> LINK NAAR TEKSTVERSIE IN HTML

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Evaluatie en versterking ENSIA –stelsel

Versie 1.0

Datum 28 mei 2020
Status Vastgesteld door de Regieraad

I-Interim Rijk| Humberto van der Star en Minke Verkerk|

Inhoud

Bijlagen

Inleiding

Op 27 juli 2017 heeft de toenmalige stuurgroep ENSIA aangegeven dat er een evaluatie moet plaatsvinden van het ENSIA-stelsel; het beheer, de governance en financiering van het stelsel.

Op 27 december 2018 heeft staatsecretaris Knops van BZK aan de Tweede Kamer aangegeven dat de systematiek van de ENSIA-zelfevaluaties geëvalueerd zal worden om tot een verbetering van de verantwoording te komen.

De stuurgroep is vervangen door de Regieraad.

De Regieraad heeft op 9 september 2019 de Stelselverantwoordelijke (BZK/ DGOO/DO) opdracht gegeven om het ENSIA-stelsel te laten evalueren en heeft, als onderdeel van die opdracht, tevens de onderzoeksvragen vastgesteld.

Ten behoeve van de onafhankelijkheid en een veilige omgeving zijn een – zonder last en ruggenspraak – voorzitter/facilitator en documentalist voor het leiden en documenteren van de verschillende groepssessies aangesteld. Beiden werkzaam voor I-Interim Rijk.

In de Regieraad zijn op 12 maart 2020 de “rode draden” besproken en op 16 april 2020 de concept versie van dit rapport. De daarbij gemaakte opmerkingen zijn verwerkt in deze definitieve versie.

Doelstelling

De opdrachtgever heeft voor deze evaluatie de volgende doelstelling geformuleerd: het evalueren van het ENSIA-stelsel en het vervolgens komen tot onderling gedragen verbeteringen/conclusies, en daarmee versterking van het ENSIA-stelsel. Dit op basis van de eigen ervaringen en inhoudelijke expertise van alle betrokken stakeholders.

Aanpak

Omdat een groot aantal partijen bij ENSIA betrokken is, is gekozen voor een aanpak waarin alle partijen zoveel mogelijk zelf aan het woord zijn gekomen over wat goed is aan het ENSIA-stelsel en wat beter zou kunnen. Dit conform de filosofie van zelf evaluatie. De vragenlijst (zie bijlage 1) werd door het evaluatieteam ruim voorafgaand aan alle deelnemers van de groep sessies (zie bijlage 2) gestuurd.

Vervolgens werden de daarop ontvangen reacties verwerkt tot een set open vragen, waar in het eerste deel van het groepsgesprek nader op werd ingegaan. Dit tevens met de vraag wat de deelnemers zelf zouden kunnen bijdragen om het ENSIA-stelsel sterker te kunnen laten functioneren.

In het tweede deel van het groepsgesprek werden de zogenoemde “rode draden”, een compilatie opgesteld op basis van de verkregen antwoorden op de vooraf gestuurde vragen en van de voorgaande groepssessies, besproken.

De rode draden en het stappenplan voor versterking zijn dus telkens opnieuw opgesteld; op basis van (per groepssessie) de beantwoording van de vooraf gestuurde vragen, de uitkomsten van de groepsgesprekken en de revisie door de deelnemers van de nieuwe versie van het conceptrapport na elk groepsgesprek. De rode draden evolueerden daardoor gedurende de gesprekken met de verschillende groepen. In dit rapport zijn de rode draden zo goed als mogelijk gekoppeld aan de evaluatievragen.

Deze systematiek is gekozen om te komen tot steeds meer diepgang, onderlinge herkenning en draagvlak.

Leeswijzer

In hoofdstuk 1 zijn de rode draden opgenomen. De rode draden zijn “rode draden” omdat deze punten telkens meer of minder gedetailleerd terugkwamen in de antwoorden op de vooraf gestuurde vragen, alsmede gedurende de besprekingen in de groepssessies. Qua formulering en inhoudelijk worden zij herkend door de deelnemers.

