Aan:	College van B&W
Van:	Michiel Broekman CISO en ENSIA-coördinator
Betreft:	ENSIA-verantwoording: stand van zaken informatiebeveiliging gemeente Oss 2021
Datum:	29 maart 2022

Inleiding
Het college van burgemeester en wethouders van de gemeente Oss legt over het jaar 2021 verantwoording af over de stand van zaken op het gebied van informatiebeveiliging in de organisatie. Dit gaat op basis van de landelijke systematiek Eenduidige Normatiek Single Information Audit (ENSIA).

Doelstelling
ENSIA heeft tot doel het verantwoordingsproces over informatiebeveiliging te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke P&C-cyclus. Hierdoor heeft het gemeentebestuur meer inzicht in de stand van zaken van informatiebeveiliging en kan het hier ook beter op sturen.

Scope
De ENSIA-verantwoording voor het jaar 2021 gaat over onderstaande onderdelen:

- Implementatie van de Baseline Informatiebeveiliging Overheid (BIO). Zelfevaluatie;
- Structuur Uitvoeringsorganisatie Werk en Inkomen (Suwinet). Extern onderzoek;
- Digitale Persoonsidentificatie (DigiD). Extern onderzoek;
- Basis Registratie Personen (BRP). Zelfevaluatie;
- Paspoort Uitvoeringsregeling Nederland (PUN). Zelfevaluatie;
- Basisregistratie Grootschalige Topografie (BGT). Zelfevaluatie;
- Basisregistratie Adressen en Gebouwen (BAG). Zelfevaluatie;
- Basisregistratie Ondergrond (BRO). Zelfevaluatie;
- Basisregistratie Waardering Onroerende Zaken (WOZ). Zelfevaluatie.



Illustratie ENSIA-onderdelen en verantwoordingslijn

ENSIA-verantwoording
Onderstaande tabel geeft per onderdeel van ENSIA een korte toelichting met de bevindingen en de stand van zaken. Voor de leesbaarheid is per onderdeel met behulp van smileys de status weergegeven. Per onderdeel zijn ook de bevindingen kort uitgewerkt ter onderbouwing van deze status.

Legenda:

			
Ruim voldoende tot Goed	***Voldoende***	***Net Onvoldoende***	***Onvoldoende***
Het onderdeel is volledig op orde, in control Wellicht zijn er minimale verbeterpunten	Het onderdeel is globaal op orde, in control Er zijn enkele verbeterpunten	Het onderdeel is net niet in control Er zijn meerdere verbeterpunten	Het onderdeel is niet in control Er zijn veel verbeterpunten, bijsturing is nodig

Verantwoording per onderdeel
Onderstaande tabel geeft per onderdeel/domein een korte toelichting, bevindingen en de stand van zaken weer.

Domein Onderdeel	Toelichting, bevindingen & stand van zaken	Status
BIO Implementatie van de Baseline Informatiebeveiliging Overheid	***Strategisch informatiebeveiligingsbeleid*** We hebben gewerkt aan het strategisch informatiebeveiligingsbeleid waarin we de doelen, uitgangspunten, rollen en verantwoordelijkheden beschrijven in het kader van informatiebeveiliging. Risicomanagement speelt een belangrijke rol: door regelmatig risico's te identificeren en te beoordelen kan onze organisatie bewust noodzakelijke maatregelen treffen en tijdelijke risico's of restrisico's accepteren. Het beleid zal de komende drie jaren als paraplu dienen voor al het tactische en operationele beleid. Het beleid is nog niet af en zal begin 2022 opgeleverd worden. ***Mens, proces en techniek*** Informatiebeveiliging gaat over mens, proces en techniek. In plaats van techniek gaat het in veel gevallen om de mens: zijn onze medewerkers zich bewust van hun manier van werken en welke risico's dit met zich meebrengt? ***Mens*** We blijven onze medewerkers bewust maken van het belang van informatiebeveiliging. Via de campagne 'Veilig werk' houden we bijvoorbeeld regelmatig phishingacties, vertellen we over actuele cyberdreigingen en leggen we uit wat we verwachten van onze medewerkers. We hebben een cybercrisis geoefend en ontdekt op welke vlakken we ons kunnen verbeteren als we daadwerkelijk getroffen worden. Verder hebben we meer kennis en slagkracht gekregen door ons informatiebeveiligingsteam uit te breiden met een technisch beveiligingsspecialist. ***Proces*** Informatiebeveiliging maakt steeds meer onderdeel uit van processen, maar dit blijft een aandachtspunt. We zijn gestart met het op orde krijgen van business continuity management (BCM) om de continuïteit van onze kritieke processen te waarborgen bij calamiteiten. Op basis van een aantal strategische uitgangspunten zullen we onze kritieke processen vaststellen waarna de proceseigenaren maatregelen kunnen treffen voor hun kritieke proces. ***Techniek*** Qua techniek hebben we onder andere tweefactorauthenticatie (2FA) ingevoerd, zodat medewerkers behalve een gebruikersnaam en wachtwoord nog een tweede factor nodig hebben in de vorm van een code. Daarnaast blijven we onze systemen voorzien van de	 **Voldoende**

