

Aan:	Gemeenteraad van de gemeente Tilburg
Van:	College van burgemeester en wethouders
Betreft:	Ensia verantwoording informatieveiligheid 2018
Datum:	9 april 2019

Inleiding

Het college van burgemeester en wethouders van de gemeente Tilburg legt over het jaar 2018 verantwoording af over de stand van zaken op het gebied van informatiebeveiliging binnen de gemeentelijke organisatie. Dit gaat op basis van de Eenduidige Normatiek Single Information Audit (= ENSIA) systematiek.

Doelstelling

ENSIA heeft tot doel het verantwoordingsproces over informatieveiligheid te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke planning & control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hier ook beter op sturen.

ENSIA neemt de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie. Hierdoor is er meer overzicht over de informatiebeveiliging van de gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad en andere belanghebbenden.

Scope van de ENSIA verklaring

De ENSIA verantwoording voor het jaar 2018 gaat over onderstaande onderdelen:

- Implementatie van de Baseline Informatiebeveiliging Gemeenten (BIG);
- Structuur Uitvoeringsorganisatie Werk en Inkomen (Suwinet);
- Digitale Persoonsidentificatie (DigiD);
- Basis Registratie Personen (BRP);
- Paspoort Uitvoeringsregeling Nederland (PUN);
- Basisregistratie Grootchalige Topografie (BGT);
- Basisregistratie Adressen en Gebouwen (BAG);
- Basisregistratie Ondergrond (BRO);





Specifiek voor de onderdelen DigiD en Suwinet is een Assurance verklaring gevraagd van een onafhankelijke en geaccrediteerde IT auditor. Deze IT auditor toetst volgens de landelijke normenkaders over de opzet en het bestaan van beheersmaatregelen. Dit laatste wordt door de verticale toezichthouders Logius, BKWI en de Inspectie SZW vereist. De overige onderdelen bestaan uit een zelfevaluatie, een door de betrokken medewerkers zelf ingevulde digitale vragenlijst.

Verantwoording over de BRO is in 2018 nieuw. Deze verantwoording is dit jaar voor gemeenten nog niet verplicht. Gemeente Tilburg heeft deze zelfevaluatie uitgevoerd als NUL-meting. Het doel hiervan is inzicht krijgen in de te nemen stappen die vertaald zijn naar een implementatieproject.

Ensia verantwoording

Onderstaande tabellen geven per (ENSIA) onderdeel een korte toelichting met bevindingen en de stand van zaken.


Legenda:



			
In Control	Voldoende	Onvoldoende	Geen verplichting
Het onderdeel is in control Wellicht zijn er minimale verbeterpunten	Het onderdeel is globaal op orde (net) in control Er zijn een aantal verbeterpunten	Het onderdeel is niet in control Er zijn veel verbeterpunten, het is niet geborgd.	Verantwoording is niet verplicht Resultaat is gebruikt als (eigen) NULmeting





Verantwoording per onderdeel ENSIA


Onderstaande tabel geeft per (ENSIA) onderdeel een korte toelichting, bevindingen en de stand van zaken weer.

Voor de leesbaarheid is per onderdeel met behulp van smileys de status per onderdeel weergegeven. Per onderdeel zijn ook de bevindingen kort uitgewerkt ter onderbouwing van de status.