In hoofdstuk 2 zijn de suggesties opgenomen. Suggesties waren antwoorden die niet door alle deelnemers werden gedeeld of voor iedereen toepasbaar waren, maar door het evaluatieteam wel als relevant voor de Regiegroep werden beoordeeld.

De discussiepunten in hoofdstuk 3 zijn antwoorden waarover de meningen verschilden en percepties uiteenliepen. Het nader uitzoeken en uitwerken van deze punten kan bijdragen aan het verkrijgen van een gedeeld standpunt en daarmee aan een betere werking van de ENSIA-systematiek.

Het stappenplan in hoofdstuk 4 is, op basis van de rode draden, de weergave van de aanbevelingen van het evaluatieteam in de tijd. Ook de conceptversies hiervan zijn telkens door ons voorgelegd aan de deelnemers. Wederom ten behoeve van herkenbaarheid en draagvlak.

1. Rode draden

1

Ondersteunt het ENSIA-stelsel voldoende bij het op orde krijgen van de informatiebeveiliging en de andere in het stelsel opgenomen domeinen?

- Zorgt het ervoor dat het onderwerp op de agenda's van bestuurders en management komt en blijft?
- Leidt het hanteren van de ENSIA-systematiek tot een groter bewustzijn op bestuurlijk niveau (bijv. bij het College van B&W en de Raad)?
- Hoe kan dit effectiever en efficiënter?

- De implementatie van het ENSIA-stelsel heeft de bewustwording over het thema informatiebeveiliging bij gemeenten bevorderd. Algemeen wordt verwacht dat de implementatie van de BIO hier binnenkort een verdere bijdrage aan zal gaan leveren (uniformeren stelsels/ eisen/ taalgebruik).

  De wens en mogelijkheid om vooral het accent op de horizontale verantwoording (betrekken College/ raad) te leggen, wordt politiek-bestuurlijk als de juiste benadering gezien. Dit om daarmee ook de belangen van de overige stakeholders te dienen en inwoners, bedrijfsleven en maatschappelijke organisaties te betrekken bij het onderwerp. De systematische aandacht voor het thema informatieveiligheid op niveau van de gehele gemeente, inclusief de taken die in samenwerkingsverbanden worden uitgevoerd, is een grote winst.

  Er is, ook bij gemeenten, intern een integraal beeld ontstaan. Gemeenten zorgen op structurele basis voor zelfevaluatie en verslaglegging aan College en Raad. De ENSIA-verantwoording is voor de stelselhouder een belangrijk vehikel omdat zij daarmee de verticale verantwoording onder de aandacht van College en raad kunnen brengen. De rapportage aan de gemeenteraad sluit echter qua verwoording nog niet goed aan bij deze doelgroep (zie verder bij rode draad 2).

  De aandacht van bestuurders en management voor informatiebeveiliging ontwikkelt zich langs een geleidelijk groeipad, waar jaren voor nodig is. Volwassenheidsmetingen, duidelijkheid in eigenaarschap en stappenplannen in de tijd kunnen helpen die ontwikkelingen in positieve zin te ondersteunen.

- De Collegeverklaring en het Assurance rapport dienen in politiek-bestuurlijk meer herkenbare termen gegoten te worden.

  De aan ENSIA gerelateerde stukken (en het aantal bijlagen!) zijn complex en leiden daardoor af van het onderwerp informatieveiligheid. De huidige wijze van verantwoording is een samenvoeging van (technische) vaktaal op het gebied van informatiebeveiliging, ICT en assurance.

De gebruikte taal sluit daardoor niet aan bij die van bestuur en management, waardoor het begrip over de stand van zaken achterblijft en dus de sturing op de informatiebeveiliging wordt bemoeilijkt. Daarbij is de nadruk op de formele aspecten van de verticale verantwoording in de Collegeverklaring en assurance rapport, (te) groot. Een meer pragmatische verticale verantwoording die op specifieke onderwerpen een College- of raadbehandeling vraagt is wenselijk.