	laatste patches (stukjes software om een fout of kwetsbaarheid op te lossen) en updates en hebben we aandacht voor het maken en terugzetten van reservekopieën. We maken steeds meer gebruik van cloudoplossingen en dat vraagt om een andere benadering van informatiebeveiliging. Net als voorgaande jaren heeft een externe partij een pentest uitgevoerd om te toetsen of er misbruik gemaakt kan worden van eventuele kwetsbaarheden.	
SUWINET Structuur Uitvoeringsorganisatie Werk en Inkomen	Suwinet wordt door ons gebruikt voor het uitvoeren van de Participatiewet, IOAW en IOAZ, adresonderzoeken burgerzaken en voor het uitvoeren van de Wet gemeentelijke schuldhulpverlening. Iedere taak gebruikt een aparte Suwinet-aansluiting. Vanwege de hoeveelheid en gevoeligheid van (persoons)gegevens binnen Suwinet heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties bepaald dat iedere aansluithouder naast de zelfevaluatie ook extern getoetst wordt op naleving van het normenkader. Het (externe) onderzoek rondom het veilig en verantwoord gebruik van Suwinet toont aan dat we voldoen aan de gestelde landelijke normenkaders voor het veilig en integer gebruik van Suwinet-gegevens.	 **Ruim voldoende tot goed**
DIGID Digitale Persoonsidentificatie	DigiD is voor inwoners de manier om zichzelf digitaal te identificeren. DigiD wordt gebruikt voor onze digitale dienstverlening via ons loket Oss.nl en de digitale loketten van burgerzaken en het sociaal domein. Onvoldoende of onjuist beheer van een DigiD-aansluiting kan grote gevolgen hebben voor de landelijke keten en uiteindelijk persoonsinformatie van inwoners. Daarom heeft de toezichthouder bepaald dat iedere DigiD-aansluiting naast een jaarlijkse zelfevaluatie ook (extern) getoetst wordt op naleving van het normenkader. Ontwikkeling en het beheer van onze digitale loketten zijn grotendeels uitbesteed. Het functioneel beheer is intern geregeld. Het externe onderzoek bij zowel onze leveranciers als onszelf toont aan dat er is voldaan aan het landelijk gestelde normenkader voor een veilig beheer van DigiD.	 **Ruim voldoende tot goed**
BRP Basisregistratie Personen	BRP is de basisregistratie waarin alle inwoners zijn geregistreerd. Gemeenten beheren deze BRP voor hun inwoners. Uiteindelijk worden alle BRP-registraties landelijk gekoppeld zodat overheidsinstanties, zorgverleners en andere dienstverleners die gebruik mogen maken van deze BRP beschikken over de juiste persoonsinformatie. Vanwege het grote landelijke belang rondom de BRP zijn gemeenten verplicht om jaarlijks een zelfevaluatie uit te voeren. Deze zelfevaluatie bestaat uit twee onderdelen. **Processen en Uitvoering:** De zelfevaluatie BRP (processen en uitvoering) over het jaar 2021 is afgerond met een score van 93,4%. Dit is boven de landelijk gestelde norm van minimaal 90%. **Inhoudelijke BRP:** Ook de inhoudelijke controle op de kwaliteit van onze Basis Registratie Personen is met een prima resultaat afgerond.	 **Ruim voldoende tot goed**
PUN Paspoort Uitvoeringsregeling Nederland (Reisdocumenten)	Gemeenten verzorgen de aanvraag en het uitreiken van reisdocumenten voor hun inwoners. Reisdocumenten zijn erg waardevol en vaak de sleutel van identiteitsfraude. De processen rondom het aanvragen en uitreiken zijn daarom strikt. De burgemeester is verantwoordelijk voor de borging van deze processen en moet hierover jaarlijks verantwoording afleggen aan de minister van Binnenlandse Zaken en Koninkrijksrelaties. Via de ENSIA-verantwoording infomeren we ook het eigen bestuur over de stand van zaken. De zelfevaluatie PUN over het jaar 2021 is afgerond met een score van 93,5%. Hiermee voldoen we aan de landelijk gestelde norm van minimaal 90%. Processen en de uitvoering rondom het aanvragen, beheren en uitreiken van reisdocumenten zijn op orde. De	 **Ruim voldoende tot goed**