Domein Onderdeel	Bevindingen	Status
Implementatie Baseline Informatiebeveiliging Gemeenten (BIG)	<p>Gemeente Tilburg is al enkele jaren bezig met de implementatie van de BIG. Er zijn al veel beheersmaatregelen geïmplementeerd. De landelijke opgave was dat alle 302 beveiligingsmaatregelen bij iedere gemeente geïmplementeerd zouden worden.</p> <p>Dit is niet haalbaar en iedere organisatie heeft uiteindelijk naast gezamenlijke uitdagingen, doelen en dreigingen ook eigen uitdagingen.</p> <p>Over het geheel gezien is informatieveiligheid bij de gemeente Tilburg voldoende geborgd. Dit blijkt ook uit externe audits. Toch blijven er aandachtspunten die middels een Plan Do Check Act (PDCA) worden opgepakt.</p> <p>In 2019 zal de BIG vervangen worden door de Baseline Informatiebeveiliging Overheid (BIO) die vanaf 2020 verplicht gesteld is voor alle overheden. De BIO geeft meer ruimte aan organisaties om op basis van een eigen risico afweging keuzes te maken in het implementeren van beheers en beveiligingsmaatregelen. Hierbij zal een klein pakket aan generieke maatregelen voor iedere (overheid)organisatie verplicht blijven.</p> <p>Vanaf 1 januari is de functie van CISO (Coördinator Informatiebeveiliging) fulltime ingevuld. Deze CISO gaat in 2019 aan de slag met de implementatie van de BIO. Daarnaast zijn bewustwording, organisatiebrede governance (taken, bevoegdheden en verantwoordelijkheden op het gebied van informatieveiligheid) en een integrale verantwoording speerpunten.</p> <p>Naast de functie van CISO is er vanaf 1 januari ook een fulltime Functionaris Gegevensbescherming aangesteld. Hij zal zich richten op het toetsen van de naleving van de AVG. Speerpunten voor 2019 zijn het verwerkingsregister, verwerkersovereenkomsten en de transparantie-eisen.</p> <p>Informatieveiligheid en privacy zijn onderwerpen die sterk afhankelijk van elkaar met als groot gezamenlijk speerpunt het de bewustwording in onze organisatie.</p>	

	Daarom trekken de CISO en FG vaak samen op.	
Domein Onderdeel	Bevindingen & verbeteracties	Status
Basis Registratie Personen (BRP)	<p>Processen en Uitvoering:</p> <p>De zelfevaluatie BRP (processen en uitvoering) over het jaar 2018 is afgerond met een score van 83,3%. Dit is volgens de landelijke norm "net onvoldoende".</p> <p>Kwaliteit inhoudelijke BRP:</p> <p>Voor dit jaar is de score voor de inhoudelijke kwaliteit van de BRP op een aantal onderdelen nog onvoldoende.</p> <p>Als het werkproces onjuist wordt uitgevoerd gaat dit ten koste van de kwaliteit van de BRP. De steekproef is uitgevoerd over persoonslijsten die de afgelopen 10 jaar in de BRP zijn opgenomen. Verbeteringen in het proces en kwaliteit zijn daardoor pas langzaam zichtbaar en hebben geen directe invloed op persoonslijsten uit het verleden.</p> <p>De score is momenteel onder het gewenste niveau omdat:</p> <ul style="list-style-type: none"> • Er het afgelopen jaar onvoldoende aandacht is geweest voor de controle op een juiste uitvoering van de processen. • Er soms (bron)documenten ontbreken in een dossier waardoor het geheel niet administratief op orde is. • Er slordigheidsfouten gemaakt worden bij met name speciale tekens (diakrieten) in namen. Deze worden dan verkeerd overgenomen uit (bron) documenten. <p>De impact voor onze inwoners is niet direct kritisch of zichtbaar. Later bij bijvoorbeeld het aanvragen van een reisdocument of uittreksel komen dit soort fouten uit. Op dat moment is dit vervelend omdat de inwoner geconfronteerd wordt met onjuiste gegevens en dit op dat moment eerst gecorrigeerd moet worden door de medewerker.</p> <p>Er is inmiddels gestart met een intensieve controle op mutaties in de BRP. Door deze controles worden fouten tijdig opgemerkt en gecorrigeerd.</p>	
Paspoort Uitvoeringsregeling Nederland (PUN)	<p>De zelfevaluatie PUN over het jaar 2018 is afgerond met een score van 94,4% Eindresultaat is het oordeel is "ruim voldoende".</p> <p>De processen en uitvoering rondom het aanvragen, beheren en uitreiken van paspoorten en identiteitsdocumenten is goed op orde.</p> <p>Voor de PUN is gemeente Tilburg niet geselecteerd voor een steekproef.</p>	
Digitale Persoonsidentificatie (DigiD);	<p>Het onderzoek van de externe auditor over DigiD geeft aan dat we goed scoren. Onze website/webwinkel Tilburg.nl voldoet aan de informatiebeveiligingsnormen en het beheer is op orde.</p> <p>Naast de formele audit heeft er ook een technische externe penetratietest plaatsgevonden op de website (Tilburg.nl). De uitkomst van deze test was erg</p>	