De assurance rapporten, die nu worden opgesteld naar aanleiding van de Collegeverklaring van de gemeenten, zijn assertion based. Een dergelijk rapport en audit spitst zich toe op het al of niet voldoen aan het normenkader.
Een weging van de specifieke risico's van een gemeente en eventuele maatschappelijke effecten worden daarin bijvoorbeeld niet meegenomen.
In plaats van de huidige baseline audit zou een risk based verantwoording en/of risk based audit, welke flexibel zou inspelen op risico's en thema's met relevante maatschappelijk effecten, meer aanspreken en dynamiek geven.

Dit zeker wanneer deze geïntegreerd zouden kunnen worden – middels te maken afspraken met NBA en NOREA[1] – in de reguliere PDCA-cyclus en jaarrapportages (Collegeplan, begroting, jaarverslag en -rekening), met een referentie naar de College doelstellingen. Immers; alles wat in de BIO staat is ook relevant voor de IT-omgeving die de processen ondersteunt die in het kader van het financieel beheer en daarmee de jaarrekening van belang zijn.

- Het is noodzakelijk dat de verantwoording en taal over de informatiebeveiliging beter aansluit bij de belevingswereld van College, raad en management.
  De omvang van de huidige rapportages moet tot het minimaal noodzakelijke worden beperkt. Het is aan gemeenten, BZK en VNG om in afstemming met de stelselhouders te zoeken naar de beste balans tussen beoogd effect en administratieve noodzaak.

  Daarbij zou een traject waarbij er, in plaats van de huidige baseline audit - wanneer het gaat om informatieveiligheid - ingezet wordt op een risk based verantwoording en risk based audit, welke flexibele zo inspelen op risico's en thema's met relevante maatschappelijke effecten, alle betrokkenen meer aanspreken en dynamiek geven.

  De mogelijkheid tot nuancering van de antwoorden en coherentie in de verschillende vragenlijsten draagt bij aan een verlaging van onnodige complexiteit en administratieve last. In de BIO-pilot is dit al beproefd en ook in de lopende aanbesteding wordt hier rekening mee gehouden. Dit onderwerp verdient desondanks blijvend aandacht.

[1] Het primaat ligt hiervoor bij de stelselverantwoordelijke BZK, die vanuit een integrale visie op verantwoording en toezicht op bedrijfsvoering (financieel en informatie-beveiliging) een integraal toezicht kader/beleid formuleert. Bestuurders en auditors kunnen dat vervolgens invullen. Dit regelen in Gemeentewet en 2e tranche WDO.

2

Ondersteunt het ENSIA-stelsel de stelselhouders/toezichthouders voldoende om in hun informatiebehoefte te voorzien?

- Krijgt de stelselhouder/ toezichthouder met de ENSIA-informatie voldoende inzicht in de situatie rond het respectievelijke domein bij de deelnemers?
- Hoe kan dit effectiever en efficiënter?

Nog niet alle (rijks)stelsel(houder)s zijn onderdeel zijn van de verantwoording. ENSIA zou logischerwijs uitgebreid kunnen worden naar andere (rijks)stelsels (houders).

Een wettelijke basis voor het gebruik van ENSIA binnen die stelsels wordt door een aantal partijen als een randvoorwaarde (zie ook rode draad 1- Wet GR) gezien. De introductie van nieuwe (rijks)stelsel(houder)s binnen ENSIA moet getrapt plaatsvinden.

Momenteel wordt alleen voor DigiD/ Logius en voor SUWI/ BKWI een assurance-rapport opgesteld. De andere toezichthouders steunen voor de beveiligings-rapportage op de zelfevaluatie van de gemeente en aparte stelsel specifieke vragenlijsten.

