

# Rapportage van BIG naar BIO

*Hoeveer zijn we?*

**DEFINITIEF**

*Deze rapportage bij voorkeur digitaal lezen  
of in kleur printen*

Concerncontrol  
Juli 2019



## **Inhoud**

### **1. Inleiding**

### **2. Conclusie**

#### **2.1 Algemene reactie CIO**

### **3. Aandachtsgebieden bij onze audit**

#### **3.1 Wat rapporteren wij per aandachtsgebied?**

### **4. Overzicht van de bevindingen**

## **Bijlagen**

### **I. Timeline 2017-2020**

### **II. Status ontvangen documenten**

# 1. Inleiding

## Aanleiding voor de audit

Gemeenten hanteren sinds 2013 de Baseline Informatiebeveiliging Gemeenten (BIG) als normenkader. Rijk, Waterschappen en Provincies hanteren hun eigen respectievelijke normen (de BIR, BIWA en IBI). Deze zijn nu samen met de BIG gebundeld in de Baseline Informatiebeveiliging Overheid (BIO). Deze nieuwe baseline wordt het nieuwe normenkader voor alle overheden. De BIO is een doorontwikkeling, ofwel een 'update', van de huidige BIG. Gemeenten baseren hun informatiebeveiligingsbeleid en hun verantwoording aan de gemeenteraad en de toezichthouders vanuit het Rijk (middels ENSIA) op deze BIG. Werkzaamheden die voor de BIG zijn verricht zijn al grotendeels in lijn met de BIO. De BIO wordt op 1 januari 2020 van kracht. In 2019 kunnen gemeenten zich voorbereiden op de overgang van de BIG naar de BIO.

Eindhoven heeft eind 2017 door Deloitte een GAP-analyse uit laten voeren op het normenkader van de BIG. Hieruit kwam naar voren dat nog veel werk moest worden verzet om aan de richtlijnen van de BIG te voldoen.

Bovenstaande vormt de aanleiding voor Concerncontrol (CC) om na te gaan in hoeverre de acties uit de GAP-analyse inmiddels zijn gevorderd en hoever Eindhoven is met de voorbereiding op de overgang van BIG naar BIO.

## Scope

Gemeentebrede implementatie van de Baseline Informatiebeveiliging Gemeenten (BIG) (Vanaf 1 januari 2020 overgaand in de Baseline Informatiebeveiliging Overheid (BIO)).

## Gehanteerde criteria

Als normenkader zijn de door de Informatiebeveiligingsdienst Gemeenten (IBD) ter beschikking gestelde kaders en richtlijnen.

## Aanpak

- Het onderzoek is uitgevoerd in mei en juni 2019;
- De werkzaamheden zijn uitgevoerd op basis van documentenonderzoek en interviews met betrokken medewerkers;
- De uitkomsten van de audit worden afgestemd met de direct betrokken medewerkers, de Chief Information Security Officer (CISO) en de Chief Information Officer (CIO);
- De definitieve rapportage wordt uitgebracht aan de CIO en de directeur Bedrijfsvoering. Eventuele aanwijzingen uit deze rapportage zullen in de periodieke DR-rapportage worden gerapporteerd aan de Directieraad.

## 2. Conclusie

### Conclusie

Uit ons onderzoek is gebleken dat Eindhoven nog *niet klaar* is om aan per 1 januari 2020 aan de Baseline Informatiebeveiliging Overheid (BIO) te voldoen maar ook *geen inzicht* heeft in *wat er nog moet gebeuren*. Er is *geen planning* met mijlpalen tijdslijnen waarop gestuurd kan worden omdat nog niet inzichtelijk is wat er moet gebeuren, hoe we dit gaan doen en welke middelen hiervoor noodzakelijk zijn.

### Aanwijzing 1

Geef de CIO de opdracht om actief te sturen op het effectueren van de organisatie-inrichting rondom informatiebeveiliging.

### Aanwijzing 2

Voer op basis van de vergelijking tussen BIG en BIO en nieuwe GAP-analyse uit om te inventariseren wat nog moet gebeuren om aan de BIO te voldoen. Verwerk deze vervolgens in de planning zoals bedoeld bij aanwijzing 3.

### Aanwijzing 3

Geef de CIO de opdracht een projectorganisatie BIO in te richten en stel o.b.v. de uitgevoerde GAP-analyse BIO een planning op (prioriteer op basis van risico-inschatting) en rapporteer periodiek over de voortgang van deze planning aan de Directeur Bedrijfsvoering.

