



EINDHOVEN

Status implementatie Baseline Informatiebeveiliging Gemeenten (BIG)

gemeente Eindhoven

CTRL - Control, CCA - Concern Control en Advies

maart 2017

Colofon

Uitgave

Gemeente Eindhoven

CTRL - Control, CCA - Concern Control en Advies

Datum

maart 2017

Inhoudsopgave

	Colofon	2
	Inhoudsopgave	3
1	Conclusie en aanbevelingen	4
1.1	Conclusie	4
1.2	Aanbevelingen	4
2	Inleiding	6
2.1	Toelichting Baseline Informatiebeveiliging Gemeenten	6
2.2	Doelstelling onderzoek	7
2.3	Scope	7
2.4	Onderzoeksaanpak	7
3	Bevindingen en Aanbevelingen	8
3.1	Organisatie en planning	8
3.2	Strategische Baseline: Welke onderdelen zijn gerealiseerd?	9
3.2.1	Beleid	9
3.2.2	Verantwoordelijkheden	10
3.3	Tactische Baseline: Welke onderdelen zijn gerealiseerd?	11
3.4	Verantwoording afleggen over de BIG	11
	Bijlage 1 Infographic van VNG over ENSIA	12

1 Conclusie en aanbevelingen

1.1 Conclusie

Uit het onderzoek komt naar voren dat:

*de gemeente Eindhoven **onvoldoende** is voorbereid op de met VNG overeengekomen implementatie van de Baseline Informatiebeveiliging Gemeenten (BIG).*

Deze conclusie is gebaseerd op onderstaande bevindingen:

- Er zijn geen expliciete verantwoordelijkheden benoemd. De interim CISO-officer voelt en neemt wel de verantwoordelijkheid maar gezien zijn beperkte aanwezigheid binnen de organisatie (1 dag per week) is het onmogelijk om naast de ad hoc opspelende zaken ook de implementatie van de BIG uit te voeren.
- Er is geen gemeentebrede GAP-analyse uitgevoerd: hierdoor is niet bekend wat er nog moet worden gedaan om aan de normen van de Baseline Informatiebeveiliging te voldoen en dus ook niet of het mogelijk is de implementatie van de BIG in 2017 te realiseren.
- Er is geen integraal implementatieplan met bijbehorende periodieke rapportages over de voortgang.

Gezien de omvang van de normen uit de Baseline Informatiebeveiliging Gemeenten is het met de huidige personele bezetting binnen de CIO-office voor deze taak onmogelijk om de doelstelling ten aanzien van de implementatie van de BIG te halen.

Een direct gevolg hiervan is dat bij de verplichte zelfevaluatie over de BIG die eind 2017 moet worden ingeleverd Eindhoven niet voldoet aan de normen. Dit is uiteraard van invloed op de inhoud van de collegeverklaring Informatieveiligheid die in Q1 2018 moet worden opgesteld.

Kanttekening

In aanvulling op het bovenstaande valt op dat het ontbreekt aan duidelijke en actieve sturing op informatiebeveiliging en dat er gemeentebreed onvoldoende intrinsiek urgentie- en verantwoordelijkheidsbesef is over het onderwerp. Als het al op de agenda staat is het vooral omdat er een externe aanleiding voor is zoals de BIG richtlijnen, een accountantsrapportage en dergelijke.

Overigens wil het niet realiseren van de Baseline Informatie Beveiliging niet meteen zeggen dat gemeente Eindhoven de gehele informatiebeveiliging niet op orde heeft. Uit bijvoorbeeld de DIGID audit blijkt dat met name de technische beveiliging van voldoende niveau is en ook uit de Suwinet audits blijkt dat we voor die applicatie voldoen aan de gestelde normen. Daarentegen blijkt uit de managementletter en de onderzoeken van concerncontrol dat er op het gebied van informatiebeveiliging dingen verbeterd kunnen worden zowel beleidsmatig als bij de inrichting en de uitvoering van onze werkzaamheden.

