ENSIA | Eenduidige Normatiek Single Information Audit

Eén slimme verantwoording voor informatieveiligheid

Handleiding ENSIA-tool

voor gemeenten

Juni 2017, versie 2.0

ENSIA is een initiatief van de VNG en de ministeries van BZK, I&M en SZW

Inhoud

Inleiding

ENSIA heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

ENSIA helpt gemeenten in één keer slim verantwoording af te leggen over informatieveiligheid gebaseerd op de BIG. De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWInet) is samengevoegd en gestroomlijnd.

Uitgangspunt is de horizontale verantwoording aan de gemeenteraad. De horizontale verantwoording vormt de basis voor de verticale verantwoording aan de toezichthouders die een rol hebben in het toezicht op informatieveiligheid. Bij het afleggen van verantwoording wordt het principe van single information audit toegepast.

Handleiding ENSIA-tool gemeenten
De ENSIA-tool ondersteunt de uitvoering van het verantwoordingsproces. Dit document is bestemd voor de **gemeentelijke coördinator ENSIA** en **de gemeentelijke gebruikers** en geeft uitleg over het gebruik van de ENSIA-tool.

1 Toegang tot ENSIA-tool

De ENSIA-tool (beschikbaar na de 'inlog' op www.ensia.nl) ondersteunt de uitvoering van het ENSIA verantwoordingsproces en omvat twee zelfevaluaties:

1) De zelfevaluatie vragenlijst informatiebeveiliging 2017
2) De zelfevaluatie vragenlijst over DigiD-Assessment 2017

Elke gemeente kan inloggen op haar persoonlijke omgeving binnen deze tool. Daar is het mogelijk om de vragenlijsten te beantwoorden, rapportages te genereren en de verantwoordingsdocumenten te uploaden. De tool onderscheidt twee soorten 'toegangsrollen':

Coördinator ENSIA :	is verantwoordelijk voor het intern organiseren van ENSIA. Dat betekent het tijdig uitzetten en inleveren van de vragenlijsten, het generen van rapportages uitvoeren en het uploaden van verantwoordingsdocumenten. Ook is hij beheerder van de gebruikers van de tool.
Gebruiker:	helpt de coördinator bij het invullen van de vragenlijsten en het verzamelen van gegevens. De gemeentelijke coördinator ENSIA wijst gebruikers aan en verleent ze toegang tot de tool.

KING verzamelt per gemeente de contactgegevens van de betreffende ENSIA coördinator. ICTU zorgt er vervolgens voor dat de ENSIA coördinator de inlogcodes ontvangt en beschikt over de juiste rechten.

1.1 Toegang – coördinator ENSIA

- De coördinator ENSIA ontvangt een gebruikersnaam en een automatisch gegenereerd wachtwoord.
- De coördinator ENSIA wordt gevraagd het automatisch gegenereerde wachtwoord te wijzigen in een persoonlijk wachtwoord. Dit gaat door middel van twee-factor authenticatie. Hiervoor wordt gebruik gemaakt van de App Google Authenticator. De App is geschikt voor Windows, IOS en Android.

- De coördinator ENSIA kan nu inloggen op www.ensia.nl
- Vanaf de hoofdpagina (na het inloggen) heeft de coördinator toegang tot zes tabbladen:
  1. Welkom
  2. Invoeren (de vragenlijsten)
  3. Rapporten
  4. Uploaden
  5. Gebruikers
  6. Help (Veel gestelde vragen en contact)

  De gemeentelijk coördinator ENSIA heeft als *enige* toegang tot de tabbladen uploaden en gebruikers en kan de gehele vragenlijst inleveren.

1.2 Toegang – gebruikers

- De coördinator ENSIA kan via het tabblad 'Gebruikers' andere medewerkers binnen de organisatie toegang verlenen tot de tool om te helpen bij het invullen van de gegevens. Denk bijvoorbeeld aan: verantwoordelijken van Bedrijfsvoering (ICT/ HR/Inkoop), Burgerzaken (BRP/PUN), Sociaal Domein (SUWInet), DigiD, BAG-beheer en BGT-beheer.
- De coördinator mag als enige de rechten voor beheer organisatiegegevens toewijzen aan de gebruiker.

De rechten kunnen per BIG-hoofdstuk worden toegekend.