	<p>positief, er zijn geen kwetsbaarheden ontdekt. De ontwikkeling en het beheer van Tilburg.nl gaat volledig vanuit intern. Dat we voor het vijfde jaar op rij in één keer slagen voor de audit is een mooie prestatie.</p>	
<p>Basisregistratie Grootchalige Topografie (BGT);</p>	<p>De zelfevaluatie BGT over het jaar 2018 is afgerond met een score van 125 van maximaal 150. Hiermee voldoen we aan de landelijk gewenste minimale norm van 120.</p> <p>De BGT een landelijke uniforme registratie die alleen gemaakt kan worden vanuit een goede samenwerking tussen de diverse bronhouders.</p> <p>Gemeente Tilburg gebruikt de BGT niet als bronbestand, maar genereert de BGT vanuit een geometrische bron-dataset: Kern Registratie Topografie (KRT).</p> <p>De Kernregistratie Topografie is de centrale geometrische registratie waar vanuit alle afnemende registraties zoals BAG, BGT, en BOR voorzien van de juiste geometrische objecten.</p> <p>De interne (bijhoudings)processen zijn zo ingericht dat we voldoen aan de eisen en verplichtingen die de wet BGT voorschrijft.</p>	
<p>Basisregistratie Adressen en Gebouwen (BAG);</p>	<p>De zelfevaluatie BAG over het jaar 2018 is afgerond met de maximale score van 205.</p> <p>Er is sprake van een goed lopend proces, waarbij periodiek afstemming plaatsvindt tussen belangrijke leveranciers van informatie (zoals o. a. omgevingsvergunningen, Geo-Informatie) en afnemers van onze basisgegevens (BRP, woningbouwmonitor etc.).</p> <p>De kwaliteit van de gegevens verbetert door tijdens het gebruik eventuele fouten en/of afwijkingen terug te melden.</p>	
<p>Basisregistratie Ondergrond (BRO);</p>	<p>De wet BRO is op 1 januari 2018 ingegaan. Conform de BRO moeten bronhouders (waaronder wij) gegevens over de ondergrond aanleveren. De implementatie van de BRO gaat landelijk in fasen. De eerste fase moet in 2020 afgerond zijn. Net zoals de meeste gemeenten was in 2018 de implementatie nog niet gestart. Ook was de verantwoording over de BRO nog niet verplicht.</p> <p>Omdat de BRO nog niet is geïmplementeerd, scoort gemeente Tilburg in deze eerste zelfevaluatie automatisch onder de landelijk gewenste norm. Om meer inzicht krijgen in de normen waaraan moet worden voldaan is ervoor gekozen om toch al een zelfevaluatie uit te voeren.</p> <p>Dat nu nog niet aan de norm wordt voldaan betekent dat inwoners via het BRO-loket nog geen gegevens van grondsonderingen en grondwatermeetputten kunnen raadplegen die in opdracht van de gemeente zijn verkregen. Met name grondsonderingen voor kunnen inwoners relevante informatie bevatten, zoals bodemopbouw en –draagkracht. Uit een inventarisatie blijkt dat het in 2018 over een beperkte hoeveelheid gegevens gaat, concreet een zestal locaties over de hele stad.</p> <p>Inmiddels is de implementatie gestart onder begeleiding van de interne projectorganisatie (PPI). Bij de implementatie wordt onder meer gebruik gemaakt van deze zelfevaluatie. Doelstelling is dat bij de volgende BRO-verantwoording wel aan de norm wordt voldaan.</p>	

<p>Gezamenlijke Elektronische Voorzieningen</p> <p>Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).</p>	<p>Suwinet wordt gebruikt voor het uitvoeren van de Participatiewet en voor het uitvoeren van adresonderzoeken (ter verbetering van de Basis Registratie Personen.</p> <p>Het onderzoek van de externe IT auditor geeft aan dat de gemeente Tilburg voldoet aan de wettelijk gestelde eisen en normen in het kader van informatieveiligheid rondom het gebruik en beheer van Suwinet.</p>	
---	---	---