NOREA-werkgroepen stellen zich voor

Werkgroep ENSIA

8 september 2019

Peter Verstege

Wat is ENSIA?

ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent eenmalige informatieverstrekking en eenmalige IT-audit. Het project ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel over informatieveiligheid bij gemeenten. Het hoofddoel is verdere professionalisering van het verantwoordingsproces over informatieveiligheid bij gemeenten. Dat gebeurt door het toezicht te bundelen en te laten aansluiten op de gemeentelijke Planning en Control-cyclus.

Waarom ENSIA?

Burgers en bedrijven verwachten een betrouwbare overheid die zorgvuldig met informatie omgaat. Gemeenten spelen hierin een belangrijke rol. Zij voeren in dat kader een groot aantal processen uit op basis van en met registraties die de Rijksoverheid voorschrijft of ter beschikking stelt.

Het gaat om de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI). Nieuwe registraties en systemen zijn aangekondigd. Deze processen kennen alle eigen verantwoordingsmomenten, toezichts- en controle-arrangementen. Verder zijn deze verantwoordingen gebaseerd op verschillende normensets en toetsingskaders. Het geheel leidt tot een grote administratieve last voor alle betrokken partijen.

Kern van alle verantwoordings-, toezichts- en controle-arrangementen is de beschikbaarheid, integriteit, vertrouwelijkheid en robuustheid (*resilience*) van informatie, in de breedste zin van het woord. Het waarborgen van de betrouwbaarheid en beschikbaarheid van informatie zorgt voor een goede kwaliteit en continuïteit van de bedrijfsvoerings- en dienstverleningsprocessen van alle betrokken organisaties.

De focus van ENSIA ligt op de horizontale verantwoording. Dat is de verantwoording binnen de gemeente zelf, met een belangrijke rol voor de gemeenteraad. Figuur 1 geeft een beeld van dit horizontale verantwoordingsproces zoals dit voor het verantwoordingsjaar 2018 is toegepast.

Figuur 1: Horizontale verantwoording: binnen de gemeente

Tegelijkertijd is deze verantwoording bruikbaar als verticale verantwoording: van de gemeente aan de toezichthouders op rijksniveau voor de verschillende domeinen. Dit proces in nader uitgewerkt in figuur 2.

Figuur 2: Verticale verantwoording: van gemeente aan de toezichthouders rijksniveau (collegeverklaring)

ENSIA helpt de gemeenten in één keer verantwoording af te leggen. Met ENSIA sluit de verantwoording over informatieveiligheid aan op de planning en control-cyclus van de gemeenten. Daarbij streeft de VNG op termijn naar een volledige integratie van de verantwoording over informatieveiligheid in de jaarrekening van de gemeenten. Als voorbeeld hiervoor geldt de wijze van verantwoorden over de subsidies die gemeenten van onder meer de Rijksoverheid en provincies Single Information, Single audit (SiSa)).

ENSIA is een initiatief van de VNG en de ministeries van BZK, van voormalig IenM en van SZW. NOREA is vanaf de start actief bij het project betrokken. Het accent van de activiteiten van NOREA ligt op het uitwerken van en invulling geven aan de auditcomponent, meer in het bijzonder gaat het hierbij om de door IT-auditors af te geven assurance bij de Collegeverklaring ENSIA.

Werkgroep ENSIA

Vanuit NOREA is en wordt een actieve bijdrage geleverd aan het ontwikkelen, implementeren en uitvoeren van ENSIA met als speerpunt invulling en uitwerking geven aan audits door IT-auditors en de op basis daarvan af te geven assurance. Daarvoor heeft het bestuur van NOREA de werkgroep ENSIA ingesteld. Hierin participeert een groot aantal direct bij ENSIA-werkzaamheden betrokken IT-auditors. Verder zijn de Vaktechnische Commissie en het bestuur van NOREA in de werkgroep vertegenwoordigd. De werkgroep vertegenwoordigt NOREA in de governancestructuur van het project ENSIA, met als onderdelen onder meer Audit Committee en Gebruikersoverleg. Daarnaast verzorgt de werkgroep binnen NOREA de noodzakelijke activiteiten zoals uitwerken Handreiking, verzorgen opleidingen en bemensing ENSIA Helpdesk.

