt gemaakt van de service van de IBD die meldingen doet van relevante beveiligingsissues en
    - dat de CISO via kwartaalrapportages bij het college aandacht vraagt voor nieuwe ontwikkelingen en voorstellen doet hoe hier op in te spelen.

- [Proces] Een risicomanagement proces is nog niet ingericht. De gemeente hanteert de risicoanalyse van de gezamenlijke nulmeting Gemert-Bakel / Laarbeek als uitgangspunt voor de selectie en implementatie van beveiligingsmaatregelen. De te implementeren maatregelen zijn daarbij gekoppeld aan proceseigenaren. Dit betreft automatisering, fysieke beveiliging en bode, Gemeentesecretaris, P&O, CISO en Systeembeheer. Andere lijnmanagers of functioneel beheerders van systemen zijn hierin niet benoemd.

- [Proces] Logisch toegangsbeheer is op hoofdlijnen beschreven in het informatiebeveiligingsbeleid. Er zijn instructies voor de helpdeskmedewerker voor de vastlegging in Topdesk. Vastgelegde operationele procedures die beschrijven wie op welke wijze en met welke instellingen gebruikers en

hun bevoegdheden inregelt, alsmede welke controles daarbij moeten worden verricht, ontbreken nog. Wij hebben aanvullend op 9 november 2018 het recent opgestelde toegangsbeleid ontvangen naar aanleiding van de implementatie van verbetermaatregelen uit de DigiD assessment. Dit bevat een uitgebreide uitwerking van het eerdere beleid op hoofdlijnen. Aandachtspunt hierin is nog de aandacht voor het gedeelde karakter van het toegangsbeheer voor de gemeenten Laarbeek en Gemert-Bakel en de beleidsuitgangspunten hiervoor.

- [Proces] Wijzigingenbeheer is op hoofdlijnen beschreven in het informatiebeveiligingsbeleid. Wijzigingen worden vastgelegd in Topdesk. Operationele procesbeschrijvingen zijn niet beschikbaar. Binnen het proces van wijzigingenbeheer wordt geen specifieke aandacht geschonken aan beveiliging.

- [Proces] Incidentenbeheer is op hoofdlijnen beschreven in het informatiebeveiligingsbeleid. Verder is het gebruikelijk dat de CISO bij bijzonderheden (security meldingen vanuit de IBD / security incidenten gemeld bij de CISO) rechtstreeks contact heeft met de portefeuillehouder informatiebeveiliging binnen het college. Dit proces is nog niet vastgelegd in een procedure. Er is wel een protocol datalekken dat de activiteiten beschrijft vanaf de melding van een mogelijk datalek. Daarbij is vastgelegd wie de uitvoerend verantwoordelijke is per activiteit. De FG is daarbij als rol nog niet opgenomen maar betrof ten tijde van de procedure een rol die was belegd bij de CISO.

- [Proces] In het informatiebeveiligingsbeleid is uitwerking gegeven aan de organisatorische inrichting van de informatiebeveiliging. Het college van burgemeester en wethouders is integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente. De managementteams zijn verantwoordelijk voor het waarborgen van een heldere koers en zichtbare ondersteuning van het beveiligingsbeleid binnen de gegeven bestuurlijke kaders. Het lijnmanagement is verantwoordelijk voor de naleving van het beveiligingsbeleid. De (destijds nog beoogde) CISO heeft als taken het centrale aanspreekpunt te zijn op het gebied van informatiebeveiligingsincidenten, de informatiebeveiligingsaudits te coördineren, het beheer en toezicht op de naleving van beveiligingsprocedures uit te voeren en zorg te dragen voor minimaal jaarlijks een voorlichting en instructie bijeenkomst voor medewerkers over informatiebeveiliging. De CISO rapporteert per kwartaal (beleid stelde minimaal jaarlijks) over de uitvoering van het beleid en de status van de implementatie van de verbetermaatregelen uit de gap analyse (2014) aan de portefeuillehouder informatiebeveiliging in het college. Verder zijn er informatiebeveiliging taken in het beleid opgenomen voor medewerkers, systeembeheerders, beveiligingsfunctionarissen reisdocumenten en rijbewijzen, applicatiebeheerders en gegevensbeheerders. De rol van de raad is niet uitgewerkt in het informatiebeveiligingsbeleid waaronder ook de communicatie en verantwoording vanuit het college aan de raad.

- [Proces] Uit de wettelijk verplichte controles voor DigiD en Suwinet, de controle van de jaarrekening zijn tekortkomingen naar voren gekomen. Voor DigiD zijn deze opgevolgd en recent beoordeeld met een ‘Voldoet’ door de DigiD auditor. Voor de Suwinet audit tekortkomingen stonden ten tijde van onderzoek zijn bij Senzer nog acties onderhanden.