De verticale verantwoording over DigiD enerzijds en SUWI anderzijds zijn van een andere orde. DigiD is een voornamelijk technische audit op een webapplicatie met een eigen vooral technisch normenkader, gebaseerd op de NCSC-beveiligings-richtlijnen voor webapplicaties, dat afwijkt van de BIO. Daarbij zijn technische penetratietesten een belangrijk onderdeel. Weliswaar is het een vitaal onderdeel van de Nederlandse generieke digitale infrastructuur, maar een te specifiek (en voor bestuurders technisch lastig leesbaar) onderdeel van het huidige ENSIA-stelsel.

De verantwoording en audit over DigiD zou daarom op een andere wijze kunnen worden georganiseerd. Het gesprek hierover is ingezet en zou - onder regie van de stelselhouder BZK DGOO/DO – met grotere snelheid moeten worden afgerond, rekening houdend met de belangen van de gemeenten (incl. de verantwoordings-rapporten aan College en raad) en Logius. Waarbij gekeken wordt hoe de DigiD audit wel kan meelopen in een efficiënt verantwoordingsproces binnen de gemeenten. Zodat voor beide partijen (verticaal en horizontaal) een pragmatische werkwijze ontstaat.

De SUWI-normen sluiten wel volledig aan op de BIO en passen goed binnen de horizontale verantwoording. Dat komt doordat de SUWI-norm gebaseerd is op de BIO en het, qua scope en opzet, nauw aansluit bij de overige bedrijfsvoering.

3

- In welke mate draagt het ENSIA-stelsel bij aan het terugdringen van de verantwoordingslast voor gemeenten?
- Wat zijn mogelijkheden om de verantwoordingslast verder terug te dringen?

Er is te veel spanning tussen de verticale en horizontale wijze van rapporteren. De druk in het verantwoordingsproces is te groot doordat, naast de opmerkingen onder rode draad 1, de Colleges en de raad ten behoeve van de verticale rapportages ook allerlei bijlagen formeel moeten goedkeuren. In het algemeen leidt dit bij gemeenten, waar het verantwoordingsproces nog onvoldoende op orde is c.q. deskundigheid ontbreekt, tot druk in het verantwoordingsproces.

Gemeenten worden op meerdere momenten in de tijd belast met audits op gelijksoortige (informatiebeveiliging) onderwerpen. Voor de verticale verantwoording en controle (niet informatiebeveiliging onderwerpen!) wordt o.a. gebruik gemaakt van monitoring op basis van de behaalde resultaten uit de zelfevaluatie. Ook vinden er onderzoeken plaats op basis van thema's en/of selecties waarbij het doel is om de effectiviteit en de betrouwbaarheid van de zelfevaluatie bij de gemeenten te toetsen.

De audit-aanpak zoals nu ingericht is dan ook niet integraal en brengt daarmee een hogere belasting bij zowel de toezichthouders en gemeenten. De inrichting van de huidige assurance kan efficiënter worden ingericht. De VNG, stelsel/ toezicht-houders en auditcommité zouden nadrukkelijker onder leiding van BZK DGOO/DO aan een voorstel moeten werken dat voorziet in een effectievere en efficiëntere inzet van audits ten behoeve van de horizontale en verticale verantwoording.

Zorg ervoor dat er voor de zelfevaluatie op één manier vragen worden gesteld, en daar dan ook één rapportage met afzonderlijke resultaten gegenereerd worden op een zodanige wijze dat de toezichthouder kan monitoren op de resultaten. De meest voor de hand liggende optie is om de vragenlijsten en inhoudelijke informatie over de persoonsgegevens te splitsen in plaats van dat nu de vragenlijsten gesplitst worden in de domeinvragen en informatiebeveiligings-vragen. Het is voor geen enkele partij handig om de verantwoording voor het uitvoeren van de zelfevaluatie in 2 tools te blijven gebruiken.

Sommige gemeenten gebruiken information security managementsystemen (ISMS) in hun dagelijkse bedrijfsvoering. De informatie uit deze tooling kan niet geïmporteerd worden in ENSIA en is niet altijd toereikend, waardoor gemeenten dubbel moeten registeren.