Uitdagingen

Bij de uitvoering van de verschillende activiteiten van de werkgroep spelen we in op de ontwikkelingen op het gebied van informatieveiligheid en de complexe werkelijkheid waarin gemeenten (moeten) opereren. Daarbij is sprake van een aantal uitdagende vraagstukken die in grote lijnen corresponderen met de letters van het acroniem ENSIA, zoals hieronder toegelicht.

Eenduidige Normatiek

ENSIA is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Het inpassen binnen de BIG-systematiek van alle specifieke vragen en eisen van de toezichthouders voor de verschillende registraties bleek in de praktijk complexer dan verwacht. Uitzonderingen en aanvullingen zijn, helaas, noodzakelijk.

Vanaf 2020 geldt een nieuw normenkader voor de informatiebeveiliging bij alle overheden: de Baseline Informatiebeveiliging Overheid (BIO). 2019 is voor ENSIA een overgangsjaar naar de invoering van de BIO. Om in 2020 verantwoordingen op basis van de BIO te kunnen realiseren zal nog veel werk verzet moeten worden. Dit geldt zeker ook nu de BIO nog verder uitgewerkt wordt. Verder krijgen alle betrokkenen bij de gemeenten en de Rijksoverheid steeds meer aandacht voor de governance rond de informatievoorziening en informatiebeveiliging bij gemeenten. Het uitwerken van de normatiek op dit punt verdient nog veel aandacht.

Single Information

Om te komen tot single information in de vorm van de Collegeverklaring was en is een groot aantal stappen nodig. Denk daarbij aan het harmoniseren van rapportagemomenten en -perioden. Verder blijken gemeenten op verschillende manieren verantwoordelijk te zijn voor delen van de informatievoorziening. In het ene geval blijft de gemeente integraal verantwoordelijk, ook al besteedt zij de uitvoering van taken en de daarbij behorende informatievoorziening geheel uit aan derden. In andere gevallen beperkt de verantwoordelijkheid van de gemeente zich tot die werkzaamheden die in eigen beheer worden uitgevoerd. Verder zijn er verschillen in de aard en omvang van de (verantwoordings-) informatie die de gemeenten aan de toezichthouders moeten verstrekken. Tot slot was het niet gebruikelijk dat het gemeentebestuur (het College) op een gestructureerde manier verantwoording over de ontwikkelingen op het gebied van de informatiebeveiliging verstrekte aan de gemeenteraad.

Hoewel het uitgangspunt van single information is bereikt, hebben de hiervoor genoemde factoren geleid tot complexe en voor relatieve buitenstaanders moeilijk te doorgronden teksten in de verantwoordingsdocumenten. Tevens is de Collegeverklaring omvangrijker geworden doordat een aantal specifieke bijlagen is toegevoegd om aan alle informatie- en verantwoordingseisen te kunnen voldoen. Op dit punt zal de komende jaren nog veel werk verzet moeten worden. De verwachting is gerechtvaardigd dat dit nog een aantal jaren zal vergen omdat op onderdelen de van toepassing zijnde wet- en regelgeving aangepast moet worden.

Audit

Assurance in de vorm van een assurancerapport op basis van Richtlijn 3000A maakt integraal onderdeel uit van ENSIA. Daarmee is een belangrijke rol in het ENSIA-proces gedefinieerd voor de IT-auditors. De werkgroep heeft een uitgebreide Handreiking ENSIA opgesteld, die richting geeft aan de werkzaamheden van IT-auditors.

De assurance wordt gegeven bij het controle-object 'Collegeverklaring ENSIA'. Deze assurance richt zich op opzet en bestaan van beheersmaatregelen op het gebied van de informatiebeveiliging en meer in het bijzonder de maatregelen die van toepassing zijn bij DigiD en Suwinet. Daarmee is ook de beperking aangegeven van de huidige

verantwoording en bijbehorende assurance. NOREA streeft naar een verbreding van de in de Collegeverklaring gerapporteerde maatregelen. Deze zal uiteindelijke de volle breedte van de BIO en alle betrokken (rijksbrede) systemen moeten omvatten. Verder dient de verantwoording en de bijbehorende assurance ook betrekking te hebben op opzet, bestaan en werking van de betreffende maatregelen. De Werkgroep ENSIA en NOREA hebben voorstellen ontwikkeld om deze doelstelling in een aantal stappen te realiseren. Het advies is op het moment van schrijven van dit artikel in behandeling bij de governance-organen van ENSIA.