ENSIA Zelfevaluatie - Informatiebeveiliging BIG - 2017

Vragenlijst BIG hs 3: Implementatie van de Tactische Baseline	○ Geen toegang	○ Bekijken	◉ Bewerken
Vragenlijst hs 4: Samenwerkingsverbanden	○ Geen toegang	○ Bekijken	◉ Bewerken
Vragenlijst BIG hs 5: Beveiligingsbeleid	○ Geen toegang	○ Bekijken	◉ Bewerken
Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	○ Geen toegang	○ Bekijken	◉ Bewerken
Vragenlijst BIG hs 7: Beheer van bedrijfsmiddelen	○ Geen toegang	○ Bekijken	◉ Bewerken
Vragenlijst BIG hs 8: Personele beveiliging	○ Geen toegang	○ Bekijken	◉ Bewerken
Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	○ Geen toegang	○ Bekijken	◉ Bewerken
Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	○ Geen toegang	○ Bekijken	◉ Bewerken
Vragenlijst BIG hs 11: Toegangsbeveiliging	○ Geen toegang	○ Bekijken	◉ Bewerken
Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	○ Geen toegang	○ Bekijken	◉ Bewerken
Vragenlijst BIG hs 13: Beheer van Informatiebeveiligingsincidenten	○ Geen toegang	○ Bekijken	◉ Bewerken
Vragenlijst BIG hs 14: Bedrijfscontinuïteitsbeheer	○ Geen toegang	○ Bekijken	◉ Bewerken
Vragenlijst BIG hs 15: Naleving	○ Geen toegang	○ Bekijken	◉ Bewerken
Verklaring College Burgermeester en Wethouders	○ Geen toegang	◉ Bekijken	○ Bewerken
Gegevens inleveren	◉ Niet toestaan		○ Toestaan
Rapportages	○ Niet toestaan		◉ Toestaan

- De gebruiker ontvangt, nadat de coördinator ENSIA hem/haar toegang heeft verleend, een mail met een automatisch gegenereerd wachtwoord.
- De gebruiker wordt gevraagd het automatisch gegenereerde wachtwoord te wijzigen in een persoonlijk wachtwoord. Dit gaat door middel van twee-factor authenticatie.
- De gebruiker kan nu inloggen op www.ensia.nl
- Vanaf de hoofdpagina (na het inloggen) heeft de gebruiker toegang tot drie tabbladen:
  1. Invoeren (de vragenlijsten)
  2. Rapporten
  3. Help (Veel gestelde vragen en contact)

1.3 Toegang - gemeenten in samenwerkingsverband

- De gemeente blijft als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van informatie. Het is aan de portefeuillehouder om hierover binnen de grenzen van het samenwerkingsverband afspraken te maken.
- De ontwikkelde tool biedt vooralsnog geen functionaliteit voor het ondersteunen van samenwerkingsverbanden.
- De coördinator kan ook medewerkers van andere organisaties toegang verlenen tot de tool, bijvoorbeeld medewerkers van een ICT ondersteuningsorganisatie of een ISD.

