gemeente Rheden

Antwoord op schriftelijke vragen van VVD over Eenduidige Normatiek Single Information Audit (ENSIA)

Datum vraag: 24 april 2022
Indiener: Sjir Hanssen
Nummer: S22/118
Datum antwoord: 3 mei 2022

Aanleiding:
Achtergrondinformatie
Op 1 juli 2017 is ENSIA (Eenduidige Normatiek Single Information Audit) geïmplementeerd en draagt zorg voor de (gestandaardiseerde) verantwoording over een achttal informatiestelsel. Ook de gemeenten zijn hierbij betrokken en kennen deze verplichting.

Het doel van ENSIA is om tot een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid te komen, gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO).
Onderstaande tekst is afkomstig vanaf de website van de VNG:
ENSIA helpt gemeenten in één keer verantwoording af te leggen over informatieveiligheid gebaseerd op de normen die gelden voor de Nederlandse overheid, de BIO. Met ENSIA sluit de verantwoording over informatieveiligheid aan op de planning en control-cyclus van de gemeente. Hierdoor heeft het gemeentebestuur meer overzicht over de informatieveiligheid van hun gemeente en kan het beter sturen en verantwoording afleggen aan de gemeenteraad.

ENSIA structureert verantwoording over de Basisregistratie Personen (BRP) en Reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI) richting de rijksoverheid.
Vraag 1: Is de ENSIA systematiek ook geïmplementeerd in de gemeente Rheden en zo ja…. Op welke wijze? Zo nee ? Waarom is dat niet gebeurd?
Antwoord:

De ENSIA-systematiek is verplicht voor gemeentes, dus ook vanaf 2017 bij ons geïmplementeerd. De ENSIA is gericht op verantwoording afleggen over de status van informatiebeveiliging binnen verschillende afdelingen van de gemeente. Hierbij wordt getoetst op diverse maatregelen, waarvan de meeste afkomstig zijn uit de BIO. De BIO vormt daarom binnen de gemeente dan ook de basis voor informatiebeveiliging. Over de ENSIA wordt ook jaarlijks een stuk opgenomen in de jaarrekening.

Jaarlijks voeren wij de ENSIA uit, waarbij de huidige status van de informatiebeveiliging getoetst wordt. Voor Suwinet en de drie Digi-D aansluitingen dienen we bij de auditor aan te tonen, dat we aan de normen voldoen. Voor de andere onderdelen (BIO, BRP, Reisdocumenten, BAG, BGT, BRO & WOZ) betreft het een volledige zelfevaluatie. Al deze (zelf)evaluaties dienen voor 31 december ingediend te worden. Vervolgens worden er rapportages opgesteld, welke gebruikt worden om de raad te informeren. Deze rapportages over 2021 zijn behandeld in college vergaderingen en terug te vinden op:

- Rapportage ENSIA controle 2021 v2 (Behandelt op 26 april, nr. 2417)
- Rapportage WOZ ENSIA 2021 (Behandelt op 26 april, nr. 2406)
- Rapportage ENSIA controle 2021 (Behandelt op 19 april, nr. 2393)

Voor de punten waaraan tijdens de evaluatie bleek dat de gemeente nog niet voldoet, is een verbeterplan opgesteld. Dit document is onderdeel van de rapportage.

Vraag 2: Op welke wijze is de raad betrokken bij de verantwoordingscyclus binnen de ENSIA systematiek?
Antwoord:
Het college is geïnformeerd over de uitkomst van de ENSIA via eerder genoemde rapportages. De raad zelf heeft hier geen actieve rol in.

Bovenstaand schema is afkomstig van de VNG website.

Vraag 3: Wanneer en op welke wijze/ is de gemeenteraad betrokken bij de verantwoording over de informatiebeveiliging?
Antwoord:
Hierbij volgen wij ook bovenstaand schema. De raad is geïnformeerd over de uitkomst van de ENSIA, zie ook de antwoorden bij vraag 1 en 2.

In de raadsinformatiebrief van 5 april 2022 (verbetermaatregelen n.a.v. toezicht verslag informatiebeheer wordt geen aandacht besteed aan de verantwoording en komt ENSIA niet eens ter sprake.

Vraag 4: Wat is de reden dat de verbetering van de verantwoording niet is opgenomen in de verbetervoorstellen/ maatregelen?
Antwoord:
De raadsinformatiebrief van 5 april 2022 is gericht op de verbetervoorstellen/maatregelen specifiek gericht op het archief en niet op informatiebeveiliging. Om de meest recente stukken over informatiebeveiliging te verkrijgen, zie de besluiten benoemd in vraag 1.

Daarnaast is het van belang om onderscheid te maken tussen informatiebeveiliging en de ENSIA. De ENSIA is een verantwoordingstraject over de informatiebeveiliging. Verantwoording is een belangrijk deel van informatiebeveiliging, maar de ENSIA is geen doel op zich. Het bovenliggende doel is niet om voldoende maatregelen voor informatiebeveiliging geïmplementeerd te hebben om door de ENSIA heen te komen, maar juist om voldoende om een veilige (digitale) omgeving te bieden. Om dit meetbaar te maken dient er voldoende vastlegging plaats te vinden, hiervoor zijn stappen opgenomen in het verbeterplan. Informatiebeveiliging is een onderwerp dat in de toekomst meer en meer aandacht vraagt van het management, college en ook de raad.