## 2.1 Algemene reactie CIO

### Algemene reactie CIO

De afgelopen jaren zijn we bezig geweest om de BIG uit 2013 te implementeren. Dit betreft 303 maatregelen om onze beveiliging verder te professionaliseren. Daar hebben we onder andere Deloitte voor ingehuurd. Helaas moeten we constateren dat hetzelfde Deloitte de door hun collega opgestelde stukken niet goed vond. Informatiebeveiliging op orde krijgen is geen eenvoudige opgave. Informatiebeveiliging is nadrukkelijk een lijnverantwoordelijkheid, ondersteund door de ISO's en CISO-team. Om die reden sluiten we ook aan bij de ontwikkeling van procesgericht werken, zodat de procesgerichte risico-analyses waar de BIO met name om vraagt, direct meegenomen kunnen worden. Ook willen we aansluiten bij het periodieke risico-analyse traject van concerncontrol ism met de domeinen.

Het informatiebeveiligingsbeleid is onlangs geactualiseerd en daarmee een kapstok van het daarvan afgeleide beleid. Het meeste daarvan is in concept aanwezig en zal, na een beperkte update, worden vastgesteld.

Voor wat betreft het belangrijke IAM/IDU beleid vind nu een review plaats door de projectorganisatie.

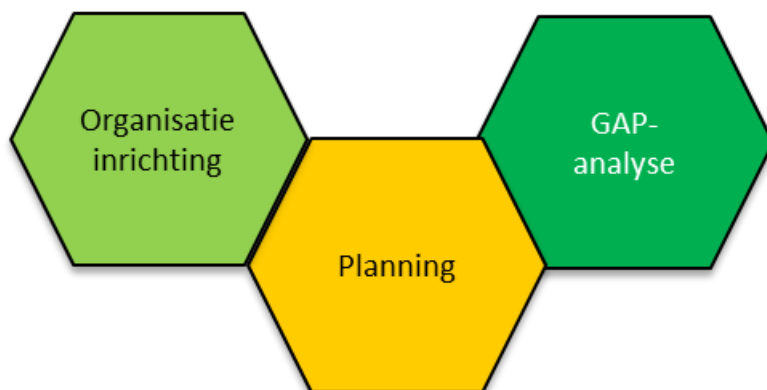
Voor wat betreft de BIG maatregelen hebben we weer een aantal maatregelen de afgelopen periode beschreven. Belangrijke aanwijzing uit de BIG-GAP analyse was immers dat de maatregelen vaak wel plaatsvonden, maar niet beschreven waren. Daarnaast is veel aandacht en tijd naar de ENSIA-rapportage en audit gegaan, waar we succesvol uit zijn gekomen.

De bezetting blijft nog een aandachtspunt. Nu de kadernota is geaccordeerd is de verwachting dat de bestaande capaciteit van 4 medewerkers in stand kan blijven. De beperkte capaciteit blijft een risico, door het uitvallen van de securitymanager de afgelopen 3 maanden, is er op onderdelen weinig voortgang geboekt.

De afgelopen periode is op de realisatie van de BIG maatregelen gestuurd, immers daarop liepen we nog achter. De verandering naar de BIO laat onverlet zo was de gedachte, dat de BIG-maatregelen op inhoud nog steeds van waarde zijn. Immers het gaat om de daadwerkelijke maatregelen in de praktijk. Eind 2020 was de planning om BIG compliant te zijn. Voor de BIO zal dat niet eerder zijn. De omslag naar de BIO betekent vooral ook een veel meer risicogerichte aanpak.

