

# Uitvoering ENSIA 2020

Handreiking



## Versiebeheer

Versie	Wijzigingen	Datum
1	Eerste versie	Juni 2020

## VNG Realisatie

Nassaulaan 12  
2514 JS Den Haag

Juni 2020



# Inhoud

1.	Leeswijzer .....	4
2.	Wijzigingen ENSIA 2020 .....	5
2.1.	Zelfevaluatie informatiebeveiliging op basis van de BIO .....	5
2.2.	DigiD.....	5
2.3.	Suwinet.....	5
2.4.	BRP en Reisdocumenten.....	6
2.5.	Waar staat je gemeente .....	6
2.6.	Gewijzigde functionaliteit van de tooling .....	6
3.	Verantwoording ENSIA .....	7
3.1.	Interne verantwoording .....	8
3.2.	Externe verantwoording .....	8
4.	Kenmerken verantwoording per Stelsel .....	10
4.1.	DigiD.....	10
4.2.	Suwinet.....	10
4.3.	BRP en Reisdocumenten.....	11
4.4.	GEO-basisregistraties (BAG, BGT en BRO).....	12
4.5.	Waar staat je gemeente .....	12

# 1. Leeswijzer

**Dit document ondersteunt de ENSIA-coördinatoren van gemeenten bij de uitvoering van het ENSIA-proces over het verantwoordingsjaar 2020.**

Op de website [vngrealisatie.nl/ensia](http://vngrealisatie.nl/ensia) vindt u aanvullend ondersteunende documenten voor de uitvoering 2020, zoals een format voor een intranetbericht, een kick-off presentatie en een format voor een plan van aanpak.

Heeft u bij het lezen van dit document vragen? Neem dan contact op via het centrale telefoonnummer 070 250 2400 of stuur een mail aan [ensia@vng.nl](mailto:ensia@vng.nl)

## 2. Wijzigingen ENSIA 2020

**In dit hoofdstuk zijn de wijzigingen voor het verantwoordingsjaar 2020 ten opzichte van het verantwoordingsjaar 2019 opgenomen.**

### 2.1. Zelfevaluatie informatiebeveiliging op basis van de BIO

#### BIG naar BIO

Er wordt dit jaar voor het eerst verantwoording afgelegd op basis van de Baseline Informatiebeveiliging Overheid (BIO). Deze vervangt de baseline voor gemeenten (BIG). De vragen die zijn opgenomen, zijn gesteld op maatregelniveau. In de toelichting bij de vragenlijst BIO zijn links opgenomen naar de BIO, Suwinet-guidance, wetsartikelen en regelgeving. Op deze manier kunt u direct vanuit de zelfevaluatie de onderliggende wetteksten en regelgeving raadplegen.

#### Specifieke vragen met betrekking tot verantwoording aan het Rijk

Er is een duidelijk onderscheid gemaakt in de vragen voor de interne verantwoording en de vragen/antwoorden die bestemd zijn voor de externe verantwoording aan het Rijk. De BIO-vragenlijst start met een inventarisatie over het gebruik van Suwinet voor niet SUWI-taken (3 vragen). Na het invullen van deze inventarisatie zijn bij de maatregel (indien dit van toepassing is) specifieke vragen over het gebruik van Suwinet voor niet SUWI-taken zichtbaar. Er zijn ook specifieke vraag/antwoord-combinaties opgenomen voor de verantwoording over de Participatiewet/IOAZ en IOAW, de BRP en uitvoering Reisdocumenten.

### 2.2 DigiD

#### Aanpassing testaanpak voor 2 normen

Bij twee normen van het DigiD-normenkader is de testaanpak door NOREA geactualiseerd. Bij de norm **U/WA.05** is het gebruik van TLS versie 1.1 en lager niet langer toegestaan; TLS (vanaf versie 1.2) dient te worden toegepast. Bij **U/PW.03** is het gebruik van HSTS, X-Content-Type-Options, Content-Security-Policy (aangescherpt), en Referrer-Policy is vanaf 2020 verplicht. De wijzigingen zijn opgenomen in de DigiD-guidance die gekoppeld is aan de zelfevaluatie DigiD.

### 2.3 Suwinet

#### Nieuwe verantwoordingsrichtlijn Suwinet

Het normenkader Suwinet is per 1 januari 2020 vervangen door de verantwoordingsrichtlijn Suwinet. Deze is volledig op basis van de BIO opgesteld en is in te zien via de site van BKWI. VNG Realisatie heeft de [guidance](#) bij de verantwoordingsrichtlijn Suwinet opgesteld.

