ENSIA | Eenduidige Normatiek Single Information Audit

Wat is ENSIA?

ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent eenmalige informatieverstrekking en eenmalige IT-audit.

Het project 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 (Baseline Informatiebeveiliging Nederlandse Gemeenten). De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Inkomen (SUWInet) is samengevoegd en gestroomlijnd.

Uitgangspunt is het horizontale verantwoordingsproces aan de gemeenteraad. Dit vormt de basis voor het verticale verantwoordingsproces aan de nationale partijen die een rol hebben in het toezicht op informatieveiligheid.

Waarom ENSIA?

Tijdens de Buitengewone Algemene Ledenvergadering van de VNG van november 2013 is de resolutie ‘Informatieveiligheid, randvoorwaarde voor de professionele gemeente’ aangenomen. Met het aannemen van de resolutie erkennen alle gemeenten het belang van informatieveiligheid en de BIG als het gemeentelijk basisnormenkader voor informatieveiligheid. In de resolutie hebben gemeenten afgesproken hun eigen toezichthouder, de gemeenteraad, in het jaarverslag te informeren over informatieveiligheid. Ook roepen de gemeenten in de resolutie op om de verantwoordingslasten over informatieveiligheid te verminderen. Dit vormde de aanleiding voor de start van het project ENSIA.

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

Wie is binnen de gemeente betrokken bij het uitvoeren van de ENSIA zelfevaluatie informatiebeveiliging?

Om het nieuwe verantwoordingsproces goed in te richten en de zelfevaluatie vragenlijsten in te vullen is betrokkenheid uit verschillende delen van de gemeenten gewenst. Denk hierbij aan: portefeuillehouder, gemeentesecretaris, de verantwoordelijke personen Bedrijfsvoering (ICT/ HR/Inkoop), Burgerzaken (BRP/PUN), Sociaal Domein (SUWInet), DigiD, BAG-beheer en BGT-beheer. Aan het College van B&W is gevraagd om een coördinator voor ENSIA aan te wijzen.

Wat houdt de rol van coördinator ENSIA in?

De coördinator werkt mee aan het begeleiden, bewaken en waar nodig bijsturen van het ENSIA- verantwoordingsproces. De kerntaken zijn het creëren van bewustzijn over informatieveiligheid voor de hele gemeente en het organiseren van samenwerking. De rol van coördinator kan goed worden vervuld door iemand met de functie van hoofd bedrijfsbureau, senior beleidsmedewerker bestuurszaken, controller, CIO, CISO of projectleider.
De coördinator heeft de volgende taken en verantwoordelijkheden. Hij/zij:

- zorgt voor brede betrokkenheid en draagvlak in de organisatie;
- zet de zelfevaluatie vragenlijst uit bij de verantwoordelijke personen Bedrijfsvoering, Burgerzaken, Sociaal Domein, DigiD, BAG-beheer en BGT-beheer;
- zorgt ervoor dat de bijbehorende documenten om de zelfevaluatie af te ronden, tijdig en compleet worden opgesteld, ingevoerd en geüpload;
- zorgt dat zowel horizontaal als verticaal verantwoording op basis van de zelfevaluatie wordt afgelegd;
- draagt zorg voor projectbemensing;
- Coördineert en bewaakt de uitvoering en voortgang;
- verleent opdracht aan de auditor voor een assurance-rapportage;
- organiseert communicatie en voorlichting;
- is contactpersoon voor vertegenwoordigers van ICT, HR [Bedrijfsvoering], Burgerzaken [BRP/PUN], Sociale Domein [SUWI], DigiD, BAG- en BGT-beheer.

Uit welke producten/onderdelen bestaat de ENSIA zelfevaluatie informatiebeveiliging?

- **Vragenlijst zelfevaluatie informatiebeveiliging**

Met de ingevulde zelfevaluatie vragenlijst en bijbehorende rapportages geeft het college van B en W aan in hoeverre de beheersmaatregelen aan de van kracht zijnde beveiligingsnormen voldoen. Bij het opstellen van deze vragenlijst is vastgesteld waar de normen van BRP, PUN, DigiD, SUWInet, BAG en BGT aansluiten op de BIG-normen en dus volstaan kan worden met vragen die gebaseerd zijn op de BIG-normen. Voor specifieke normen van BRP, PUN, DigiD, SUWInet, BAG en BGT zijn aanvullende vragen geformuleerd. De paragraaf Informatiebeveiliging en als onderdeel daarvan de Collegeverklaring ENSIA zijn onder meer gebaseerd op de zelfevaluatie.