2 Invoeren zelfevaluatie vragenlijsten

2.1 Tabblad 'Invoeren'

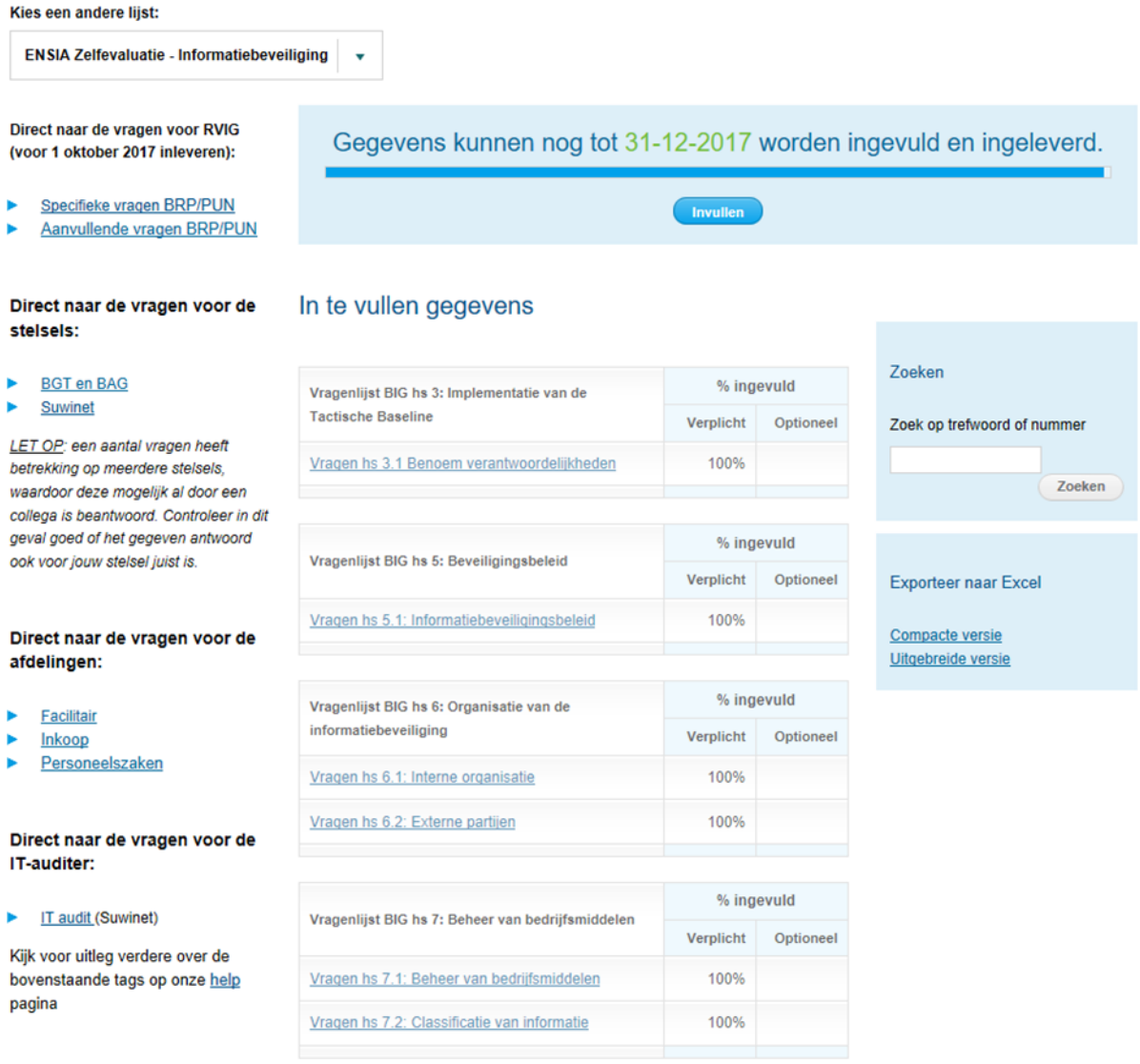
- Onder 'Invoeren' staan de vragenlijsten. Er zijn twee afzonderlijke vragenlijsten:
  1) De zelfevaluatie vragenlijst informatiebeveiliging 2017
  2) De zelfevaluatie vragenlijst DigiD-assessment 2017

2.1.1 Zelfevaluatie vragenlijst informatiebeveiliging 2017

1 De vragenlijst informatiebeveiliging is onderverdeeld **in 15 verschillende hoofdstukken (begint vanaf hoofdstuk 3),** gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) aangevuld met vragen die wettelijk verplicht zijn over de PUN, BRP, SUWInet, BAG en BGT.

2 Alle vragen zijn voorzien van een identieke i-code. Deze code staat onder de vraag. Gebruik dit nummer altijd als je meer informatie wilt hebben over de vraag of vraagstelling.

3 De hoofdstukken van de vragenlijsten **kunnen afzonderlijk van elkaar worden ingevuld** en tussentijds worden opgeslagen. De tool houdt bij welke gebruiker op welk tijdstip de vragen heeft beantwoord. Gebruikers kunnen dit zelf ook zien door op de 'i' te klikken in het opmerkingenveld.