#### Carve-out methodiek voor de audit van de collegeverklaring

Voor Suwinet geldt vanaf dit jaar de carve-out-methodiek voor de audit van de collegeverklaring. Wanneer u gebruik maakt van een TPM van uw serviceorganisaties is de auditor van de collegeverklaring niet verantwoordelijk voor de inhoudelijke toetsing van de ontvangen TPM's. De

verantwoordelijkheden van uw auditor zijn nu gelijk aan die van de toetsing van de ontvangen TPM's van de leveranciers waar u gebruik van maakt voor DigiD. Er is een [toelichting](#) van de carve-out methodiek beschikbaar.

#### [Specifieke vragen met betrekking tot gebruik \(niet\) SUWI-taken](#)

In de BIO-vragenlijst kunt u de antwoorden over de verschillende bevestigingen over het gebruik van Suwinet kwijt. Voorheen was er één vraag met betrekking tot het gebruik van Suwinet opgenomen. Nu kunt u uw antwoorden differentiëren naar het gebruik voor de P-wet/IOAZ/IOAW en (indien u hier gebruik van maakt) voor de bijhouding BRP door Burgerzaken en de gemeentelijk gerechtsdeurwaarders (inning) en wanneer u aangewezen RMC-gemeente bent. Deze vragen zijn verplichte vragen. Zonder het beantwoorden van deze vragen kunt u de BIO-vragenlijst niet inleveren voor 31 december 2020. **Het is belangrijk dat de TPM's van mogelijke samenwerkingsverbanden (ISD/RSD, belastingsamenwerking) op 15 oktober ontvangen zijn, anders kunt u de BIO-vragenlijst voor uw gemeente niet tijdig voor 31 december afronden.**

## 2.4 BRP en Reisdocumenten

#### [Aansluiten op de BIO](#)

De wetgeving voor BRP en Reisdocumenten is op de BIO-maatregelen geplot. In de toelichting vindt u directe links naar de wet- en regelgeving die van toepassing is op de BRP en Reisdocumenten bij deze maatregelen. De wet- en regelgeving prevaleert boven het verplichtend karakter van de BIO.

#### [Rapport met puntentelling per vraag/antwoord](#)

Er is een nieuwe rapportage beschikbaar waarmee de score voor de BRP en Reisdocumenten op vraag/antwoord-niveau getoond wordt. Deze wordt na 1 januari 2021 in het tabblad Rapporten getoond en is gekoppeld aan de BIO-zelfevaluatie.

#### [Toelichting op verantwoordingsproces](#)

De uittreksels die u na 31 december 2020 kunt downloaden, zijn voorzien van een toelichting voor uitvoering van het verantwoordingsproces.

## 2.5 Waar staat je gemeente

De Waarstaatjegemeente (WSJG) vragenlijst is aangepast. De BIG-vragen zijn vervangen door BIO-vragen. De publicatie van deze antwoorden worden in 2021 prominenter op [waarstaatjegemeente.nl](http://waarstaatjegemeente.nl) gepubliceerd onder het onderwerp Openbare Orde en Veiligheid.

## 2.6 Gewijzigde functionaliteit van de tooling

#### [Beheer](#)

De default-inrichting voor de beheerdersomgeving is gewijzigd. Wanneer u een nieuwe gebruiker aanmaakt in ENSIA staan alle rechten nu standaard uit in plaats van aan.

### Signaalfunctie vragenlijst BIO

Wanneer het antwoord op een gemeente-brede vraag (voor de interne verantwoording) 'Nee' is, en u antwoordt vervolgens dat u wel voldoet (antwoord 'Ja') voor de verantwoording aan het Rijk, dan geeft de tooling een signaal dat het antwoord voor de externe verantwoording mogelijk afwijkt van het antwoord voor de interne verantwoording. U kunt beide antwoordmogelijkheden behouden.

## 3 Verantwoording ENSIA

**In dit hoofdstuk wordt ingegaan op de te nemen stappen voor de interne verantwoording ENSIA en de verantwoording aan de toezichthouders van het Rijk.**

Het volgende schema is ondersteunend aan de toelichting in dit hoofdstuk. Er wordt onderscheid gemaakt in de interne verantwoording (via college van B & W naar de gemeenteraad) en de externe verantwoording aan het Rijk. De belangrijkste mijlpalen zijn 31 december, de laatste dag waarop de vragenlijsten van de zelfevaluaties kunnen worden ingediend. En 30 april, de laatste dag waarop de verantwoordingsdocumenten aan de toezichthouders van het Rijk kunnen worden geüpload.