- [Proces] Uit de zelfevaluaties op de BAG en BGT normen zijn enkele tekortkomingen naar voren gekomen. Deze betreffen de integriteit van de opgeslagen gegevens. De gemeente Laarbeek heeft maatregelen gedefinieerd om deze tekortkomingen op te heffen.

Wij hebben gevraagd aan de CISO en de portefeuillehouder informatiebeveiliging wat hun inschatting is van het beheersingsniveau van informatieveiligheid bij de gemeente. Beide kwamen tot de inschatting van level 4:

Level	Definitie status informatieveiligheid	Risico
4	Voldoende, de grootste risico's zijn teruggebracht tot een acceptabel niveau, de andere risico's beheerst.	Op basis van de in een initiële meeting vastgestelde risico's geen materiële risico's meer aanwezig en voldoende maatregelen voor de overige risico's / het restrisico accepterend.

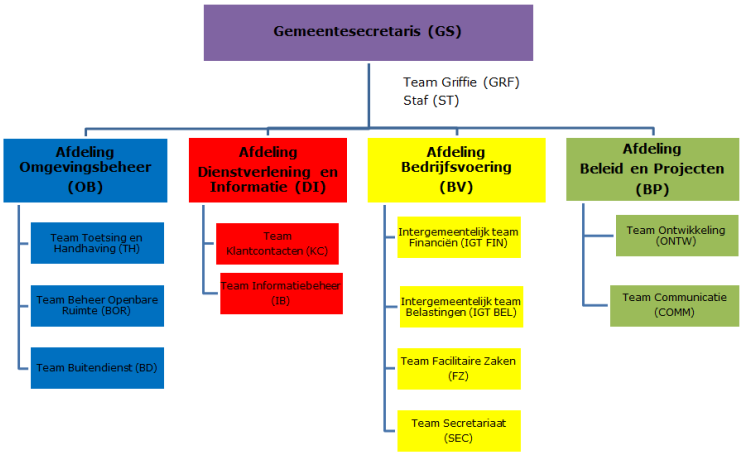
Het vooronderzoek geeft aan dat een actualisering van het informatiebeveiligingsbeleid noodzakelijk is en dat tevens hiervoor een risicoanalyse (met een afhankelijkheden- en kwetsbaarheden analyse) nodig is. Dan is het mogelijk vast te stellen in hoeverre de gemeente voldoende maatregelen heeft getroffen. Wel constateren wij dat door de aanwezigheid van een CISO functionaris, die korte lijnen heeft naar de portefeuillehouder informatiebeveiliging in het college van b&w alsmede het gebruik van de diensten van de IBD, de gemeente in staat is bij incidenten snel op te treden en aandacht heeft voor nieuwe algemene risico's die de IBD onder de aandacht brengt.

5.3. Hoe is de organisatorische inrichting van de informatiebeveiliging?

De organisatie van de informatiebeveiliging moet onderdeel zijn van de planning- en control cyclus om te waarborgen dat informatiebeveiliging een integraal onderdeel is van de gemeente en een aspect is waarover de gemeente via de reguliere verantwoordingslijnen transparant over kan zijn naar haar burgers, andere belanghebbenden en toezichthouders. Door de organisatieonderdelen verantwoording te laten afleggen via reguliere voortgangsrapportages, wordt beveiliging zowel bestuurlijk als ambtelijk in de organisatie te geborgd. Alle geledingen van de organisatie zijn betrokken. Aansluiting op de planning & control cyclus voorkomt daarmee dat informatiebeveiliging als een zelfstandig onderwerp een lage prioriteit krijgt.

Volgens het informatiebeveiligingsbeleid is het college van b&w verantwoordelijk voor de implementatie en het monitoren van de informatiebeveiliging in de gemeente. In het informatiebeveiligingsbeleid is verder vastgelegd wat de verantwoordelijkheid is van de medewerkers, systeembeheerders, beveiligingsfunctionarissen reisdocumenten en rijbewijzen, applicatiebeheerders en gegevensbeheerders. De volgende organisatorische inrichting bestaat bij de gemeente Laarbeek voor de functies rond informatiebeveiliging en privacy:

- College b&w;
- Portefeuillehouder informatiebeveiliging en privacy binnen het college b&w;
- Bedrijfsvoering;
- CISO (security officer);
- FG (Functionaris gegevensverwerking);
- PO (Privacy Officer);
- ENSIA coördinator.



De werving van een privacy officer en een (nieuwe) full time CISO/coördinator ENSIA zijn nog onderhanden. De privacy officer en CISO zal de gemeente Laarbeek delen met gemeente Gemert-Bakel en de Gemeenschappelijke regeling Peelgemeenten.