4 Om gebruikers **snel toegang** te geven tot specifieke vragen over PUN, BRP, DigiD, SUWInet, BAG en BGT zijn de vragen voorzien van een ‘tag’ (zie de afbeelding hierboven, linkerkolom). Klikt u op een van deze tags links in beeld, dan filtert de tool de vragen voorzien van de betreffende tag uit alle hoofdstukken. U kunt deze vragen invullen en opslaan. Via de tags, die links van de vragenlijsten, staan zijn de tags aangegeven:

Afdeling/doelgroep	Onderdeel vragenlijst	Tag
Burgerzaken	BRP en PUN	ensia-burgerzaken
(intergemeentelijke) Sociale Dienst	SUWInet	ensia-isd
Bouwen en Wonen	BAG en BGT	ensia-bouwenenwonen
CISO en ICT	DigiD	ensia-ict
IT-auditor	SUWInet en DigiD	ensia-itaudit
Inkoop		ensia-inkoop
Personeelszaken		ensia-hrm
Facilitair		ensia-facilitair

5 Op vergelijkbare wijze is er snelle toegang voor vragen t.b.v. facilitaire zaken, inkoop en personeelszaken.

6 Bepaalde vragen hebben betrekking op verschillende stelsels hierdoor kan het zijn dat sommige vragen **al ingevuld** zijn. Via de 'i' rechts in het toelichtingenveld is zichtbaar welke collega de vraag heeft ingevuld.

7 De **IT-audit** voor 2017 beperkt zich tot DigiD en SUWInet. Deze specifieke vragen zijn via de tag [IT-audit] links in beeld op te vragen.

   a. De vragen worden gecontroleerd door de IT-auditor en zijn voor hem/haar op te vragen via de tag IT-audit links in beeld. Let op: dit kan pas als coördinator de IT-auditor als gebruiker heeft toegevoegd!

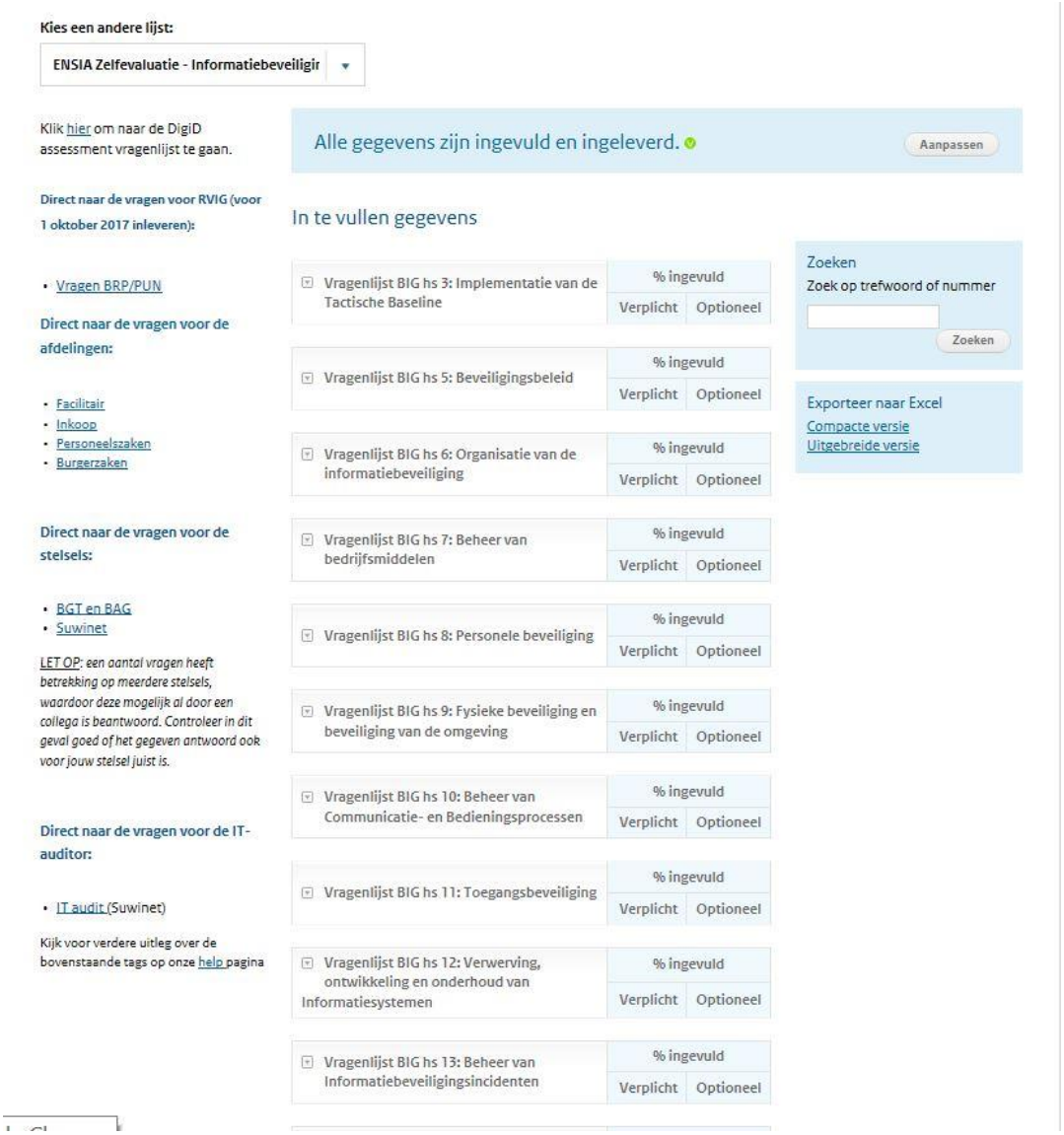
   b. Als de IT-auditor bij de coördinator ENSIA langs komt, dan kan hij/zij van de coördinator een uitdraai van de vragenlijst in Excel krijgen **of** de coördinator voegt de IT-auditor toe met de daar bij horende toegangsrechten.