### Zo werkt ENSIA



ENSIA	Verantwoording over informatiebeveiliging aan gemeenteraad	Verantwoording over BRP, Reisdocumenten, Suwinet, DigiD, BAG, BGT en BRO aan toezichthouders
<b>Zelfevaluatie</b>	<ul style="list-style-type: none"> <li>- Informatiebeveiliging binnen gemeente volgens Baseline Informatiebeveiliging Overheid (BIO).</li> <li>- Zelfevaluatie afronden en vastleggen in ENSIA.</li> </ul>	<ul style="list-style-type: none"> <li>- Informatiebeveiliging BRP &amp; Reisdocumenten en Suwinet (BIO).</li> <li>- Informatiebeveiliging DigiD.</li> <li>- Informatiebeveiliging BAG, BGT en BRO.</li> <li>- Zelfevaluatie afronden en vastleggen in ENSIA.</li> </ul>
<b>Opstellen</b>	<ul style="list-style-type: none"> <li>- Rapportage informatiebeveiliging.</li> <li>- Paragraaf verantwoording informatiebeveiliging voor jaerverslag.</li> </ul>	<ul style="list-style-type: none"> <li>- Rapportage BRP en Reisdocumenten.*</li> <li>- Collegeverklaring over Suwinet en DigiD.</li> <li>- Rapportage BAG, BGT en BRO door college B&amp;W.</li> </ul>
<b>Verantwoorden</b>	<ul style="list-style-type: none"> <li>- Rapportage informatiebeveiliging naar gemeenteraad.</li> <li>- Verantwoording informatiebeveiliging in jaerverslag.</li> <li>- College B&amp;W stelt jaerverslag vast.</li> <li>- Gemeenteraad keurt jaerverslag goed.</li> </ul>	<ul style="list-style-type: none"> <li>- Ondertekenen uittreksels BRP en Reisdocumenten.</li> <li>- Audit door gecertificeerde IT-auditor over collegeverklaring Suwinet en DigiD.</li> <li>- College B&amp;W stelt rapportage BAG, BGT en BRO vast.</li> </ul>
<b>Versturen</b>	<ul style="list-style-type: none"> <li>- Het college van B&amp;W stuurt het gemeentelijk jaerverslag aan het ministerie van BZK.</li> </ul>	<ul style="list-style-type: none"> <li>- Gemeentebestuur verstuurt collegeverklaring en bijlagen, assurance rapport, TPM, rapportage BAG, BGT en BRO.</li> </ul>

\* uiterlijk 14 februari 2021 aanleveren via kwaliteitsmonitor.



### 3.1 Interne verantwoording

De interne verantwoording over informatiebeveiliging verloopt via het college van B&W naar de gemeenteraad. De gemeenteraad houdt toezicht op de uitvoering van het gemeentebestuur. Het is belangrijk om de gemeenteraad te informeren over de status van informatiebeveiliging. Zonder de juiste informatie kunnen zij hun toezichthoudende rol niet uitvoeren. Rapporteren over informatiebeveiliging betekent rapporteren over de volledige breedte van de BIO. Vanuit de resolutie is afgesproken om de raad in elk geval via het jaarverslag te informeren. De meeste gemeenten (94,6%<sup>1</sup>) nemen een tekstpassage over informatiebeveiliging in het jaarverslag op. Om de raad op inhoud te informeren, stelt u een rapportage informatiebeveiliging op op basis van de BIO. U biedt deze onder geheimhouding aan. Via de website [vngrealisatie.nl/ensia](http://vngrealisatie.nl/ensia) en via de ensia tooling ([ensia.nl](http://ensia.nl)) vindt u hier passende sjablonen en formats voor.

### 3.2 Externe verantwoording

De informatiebehoefte van de verschillende toezichthouders van het Rijk zijn van een meer gedetailleerd niveau dan het niveau waarop het college de gemeenteraad informeert. De informatie, die nodig is voor deze externe verantwoording, wordt afgeleid uit de zelfevaluaties die u gebruikt voor de interne verantwoording.