Politiek-bestuurlijke context

Bij het realiseren en uitvoeren van het ENSIA-project is een groot aantal actoren betrokken. Deze hebben allen hun eigen wensen. Tevens opereren deze actoren in een complexe en snel veranderende omgeving en hebben zij, zoals hiervoor al is aangegeven, te maken met specifieke wet- en regelgeving. Tegelijkertijd zijn er ook ontwikkelingen op het gebied van auditing, zoals het streven naar assertion-based assurance en de carve-out benadering bij het afgeven van assurance ten behoeve derde partijen. Deze leiden ook tot toegenomen regeldruk en geformaliseerde werkprocessen.

Al deze factoren leiden ertoe dat de uitwerking van ENSIA sterker geformaliseerd is en wordt dan oorspronkelijk gedacht. Dit roept bij de gemeenten en auditors vragen op over de administratieve lasten die gemoeid zijn met de uitvoering van ENSIA. Alle betrokkenen, en niet in de laatste plaats ook NOREA, zullen de komende jaren het hoofddoel van ENSIA, verbeteren van de informatieveiligheid bij gemeenten, in het oog moeten houden.

Ambities NOREA

In de voorgaande paragrafen is aangegeven wat in de afgelopen jaren bereikt is. Daarnaast is inzicht gegeven in de ambities van NOREA voor ENSIA. De essentie is dat NOREA wil blijven bijdragen aan ENSIA en daarbij als speerpunt heeft invulling en uitwerking te geven aan audits door IT-auditors en de op basis daarvan af te geven assurance. Hiermee geeft NOREA samen met alle andere betrokken partijen actief invulling aan het maatschappelijke belang van informatieveiligheid bij gemeenten.

Het is dit belang, en daarmee de impact van werkzaamheden van IT-auditors op maatschappelijk relevante processen, die een belangrijke motivatie vormt voor de werkgroep ENSIA. Want één ding is helder: het einddoel kan slechts met grote inspanningen en oog voor het belang van alle betrokkenen bereikt worden. Daarvoor zijn de kennis en ervaring van leden van NOREA onontbeerlijk. Ook binnen NOREA is bundeling van specialistische kennis en ervaring – organisatorisch, technisch en vaktechniek auditing – noodzakelijk om tot passende antwoorden te komen. Daar toont zich ook de kracht van een beroepsorganisatie die maatschappelijk relevant wil blijven.

De werkgroep ENSIA richt zich in eerste instantie op de vaktechnische aspecten van de ENSIA-audits. Daarnaast speelt de werkgroep een centrale rol bij de informatie-uitwisseling tussen partijen. Het gaat daarbij om het vergroten van het begrip voor de voorwaarden voor de uitvoering van de controlewerkzaamheden bij de gemeenten en de bijdrage die dit kan hebben voor (de verbetering van de processen bij) de gemeenten. Tegelijkertijd gaat het om het vergroten van het begrip bij de IT-auditors voor de politiek-bestuurlijke processen en de uitvoeringsproblematiek bij de gemeenten. Hiervoor wordt intensief samengewerkt met vertegenwoordigers van gemeenten (vooral via de VNG), Rijksoverheid (bijvoorbeeld ministeries van BZK en SZW) en de IT-auditors.

Op deze wijze speelt NOREA in op maatschappelijk relevante ontwikkelingen. De verwachting is gerechtvaardigd dat in de komende jaren overheden NOREA om vergelijkbare inzet zullen vragen op een aantal andere beleidsterreinen, denk aan privacy, e-Herkenning en ontwikkelingen in de gezondheidszorg.

Informatie
Uitgebreide en actuele informatie over ENSIA en de door IT-auditors uit te voeren werkzaamheden is te vinden op de websites van VNG-realisatie en NOREA.

Drs. ing. Peter D. Verstege RE RA | Voorzitter Werkgroep bij *ENSIA*