De verantwoordelijkheid voor het coördineren van de implementatie van informatiebeveiligings-maatregelen, het monitoren van de status van informatiebeveiliging, en tijdig en adequaat opvolging geven aan beveiligingsincidenten, zijn onderdeel van het takenpakket van de CISO. Gemeente Laarbeek

heeft één CISO. Dit betreft geen full time taak. De CISO valt onder de verantwoordelijkheid van de Gemeentesecretaris en rapporteert aan de portefeuillehouder informatiebeveiliging in het college b&w. De CISO vervulde ook de taken van de FG, PO en was de ENSIA coördinator. De FG is aangesteld.

Relevante bevindingen uit ons vooronderzoek over het proces rond de vastlegging en het opvolging geven aan beveiligingsincidenten (potentiële datalekken) zijn:

- In geval van beveiligingsincidenten, die mogelijk kunnen leiden tot een (te melden) datalek, schrijft het “Protocol datalek Gemeente Gemert-Bakel en Laarbeek” voor dat de CISO op de uitvoering van het stappenplan afhandeling datalekken toeziet. Beveiligingsincidenten dienen medewerkers daarom te melden bij de CISO. In het stappenplan is voor de risicoafweging en de besluitvorming over het wel/niet melden van een datalek bij de AP nog geen rol weggelegd voor een FG (Functionaris gegevensverwerking). De CISO vertegenwoordigde ook de functie FG tot het moment dat deze recent in dienst is gekomen. De activiteiten van de CISO in het datalekproces gaan over naar de FG.

- Uit het “Protocol datalek Gemeente Gemert-Bakel en Laarbeek” blijkt nog niet dat beveiliging incidenten worden vastgelegd in het ticketsysteem Topdesk. Daarin worden enkel de ICT gerelateerde incidenten vastgelegd. Bij een impact voor meer dan 10 betrokkenen dient de burgemeester en de gemeentesecretaris te worden geïnformeerd door de CISO.

- Uit het “Protocol datalek Gemeente Gemert-Bakel en Laarbeek” blijkt niet dat de behandeling van beveiligingsincidenten die mogelijk een datalek zijn een integraal onderdeel zijn van het incidentenbeheer.

- De gemeente houdt een apart register bij met meldingen van beveiligingsincidenten en de daarvan relevante informatie zoals wie heeft gemeld, wanneer is er gemeld (niet met informatie van het tijdstip), aard van het incident voor zover het een datalek zou kunnen zijn en de motivatie of het een datalek is. Niet is vastgelegd wie de besluitvorming wanneer heeft gedaan en op welke wijze de verantwoordelijke voor de relevante verwerking(en) en de melder worden geïnformeerd. Wel is in de datalek procedure vastgelegd dat dit de verantwoordelijkheid is van de CISO. Overigens is de eventuele meldingsdatum bij de AP opgenomen en door wie dat is gebeurd. Tevens is toegelicht hoe betrokkenen zijn geïnformeerd.

Er is een periodiek overleg tussen de portefeuillehouder en de CISO. In principe om de twee weken. Afhankelijk van het te bespreken thema kunnen andere functionarissen bij het periodiek overleg aanhaken. Van de periodieke overleggen wordt een actielijst bijgehouden die ook beschikbaar wordt gesteld aan de andere leden van het college.
De CISO verantwoordt zich over de werkzaamheden in een kwartaalrapportage informatiebeveiliging. In deze verantwoording schenkt de CISO aandacht aan beveiligingsincidenten en meldingen (op basis van Topdesk). Dit betreft ook de door de beveiligingsdienst IBD afgegeven beveiligingswaarschuwingen en de opvolging daarvan binnen de gemeenten. Tevens bevat de verantwoording een overzicht en toelichting op beveiligingsincidenten en meldingen van derden partijen. In de paragraaf over de uitvoering van het informatiebeveiligingsbeleid komen diverse projecten en activiteiten op het gebied van informatiebeveiliging aan de orde. Deze hebben een directe of indirecte relatie met het nog onderhanden verbeterplan dat is gemaakt op basis van de uitkomsten van de gap analyse uit 2014. In de bijlage van de kwartaalrapportage zijn de normen opgenomen waarvan de implementatie van maatregelen nog onderhanden is. In een aparte paragraaf gaat de CISO nog in op recente ontwikkelingen en komt in de slotparagraaf tot een advies aan het college.
Overigens vinden geen verantwoordingen over informatiebeveiliging relevante zaken door andere managers dan via de CISO. In de kwartaalrapportage wordt ook de stand van zaken rondom (implementatie van) de AVG geformuleerd.