8 Voor de zelfevaluatie is bij elke vraag aangegeven welke **documentatie** beschikbaar dient te zijn om aan te tonen dat de vraag naar waarheid is beantwoord. In het opmerkingenveld kan een link naar de benodigde documentatie worden opgenomen.

9 Bij elke vraag is er de mogelijkheid om in het **opmerkingenveld** opmerkingen over de vraag te plaatsen. Het veld kan gebruikt worden om over de vraag te communiceren met collega's. De opmerkingen zijn niet zichtbaar in de rapportages. Ook kan het veld gebruikt worden om de auditvragen van extra toelichting te voorzien. De toelichtingen gaan niet mee bij het uploaden

10 **Status invullen.** Op de hoofdpagina van de vragenlijsten is te zien hoe ver u bent met het invullen van de afzonderlijke deelhoofdstukken en met het invullen van alle vragenlijsten bij elkaar.

11 **Afronden en inleveren.** In de statusbalk bovenin is zichtbaar wanneer alle vragen zijn ingevuld. Pas als alle vragen zijn beantwoord wordt, voor de coördinator, de knop 'Inleveren' zichtbaar. Dan kan de coördinator de vragenlijst inleveren.



12 Voor vragen over **Gemeenten die in een samenwerkingsverband** zitten neem contact op met KING.

2.1.2 Zelfevaluatie assessment DigiD 2017

1. Voor DigiD is er een **aparte vragenlijst** voor de zelfevaluatie.
2. De vragenlijst voor DigiD is voorzien van **guidance en toelichting**. Verder is voor DigiD een algemene toelichting beschikbaar.
3. Per DigiD-aansluiting moet een vragenlijst worden ingevuld.
4. De ENSIA-coördinator heeft tot 31 december de tijd om de DigiD vragenlijst in te vullen. Na invulling van de DigiD-vragenlijst dienen de uitkomsten te worden beoordeeld met inachtneming van de ontvangen TPM-verklaringen **per aansluiting**. Deze beoordeling vindt plaats in

een daartoe opgenomen rapportageformat "**Bijlage C**". Dit format is te vinden onder tabblad rapporten, kies vervolgens bij de dropdown menu ENSIA Zelfevaluatie - DigiD Assessment 2017.

In de **Collegeverklaring Informatiebeveiliging** wordt - mede vanwege de vertrouwelijke aard van de informatie - een samenvatting van de bevindingen op hoofdlijnen opgenomen. (zie 3.2. Tabblad 'Uploaden verantwoordingsdocumenten').

Rapportage Template rapportage DigiD Assessment 2017 - Bijlage B + C: dit is een **aparte rapportage** die via de ENSIA-tool aan **de toezichthouder, Logius**, moet worden opgeleverd.

5. **Afronden en Uploaden.** De coördinator levert vóór 1 mei 2018 de gevulde Template rapportage DigiD Assessment 2017 - Bijlage B + C op aan de toezichthouder, samen met de ontvangen TPM's en het Assurancerapport. Voor alle documenten geldt dat dit kan via de ENSIA-tool.

