

## Wat is ENSIA?

ENSIA staat voor Eenduidige Normatiek Single Information Audit. Het doel van ENSIA is om het verantwoordingsproces over informatieveiligheid bij gemeenten te verbeteren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft de gemeente een beter overzicht over de stand van zaken van de informatieveiligheid en kan zij hier ook beter op sturen.

## Horizontale en verticale verantwoording

Met de resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" van 2013 is door de gemeenten afgesproken om de Baseline Informatieveiligheid Gemeenten te implementeren. Deze baseline vormde de kern van de verantwoording over informatieveiligheid aan de gemeenteraad en is inmiddels opgevolgd door de nu geldende Baseline Informatiebeveiliging Overheid (BIO).

ENSIA kent een horizontale en een verticale verantwoording. De horizontale verantwoording gaat richting gemeenteraad en bestaat uit de zelfevaluatie over de implementatie van de BIO, het ENSIA assessment, een verklaring van het College van B&W en een passage over informatieveiligheid in het jaarverslag.

Over de BRP, PUN, Suwinet, BAG, BGT, BRO en DigiD moeten gemeenten ook verticaal verantwoording richting toezichthouders afleggen. De horizontale verantwoording richting gemeenteraad vormt hiervoor de basis.

## Wat is Single Information Single Audit?

Uitgangspunt van ENSIA is *de single information single audit*. Dit betekent dat de gemeente maar één keer per jaar de zelfevaluatielijst hoeft in te vullen. De informatie wordt gebruikt voor de horizontale verantwoording en tevens voor de diverse verticale verantwoordingslijnen richting departementen. De zelfevaluatie is ook de belangrijkste input voor het door BKBO uit te voeren ENSIA assessment. De ENSIA assurance rapportage van BKBO, moet ook mee met de verticale verantwoording richting de toezichthouders.

## Waaruit bestaat het ENSIA assessment?

Het ENSIA assessment over verantwoordingsjaar 2020 bestaat uit een controle op alle DigiD aansluitingen die u voor 1 mei 2020 al gebruikte en alle Suwinet toepassingen die u als gemeente heeft. Veel gemeenten hebben twee Suwinet aansluitingen: één voor de uitvoering van de Participatiewet en één voor het uitvoeren van een adresonderzoek door Burgerzaken. Het ENSIA assessment moet voor 1 mei zijn afgerond en wordt daarna jaarlijks herhaald. De organisatie die als verticale toezichthouder bepaalt wat verplicht gesteld wordt voor DigiD is Logius. BKWI is daarvoor de evenknie voor Suwinet.



Het ENSIA assessment is een in vaktermen "assertion based" audit. Dit betekent dat wij als auditors zoveel mogelijk "steunen" op het door de gemeente al voor het invullen van de zelfevaluatie vergaarde bewijsmateriaal. Idealiter levert de gemeente als klant dus al het bewijsmateriaal zelf aan. In de praktijk ondersteunen wij u als klant met ons heldere documentatieverzoek. Zie ook de animatie op het BKBO YouTube kanaal <https://youtu.be/ujWwmkavWBI>.

## Wat kunnen wij u bieden?

BKBO is een klein audit bedrijf. In gemeenteland zijn we al jaren goed thuis en in de "gemeentelijke auditmarkt" behoren we tot de grootste auditororganisaties. Wij zijn gespecialiseerd in de IT van de lokale overheid. Met onze bewezen kennis en ervaring, voeren we voor meer dan 90 gemeenten het ENSIA assessment uit.

## Wat is uw voordeel?

BKBO is onafhankelijk en goed ingevoerd in gemeenteland. We zijn deskundig, goed bereikbaar en geven direct terugkoppeling. BKBO is een "platte" organisatie en de audit wordt niet over verschillende schijven uitgevoerd. We zetten samen een planning met u uit waarbij we alles op alles zetten om de deadline van 1 mei te halen. Wij ondersteunen u met een aanpak die zowel tijd als kosten bespaart. Wij zijn zeker van onze zaak en bieden u dus een vaste prijs. Dat is voordelig en compleet want het is inclusief eventuele heraudits. Wij bieden gemeenten en sociale diensten de mogelijkheid om een TPM-verklaring te verkrijgen voor het Suwinet deel van ENSIA. Met een Third Party Memorandum bespaart u op de auditkosten omdat de deelnemers dan maar een beperkt assessment hoeven te ondergaan.



## Hoe pakken wij dat aan?

Wij hebben een gestandaardiseerde en beproefde uitvoeringswijze ontwikkeld. U bepaalt met een zelfonderzoek moeiteloos wat uw situatie is. Dit begint met een documentatieverzoek. Hierdoor brengt u eenvoudig uw situatie overzichtelijk in kaart. Wanneer alle bewijsstukken zijn verzameld en aangeleverd, wordt door ons een audit uitgevoerd op uw contracten, procedures en de beveiligingsorganisatie. Wij zorgen dat voor u alles compleet, geordend en begrijpelijk is.

We leggen onze bevindingen vast in een overzichtelijke conceptrapportage. We doen concrete aanbevelingen om de tekortkomingen efficiënt op te heffen. Daarna wordt de rapportage definitief gemaakt. Het assessment wordt afgesloten met een digitale evaluatie.

## Wat is uw investering?

Afhankelijk van wat u wilt dat onderzocht wordt, variëren de kosten tussen de € 2.000,- en € 9.000,-. Afhankelijk van het aantal en type DigiD en Suwinet aansluitingen en of er penetratietesten moeten worden uitgevoerd. De genoemde prijzen zijn exclusief BTW en inclusief reis- en verblijfskosten.

## Geen gekibbel garantie

Onze garantie is uniek in de branche! Wij garanderen u een vaste prijs. De prijs is dus inclusief een eventuele heraudit nadat u verbetermaatregelen heeft kunnen doorvoeren. Door onze bewezen aanpak durven wij hiervoor in te staan. Wij noemen dat onze "geen gekibbel garantie".

## Wilt u meer weten?

Wij staan voor u klaar en gaan graag met u in gesprek. U kunt direct bellen met BKBO op telefoonnummer: 073 – 211 03 37. Is het voor u duidelijk? Dan kunt u ook meteen een offerte aanvragen via [info@bkbo.nl](mailto:info@bkbo.nl)