De portefeuillehouder informatiebeveiliging, binnen het college van b&w, ontvangt de kwartaalrapportage over de informatiebeveiliging van de CISO. In geval van incidenten vindt rechtsreeks contact plaats tussen de CISO en de portefeuillehouder. De rapportage bespreekt de portefeuillehouder binnen het reguliere college overleg. Bij grotere incidenten wordt de gemeenteraad betrokken. Wij hebben dit ook kunnen vaststellen aan de hand van een Raadsinformatiebrief (RIB) over een eerder beveiligingsincident rond een gestolen laptop van een dienstverlener. De kwartaalrapportage wordt door de portefeuillehouder Informatiebeveiliging toegevoegd aan de stukken voor de college-overleggen en besproken als er vragen over zijn of bijzonderheden besproken dienen te worden.

In de gemeente Laarbeek hebben gedurende 2017 diverse, vooral kennisgerichte, activiteiten plaatsgevonden om de medewerkers bewust te maken van het belang van informatiebeveiliging en de rol die zij daarin hebben:

- Intranet informatie over informatiebeveiliging;
- Intranet meldingen / waarschuwingen waarbij acuut specifieke aandacht wordt gevraagd over actuele ontwikkelingen of gemelde incidenten, deze worden ook naar verluidt doorgespeeld naar het management team voor de wekelijkse werkoverleggen;
- Presentatie AVG in het sociaal domein, 24 mei 2018;
- Presentatie AVG 26 juni 2018;

Tevens bevat het informatiebeveiligingsbeleid een uitwerking van de beveiligingseisen waarvoor maatregelen in het personeelsmanagement proces dienen te zijn opgenomen zoals het ondertekenen van een integriteitsverklaring.

Betrokken derde partijen bij kritieke gegevensverwerkingen volgens gemeente Laarbeek:

- Dimpact: [privaatrechtelijk] De gemeente Laarbeek neemt deel aan de coöperatieve vereniging Dimpact waar onder andere een platform beschikbaar is voor de e-dienstverlening. Het biedt niet alleen voor de burgers een compleet beeld van hun aanvragen en de status daarvan, maar ondersteunt ook het KCC (Klant Contact Center) bij de afhandeling van telefonische vragen (de e-suite). Dimpact op haar beurt maakt gebruik van subservice organisaties Atos en SSC (Shared Service Center) Twente. De ontwikkelde en beheerde webapplicatie maakt gebruik van DigiD voor de identificatie en authenticatie van gebruikers. Afspraken over te nemen beveiligingsmaatregelen zijn op hoofdlijnen vastgelegd in een verwerkersovereenkomst in de vorm van:
  - Informatiebeveiliging vindt plaats volgens de BIG;
  - Het aan de BIG voldoen dient te blijken uit externe periodieke audits zoals TPM's.

  Overigens betreft de TPM die wordt verkregen van Dimpact enkel een externe periodieke toets aan de hand van het normenkader DigiD en niet de BIG.

- Senzer: [publiekrechtelijk] Senzer voert als werkbedrijf de Participatiewet uit voor zes Peelgemeentes waaronder de gemeente Laarbeek en Geldrop-Mierlo. Hierbij wordt gebruik gemaakt van Suwinet-Inkijk. Er zijn beveiligingsafspraken, op het niveau van relevante BIG normen, vastgelegd in een door Senzer en gemeente Laarbeek ondertekende verwerkersovereenkomst. De periodieke externe toetsing is beperkt tot de Suwinet audit (subset maatregelen BIG).

5.4. Welke beveiligingschecks worden zoal uitgevoerd?

Op basis van de door de gemeenten aangeleverde onderzoeksrapporten zijn wij gekomen tot de volgende opsomming, naast de uitgevoerde nulmeting BIG uit 2014:

- Accountantscontrole met managementletter van de gemeente Laarbeek 2017;
- DigiD assessment Laarbeek (aansluiting 999702) rapportagedatum april 2018;

- Suwinet audit gemeente Laarbeek;
- Zelfevaluatie ENSIA en BRP;