2.1.3 Voor alle vragenlijsten geldt…

- **Ingeleverde vragenlijsten kunnen in principe niet meer worden gewijzigd.** Wilt u bepaalde antwoorden toch nog veranderen, dan dient de coördinator ENSIA contact op te nemen met ICTU via ensia@ictu.nl. Zij zetten de vragenlijsten dan weer open.
- **Exporteren vragenlijsten**. Het is mogelijk om de zelfevaluatie vragenlijsten te exporteren naar een Excel. Zie hiervoor het blauwe kader rechts op de pagina van de betreffende vragenlijsten. Hierbij is de keuze voor de compacte versie of de uitgebreide versie. De compacte versie geeft een overzicht van de vragen en de gegeven antwoorden. De uitgebreide versie geeft een overzicht van de vragen, gegeven antwoorden, routing en toelichting.
- **De deelnemende gemeenten zijn zelf verantwoordelijk voor de kwantiteit en kwaliteit van de ingevoerde data.**

3 Rapporten en uploaden verantwoordingsdocumenten

3.1 Tabblad 'Rapporten'

3.1.1 Voor horizontale verantwoording en eigen gebruik

- Als de zelfevaluatie vragenlijst is ingevuld en ingeleverd, biedt de tool de mogelijkheid om voor eigen gebruik verschillende rapporten te genereren. Het gaat om de volgende rapportages:
  1. Rapportage zelfevaluatie informatieveiligheid. Deze rapportage is bedoeld voor de horizontale verantwoording over informatiebeveiliging. Er is de mogelijkheid om de rapportages te selecteren op de verschillende BIG-hoofdstukken en op stelselniveau:
     a. Rapportage SUWInet
     b. Rapportage BRP en PUN
     c. Rapportage informatieveiligheidsvragen BAG en BGT
  2. Rapportages DigiD
     a. Rapportage DigiD Assessment bijlage B + C

  Let op: de rapportage kan alleen worden gedownload als de vragenlijsten volledig zijn ingevuld én ingeleverd!
  Wel is het mogelijk om een tussentijdse rapportage of de vragenlijsten te exporteren naar een Excel-bestand.
  Via tabblad 'invoeren' kan je de gehele Excel-rapportage downloaden. Hierbij is de keuze voor de compacte versie of de uitgebreide versie. De compacte versie geeft een overzicht van de vragen en de gegeven antwoorden. De uitgebreide versie is een overzicht van de vragen, gegeven antwoorden, routing en toelichting.

3.1.2 Voor verantwoording aan toezichthouders

- Via de ENSIA-tooling stellen gemeenten op digitale wijze rapportages en informatie beschikbaar over de zelfevaluatie, de Collegeverklaring en het Assurance-rapport aan diverse ministeries:
  1. De minister van BZK ten behoeve van het toezicht op de BRP, de PUN en DigiD.
  2. Verder bieden gemeenten via ENSIA transparantie aan de beheerder van de centrale omgeving van de GeVS[1] (BKWI) ten behoeve van het jaarlijks opstellen van een totaaloverzicht van de beveiliging van de GeVS.

[1] GeVS staat voor Gezamenlijke Elektronische Voorzieningen SUWI, en wordt veelal aangeduid als SUWInet.

- De toezichthouders (IenM, BKWI en RVIG) krijgen enkel dat deel van de zelfevaluaties en rapportages te zien dat voor de uitvoering van hun taak noodzakelijk is. Dit gebeurt automatisch. De coördinator ENSIA hoeft hiervoor niets te doen.
- De coördinator ENSIA uploadt de Collegeverklaring Informatiebeveiliging en het Assurancerapport. De Collegeverklaring is nodig en toegankelijk voor het ministerie van SZW. Het Assurance rapport is nodig en toegankelijk voor het ministerie van SZW en BZK (zie 3.2. Tabblad 'Uploaden').
- Zodra de vragenlijsten zijn ingeleverd en de daarbij benodigde documenten zijn geüpload krijgt de toezichthouder een attenderingsbericht. De toezichthouder heeft vanaf dat moment toegang tot de ingevulde vragenlijsten.

3.2 Tabblad 'Uploaden'

Nadat de zelfevaluatie vragenlijsten door de coördinator ENSIA zijn ingeleverd dienen er, om het verantwoordingsproces informatieveiligheid te kunnen afronden, de volgende documenten te worden geüpload.