1.2 Aanbevelingen

Om de implementatie van de BIG in 2017 succesvol af te kunnen ronden is het essentieel om op zeer korte termijn:

1. De verantwoordelijkheden voor de implementatie van de BIG duidelijk te benoemen en te beleggen (rekening houdend met de nieuwe ENSIA¹-verantwoordingsrichtlijn);
2. Een projectorganisatie implementatie BIG op te richten met daarin vertegenwoordigers van de belangrijkste betrokken organisatie-onderdelen (CIO-office, Sociaal Domein, Ruimtelijk Domein, Bedrijfsvoering (P&O, I&B)).

¹ ENSIA staat voor Eenduidige Normatiek Single Information Audit zie hoofdstuk 3.4 voor een toelichting

3. Op korte termijn een gemeentebrede GAP-analyse uit te voeren en basis hiervan een implementatieplan opstellen;
4. Maandelijks te rapporteren aan de directeur Bedrijfsvoering over de voortgang van de implementatie van BIG en ENSIA en dit ook te agenderen voor de DR.

en ***

2 Inleiding

Gemeenten zijn voor steeds meer beleidsterreinen verantwoordelijk. Zij maken daarbij gebruik van de mogelijkheden van informatie-uitwisseling. Door informatie te delen en processen te optimaliseren kunnen gemeenten onder andere hun dienstverlening beter organiseren, de veiligheid van burgers verbeteren en meer mensen aan het werk krijgen.

Als professionele organisatie past hierbij dat gemeenten ook de beveiliging van informatie professioneel organiseren. Informatie moet immers beschikbaar en betrouwbaar zijn en mag alleen door bevoegden in te zien zijn. Bij de uitwisseling van gegevens moeten gemeenten voldoende rekening houden met beveiligings- en privacyaspecten. Informatieveiligheid is veel meer dan ICT, het gaat in veel gevallen om de mens in de organisatie en de manier waarop deze met risico's omgaat. Is de medewerker zich bewust van die risico's? Zijn bestuurders zich bewust van de risico's van en voor de organisatie? In de kern raakt informatievoorziening en -veiligheid de legitimatie van het werk van de gemeentelijke bestuurders. Het is namelijk niet alleen een technische vraag maar ook een politieke en bestuurlijke. Het raakt de bedrijfsvoering van de gemeente en vraagt daarom om een bestuurlijke visie, focus en draagvlak. Om informatieveiligheid te garanderen zal iedere gemeentelijke organisatie daarom actie moeten ondernemen. Zowel technisch als organisatorisch.

In de Baseline informatiebeveiliging Gemeenten (BIG) staat op hoofdlijnen beschreven op welke manier gemeenten hun informatiebeveiliging inrichten. In 2013 hebben alle Nederlandse gemeenten zich gecommitteerd aan de BIG als normenkader voor informatiebeveiliging. Eindhoven is medio 2014 gestart met de implementatie van de BIG. De implementatie moet eind 2017 afgerond zijn en vormt de basis voor de in 2018 op te stellen collegeverklaring informatiebeveiliging.

2.1 Toelichting Baseline Informatiebeveiliging Gemeenten

De integrale Baseline Informatiebeveiliging Nederlandse Gemeenten bestaat uit drie delen:

en *****

1. BIG – Strategische Baseline

De Strategische Baseline kan gezien worden als de 'kapstok' waaraan de elementen van informatiebeveiliging opgehangen kunnen worden. Centraal staan de organisatie en de verantwoording over informatiebeveiliging binnen de gemeente.

2. BIG – Tactische Baseline

De Tactische Baseline beschrijft de normen en maatregelen ten behoeve van controle en risicomanagement. De Tactische Baseline beschrijft aan de hand van dezelfde indeling als de internationale beveiligingsnorm ISO/IEC 27002:2007, de controls/maatregelen die als Tactische Baseline gelden voor de gemeenten.