Er zijn performance problemen met de huidige ENSIA tooling. De huidige ENSIA tooling kost veel tijd, er zijn veel redundante handelingen nodig.

4

- Voldoet de governance rond het ENSIA-stelsel?
- Op welke punten kan de governance van het stelsel worden verbeterd?

Er is qua governance onvoldoende eenduidigheid over de rollen van de verschillende partijen/ ministeries en er moet meer ruimte zijn om met nieuwe ontwikkelingen mee te bewegen. Een interdepartementale en integrale visie/beleid op toezicht ontbreekt.
Dat is beleidsmatig onverstandig. De integraliteit is onvoldoende geborgd en checks en balances verdienen meer aandacht.

De huidige inrichting van de governance kent bij bepaalde overleggen overlappingen die de bestuurbaarheid van het stelsel (en de samenwerking) bemoeilijken. Een herijking van de bestaande governance leidend tot een adequatere uitwisseling van agenda's, onderlinge informatie en (te maken en gemaakte) afspraken, mede ten behoeve van het meenemen van eenieders achterban in het besluitvormingsproces, is gewenst.

Er is geen beleidscyclus waardoor uitvoeringsproblemen onvoldoende gestructureerd bij de regiegroep ENSIA of BZK DGOO/DO terecht komen en vice versa. De implementatie van de BIO is belangrijk. De stelselhouders zouden zich uit moeten spreken over de BIO binnen hun stelsel inspanningen van de gemeenten en inspanningen van de stelselhouders. Bij SZW/SUWI is het gevolgde keten(overleg) model relevant. BZK DGOO/DO, als stelselhouder, zou – evt. op een vergelijkbare wijze - een sterkere regierol dienen te gaan spelen. Dit ook door een centrale, op risicoafweging gebaseerde, overheid brede toezicht visie te ontwikkelen.

De financiering is nog onvoldoende robuust verankerd in de planning- en control cyclus van BZK waardoor er voor de beheerder van de tooling en voor NOREA-risico's voor de continuïteit en/of inzetbaarheid kunnen ontstaan. Bij de gewenste, nieuwe rolverdeling tussen BZK en VNG, zal ook duidelijkheid over de financiering en de verankering in de P&C-cyclus moeten worden gegeven.

5

- Wat gaat goed in het ENSIA-stelsel en moet zeker blijven?
- Wat gaat niet goed in het ENSIA-stelsel en moet worden veranderd?
- Wat ontbreekt in het ENSIA-stelsel en zou moeten worden toegevoegd?
- Is het ENSIA-stelsel voldoende toekomst vast?
- Wat zijn kansen en wat zijn de bedreigingen?

Niets veranderen wordt door alle betrokkenen als een bedreiging voor het ENSIA – stelsel en doelstellingen beschouwd!

Vooral de spanning tussen de belangen, gegeven de verschillende doelstellingen en eisen van de verticale en de horizontale rapportages, is een aandachtspunt.

Aanpassing van de wijze waarop de DigiD en RvIG (informatiebeveiliging) audits nu verticaal binnen ENSIA zijn geregeld (met aandacht voor DGBRW) onder de voorwaarde dat die aanpassing niet leidt tot minder integraliteit van de horizontale rapportage, zou (ook vanwege de huidige deadline problematiek van de RvIG audit[2]) al tot sterke verbeteringen kunnen leiden.

Ook de overgang naar de BIO, mits uniform, wordt als een kans beschouwd.
Een traject waarbij er, in plaats van de huidige baseline audit, ingezet wordt op een risk based verantwoording en risk based audit, welke flexibel zou inspelen op risico's en thema's met relevante maatschappelijk effecten, zou alle betrokkenen meer aanspreken en dynamiek geven.

Dit zeker wanneer deze geïntegreerd zou worden in de reguliere PDCA-cyclus en jaarrapportages, met een referentie naar de college doelstellingen. Immers; alles wat in de BIO staat is relevant voor de jaarrekening[3].