De gemeente Laarbeek maakt voor haar webapplicaties, die gebruik maken van DigiD, gebruik van derde partijen. Dimpact (zie 5.3) heeft het ontwikkelen van de webapplicatie en het beheer van de infrastructuur uitbesteed aan respectievelijk subservice organisaties Atos Nederland B.V. (hierna: Atos) en Shared Service Center Twente (hierna: SSC Twente).
Voor de gemeente Laarbeek is voor de DigiD assessment 2017 sprake van een 'carved-out' scope van het onderzoek waardoor de beheersmaatregelen bij de betrokken derde partij Dimpact niet zijn beoordeeld. De voor de DigiD assessment verantwoordelijke RE verwijst naar toetsingen bij de leverancier vastgelegd in TPM's met 'Voldoet' oordelen op alle 20 DigiD normen. Van Dimpact is een TPM DigiD beschikbaar volgens de 'inclusive method' waarin tevens de relevante interne beheersingsdoelstellingen van de subservice organisatie zijn opgenomen. In de TPM is ook een paragraaf opgenomen met aandachtspunten voor de gebruikersorganisatie om te voldoen aan de vereisten van het Logius normenkader. Deze zijn niet opgenomen in de kwartaalrapportage informatiebeveiliging.
Van de beoordeelde 6 normen bij de gemeente Laarbeek kregen er 2 het oordeel voldoet niet. In de rapportage informatiebeveiliging 2e kwartaal 2018 is aangegeven dat de gemeenten een verbeterplan hebben opgesteld. Wij hebben op 14 november 2018 de uitkomsten van de herassessment mogen ontvangen die bevestigen dat de twee 'Voldoet niet' normen nu wel voldoen.

Een technische beveiligingsonderzoek heeft enkel plaatsgevonden als onderdeel van de DigiD assessment op de daarvoor relevante webapplicaties. Het rapport met de uitkomsten van de technische audit hebben wij niet beschikbaar gekregen. Andere technische beveiligingsonderzoeken, anders dan geautomatiseerde vulnerability scans, hebben in 2017 en 2018 niet plaatsgevonden.

Bij de gemeente Laarbeek is het proces van de re-integratie van uitkeringsgerechtigden en het verstrekken van uitkeringen ondergebracht bij de gemeenschappelijk regeling Senzer. Bij de Suwinet audit is vastgesteld dat Senzer, op 2 normen na, niet voldoet aan de Suwinet normen. De uitkomsten van de Suwinet audit bevestigen dat er tekortkomingen zijn in de beheersing van uitbestede diensten in de vorm van beleid, afspraken en toezicht op de naleving van die afspraken. Senzer heeft aangegeven een verbeterplan te hebben en opvolging te geven aan de geconstateerde tekortkomingen. De gemeente Laarbeek heeft de actie van een sommatiebrief genomen en wacht tot de bevestiging van de opvolging komt van Senzer en bevestigd door de ENSIA audit 2018. De bevindingen uit de Suwinet audit benadrukken ook de rol van de gemeente zelf "Uitbestede diensten voldoen niet aan de norm. Beleid ontbreekt binnen de gemeente en er is geen toezicht op de naleving van de norm." Naar verluidt krijgt de informatiebeveiliging rond uitbestede diensten aandacht in het nog ontwikkeling zijn informatiebeveiligingsbeleid 2018 – 2020.

In de ENSIA audit zijn de uitkomsten van de DigiD assessment en de Suwinet audit in de scope meegenomen. De colleges van beide gemeenten hebben de ENISA collegeverklaring opgesteld en laten toetsen door een onafhankelijke Register EDP Auditor.
Er is een ENSIA zelfevaluatie uitgevoerd. Er is nog geen actieplan opgesteld om de vastgestelde tekortkomingen en verbetermogelijkheden uit deze zelfevaluatie op te volgen.

Bij de controle van de jaarrekening 2017 zijn bij de gemeente Laarbeek in de managementletter aandachtspunten opgenomen die ook de kwaliteit van de informatiebeveiliging betreffen. Deze zijn in de kwartaalrapportage over informatiebeveiliging opgenomen met uitzondering van de bevindingen rond de authenticatie van gebruikers op het netwerk. De opvolging is uitgesteld tot het definitief maken van het nieuwe informatiebeveiligingsbeleid.

5.5. Welke maatregelen zijn getroffen rond back-ups?

Voor het verkrijgen van inzicht in de getroffen maatregelen in de vorm van back-ups (en restore) hebben wij informatie opgevraagd over beleid, continuïteitsplan, risicoanalyses en vervolgens de bestaande procedures. Het beheer van de back-ups en onderhouden en testen van de restore procedures zijn ondergebracht bij de Gemeente Gemert-Bakel.

- Een continuïteitsplan is nog niet opgesteld maar is wel benoemd in het informatiebeveiligingsbeleid. Ondanks het ontbreken van een analyse van beschikbaarheidsrisico's en daarvoor benodigde maatregelen in de vorm van o.a. back-up is een back-up procedure ingericht.

- De back-up en restore procedure is vastgelegd. De uitvoering van de back-ups vindt geautomatiseerd plaats op basis van een ingeregeld schema en inclusief controle op de volledigheid en het kunnen terug lezen van data. De back-ups vinden niet versleuteld plaats. De back-up vindt eerst plaats naar een disk library en van daaruit naar tapes.

- Van de gemaakte back-ups wordt een geautomatiseerd logboek bijgehouden. De systeembeheerder controleert het logboek op fouten en legt die controle vast in een handmatig logboek.