	beveiligingsfunctionaris reis- en waardedocumenten heeft in de rapportage 'Informatiebeveiliging PNIK aan de burgemeester' vijf aandachtspunten benoemd.	
BGT Basisregistratie Grootschalige Topografie	De BGT is een digitale kaart van Nederland waarop gebouwen, wegen, waterlopen, terreinen en spoorlijnen eenduidig zijn vastgelegd. Kortom: de inrichting van de fysieke omgeving. Gemeenten zijn als bronhouder mede verantwoordelijk voor de kwaliteit van deze landelijke basisregistratie. Net als alle andere bronhouders verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BGT. De zelfevaluatie BGT over het jaar 2021 is afgerond met een score van 77%. Hiermee voldoen we aan de landelijk gestelde norm van minimaal 75% voor een positief resultaat. In 2020 was de score 97% . Dit is voldoende en daarmee is onze BGT een betrouwbare basisregistratie. Voor de BGT zijn in 2021 wat achterstanden ontstaan door een capaciteitstekort bij de afdeling IBOR-VS. Inmiddels is binnen deze afdeling een halve FTE-uitbreiding toegezegd. *De volledige BGT rapportage is te vinden in de bijlage "Verantwoordingsrapportage ENSIA BAG-BGT-BRO Gemeente Oss 2021" .*	 **Voldoende**
BAG Basisregistratie Adressen en Gebouwen	De BAG bevat gemeentelijke basisgegevens van alle adressen en gebouwen in een gemeente. Kopieën van al deze gegevens zijn verzameld in een landelijke voorziening. Deze voorziening wordt landelijk gebruikt door overheden, organisaties en particulieren. Net als alle andere bronhouders verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BAG. De zelfevaluatie BAG over het jaar 2021 is afgerond met een score van 82%. Deze score ligt boven de landelijk gestelde norm van minimaal 75% voor een positief resultaat. In 2020 was de score 83%. De BAG is daardoor een betrouwbare basisregistratie. In 2021 was het verwerken van de definitieve pandgeometrie een aandachtspunt. We halen nu geen 100% omdat voor een aantal panden het meer dan 6 maanden duurt voordat de definitieve geometrie voor de BAG beschikbaar komt. In het eerste half jaar is het werkproces verbeterd waardoor minder panden de termijn van 6 maanden overschreden. *De volledige BAG rapportage is te vinden in de bijlage "Verantwoordingsrapportage ENSIA BAG-BGT-BRO Gemeente Oss 2021" .*	 **Ruim voldoende tot goed**
BRO Basisregistratie Ondergrond	De BRO bevat bodem- en ondergrondgegevens. Het gebruik van deze gegevens is de laatste decennia sterk toegenomen. Deze gegevens spelen een cruciale rol op uitvoerend niveau, maar zijn ook van belang bij het oplossen van maatschappelijke vraagstukken. Daarbij valt onder meer te denken aan het rekening houden met de gevolgen van klimaatverandering, zoals het stijgen van de zeewaterspiegel en bodemdaling. De gemeente is bronhouder voor deze basisregistratie. Net als alle andere bronhouders verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BRO. De zelfevaluatie BRO over het jaar 2021 is afgerond met een score van 94%. Deze score ligt ruim boven de landelijk gestelde norm van minimaal 75% voor een positief resultaat. In 2020 was de score 83%. De BRO is landelijk (bij gemeenten) nog in opbouw. Bij ons zien we een stijgende lijn omdat processen rondom de BRO inmiddels zijn uitgewerkt. De score is erg theoretisch en moet dan ook met enige nuance bekeken worden. Als men kijkt naar de geproduceerde hoeveelheid gegevens die onder de eerste 4 tranches van de BRO valt, is dat weinig te noemen. Dat heeft als gevolg dat er nog weinig ervaring is opgedaan met het uitvoeren van processen. *De volledige BRO rapportage is te vinden in de bijlage "Verantwoordingsrapportage ENSIA BAG-BGT-BRO Gemeente Oss 2021"*	 **Ruim voldoende tot goed**

WOZ Basisregistratie Waardering Onroerende Zaken	De WOZ staat voor Waardering Onroerende Zaken. De WOZ-waarde wordt zowel intern als extern gebruikt. Intern bij het bepalen van de hoogte van verschillende belastingsoorten (onder andere onroerende-zaakbelastingen) en extern door de Belastingdienst (Inkomsten- en vermogensbelasting), Waterschappen en het CBS voor de berekening van de belastingcapaciteit. Gemeenten bepalen de hoogte van de WOZ-waarde. Dit doen ze vanuit de Wet waardering onroerende zaken. Het is van belang dat WOZ-gegevens actueel zijn en op een juiste wijze worden beheerd. Een onjuiste WOZ-registratie resulteert enerzijds in een te hoge kostendoorberekening aan inwoners en bedrijven en anderzijds in een onjuiste opbrengst voor gemeenten en afnemers. Gemeente Oss heeft de taken rondom WOZ-processen uitbesteed aan de Belastingsamenwerking Oost-Brabant (BSOB). De verantwoording over 2021 is geschreven vanuit BSOB. In 2021 is de zelfevaluatie WOZ toegevoegd aan de ENSIA-verantwoording. Deze zelfevaluatie is nog niet gekoppeld aan een normenkader en scorematrix en geeft daarmee nog geen direct waardeoordeel over het beheer en de kwaliteit bij gemeenten. De WOZ-rapportage geeft het bestuur wel een globaal inzicht in de stand van zaken bij de BSOB. *De volledige WOZ-rapportage is te vinden in de bijlage* *"Verantwoordingsrapportage ENSIA WOZ Gemeente Oss 2021"*	**Geen oordeel**