3. BIG – Operationele baseline

Om de invoering van de Strategische en Tactische Baseline te ondersteunen, zijn door de IBD producten ontwikkeld op operationeel niveau. Deze producten zijn samen met een groot aantal betrokken gemeenten vervaardigd, vertegenwoordigers van deze gemeenten hebben de producten gereviewd.

2.2 Doelstelling onderzoek

De doelstelling van het onderzoek luidt als volgt:

Ligt de gemeente Eindhoven met de implementatie van de Baseline Informatiebeveiliging Gemeenten (BIG) op schema zodat Eindhoven eind 2017 voldoet aan de richtlijnen uit de BIG?

2.3 Scope

Tijdens dit onderzoek is gekeken naar de strategische en tactische baseline voor informatiebeveiliging. De tactische baseline is een heel gedetailleerd kader. Dit onderzoek heeft niet tot doel in detail te toetsen of Eindhoven voldoet aan dit kader maar om te kijken in hoeverre de implementatie van de baseline op schema ligt.

Ook de operationele baseline is niet meegenomen in dit onderzoek omdat deze afgeleid is van de strategische en tactische baseline.

2.4 Onderzoeksaanpak

Het onderzoek is uitgevoerd door het houden van interviews met de interim CISO-officer, de Security Officer Sociaal Domein, en het bestuderen van relevante documentatie.

3 Bevindingen en Aanbevelingen

3.1 Organisatie en planning

Organisatie

De volgende logische stappen zijn belangrijk bij de implementatie van de BIG:

1. Benoem verantwoordelijken.
2. Voer een GAP-analyse uit.
3. Benoem quick wins en voer deze uit, bijvoorbeeld het beschrijven en implementeren van procedures.
4. Maak een integraal implementatieplan (Information Security Management System - ISMS) en begin met periodiek rapporteren over de voortgang.

Hieronder volgt per stap de situatie binnen de gemeente Eindhoven:

Benoem verantwoordelijkheden:

Binnen de gemeente Eindhoven zijn de verantwoordelijkheden voor de implementatie van de BIG niet duidelijk benoemd en belegd. Er is geen opdrachtgever, er is geen opdrachtnemer en er is ook bijvoorbeeld geen projectteam opgericht. Vanuit de sector Strategie houdt de CISO-officer werkzaam bij de CIO-office zich bezig met deze taak. Deze functie is momenteel echter niet structureel ingevuld maar wordt voor 1 dag in de week ingevuld door een externe medewerker. Gezien deze beperkte invulling is het onmogelijk om structureel aandacht te besteden aan de implementatie van de BIG.

Recentelijk is er een werving- en selectieprocedure gestart om de functie in te vullen.

Binnen het sociaal domein zijn door de security officer (samen met de security manager van de sector I&B en de ingehuurd CISO-officer) wel al enige stappen gezet om waar mogelijk voor het sociaal domein maatregelen te nemen om aan de BIG te voldoen.

Lastig hierbij is dat veel gemeentebreed beleid nog niet aanwezig is (zie hiervoor 3.2).

Voer een GAP-analyse uit:

De GAP-analyse geeft antwoord op vragen als: 'Waar zijn we nu' en 'Waar willen we heen'. Door deze uit te voeren weet de gemeente wat er gedaan moet worden om de BIG ingevoerd te krijgen. Op basis hiervan kan een implementatieplan worden opgesteld en kunnen de actiehouders beginnen met het invoeren van maatregelen en hierover periodiek in de managementrapportages rapporteren.

Er is geen gemeentebrede GAP-analyse uitgevoerd. Binnen het sociaal domein is een beperkte GAP-analyse uitgevoerd. Deze is gebaseerd op de tactische baseline uit de BIG maar moet gezien worden als een eerste aanzet en is niet een volledige GAP-analyse zoals bedoeld in de BIG.