- Dagelijks vindt een volledige back-up plaats van de databaseservers. Verder vindt er van het systeem per maand één keer een full back-up plaats en vervolgens incremental.

- De server van beide gemeenten staat in het gemeentehuis van Gemert-Bakel. De back-up tapes worden bewaard op de locatie gemeentehuis Laarbeek. De back-up op tapes worden één maand bewaard. De maand back-ups worden 2 jaar bewaard. De jaar back-ups 5 jaar.

- De restore procedure is inclusief de controlehandelingen uitgeschreven. De volledige restore wordt ook extern eenmaal per jaar tijdens de uitwijktest getest door de systeembeheerder en de applicatiebeheerder. In augustus 2018 heeft een uitwijktest plaatsgevonden waarbij is vastgesteld dat de VMware omgevingen beschikbaar konden komen en de toegang tot de BAG en de verbinding met Gemnet is getest.

5.6. Hoe vindt de opvolging plaats bij gesignaleerde tekortkomingen?

Hiervoor lopen geen aparte projecten. In de kwartaalrapportage informatiebeveiliging vindt de verantwoording plaats over de onderhanden activiteiten om verbetermaatregelen te implementeren. Het betreft hier o.a.

- de opvolging van gemelde potentiële datalekken,
- status van de implementatie van de aanbevolen verbetermaatregelen uit de gap analyse van 2014;
- de opvolging van de geconstateerde tekortkomingen uit de ENSIA audit (en daarmee de tekortkomingen uit de DigiD assessment en Suwinet audit);
- de voortgang op de implementatie van diverse maatregelen uit hoofde van de AVG.

5.7. Hoe is de monitoring ingericht door de raad?

Er zijn nog geen afspraken vastgelegd over de communicatie vanuit het college b&w over informatiebeveiliging aan de Gemeenteraad. Wel is vastgesteld dat in verband met een significant incident (potentieel datalek) er communicatie is geweest vanuit het college b&w en de CISO naar de

Gemeenteraad via een Raad informatiebrief (RIB). Jaarlijks wordt via het jaarverslag in een paragraaf informatieveiligheid de gemeenteraad geïnformeerd door het college.

6. IMPLEMENTATIE AVG

Binnen het door ons uitgevoerde vooronderzoek is ook navraag gedaan naar de aanpak en status van het AVG compliant maken van de gemeente Laarbeek.

Vanaf januari is een extern ingehuurde deskundige bezig met de implementatie van diverse maatregelen op het gebied van privacy. De afgesproken voornaamste activiteiten zijn:

- Opzetten en zo compleet mogelijk maken van een Register van verwerkingen;
- Opzetten en regelen van Verwerkersovereenkomsten met verwerkers waar verwerkingen van persoonsgegeven van burgers uit de gemeente Laarbeek plaatsvinden. Indien Laarbeek van dezelfde verwerkersorganisatie gebruik maakt die dan meteen meenemen.
- Bewustwording binnen de organisatie vergroten.

Recent zijn er 2 FG's (Functionarissen gegevensverwerking) in dienst getreden bij de GR (Gemeenschappelijk regeling Peelgemeenten). Inzet van de FG's loopt via de GR in de vorm van een samenwerkingsovereenkomst tussen de betrokken gemeenten. Één FG is aangewezen voor de GR Peelgemeenten, Laarbeek en Gemert-Bakel. De andere FG voor de andere 3 organisaties in de GR. De FG's vervangen elkaar. De twee FG's zijn bezig met een inventarisatie van de huidige situatie en status bij de gemeenten waaronder ook de gemeente Laarbeek.

1. Er is geen privacybeleid. Deze is wel in ontwikkeling maar nog niet voltooid. Inschatting eind 2018 beschikbaar.

2. Bij het inventariseren van de verwerkingen van persoonsgegevens vindt een risico inschatting plaats. Dat gebeurd in samenspraak met de eigenaar (verantwoordelijke) van de verwerking. De risico inschatting wordt vastgelegd in het Register van verwerkingen (vertrouwensklasse). Er bestaan geen algemene richtlijnen voor de wijze van risicobepaling.

3. De identificatie van (potentiële) verwerkingen van persoonsgegeven of wijzigingen daarop zijn nog geen voorgeschreven aandachtspunt in het wijzigingenbeheerproces. Er is nog geen proces ingericht om vast te stellen voor welke verwerkingen een DPIA (Data Protection Impact Assessment) verplicht is en op welke wijze dan is uit te voeren. De DPIA is het handvat om privacy by design en privacy by default aantoonbaar te implementeren. In het onderhanden Register van verwerkingen staat bij een groot aantal verwerkingen dat nog geen DPIA is uitgevoerd.