- **Collegeverklaring informatiebeveiliging**
  Met deze verklaring geeft het college van B en W aan in hoeverre bij de gemeente de beheersingsmaatregelen hebben voldaan aan de voor de ENSIA verantwoording geselecteerde normen en indien aan de orde welke onderdelen daarvan zijn uitgezonderd. Ook wordt melding gemaakt van eventuele verbetermaatregelen die de gemeente gaat treffen. De Collegeverklaring informatiebeveiliging wordt gezamenlijk met het Assurancerapport separaat van het jaarverslag aan de gemeenteraad aangeboden.

- **Assurancerapport IT-auditor**
  Een bij de NOREA geregistreerde IT-auditor controleert de Collegeverklaring en stelt een Assurancerapport op. Deze werkzaamheden van de IT-auditor duiden we ook wel aan als de IT-audit. De IT-auditor verklaart in het Assurancerapport dat de Collegeverklaring een getrouw beeld geeft. Getrouw betekent dat de Collegeverklaring met een redelijke mate van zekerheid juist en volledig is. Deze verklaring van getrouwheid geeft aanvullende zekerheid over de juistheid en volledigheid van de Collegeverklaring. Het Assurancerapport kan alleen als PDF-document worden geüpload.

- **Rapportage DigiD Assessment bijlage B + C**
  Nadat de auditor het Assurancerapport heeft opgesteld kunt u de rapportage over DigiD uploaden.

- **TPM's in kader van DigiD**
  Indien uw gebruik maakt van leveranciers in het kader van DigiD die een TPM verklaring afgeven dan kunt u de TPM verklaringen uploaden. Het is mogelijk om meerdere bestanden na elkaar te uploaden.

In de ENSIA-tool zijn **formats** beschikbaar voor de **Collegeverklaring informatiebeveiliging en het Assurance rapport.**

4 Verantwoording informatiebeveiliging in gemeentelijk jaarverslag

- Het college van B en W neemt in **het jaarverslag** in **de paragraaf Bedrijfsvoering** een **aparte paragraaf op over informatiebeveiliging**.[2] Deze paragraaf omvat informatie over de informatiebeveiliging in brede zin. Hierin rapporteert het college aan haar toezichthouder (de gemeenteraad) over informatiebeveiliging. Deze rapportage vloeit voort uit de afspraken in de gemeentelijke resolutie 'Informatiebeveiliging randvoorwaarde voor een professionele gemeente'. De gemeenteraad stelt de jaarstukken, waaronder het jaarverslag, vast. In de paragraaf informatiebeveiliging verwijst het college naar de Collegeverklaring informatiebeveiliging. De Collegeverklaring informatiebeveiliging maakt geen deel uit van het jaarverslag.[3] Gemeenten kunnen ervoor kiezen om een **separate Rapportage Informatiebeveiliging** aan de gemeenteraad te verstrekken. Deze rapportage omvat zowel de informatie over informatiebeveiliging in brede zin als de Collegeverklaring ENSIA. In dit geval kan in het jaarverslag kort verwezen worden naar deze separaat uitgebrachte rapportage. Een aantal gemeenten kiest nu al voor deze behandeling omdat zij verwacht een grotere aandacht voor het onderwerp in de raadsbehandeling te krijgen. Een separate rapportage waarbij het College van B en W alle informatie over de informatiebeveiliging in samenhang aan de gemeenteraad voorlegt, verdient dan ook de voorkeur.

[2] Resolutie Informatieveiligheid, randvoorwaarde voor de professionele gemeente, BALV 29-10-2013: "Gemeenten zorgen voor verankering van informatieveiligheid op de gemeentelijke agenda, waarbij het college de gemeenteraad informeert. Dit gebeurt door middel van een aparte paragraaf informatieveiligheid in het jaarverslag".
[3] Om ongewenste samenloop met regelgeving voor accountants te voorkomen, is vooralsnog gekozen voor het niet opnemen van de door IT-auditor gecontroleerde Collegeverklaring in het jaarverslag.

5 Contact

Voor alle vragen over ENSIA kunt u contact opnemen met KING via telefoonnummer: 070 2502400

ENSIA-tool
Heeft u vragen over de werking en het gebruik van de ENSIA-tool dan kunt u mailen naar ensia@ictu.nl.

Implementatie ENSIA
Heeft u vragen over de rol van de coördinator, over de inrichting van het verantwoordingsproces binnen uw gemeente? Of heeft u ondersteuning nodig bij de implementatie van ENSIA? Neem dan contact op met KING via ensia@kinggemeenten.nl.

Of kijk op www.kinggemeenten.nl/ensia