### 3. Aandachtsgebieden bij onze audit

#### Van BIG naar BIO



### 3.1. Wat rapporteren wij per aandachtsgebied?

<b>Bevinding</b> De bevindingen die we hebben voor het betreffende aandachtsgebied	<b>Onderwerp</b> Het onderwerp dat extra aandacht vereist binnen het aandachtsgebied
<b>Sterke punten</b> Volgens ons is dit een werkwijze die als voorbeeld kan dienen voor de organisatie/het proces/het project.	<b>Verbeterpunten</b> Volgens ons is dit een punt waarop het proces verbetering behoeft en/of kan leren van andere sectoren.*
<b>Reactie verantwoordelijke</b> De reactie van de verantwoordelijke op de aanbeveling.	<b>Zaken die niet worden genoemd</b> Dit rapport betreft een uitzonderingsrapportage. Indien in dit rapport niet wordt ingegaan op zaken die in hoofdstuk 1 als aandachtpunt zijn genoemd, hebben wij hierbij geen zwaarwegende bevindingen.
<b>Aanwijzing of aanbeveling?</b> <ul style="list-style-type: none"><li>• Aanwijzingen: dit zijn dusdanige tekortkomingen die wij tevens aan de directieraad rapporteren .</li><li>• Aanbevelingen: hierbij heeft het sector/project of procesmanagement vanuit zijn verantwoordelijkheid voor het beheer binnen de sector de vrijheid om te beslissen of een aanbeveling wordt opgevolgd of dat andere maatregelen worden getroffen om het gesignaleerde risico te beperken.</li></ul>	

## 4.1 Overzicht van de bevindingen

Organisatie  
inrichting

### Organisatie

De Chief Information Security Officer (CISO) functie is momenteel gepositioneerd binnen de CIO-office binnen de sector Strategie en wordt aangestuurd door de Chief Information Officer (CIO). In de afgelopen periode zijn er veel wisselingen (4 in de afgelopen 3 jaar) geweest in de CISO functie. In 2017 is de CISO functie voor 2 dagen in de week uitgevoerd door een externe medewerker, in 2018 is de functie tot en met december full time vervuld door een vaste medewerkers. In 2018 zijn er 2 full time medewerkers ter ondersteuning toegevoegd aan de CISO. In eerste instantie was dit tijdelijk inmiddels is dit geformaliseerd. In december 2018 is de CISO-functie weer vacant geworden. Vanaf maart 2019 is de functie weer vervuld door een vaste medewerker. In 2018 zijn er binnen de verschillende sectoren Information Security Officers (ISO) aangesteld. Maandelijks vindt er overleg plaats op basis waarvan de ISO's informatiebeveiliging in de sectoren onder de aandacht kunnen brengen en hun dilemma's en ervaringen kunnen bespreken. Zij voeren deze taak uit naast hun bestaande werkzaamheden. In 2018 speelde met name de inrichting van deze structuur en de opleiding van de betreffende medewerkers. In bijlage 1 is een tijdslijn geschetst van de situatie van de afgelopen 3 jaar.

### Sterk punt

Inrichting CISO organisatiestructuur met een vaste CISO, 2 beleidsmedewerkers en ISO-functionarissen in de sectoren.

### Onderwerp

Effectueren organisatie-inrichting rondom informatiebeveiliging

### Verbeterpunten

De organisatie-inrichting rondom informatiebeveiliging is opgezet. Na een aantal wisselingen op sleutelposities en tijdelijke invulling van functies is het nu zaak om daadwerkelijk en gestructureerd te gaan werken conform de structuren, taken en verantwoordelijkheden.

### Aanwijzing 1

Geef de CIO de opdracht om actief te sturen op het effectueren van de organisatie-inrichting rondom informatiebeveiliging.

### Reactie CIO

Bij het vaststellen van het informatiebeveiligingsbeleid in het DSO zijn ook de verantwoordelijkheden en de voorgestelde structuur benoemd. Het management is verantwoordelijk voor zijn eigen processen en ook voor de risico-analyse en informatiebeveiliging van elk proces. Het management wordt daarin ondersteund door ISO's en door een CISO team van 4 medewerkers. Van dat CISO team is de financiering van 2 medewerkers opgenomen in de kadernota. De definitieve financiering is pas bij de begroting geregeld.



## 4.2 Overzicht van de bevindingen

GAP-  
analyse

### Overzicht bevindingen

Eind 2017 heeft Deloitte een GAP-analyse uitgevoerd op basis van de BIG. Op basis hiervan is in 2018 een globale planning opgesteld om de (aanzienlijke) knelpunten die hieruit naar voren zijn gekomen op te lossen. Uit de GAP analyse bleek onder andere dat het in 2017 opgestelde informatiebeveiligingsbeleid, wachtwoordbeleid en cloudbeleid niet voldeden aan de eisen van de BIG en moesten worden geactualiseerd.

Het *informatiebeveiligingsbeleid* is in 2018 geactualiseerd en begin 2019 vastgesteld door het college. Een nieuw *toegangsbeveiligingsbeleid* (inclusief wachtwoordbeleid) is inmiddels opgesteld maar moeten nog worden vastgesteld. CC heeft dit beleid gereviewed en heeft hierbij nog een aantal opmerkingen/vragen. Deze zijn gedeeld met de CIO en CISO.