Stelsel	Zelfevaluatie	Document	Proces	Uploaden
DigiD	DigiD	Collegeverklaring en bijlage DigiD	<ul style="list-style-type: none"><li>• Opstellen concept collegeverklaring</li><li>• Toetsing door IT-auditor</li><li>• Verklaring laten vaststellen door College</li></ul>	ENSIA.nl
Suwinet	BIO	Collegeverklaring en bijlage Suwinet	<ul style="list-style-type: none"><li>• Opstellen concept collegeverklaring</li><li>• Toetsing door IT-auditor</li><li>• Verklaring laten vaststellen door College</li></ul>	ENSIA.nl
BRP	BIO	Uittreksel BRP	<ul style="list-style-type: none"><li>• Downloaden uittreksel</li><li>• Ondertekenen door burgemeester en gemeentesecretaris</li></ul>	Kwaliteitsmonitor <sup>2</sup>
Reisdocumenten	BIO	Uittreksel Reisdocumenten	<ul style="list-style-type: none"><li>• Downloaden uittreksel</li><li>• Ondertekenen door burgemeester</li></ul>	Kwaliteitsmonitor <sup>3</sup>

<sup>1</sup> Bron: Waarstaatjegemeenten.nl, verantwoording over 2019

<sup>2</sup> Vooralsnog uiterlijk 14 februari 2021. Deze datum kan mogelijk wijzigen gedurende het verantwoordingsjaar als gevolg van wijziging wetgeving.

<sup>3</sup> Vooralsnog uiterlijk 14 februari 2021. Deze datum kan mogelijk wijzigen gedurende het verantwoordingsjaar als gevolg van wijziging wetgeving.

Stelsel	Zelfevaluatie	Document	Proces	Uploaden
<b>BAG</b>	BAG	Bestuurlijke verantwoording	<ul style="list-style-type: none"> <li>• Bestuurlijke verantwoording downloaden en aanvullen</li> <li>• Vaststelling door College</li> </ul>	ENSIA.nl
<b>BGT</b>	BGT	Bestuurlijke verantwoording	<ul style="list-style-type: none"> <li>• Bestuurlijke verantwoording downloaden en aanvullen</li> <li>• Vaststelling door College</li> </ul>	ENSIA.nl
<b>BRO</b>	BRO	Bestuurlijke verantwoording	<ul style="list-style-type: none"> <li>• Bestuurlijke verantwoording downloaden en aanvullen</li> <li>• Vaststelling door College</li> </ul>	ENSIA.nl

De documenten die u laat vaststellen, uploadt u voor 1 mei in ENSIA. U hoeft deze documenten niet ter informatie aan de raad aan te bieden. U informeert hen uiteraard wel over de strekking van de informatiebeveiligingsaspecten uit deze rapportages. Dit doet u via de rapportage informatiebeveiliging (zie 3.1 Interne verantwoording).

## 4 Kenmerken verantwoording per Stelsel

In dit hoofdstuk zijn de kenmerken per stelsel uitgewerkt. Per stelsel is een schema opgenomen met hierin links naar documenten die op onderwerpen verdieping bieden.

### 4.1 DigiD

DigiD	Kenmerkend
<b>Tooling</b>	DigiD-vragenlijst per aansluiting
<b>Toezichthouder</b>	Logius voor BZK
<b>Verantwoording</b>	Via een gecombineerde, getoetste en gewaarmerkte collegeverklaring over Suwinet en DigiD door een IT-auditor TPM's van serviceorganisaties dienen voor 15 oktober ontvangen te zijn.
<b>Documenten</b>	DigiD guidance via <a href="https://ensia.nl">ensia.nl</a>
<b>Let op</b>	Opdracht voor pentest Opdracht IT-auditor Opdracht voor verstrekking TPM's aan leveranciers Testaanpak voor twee normen aangescherpt
<b>Upload ENSIA</b>	1 Collegeverklaring 1 Assurancerapport Bijlage DigiD (x aantal aansluitingen) TPM's

### 4.2 Suwinet

Suwinet	Kenmerkend
<b>Tooling</b>	Verantwoordingsrichtlijn en zelfevaluatie is geïntegreerd in BIO-zelfevaluatie
<b>Toezichthouder</b>	BKWI voor SZW
<b>Verantwoording</b>	Via een gecombineerde, getoetste en gewaarmerkte collegeverklaring over Suwinet en DigiD door een IT-auditor TPM's van serviceorganisaties dienen voor 15 oktober ontvangen te zijn.
<b>Documenten</b>	<a href="#">Suwinet-guidance</a> <a href="#">Toetsing middels carve-out methodiek</a> <a href="#">Interventieprotocol Suwinet</a>
<b>Let op</b>	De gemeente legt verantwoording af over het gebruik van Suwinet, ook als dit bij een serviceorganisatie is belegd. Opdracht IT-auditor

