

## BESTUURLIJKE RAPPORTAGE INFORMATIEVEILIGHEID GEMEENTEN IN KADER ENSIA

### Verantwoordelijkheid College

Het algemene doel van ENSIA is het versterken van de informatieveiligheid bij en door gemeenten. Onderdeel van ENSIA is het afleggen van verantwoording door het College van BenW aan zowel de gemeenteraad als de toezichthouders over de informatieveiligheid bij de gemeenten. Hiervoor was / is de Collegeverklaring ENSIA en het bijbehorende assurance-rapport van een IT-auditor (als onderdeel van de rapportage informatieveiligheid) voorzien.

Vanuit BZK / VNG-realisatie is gebleken dat gemeenten, om verschillende redenen, sterk verschillend invulling hebben gegeven aan de verplichting tot het uitbrengen van een volledige rapportage aan de gemeenteraad<sup>1</sup>. Deze verplichting is vastgelegd in de VNG-resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" uit 2013.

De Regieraad ENSIA heeft met ingang van het verantwoordingsjaar 2020 besloten tot een herijking van de verplichting tot rapportage over de informatieveiligheid aan de gemeenteraad. Deze herijking is neergelegd [in de Notitie Verantwoordingsstelsel ENSIA 2020 - 2021](#) (zie Bijlage 1).

De herijking betreft de ontwikkeling van een voor de doelgroep (raad en college) inzichtelijk rapportagesjabloon. Dit sjabloon bouwt voort op de voorbeelden die door gemeenten zijn aangedragen. Dit sjabloon is ook één van de resultaten van de BIO Pilot van eerder dit jaar. Daarmee wordt een voor gemeenten betere invulling gegeven aan de rapportageverplichting uit bovengenoemde resolutie.

Ten einde het proces te faciliteren is de leidraad "[Bouwstenen oplegnotitie bestuurlijke verantwoording](#)" (zie bijlage 2) opgesteld. Deze is leidend voor proces rond en inhoud van de op te stellen rapportage.

Gemeenten kunnen de rapportageverplichting invulling geven door:

- a. Het toezenden van een oplegnotitie en de achterliggende ENSIA documenten zoals de collegeverklaring ENSIA en het daarbij door de IT-auditor afgegeven assurance-rapport;
- b. Een brede rapportage informatieveiligheid conform een daartoe opgestelde [handreiking / model- c.g. voorbeeldrapportage](#) (zie Bijlage 3);
- c. Een rapportage volgens een eigen model van de gemeente die minimaal voldoet aan de in de leidraad "Bouwstenen oplegnotitie bestuurlijke verantwoording" opgenomen aspecten.

---

<sup>1</sup> Hierbij is kennis genomen van feit dat gemeenten hier divers mee omgaan. Sommige volstaan met de paragraaf in de jaarrekening, anderen met het toezenden van de collegeverklaring (met bijbehorende assurancerapport). Een aantal gemeenten brengt een uitgebreide rapportage uit. Tot slot is er een aantal gemeenten dat in het geheel niet rapporteert.

Het staat de gemeente vrij om bij rapportages in het kader van de onder b. en c. vermelde opties ook de collegeverklaring ENSIA en het daarbij door de IT-auditor afgegeven assurance-rapport ter beschikking te stellen aan de gemeenteraad.

#### Verantwoordelijkheid IT-auditor

De IT-auditor belast met de uitvoering van de ENSIA-audit dient in het kader van de uitvoering van de assurance-opdracht na te gaan op welke wijze de gemeente (opdrachtgever) invulling gaat geven aan de verplichting om aan de gemeenteraad te rapporteren over het thema informatieveiligheid bij de gemeente. Meer in het bijzonder gaat het over de wijze waarop in dit kader over de uitkomsten van de ENSIA-audit (collegeverklaring en daarbij verstrekte assurance-rapport).

Daarbij dient de IT-auditor in overleg met de gemeente kennis te nemen van de rapportage informatieveiligheid. Meer in het bijzonder dient de IT-auditor vast te stellen dat de wijze waarop over de uitkomsten van de uitgevoerde assurancewerkzaamheden (zowel Collegeverklaring als het daarbij afgegeven assurance-rapport) wordt gerapporteerd niet strijdig is met de inhoud van deze documenten. Verder dient de IT-auditor vast te stellen dat ook de overige informatie in de bestuurlijke rapportage niet strijdig is met de bevindingen die ten grondslag liggen aan het afgegeven assurance-rapport. Daarbij geldt dat de resultaten van het bredere zelfevaluatie ENSIA leidend voor de rapportage leidend zijn. Eventuele tekortkomingen in de scope DigiD en Suwi kunnen daardoor in een ander daglicht staan maar mogen er niet strijdig mee zijn.

Voor de volledigheid attenderen wij erop dat het hierbij in het kader van de ENSIA-audit gaat om een marginale toets en niet om het uitvoeren van een volledige assurance-opdracht gericht op deze rapportage.<sup>2</sup>

#### Bijlage: Verantwoordingsdocumenten

1. Notitie Verantwoordingstelsel ENSIA 2020 – 2021

<https://www.vngrealisatie.nl/sites/default/files/2020-12/20200828%20Notitie%20verantwoordingstelsel%20ENSIA%202020%20-%202021%20inc%20bijlagen%20-%20definitief.pdf>

2. Bouwstenen oplegnotitie bestuurlijke verantwoording

[https://www.vngrealisatie.nl/sites/default/files/2020-11/Ensia.bouwstenen.bestuurlijke.verantwoording\\_0.pdf](https://www.vngrealisatie.nl/sites/default/files/2020-11/Ensia.bouwstenen.bestuurlijke.verantwoording_0.pdf)

3. Handreiking bestuurlijke rapportage

<http://www.vngrealisatie.nl/sites/default/files/2020-11/Handreiking%20bestuurlijke%20rapportage.pptx>

---

<sup>2</sup> Hierbij kan het zo zijn dat de bestuurlijke rapportage op een ander, later, tijdstip verschijnt dan de voor de ENSIA-rapportage voorgeschreven momenten