Naast deze knelpunten stonden er nog andere knelpunten in de GAP-analyse zoals het *Identity Access Management* (IAM). Hiervoor is in 2018 een project gestart. In Q2 2019 is hiervoor een externe partij (Atos) ingehuurd. Volgens de roadmap van dit project is in Q4 2019 de IAM applicatie geconfigureerd.

Daarnaast zijn er nog voor diverse andere onderwerpen concept beleidsstukken aanwezig. In bijlage II staat een overzicht van deze documenten met de versiedatum en de status en een globale beoordeling door CC. Hieruit blijkt dat er stukken in diverse stadia aanwezig zijn maar dat het definitief maken van de beleidsstukken niet vaak voorkomt. Ook worden stukken niet altijd door de juiste personen gereviewed en /of niet met de juiste aandacht of expertise.

Ten aanzien van andere knelpunten zoals *continuïteitsbeleid*, *ontwikkeling* en *onderhoud*, en *fysieke beveiliging* zijn nog beperkt of geen acties in gang gezet. Er is binnen de CIO office een globaal overzicht van de status van de knelpunten uit de BIG GAP-analyse. Echter gezien het feit dat vanaf 1 januari 2020 de BIO geldt is het niet meer zinvol de knelpunten uit de GAP-analyse verder op te lossen.

Er wordt nu zoals hierboven beschreven gekeken wat de verschillen zijn tussen BIG en BIO en dan geïnventariseerd wat er nog moet gebeuren om te voldoen aan de BIO. Echter gezien het grote aantal knelpunten blijkt de GAP-analyse en de beperkte voortgang /afronding hiervan is de verwachting dat nog veel moet gebeuren om aan de BIO te voldoen.

## 4.2 Overzicht van de bevindingen

GAP-  
analyse

### Overzicht bevindingen

Onderwerp	Verbeterpunten
GAP-analyse BIO	Een GAP-analyse op basis van de vergelijking tussen BIG en BIO om te inventariseren wat er nog moet gebeuren om aan de BIO te voldoen is nog niet aanwezig.
Reviewproces	Stuur strak op het opstellen van beleid inclusief het reviewproces. Betrek de juiste medewerkers, stel strakke deadlines en schaal waar nodig op indien mensen niet (tijdig) reageren.
Implementatie BIO	Investeer niet meer in het voldoen aan de BIG maar richt aandacht en capaciteit op de nieuwe richtlijnen van de BIO.

### Aanbeveling 1

Richt het beleidsontwerp-proces (inclusief review) strak in met mijlpalen en een duidelijke planning. Betrek de juiste mensen en stuur strak op de deadlines.

### Aanwijzing 2

Voer op basis van de vergelijking tussen BIG en BIO en nieuwe GAP-analyse uit om te inventariseren wat nog moet gebeuren om aan de BIO te voldoen. Verwerk deze vervolgens in de planning zoals bedoeld bij aanwijzing 3.

### Reactie CIO

De CISO komt eind volgende week met een (concept) plan van aanpak

## 4.3 Overzicht van de bevindingen - Planning

Planning

### Overzicht bevindingen

Er is geen planning waarin staat wat er wanneer moet gebeuren om de overgang van BIG naar BIO te realiseren. Om een realistische planning op te kunnen stellen wordt door de CISO geïnventariseerd wat de verschillen zijn tussen BIG en BIO. Vervolgens wordt gekeken wat er al is en wat nog gerealiseerd moet worden en kan op basis daarvan een planning worden opgesteld.

De implementatie van de BIO is nog niet expliciet belegd binnen de organisatie.

Onderwerp	Verbeterpunten
Implementatie BIO	Richt een projectorganisatie BIO in met de CISO als projectleider. Sluit hier vwb de risicogerichte aanpak aan bij de werkgroep procesmanagement. De beleidsmatige en IT kant kunnen worden afgedekt door de CISO-medewerkers en de Security Manager.
Planning	Stel een plan van aanpak op met concrete mijlpalen en tijds- en resource planning en stuur hierop.

### Aanwijzing 3

Geef de CIO de opdracht een projectorganisatie BIO in te richten en stel obv de uitgevoerde GAP- analyse BIO een planning op (prioriteer op basis van risico-inschatting) en rapporteer periodiek over de voortgang van deze planning aan de Directeur Bedrijfsvoering.