De oplossing van de verbetering van de werking van het ENSIA-stelsel ligt in het antwoord op de vraag waar de verschillende groepen elkaar kunnen vinden. Een sterke(re) regierol van BZK DGOO/DO is hierbij randvoorwaardelijk. Een toekomstig centraal toezichtbeleid zal hierbij sterk behulpzaam zijn.

[2] Deze wordt overigens binnenkort al aangepast van 14-2 naar 1-5
[3] Begroting en fin. Verantwoording is een volwassen proces, verantwoording over IT/informatieveiligheid nog niet

2. Suggesties

A. Met betrekking tot de financiën is het gewenst om bij de komende, nieuwe rolverdeling tussen BZK en VNG, ook duidelijkheid over de financiering en de verankering in de P&C-cyclus te geven.

B. Vanuit de NOREA wordt gesteld dat de reguliere inzet die BZK van NOREA vraagt in het algemeen - dus ook voor de ENSIA governance - meer is dan de reguliere/vrijwillige inzet van auditors voor versterking[4] van de vaktechniek binnen de NOREA.

C. Onderzoek de mogelijkheid om andere domeinen te betrekken in het ENSIA-stelsel. Het sociaal/zorgdomein is een goed voorbeeld omdat binnen dat domein veel (risicovolle) informatie wordt gedeeld.

[4] Generiek thema NORA (niet alleen voor ENSIA, maar ook m.b.t. AVG, VIPP en WDO

3. Discussiepunten

A. De ENSIA-doelstelling is tweeledig; eenduidige normatiek (dus overal dezelfde normen) en single information audit = eenmalige audit. Door gebruikers (gemeenten en toezichthouders) worden verschillende accenten gelegd. De toezichthouders leggen daarbij vooral het accent op het verkrijgen van verantwoordingsinformatie over informatieveiligheid, terwijl de gemeenten juist meer belang hebben bij integraal overzicht (waaronder informatie-veiligheid) en eenmalige (IT) audit. Deze verschillende benaderingswijzen leiden ertoe dat waar verticaal eerder sprake is van minder via het ENSIA-stelsel, er een horizontale wens is tot meer integratie en uitbreiding van stelselhouders.

B. Door sommigen wordt ENSIA niet als “stelsel” gezien, maar meer als een platform waar verschillende stelsels, kaders en toezichthouders op samenkomen.

C. Informatieveiligheid, de verantwoording daarover, wordt niet opgeleverd door de samenwerkingsverbanden. De wettelijke kaders laten dat niet toe[5], waardoor er in de uitvoering onduidelijkheid ontstaat over mandatering en delegatie. De Wet Gemeenschappelijke Regelingen (WGR) heeft een oplossing daarvoor niet in zich. De Baseline Informatiebeveiliging Overheid (BIO) ondersteunt het definiëren van groeipaden, maar biedt niet het noodzakelijke wettelijke kader voor deze vraagstukken.

[5] In de praktijk is alleen het financieel beheer geregeld en niet de informatiebeveiliging.

4. Aanbevolen stappenplan voor versterking in de tijd

Korte termijn (1-2 jaar)
Acties

1. Allereerst de lopende trajecten afronden (bijvoorbeeld de recent afgeronde BIO-pilot, de aanpassingen van het SUWI-normenkader (UVW/ SVB/ Gemeenten) en de uitvoering van het project vervanging ENSIA tooling.

   Duidelijk maken op welke wijze evaluatie/toezicht/audit zal plaatsvinden op basis van BIO-Implementatie.

2. Ga, onder duidelijke regie c.q. het primaat van de stelselhouder BZK DGOO/DO (in onze optiek is het voor onderstaande stappen een randvoorwaarde dat in deze er bestuurlijke betrokkenheid vanuit BZK DGOO/DO plaats dient te vinden), gesprekken aan ten behoeve van oplossingen van de volgende, grootste uitdagingen, en neem daarbij in acht dat dit tevens een cultuurveranderingstraject is.