Suwinet	Kenmerkend
	Opdracht voor verstrekking TPM's aan serviceorganisaties voor tijdige aanlevering i.v.m. tijdige verwerking in de BIO-vragenlijst (zijn verplichte vragen!).
	Inventariseer gebruik Suwinet voor niet SUWI-taken <ul style="list-style-type: none"> <li>• Burgerzaken (bijhouding BRP)</li> <li>• Gemeentelijk gerechtsdeurwaarders (vaak belegd bij gemeenschappelijke regeling)</li> <li>• Coördinatiepunt <a href="#">RMC-gemeente</a> (voortijdig schoolverlaters)</li> </ul>
	Inventariseer gebruik DKD-Inlezen (naast Suwinet-Inkijk)
	De toezichthouder ontvangt geen TPM's. De auditor controleert op de ontvangen TPM's tezamen met de normen die in de eigen organisatie zijn getoetst, tezamen het normenkader afdekken.
<b>Upload ENSIA</b>	1 Collegeverklaring 1 Assurancerapport Bijlage Suwinet

### 4.3 BRP en Reisdocumenten

BRP en Reisdocumenten	Kenmerkend
<b>Tooling</b>	Wet- en regelgeving en zelfevaluatie geïntegreerd in de BIO-zelfevaluatie.
<b>Toezichthouder</b>	RvIG voor BZK
<b>Verantwoording</b>	Via te downloaden uittreksels (sjablonen) uit ENSIA
	De uittreksels dienen ondertekend te worden door burgemeester én gemeentesecretaris (BRP) en door de burgemeester (Reisdocumenten).
<b>Documenten</b>	-
<b>Let op</b>	Verbinding met de kwaliteitsmonitor bij Burgerzaken (domeinspecifieke vragenlijsten)
	De uittreksels uit ENSIA zijn voorzien van een stappenplan voor de verantwoording
	Er is na het inleveren van de vragenlijsten (31 december) een rapport beschikbaar met de uitwerking van de puntentelling.
	Afwijkende inleverdatum van verantwoordingsdocumenten van uiterlijk 14 februari.
	Het is mogelijk dat gedurende dit verantwoordingsjaar de inleverdatum wijzigt en in lijn gebracht wordt met de datum die voor de overige verantwoording aan het Rijk geldt, uiterlijk 30 april van elk jaar.
<b>Upload ENSIA</b>	Geen, dit proces verloopt via de kwaliteitsmonitor

#### 4.4 GEO-basisregistraties (BAG, BGT en BRO)

GEO-basisregistraties	Kenmerkend
<b>Tooling</b>	1 vragenlijst per basisregistratie in ENSIA over (data)kwaliteit van de basisregistraties. <ul style="list-style-type: none"> <li>• BAG</li> <li>• BGT</li> <li>• BRO</li> </ul>
<b>Toezichthouder</b>	DGBRW voor BZK
<b>Verantwoording</b>	Via te downloaden bestuurlijke verantwoordingsrapportages per basisregistratie uit ENSIA.nl De verantwoordingsrapportages dienen te worden vastgesteld in het college.
<b>Documenten</b>	-
<b>Let op</b>	Er hoeft geen handtekening op de verantwoordingsrapportages, een vaststellingsdatum door het college volstaat.  De BRO wordt in tranches geïmplementeerd. Wanneer een gemeente niet over deze gegevens beschikt en deze worden ook niet in opdracht ingewonnen, dan hoeft hierover geen verantwoording over te worden afgelegd. U vult de eerste twee inventariserende vragen in binnen de tooling. De vragenlijst zal in dat geval niet verschijnen. Zie ook de toelichting in de tooling.
<b>Upload ENSIA</b>	Voor elke basisregistratie een vastgestelde (en aanvulde) bestuurlijke rapportage.

#### 4.5 Waar staat je gemeente

WSJG	Kenmerkend
<b>Tooling</b>	1 vragenlijst in ENSIA
<b>Toezichthouder</b>	Geen, voortgekomen uit de <a href="#">resolutie</a> "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" tijdens de Buitengewone Algemene Ledenvergadering van de VNG (november 2013)
<b>Verantwoording</b>	Geen
<b>Documenten</b>	Geen
<b>Let op</b>	Deelname is op vrijwillige basis. Bij deelname worden de gegevens gepubliceerd.
<b>Upload ENSIA</b>	Niet van toepassing, de uitkomsten worden openbaar gepubliceerd via <a href="http://www.waarstaatjegemeente.nl">www.waarstaatjegemeente.nl</a> bij het onderdeel 'Openbare orde en Veiligheid'.