### Reactie CIO

De CISO is expliciet systeem-verantwoordelijk voor de BIG. De vervanging van de BIG door de BIO verandert daarin niets. De CISO komt eind volgende week met een (concept) plan van aanpak.

## **Bijlagen**

- I.     Timeline 2017-2020**
- II.    Status ontvangen documenten**

# Timeline implementatie BIG -BIO

Wat is er tot nu toe gebeurd?

## 2017

### Ontwikkeling



Gemeenten moeten zich voor het eerst **verantwoorden** over de **volle breedte** van de **BIG**

**GAP -analyse** uit laten voeren door Deloitte

Externe ingehuurd CISO voor 2 dagen per week

Opstellen **beleid**:  
informatiebeveiligings-  
beleid  
wachtwoordbeleid

## 2018

### Ontwikkeling



Verantwoording op basis van de **BIG**

Opzet CISO organisatie door **aanwijzen SO-functionarissen** bij sectoren  
**Herzien** Informatiebeveiligingsbeleid en wachtwoordbeleid  
Start **IAM** project

Nieuwe vaste full time CISO ondersteund door 2 full time medewerkers (**tijdelijk**) en de ISO's in de sectoren.

## 2019

### Ontwikkeling



Verantwoording op basis van de **BIG**.  
**BIG wordt BIO** van 1 januari 2020 verantwoording op basis van BIO.

Opzet CISO organisatie door **aanwijzen SO-functionarissen** bij sectoren  
**Vaststelling** Informatiebeveiligingsbeleid  
**Herzien** wachtwoordbeleid  
**Inventarisatie** impact overname naar **BIO**

Vanaf Q2 vaste full time CISO ondersteund door 2 full time medewerkers en de ISO's in de sectoren.

## 2020

### Ontwikkeling



Verantwoording op basis van de **BIO**.

**BIO** Baseline Informatiebeveiliging Gemeenten  
**ENSIA** Eenduidige Normatiek Single Information audit  
**BIG** Baseline Informatiebeveiliging Overheid  
**CISO** Chief Information Security Officer  
**SO** Security Officer  
**IAM** Identity Access Management

## II. Status ontvangen documenten

Onderwerp	Ontvangen documenten	Versie	Versiedatum	Status	Opmerking CC
Algemeen beleid	Informatiebeveiligingsbeleid Gemeente Eindhoven	1.0	maart 2019	Definitief	Goedgekeurd door college
Toegangsbeveiliging	Beleid-logische-toegangsbeveiliging	Voorbeeld van IBD			
	Toegangsbeveiliging beleid	0.5	maart 2019	Concept	CC heeft gereviewed in juli 2019 opmerkingen/vragen staan nog open
Identity Access Management	IAM beleid Gemeente Eindhoven strategisch	0.9	maart 2018	Concept	Status van deze documenten in relatie IAM/IDM project is niet duidelijk. Is nog geen vastgesteld beleid documenten lijken deels te overlappen. Niet duidelijk of dit is afgestemd met de organisatie. In elk geval niet met CC.
	IAM beleid Gemeente Eindhoven tactisch	0.9	maart 2018	Concept	
	Toelichting IAM beleid Gemeente Eindhoven	0.9	maart 2018	Concept	
	Raamwerk IDU+IAM	4	februari 2019	Concept	
Mobiele gegevensdragers	Mobiele-gegevensdragers	Voorbeeld van IBD			
	Mobiele Apparaten Beleid	1.0	april 2017	Definitief	Beleid is in 2017 opgesteld door toenmalige CISO van Deloitte maar is niet toepasbaar in huidige organisatie.
	Mobile Device Management (MDM)	0.3	februari 2019	Concept	Onder contractie/Eerste concept nog niet afgestemd met de organisatie.
Inkoopvoorwaarden	Informatiebeveiligingseisen tbv Inkoopvoorwaarden	0.2	januari 2019	Concept	Onder contractie/Eerste concept nog niet afgestemd met de organisatie.
Beveiligingsbeleid	Beveiligingsbeleid	?	februari 2019	Concept	Onder contractie/Eerste concept nog niet afgestemd met de organisatie.
Incidentmanagement	PB-Incidentmanagement-Proces	?	januari 2016	Definitief	Is document van I&B niet zichtbaar afgestemd op BIG maatregelen (mn tav security incidenten).
Personele beveiliging	Personele beveiliging	?	oktober 2018	Concept	Afgestemd met P&O, geen uitgebreide review door CC