Quick wins benoemen en uitvoeren

Quick wins zijn niet als zodanig benoemd (in lijn met bovenstaande bevindingen). Wel wordt op een aantal gebieden momenteel beleid ontwikkeld. Dit zijn het informatiebeveiligingsbeleid (zie hoofdstuk 3.2), gemeentelijk cloudbeleid en het project dataclassificatie.

Integraal implementatieplan

Er is geen integraal implementatie plan en dus ook geen planning hoe de implementatie van de BIG plaatsvindt. Hierdoor is het onmogelijk vast te stellen wat er al is gebeurd en wat er nog moet gebeuren. Ook rapportages over de voortgang ontbreken.

3.2 Strategische Baseline: Welke onderdelen zijn gerealiseerd?

Omdat er geen projectplan en planning is konden we deze niet gebruiken om de status van de implementatie van de BIG te bepalen. In onderstaande tabel hebben we de hoofdlijnen van de BIG opgenomen en per onderdeel een inschatting gemaakt van de mate waarop dit onderdeel is gerealiseerd. We zijn hierbij uitgegaan van de Strategische Baseline. Deze kan gezien worden als de 'kapstok' waaraan de elementen van informatiebeveiliging opgehangen kunnen worden. Centraal staan de organisatie en de verantwoording over informatiebeveiliging binnen de gemeente. Deze Strategische Baseline geldt voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.

In paragraaf 3.2.1 en 3.2.2 wordt het oordeel met betrekking tot de mate van realisatie voor beide onderdelen van de Strategische Baseline nader toegelicht.

	Onderwerp BIG	Mate van realisatie	
Beleid	Het College van Burgemeester en Wethouders van een gemeente stelt het informatiebeveiligingsbeleid vast en draagt dit uit.	Er is een concept informatiebeveiligingsbeleid. Dit is nog niet vastgesteld door het college en wordt ook nog niet uitgedragen. De verwachting is dat dit onderdeel in 2017 kan worden afgerond.	
Verantwoordelijkheden	Het lijnmanagement is verantwoordelijk voor de beveiliging van informatiesystemen.	Het lijnmanagement is onvoldoende bewust van de verantwoordelijkheden op het gebied van informatiebeveiliging. De verwachting is dat dit onderdeel niet in 2017 kan worden afgerond.	

Tabel 1 Strategische Baseline

3.2.1 Beleid

Er is een concept informatiebeveiligingsbeleid opgesteld. Dit beleid ligt momenteel ter review bij de verschillende stakeholders binnen de organisatie.

In onderstaande tabel wordt het concept informatiebeveiligingsbeleid vergeleken met de zeven minimale richtlijnen die de strategische baseline stelt aan een informatiebeveiligingsbeleid.

	Richtlijn vanuit strategisch baseline	Aanwezig in concept IB beleid Eindhoven
1	De strategische uitgangspunten en randvoorwaarden die de gemeente hanteert ten aanzien van informatiebeveiliging, waaronder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid.	
2	Het doel van het informatiebeveiligingsbeleid.	

	Richtlijn vanuit strategisch baseline	Aanwezig in concept IB beleid Eindhoven
3	De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden.	
4	De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers.	Niet heel expliciet benoemd.
5	De gemeenschappelijke betrouwbaarheidseisen en normen die voor de gemeente van toepassing zijn.	
6	De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd.	Er is aandacht voor evaluatie (dmv de pdca-cyclus) echter er is geen concrete frequentie bepaald (1 maal per 3 jaar conform tactische baseline)
7	De bevordering van het beveiligingsbewustzijn.	

Tabel 2 Beoordeling onderdeel Beleid uit Strategische Baseline

Het concept informatiebeveiligingsbeleid besteed op hoofdlijnen ook aandacht aan de onderwerpen uit de Tactische Baseline van de BIG.