- **Collegeverklaring ENSIA inzake informatiebeveiliging**

Met deze verklaring geeft het college van B en W aan in hoeverre bij de gemeente de beheersingsmaatregelen voldoen 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 wordt gezamenlijk met het Assurance rapport separaat van het jaarverslag aangeboden aan de gemeenteraad.[1]

- **Assurance rapport**

Een bij de NOREA geregistreerde IT-auditor controleert de Collegeverklaring en stelt een Assurance rapport op. Deze werkzaamheden van de IT-auditor duiden we ook wel aan als de IT-audit. De IT-auditor verklaart in het Assurance rapport 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.

- **Paragraaf Informatiebeveiliging in het jaarverslag /Separate Rapportage Informatiebeveiliging**

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. De Collegeverklaring maakt geen deel uit van het jaarverslag[3]. Gemeenten kunnen ervoor kiezen om een separate rapportage informatiebeveiliging aan de Raad te verstrekken. Deze rapportage omvat zowel de informatie over informatiebeveiliging in brede zin als de College Verklaring ENSIA. Een aantal gemeenten kiest nu al voor deze behandeling omdat zij verwacht een grotere aandacht voor het onderwerp in de raadsbehandeling te krijgen. De Assuranceverklaring maakt geen onderdeel uit van de paragraaf Informatiebeveiliging.

---

[1] Het opnemen van de ENSIA-verantwoordingsinformatie over informatiebeveiliging zal worden opgenomen met de Commissie Besluit begroting en verantwoording (BBV) die de regelgeving voor de jaarlijkse begrotings- en verantwoordingsstukken van gemeenten, provincies en waterschappen opstelt.

[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.

Voor verantwoording domeinspecifieke aspecten BAG en BGT:

- **Rapportage BAG en BGT**
  Na het inleveren van de zelfevaluatie vragenlijst BAG en BGT moeten er separaat rapportages worden ingeleverd. De conceptrapportages zijn beschikbaar via de ENSIA-tool en kunnen volgens instructie in de tool verder worden gecompleteerd en vastgesteld.

Hoe ziet de planning van het ENSIA-proces over het verantwoordingsjaar 2017 er uit?

Op hoofdlijnen verloopt de planning als volgt:
➢ *Invullen en aanleveren zelfevaluatie vragenlijst (juli – december 2017)*

- peildatum 01-10-2017 - inleveren antwoorden die nodig zijn voor zelfevaluatie informatieveiligheid BRP en PUN

- peildatum 31-12-2017 - inleveren antwoorden die nodig zijn voor zelfevaluatie over de volle breedte van de BIG (dus met inbegrip van de zelfevaluatie DigiD, SUWInet, BAG en BGT) ten behoeve van de horizontale verantwoording informatieveiligheid aan de gemeenteraad.

➢ *Opstellen en uploaden Collegeverklaring informatiebeveiliging; uitvoeren IT-audit en opstellen en oploaden van Assurance rapport (vóór 01-05-2018)*
➢ Opstellen en uploaden rapportage BAG en BGT (vóór 01-05-2018)
➢ *Het College van B&W legt verantwoording af over informatieveiligheid aan de gemeenteraad en toesturen van de jaarstukken aan de minister van BZK (vóór 15-07-2018)*

Waarom moet in 2017 de zelfevaluatie voor BPR en PUN vóór 1/10 worden aangeleverd?

De reden waarom voor de peildatum van 1 oktober is gekozen is dat voor de BRP[4]/PUN[5] wettelijk is vastgelegd dat de verantwoordingsinformatie informatieveiligheid uiterlijk 30 september van het verantwoordingsjaar bekend moet zijn. Vanaf 2018 wordt toegewerkt naar één verantwoordingsmoment per jaar, te weten peildatum 31/12.

[4] Besluit BRP art. 47.1: De onderzoeken, bedoeld in artikel 4.3 van de wet, geschieden jaarlijks, uiterlijk op 30 september.
[5] Paspoortuitvoeringsregeling Nederland, art.94.1: De burgemeester of de gezaghebber voert voor 1 oktober van ieder jaar een controle uit op de toepassing van de beveiligingsmaatregelen, genoemd in de artikelen 90 tot en met 93, en de overige aspecten van het aanvraag- en uitgifteproces van reisdocumenten en informeert voor 1 november van ieder jaar de Minister van Binnenlandse Zaken en Koninkrijksrelaties over de bevindingen van de controle.

Hoe verloopt de verantwoording over de domeinspecifieke vragen van de BAG, BGT, BRP en PUN?

Voor 2017 zijn in de ENSIA-tool alleen de domeinspecifieke vragen opgenomen ten behoeve van de verantwoording over de BAG en BGT. De ambitie is om vanaf 2018 ook de verantwoording over de domeinspecifieke vragen voor BRP en PUN op te nemen in de ENSIA-tool en gelijk te laten lopen met het verantwoordingsproces informatieveiligheid. De domeinspecifieke vragen BRP en PUN verlopen voor 2017 nog via de Kwaliteitsmonitor.