   Een cultuurveranderingsproces waarin men het goede gesprek, met oog voor elkaars en het gemeenschappelijk belang en minder vanuit (eigen) deelbelangen, met elkaar heeft. Dit om onderling te komen tot gemeenschappelijkheid en eenduidigheid over zaken als verantwoordelijkheden, rollen, taken, begrippen en de te ondernemen acties. Waarbij in de totstandkoming daarvan ieder Regieraad lid zijn eigen achterban voldoende meeneemt. Zodanig dat ook de achterban de keuzes in het kader van het gezamenlijk belang kan accepteren.

   a. Expliciteer de tweeledigheid[6] van de doelstelling van het ENSIA-stelsel en organiseer dat daar verdere invulling aan kan worden gegeven;
   b. Per verticale rapportagelijn een pragmatische(r) werkwijze vinden;
   c. Begin daarmee bij de huidige DigiD audit;
   d. Ga daarbij ook het gesprek aan hoe het aantal bijlagen, ten behoeve van de verticale rapportages, zo beperkt mogelijk zouden kunnen worden. Maak daarbij gebruik van de nieuwe (management by exception) rapportagevorm, zoals afgesproken naar aanleiding van de BIO-pilot;
   e. De informatiebehoefte van de verschillende stelsel- en toezichthouders uniform[7] maken;
   f. Dit mede alvast in gedachten van cq vooruitlopend op een, vanuit BZK op te stellen, centraal toezichtbeleid;
   g. De uitdaging ligt in het leren praten over de informatiebeveiligingsrisico's, de noodzaak van datakwaliteit, en het maatschappelijk effect daarvan;

[6] Eenduidige normatiek (dus overal dezelfde normen) en single information audit = eenmalige audit
[7] Zie, bij de rode draden, de suggesties m.b.t. DigiD en RvIG.

h. De effectiviteit zou hoger zijn bij het, gezamenlijk met alle betrokkenen, vinden van een betere balans tussen leesbaarheid en assurance;
i. Afspraken beginnen te maken t.b.v. integratie IT auditing en RA-jaarrapportage;
j. Risico gestuurd (op basis van actuele risico's), thema gerelateerd (bijv. toegangsbeveiliging) en begrijpelijk voor de business (wethouders en gemeenteraad) rapporteren en auditen;
k. Vooral inzetten op aantoonbare groei van de volwassenheid op de horizontale rapportage en op de werking van informatiebeveiliging focussen.
l. Houdt haalbaarheidstoetsen in geval van nieuw beleid.

3. Zorg, middels een herijking, voor een aangescherpte en voor alle partijen zeer duidelijke invulling van de governance. Waarin bestuurders in de Regieraad richting geven, stevig koers houden en besluiten nemen over verschillende zienswijzen en uitgangspunt en die bij de partijen bestaan en momenteel in de operatie tot inefficiëntie en irritatie leiden. Daarbij (middels reguliere agendering als een soort lopende actielijst) gebruik makend van een gezamenlijk vastgesteld stappenplan.

4. Denk na en ga oriënterend al het gesprek aan[8], over een vergelijkbaar governance model, met andere stelselhouders (zoals IenM bij waterschappen), t.b.v. provincies en waterschappen onder (stelsel)verantwoordelijkheid van BZK/DGOO.

5. Begin alvast vanuit ENSIA-perspectief – voorafgaand aan komende wetgeving - over de te ontwikkelen centrale, op risicoafweging gebaseerde, rijksoverheid brede toezicht visie na te denken.

Langere termijn 3-4 jaar

Acties

6. De te auditen systemen (bijv. BRP – basisregistratie persoonsgegevens) uitbreiden.

[8] Dit past binnen 2e tranche WDO en eerder onderzoek

1. Bijlage 1: Onderzoeksvragen t.b.v. de evaluatie van het ENSIA-stelsel

Generieke vragen (opgesteld door de Regiegroep d.d. 9-9-2019)

1. Ondersteunt het ENSIA-stelsel voldoende bij het op orde krijgen van de informatiebeveiliging en de andere in het stelsel opgenomen domeinen?

a) Zorgt het ervoor dat het onderwerp op de agenda's van bestuurders en management komt en blijft?

b) Leidt het hanteren van de ENSIA-systematiek tot een groter bewustzijn op bestuurlijk niveau (bijv. bij het College van B&W en de Raad)?

c) Hoe kan dit effectiever en efficiënter?