3.2.2 Verantwoordelijkheden

Het lijnmanagement is verantwoordelijk voor de kwaliteit van de bedrijfsvoering. Die verantwoordelijkheid wordt verticaal in de lijn verdeeld, van organisatietop tot afdelingshoofden. Informatiebeveiliging geldt als een integraal onderdeel van de bedrijfsvoering. Zo is het lijnmanagement ook verantwoordelijk voor informatiebeveiliging. Het begrip lijnmanagement wordt hierbij ruim opgevat, dus kan ook een afdelingshoofd of een manager van een stafafdeling onder het lijnmanagement worden verstaan.

*** en

	Richtlijn voor het lijnmanagement vanuit strategisch baseline	Gerealiseerd in Eindhoven
1	stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast	
2	is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen	
3	controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze maatregelen worden nageleefd.	
4	evalueert periodiek de betrouwbaarheidseisen en stelt deze waar nodig bij.	
5	rapporteert over de implementatie van de maatregelen in de managementrapportages.	

Tabel 3 Beoordeling onderdeel Verantwoordelijkheden uit Strategische Baseline

3.3 Tactische Baseline: Welke onderdelen zijn gerealiseerd?

De tactische baseline bestaat uit een grote hoeveelheid uiteenlopende normen. Hieronder volgt een opsomming van de onderwerpen conform de hoofdstukken van de tactische baseline. Elk hoofdstuk is verdeelt in onderwerpen die elk hun eigen normen bevatten. Uit de eerder genoemde GAP-analyse moet blijken aan welke normen de organisatie al voldoet en aan welke niet en wat er moet gebeuren om wel te gaan voldoen. Zoals gezegd hebben wij bij voor dit onderzoek zelf geen GAP-analyse uitgevoerd. Hierdoor is het onmogelijk om aan te geven in hoeverre de organisatie al dan niet compliant is. Onze inschatting op basis van eerdere onderzoeken (met uiteraard een andere scope) is echter dat er nog veel werk verzet moet worden om compliant te worden. Dit betreft dan enerzijds het opstellen van beleid voor de verschillende onderwerpen maar ook vervolgens ook de naleving van dit beleid en het handhaven ervan.

Onderwerpen uit de Tactisch Baseline informatiebeveiliging
Beveiligingsbeleid
Organisatie van de informatiebeveiliging
Beheer van bedrijfsmiddelen
Personele beveiliging
Fysieke beveiliging en beveiliging van de omgeving
Beheer van communicatie- en bedieningsprocessen
Toegangsbeveiliging
Verwerving, ontwikkeling en onderhoud van informatiesystemen
Beheer van informatiebeveiligingsincidenten
Bedrijfscontinuïteitsbeheer
Naleving

3.4 Verantwoording afleggen over de BIG

Gemeenten leggen verantwoordelijkheid af over hun informatieveiligheid in het jaarverslag, dit is in 2013 afgesproken in de resolutie 'informatieveiligheid, randvoorwaarde voor de professionele gemeente'.

In 2017 gebeurt dit voor het eerst met een nieuwe Audit systematiek: de Eenduidige Normatiek Single Information Audit (ENSIA). Deze nieuwe systematiek maakt het inzicht in de stand van zaken rondom informatieveiligheid gemakkelijker en efficiënter. Met ENSIA wordt de situatie van de gemeente getoetst aan de normen uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)². Concreet moeten gemeenten uiterlijk:

- 5 april 2017 een coördinator ENSIA benoemen en doorgeven aan de VNG/KING;
- 31 december 2017 de antwoorden op de vragen van de zelfevaluatie over de volle breedte van de BIG inleveren;
- Q1 2018 de collegeverklaring informatiebeveiliging opstellen;
- 1 mei 2018 uploaden van het assurance rapport van de externe auditor en de collegeverklaring informatiebeveiliging;
- 15 juli 2018 moet het college verantwoording afleggen over informatieveiligheid aan de gemeenteraad.

Bijlage 1 bevat een infographic van de VNG met het complete tijdspad voor deze verantwoording.

² Tevens geeft de werkwijze invulling aan de verantwoording naar de Rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).

Bijlage 1 Infographic van VNG over ENSIA