4. Classificatie richtlijnen van de vertrouwelijkheid of gevoeligheid van persoonsgegevens en verwerkingen daarvan ontbreken nog. In het Register van verwerkingen is een classificatie aangebracht van:
   - Openbaar;
   - Vertrouwelijk;
   - Bedrijfsvertrouwelijk;
   - Geheim.

   En diverse afgeleide 'vertrouwensklassen'. De impact van deze classificatie is verder nog niet uitgewerkt.

5. Een Register van verwerkingen is beschikbaar en wordt nu aan de hand van de inventarisatie gecompleteerd. Hierbij is gestart vanuit het bestaande overzicht van verwerkingen en is door gesprekken met verantwoordelijke verwerkers meer in detail in kaart gebracht welke verwerkingen aanwezig zijn. Per verwerking zijn gegevens vastgelegd over o.a.:
   Doel van de verwerking, verwerkingsverantwoordelijke, aard verwerkte gegevens, betrokkenheid BSN, (wettelijke)grondslag, bewaartermijn, soort verwerking, eventueel betrokken derde partij,

aanwezigheid van een verwerkersovereenkomst, vertrouwensklasse en of er een DPIA (Data Protection Impact Assessment) is uitgevoerd.
Van een aantal verwerkingen is nog niet bekend welke bewaartermijn van toepassing is of nog niet vastgesteld.
Er zijn verwerkingen waar gemeente Laarbeek gebruik maakte van cloudservices van Wetransfer en Dropbox. Wij hebben begrepen dat dit per ultimo oktober 2018 is vervangen door FileCap, deze hebben wij verder in het onderzoek niet betrokken.
In een apart overzicht houdt de Gemeente Laarbeek bij voor welke derde partijen een verwerkersovereenkomst is afgesloten en of deze voldoet. Het compleet maken van dit register is nog onderhanden maar naar verluidt ver gevorderd. De ingehuurde deskundige is deze ook aan het completeren. Nog niet voor alle relevante derde partijen is volgens het overzicht een adequate verwerkersovereenkomst afgesloten.

6. De voortgang rapporteert de externe deskundige aan de CISO. Dit gebeurt niet op basis van (performance) indicatoren (zoals bv. aantal verwerkersovereenkomsten definitief / onderhanden versus totaal aantal betrokken derden organisaties).

   De verantwoorde status over Q2:

Nr	Actie	Status
1.	Meldplicht datalekken	√
2.	Leidende toezichthouder	√
3.	Functionaris gegevensbescherming	√
4.	Rechten van betrokkenen	√
5.	Bewustwording	√
6.	Data protection impact assessment	√
7.	Verwerkersovereenkomsten	O
8.	Overzicht verwerkingen	O
9.	Privacy by design en by default	O
10.	Toestemming	X

7. De verwerkingen van persoonsgegevens in het sociaal domein zijn geïnventariseerd en opgenomen in het Register van Verwerkingen. Naar verluidt is dit deel van de inventarisatie van verwerkingen afgerond.

8. Er bestaat nog geen proces voor het actueel houden van het Register van verwerkingen. In het wijzigingen beheer proces zijn nog geen maatregelen getroffen voor het expliciet identificeren van verwerkingen van persoonsgegevens of wijzigingen op bestaande verwerkingen.

9. Het aantal verwerkingen met Hoog risico is 10.

10. De gemeente Laarbeek beschikt over een Datalekprotocol. Overigens verwijst dit protocol naar een centraal emailadres en een contactpersoon (nog aan te passen met nieuwe FG's). Het protocol verwijst nog naar de WBP en behoeft nog een update voor de AVG. Dit is als een actie benoemd voor de extern ingehuurde deskundige.

11. Een standaardprocedure voor situatie dat betrokkenen aanspraak maken op hun rechten volgens de AVG (rectificatie, verwijderen, opvragen van verwerkingen) is onderhanden. Bij de afstemming van de conceptbevindingen is dit afgerond en is een schema van het onderliggende werkproces en beschikbare registratieformulier opgeleverd. Daarnaast zijn er formulieren bij de balie die uitleg

geven over welke gegevens de gemeente verwerkt met welk doel en kan een betrokkene online een verzoek doen.

12. In het register datalekken zijn ook de potentiële datalekken opgenomen. Tevens bevat dit register de (eventuele) meldgegevens aan de AP en informatie over het inlichten van betrokkenen. (Potentiële) datalekken staan ook vermeld in de kwartaalrapportage informatiebeveiliging. [zie eerdere bevindingen over deze vastlegging en het protocol]

13. Recente activiteiten, gericht op het realiseren van meer bewustzijn van het belang van de verwerkingen van persoonsgegevens en de daarvoor noodzakelijke procedures, hebben betrekking op informatie op intranet, de kennismeeting over de AVG (juni 2018), de registratie van privacy gerelateerde meldingen in het register (potentiële) datalekken en de afhandeling daarvan.