2. Ondersteunt het ENSIA-stelsel de stelselhouders/toezichthouders voldoende om in hun informatiebehoefte te voorzien?

a) Krijgt de stelselhouder/ toezichthouder met de ENSIA-informatie voldoende inzicht in de situatie rond het respectievelijke zorgdomein bij de deelnemers?

b) Hoe kan dit effectiever en efficiënter?

3. In welke mate draagt het ENSIA-stelsel bij aan het terugdringen van de verantwoordingslast voor gemeenten?

   Wat zijn mogelijkheden om de verantwoordingslast verder terug te dringen?

4. Voldoet de governance rond het ENSIA-stelsel?

   Op welke punten kan de governance van het stelsel worden verbeterd?

5. Voldoet de huidige financieringsstructuur?

   Op welke punten kan de financieringsstructuur worden verbeterd?

6. Wat gaat goed in het ENSIA-stelsel en moet zeker blijven?

7. Wat gaat niet goed in het ENSIA-stelsel en moet worden veranderd?

8. Wat ontbreekt in het ENSIA-stelsel en zou moeten worden toegevoegd?

9. Is het ENSIA-stelsel voldoende toekomst vast?

a) Wat zijn kansen?

b) Wat zijn bedreigingen?

Specifieke/aanvullende vragen (opgesteld door het evaluatieteam)

Auditors

- Hoe waardeert u de huidige audit uitgangspunten en –praktijk van het ESIA-stelsel?
- Geven de oordelen (van de audits) een reëel beeld (opzet, bestaan en werking)?

Gebruikers

- Leidt het hanteren van de ESIA-systematiek tot een goed beeld van de situatie van de werking van de informatiebeveiliging?
- Leidt het hanteren van de ENSIA-systematiek tot een groter bewustzijn in de dagelijkse uitvoering?
- Hoe kan dit effectiever en efficiënter?

Procesbegeleiders

- Hoe waardeert u de werkbaarheid van de ESIA-systematiek voor gebruikers?
- Ziet u mogelijkheden tot verbetering?

2. Bijlage 2 Lijst met deelnemende partijen en evaluatiegesprekken

Datum	Groep
16-jan 6-feb	Auditor/Bas de Wit Auditors
21-feb	BZK/DGOO/DO/cluster cybersecurity en openbaar bestuur Frank Heijligers
10-feb	Toezichthouders
12-feb 20-feb	Procesbegeleiders
13-feb	Beheerder tooling
27-feb	Gemeenten
27-feb	Regiegroep

3. Bijlage 3: Lijst met gebruikte afkortingen

Afkorting	Definitie
BIO	Baseline Informatiebeveiliging Overheid
BKWI	Bureau Keteninformatisering Werk en Inkomen
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
DGOO	Directoraat-generaal Overheidsorganisatie
DGOO/DO	Directoraat-generaal Overheidsorganisatie/Directie Digitale Overheid
DigiD	Digitale Identiteit
ENSIA	Eenduidige Normatiek Single Information Audit
ISMS	Information Security Management System
NBA	Koninklijke Nederlandse Beroepsorganisatie van Accountants
NOREA	Nederlandse Orde van Register EDP-auditors
PDCA-cyclus	plan-do-check-act cyclus
RA	Registeraccountant
RvIG	Rijksdienst voor Identiteitsgegevens
SUWI	Structuur Uitvoeringsorganisatie Werk en Inkomen
SZW	Ministerie van Sociale Zaken en Werkgelegenheid
VNG	Vereniging van Nederlandse Gemeenten
VNGR	Vereniging van Nederlandse Gemeenten Realisatie
WGR	Wet gemeenschappelijke regelingen