14. (Potentiële) datalek incidenten komen binnen op centrale emailadressen en worden vervolgens door de CISO (straks FG) vastgelegd in het register en van daaruit behandeld volgens het datalekprotocol.

BIJLAGE 1: GEBRUIKTE BEGRIPPEN EN AFKORTINGEN

Afkorting / begrip	Toelichting
BIG	Baseline Informatiebeveiliging Gemeenten. Het is de minimumnorm voor informatiebeveiliging bij gemeenten. Het is een baseline voor het vaststellen, onderhouden en formuleren van strategische beleid (Strategische BIG), uitwerking van richtlijnen en maatregelen (Tactische BIG).
BIO	Baseline Informatiebeveiliging Overheid. Deze baseline zal diverse sectorale baselines binnen de overheid vervangen en is gebaseerd op de internationale best practice voor informatiebeveiliging ISO 27001:2013. De aangekondigde in werking treden is 1 januari 2019.
IBD	'Informatiebeveiligingsdienst'. De IBD is de sectorale CERT/CSIRT *(Landelijk opererend team dat in actie komt bij beveiligingsincidenten)* voor alle Nederlandse gemeenten en onderdeel van de Vereniging Nederlandse Gemeenten (VNG). De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD beheert de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling. https://www.informatiebeveiligingsdienst.nl .
ISMS	'Information Security management System'. Dit is een managementsysteem voor informatiebeveiliging en gaat uit van de zogenaamde PDCA cyclus (Plan, Do, Check, Act). Generieke stappen daarin zijn vast te stellen wat bedrijfskritiek is en het uitvoeren van een risicoanalyse (Plan), vaststellen wat moet je verbeteren (Do), verifiëren of er voldoende maatregelen zijn (Check) en hoe acteer je op eerdere stappen, verbeter je de organisatie, het proces, de techniek en het handelen van medewerkers (Act)? Continu anticiperen en verbeteren is het uitgangspunt om goed te kunnen acteren op steeds veranderende dreigingen.
AVG	'Algemene verordening gegevensbescherming'. Engels: General Data Protection Regulation (GDPR). Dit is een Europese verordening (dus met rechtstreekse werking) die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert. Per 25 mei 2018 zijn deze regels afdwingbaar.
GR	Gemeenschappelijke regeling. Deze bestaat voor de peelgemeenten waarin meerdere gemeenten waaronder Laarbeek samenwerken op diverse (beleids)terreinen.
DPIA	Data Protection Impact assessment. Een DPIA geeft inzicht in de aard en het doel van de verwerking en de daarmee samenhangende risico's voor de beveiliging van persoonsgegevens op basis waarvan vervolgens maatregelen worden gedefinieerd om het risico zoveel mogelijk te beperken en vast te stellen of de verwerking wel is toegestaan. Kort gezegd is de DPIA de basis voor het, ook door de AVG verplichte, privacy by design. Voor gemeenten (overheid) voorgeschreven.
AP	De Autoriteit Persoonsgegevens. Deze houdt toezicht op de naleving van de AVG en daarmee verbonden regelgeving.
Informatiebeleid	Beleid met het geheel van doelstellingen, uitgangspunten en richtlijnen voor het omgaan met informatie en informatietechnologie binnen een organisatie.
Informatiebeveiligingsbeleid	Beleid gericht op het nemen van passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen, dat de gemeente voldoet aan relevante wet en regelgeving.
SUWINET	Suwinet is een digitale infrastructuur die is ontwikkeld door en om ervoor te zorgen dat, de Suwipartijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak. Er worden alleen gegevens uitgewisseld voor zover daar een wettelijke grondslag voor is.
Topdesk	Tooling voor het vastleggen van te behandelen (gebruikers)vragen waaronder ondersteuning in het gebruik, nieuwe aanvragen, melden van incidenten etc. De tooling ondersteunt de workflow rond de (aantoonbare) afhandeling van deze vragen.

DigiD	DigiD staat voor Digitale Identiteit. Burgers hebben een DigiD en kunnen daarmee inloggen op websites van de overheid en in de zorg. Periodiek dient de beveiliging van deze toegang door middel van een DigiD Assessment door een onafhankelijke deskundige te worden getoetst.
CISO	Centraal information Security Officer. Een functionaris die zich binnen de organisatie bezig houdt met de coördinatie van de werkzaamheden rond informatiebeveiliging en hierover verantwoording afdraagt aan de portefeuillehouder informatiebeveiliging in het college van b&w.
FG	Functionaris gegevensbescherming. Een door de AVG verplicht gestelde functie die binnen de organisatie toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming.