KWALITEITS INSTITUUT NEDERLANDSE GEMEENTEN

ENSIA IMPACTANALYSE

Een onderzoek naar impact van de implementatie van ENSIA

KWALITEITS INSTITUUT NEDERLANDSE GEMEENTEN

Datum	28 februari 2017
Versie	1.1/2.0

INHOUD

1 MANAGEMENTSAMENVATTING

1.1 Achtergrond

In 2013 hebben gemeenten een VNG-resolutie aangenomen waarin staat dat informatieveiligheid een randvoorwaarde is voor de professionele gemeente. In de resolutie hebben gemeenten afgesproken hun eigen toezichthouder, de gemeenteraad, in het jaarverslag te informeren over informatieveiligheid. Met de resolutie namen gemeenten de BIG (Baseline Informatieveiligheid Nederlandse Gemeenten) aan als het gemeentelijke basisnormenkader voor informatieveiligheid. Daarnaast vroegen ze aan de minister van BZK de audit- en monitorlast van gemeenten te verminderen. Dat gebeurt met het ENSIA-principe. ENSIA staat voor Eenduidige Normatiek Single Information Audit. D afzonderlijke audits en verantwoording voor BRP, PUN, DigiD, BAG, BGT en Suwi zijn opgenomen in één verantwoordingssystematiek die uitgaat van de BIG en aansluit bij de planning- en controlcyclus van gemeenten en wordt ondersteund door de ENSIA-tool. ENSIA is een gezamenlijk project van de ministeries van BZK, SZW en I&M in samenwerking met VNG.

In de periode augustus tot en met december 2016 is een pilot uitgevoerd in zeven gemeenten om de in dit kader ontwikkelde vragenlijst en tool te beproeven. Het ministerie van BZK heeft, met het oog op de naderende uitrol bij gemeenten, KING gevraagd om een impactanalyse te maken over de impact die de implementatie van ENSIA op gemeenten heeft.

1.2 Aanpak

Aan de hand van een uitgewerkte vragenlijst impactanalyse heeft KING interviews gehouden met ondersteunende organisaties (IBD, ICTU, BZK), met verticale toezichthouders (Logius, BZK, BKWI, SZW, RvIG, IenM) en met gemeenten. Bij gemeenten is zowel gekeken naar de ervaringen van de zeven pilotgemeenten als van gemeenten die niet aan de pilot hebben deelgenomen. Er is gesproken met portefeuillehouders, managers, CISO’s en vragenlijstinvullers vanuit de diverse domeinen. De totstandkoming van de impactanalyse is begeleid door een begeleidingscommissie met vertegenwoordigers van BZK, VNG en KING. De werkgroep Implementatie en Communicatie vormde de klankbordgroep. KING heeft de impactanalyse uitgevoerd in de periode 1 oktober t/m 16 november 2016.

1.3 Conclusie

Op basis van de impactanalyse trekt KING de conclusie dat alle betroken stakeholders enthousiast zijn over het idee van ENSIA en dat de tool en vragenlijst rijp genoeg zijn voor uitrol.
Randvoorwaarden voor een succesvolle uitrol in 2017 zijn:

1. verschuiven van periode van invullen van ENSIA-tool naar 1 juli tot 31 december
2. een eenduidig vastgesteld en gedocumenteerd verantwoordingsproces, inclusief normen, tijdpad en rapportage;
3. een eenduidig vastgesteld en gedocumenteerd auditproces inclusief scope, reikwijdte, normering en ondersteuningsproducten voor de audit;
4. het beperken van ENSIA- verantwoording en audit tot DigiD en Suwi;
5. het realiseren van deze randvoorwaarden uiterlijk drie maanden voor de start van de implementatie.

KING adviseert het Ministerie van BZK om in 2017 te starten met de implementatie van ENSIA en 2017 te beschouwen als een gezamenlijk leerjaar.

2 ONDERZOEK

2.1 Aanleiding

Sinds het Diginotar-incident en Lektober in 2011 staat informatieveiligheid op de politiek-bestuurlijke agenda. De Onderzoeksraad voor Veiligheid heeft onderzoek gedaan naar het Diginotar-incident en constateerde onder meer dat er een noodzaak was tot versterking van het bewustzijn ten aanzien van informatieveiligheid en daaraan gerelateerde risico's, alsmede de sturing daarop. In reactie daarop heeft de minister van BZK op 13 februari 2013 met de verschillende overheidslagen afgesproken dat zij elk werk zullen maken van verplichtende zelfregulering op informatieveiligheid. De minister heeft de Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID) ingesteld om de verschillende overheidslagen hierbij te ondersteunen. Deze Taskforce was belast met het verhogen van het bewustzijn over het belang van en de kennis over informatieveiligheid bij bestuurders en topmanagers in het openbaar bestuur.

De Taskforce BID heeft haar werkzaamheden inmiddels afgerond. De gemeenten hebben tijdens de BALV VNG op 29 november 2013 de Resolutie informatieveiligheid aangenomen. Daarin onderkennen gemeenten het belang van informatieveiligheid en wordt de Baseline Informatieveiligheid Gemeenten (BIG) vastgesteld als hét gemeentelijk basisnormenkader en de basis voor het gemeentelijk informatieveiligheidsbeleid. Wel vragen gemeenten van het Rijk dat de BIG als basisnormenkader wordt erkend en dat wet- en regelgeving zo beperkt mogelijk worden gehouden. Specifiek aan de minister van BZK vraagt de VNG namens de gemeenten om hergebruik van bestaande informatie en beperking van audit- en monitorlast met het principe van Single Information Single Audit als uitgangspunt. Dit verzoek van de VNG vormt de aanleiding voor het project ENSIA: Eenduidige Normering Single Information Audit.

In het kader van het project ENSIA zijn in periode juli 2015 – september 2016 de volgende producten ontwikkeld:

- Een zelfevaluatievragenlijst informatieveiligheid over de BIG, BRP, PUN, DigiD, BAG, BGT en SUWI
- Een verantwoordingsstructuur voor ENSIA
- Informatievoorziening in de vorm van een tool voor het uitvragen van de zelfevaluatie
- Communicatieproducten zoals artikelen en workshops

Dit document is een impactanalyse t.b.v. de invoering van ENSIA-Verantwoordingsproces met bijbehorende tool bij alle gemeenten.

2.2 Opdrachtgever

Opdrachtgever voor het schrijven van de impactanalyse is het Ministerie van BZK. KING is de opdrachtnemer.

2.3 Stakeholders

Er is een groot aantal stakeholders bij het project ENSIA betrokken:

- BZK – als trekker van het project
- Gemeenten – verantwoordelijk voor horizontale en verticale verantwoording
- VNG – belangenbehartiger van gemeenten
- ICTU – beheerder van tool
- IBD – ontwikkeling van de vragenlijst
- Toezichthouders – als afnemers van verticale verantwoording - Logius, BKWI, RvIG, I&M
- Departementen – in beleidsontwikkeling t.b.v. toezichthouders – SZW, BZK, I&M

2.4 Doel en afbakening

Scope ENSIA

De scope van ENSIA is het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid gebaseerd op de BIG dat in 2017 door alle gemeenten wordt gebruikt voor de verantwoording over BRP, PUN, Digid, SuwiNet, BAG en BGT. Uitgangspunt hierbij is dat het horizontale verantwoordingsproces aan de gemeenteraad de basis vormt voor het verticale verantwoordingsproces aan nationale partijen die een rol hebben in het toezicht op informatieveiligheid. Bij het afleggen van verantwoording wordt het principe van single information audit toegepast; alle informatie die noodzakelijk is voor verticale verantwoording is ook onderdeel van het horizontale verantwoordingsproces.

Doel impactanalyse

Het doel van de impactanalyse is om te toetsen of het verantwoordingstelsel ENSIA met bijbehorende tool aansluit bij de behoeften van gemeenten, nieuwe gemeentelijke ontwikkelingen en of succesvolle grootschalige implementatie binnen gestelde kaders van het verantwoordingsstelsel ENSIA.

Prestatie-indicatoren

In de offerte die KING voor het ministerie van BZK heeft opgesteld zijn zes prestatie-indicatoren benoemd. De impactanalyse zal inzicht moeten leveren op deze prestatie-indicatoren:

1. Business Case (verwachtte kosten en baten voor een gemiddelde gemeente)
2. Effect op Werkprocessen, Organisatie en Informatievoorzieningen.
3. Gemiddelde doorlooptijd van implementatie (aansluiting en inregeling)
4. Behoefte aan implementatie-ondersteuning, collectieve aanpak (Check Digitale agenda 2020) en inrichting en planning van de gewenste ondersteuning.
5. De wijze van organiseren van het verantwoordingsstelsel, inclusief beheerorganisatie) en op welke wijze naast de inspecties (inclusief beleidsdepartementen en beheerpartijen) ook de gemeenten de resultaten kunnen gebruiken voor doorvoeren van verbeteringen.
6. De vraag hoe externe audit vorm kan worden gegeven.

Afbakening

Naast de impactanalyse zijn een aantal andere evaluaties uitgevoerd:

- Evaluatie van vragenlijst en tool door ICTU
- Evaluatie van auditproces door ADR
- Evaluatie van inhoudelijke vragenlijst BAG/BGT door Ministerie van I&M.

Meer gedetailleerde ervaringen t.a.v. tool en vragenlijst zijn aan ICTU teruggekoppeld; t.a.v. auditproces aan ADR. Ervaringen t.a.v. de inhoudelijke vragenlijst BAG/BGT die door gemeenten naar voren zijn gebracht zijn opgenomen in bijlage 1.

De impactanalyse is uitgevoerd op de ervaringen van de (pilot)gemeenten en toezichthouders in de periode 1 oktober t/m 16 november. Sommige geconstateerde verbeterpunten zijn reeds opgepakt in het project. Voor de volledigheid hebben we deze nog wel opgenomen in het rapport.

2.5 Projectaanpak

De totstandkoming van de impactanalyse is begeleid door een begeleidingscommissie met vertegenwoordigers van BZK, VNG en KING. De werkgroep Implementatie en Communicatie vormde de klankbordgroep voor de impactanalyse. Hier is op 11 oktober de aanpak gepresenteerd;

op 8 november zouden de eerste resultaten worden voorgelegd (bijeenkomst is vervallen) en op 28 november zijn de eindresultaten gepresenteerd.

Voor deze impactanalyse zijn de volgende activiteiten uitgevoerd:
- Achtergronddocumentatie verzameld en verwerkt
- Interviews met vertegenwoordigers van IBD, KING, ICTU, BZK, VNG
- Vragenlijst opgesteld op basis van checklist impactanalyse KING. Deze checklist impactanalyse is vergeleken met vragenlijst evaluatieprotocol, zoals vastgesteld in stuurgroep, en vervolgens getoetst aan hoofdvragen van het plan van aanpak Impactanalyse KING en de daarin geformuleerde prestatie-indicatoren. De vragenlijst bevatte uiteindelijk een groslijst van hoofdthema's per gemeentelijke doelgroep met verdiepingsvragen.
- Diepte-interviews pilot-gemeenten Arnhem, Zeewolde, Edam-Volendam
  Gesprekken met CISO, invullers van de zelfevaluatie vanuit de verschillende domeinen, concerncontrol en indien mogelijk portefeuillehouder
- Validerende interviews met projectleiders pilots Den Bosch, Het Bildt, Zaandam en Tiel
- Gesprek met portefeuillehouders in Zeewolde, Zaandam en Het Bildt
- Diepte-interviews niet-pilotgemeenten Haaren en Vught (Via het VIAG-netwerk zijn gemeenten opgeroepen voor deelname aan een groepsinterview. Aan deze gesprekken deden vertegenwoordigers vanuit alle domeinen, ict en CISO mee.
- Interviews met toezichthouders Logius, BZK, BKWI, SZW, RvIG, IenM
- Van alle interviews zijn gespreksverslagen gemaakt die zijn teruggelegd bij de geïnterviewden.

Voor een overzicht van geraadpleegde bronnen en geïnterviewden zie bijlage 2.

Kanttekening
De pilotgemeenten kenmerken zich door een geschiedenis met de totstandkoming van de BIG en de ontwikkeling van ENSIA zelf. Zij zijn hierdoor goed op de hoogte. Voor een goede toetsing van de impact op gemeenten had KING graag meer gemeenten geïnterviewd die nog niet bij de pilot waren betrokken. Vanwege de korte doorlooptijd van de impactanalyse is dit slechts bij twee gemeenten gelukt. Het is van belang om de resultaten van de impactanalyse in dit licht te beschouwen.

2.6 Leeswijzer

Dit rapport gaat allereerst in op de ervaringen van gemeenten gerelateerd aan de scopafijth. Hierbij worden ook beantwoording van de vragen van het evaluatieprotocol meegenomen (hoofdstuk 3). Hoofdstuk 4 bevat de visie en ervaringen van de toezichthouders. Hoofdstuk 5 toetst de resultaten aan de prestatie-indicatoren. De impactanalyse sluit af met conclusie en aanbevelingen in hoofdstuk 6. In de bijlage is een overzicht opgenomen van interviews.

3 IMPACT OP INDIVIDUELE GEMEENTE

Dit hoofdstuk gaat in op de ervaringen van gemeenten met de vragenlijst, tool, verantwoordingsproces en audit aan de hand van SCOPAFIJTH-vragen.[1]

3.1 Security en privacy

De ENSIA-tool is een webapplicatie op basis van Cviews platform in beheer van een niet-overheidspartij, Totta. Het platform wordt gebruikt voor Vensters voor Bedrijfsvoering (VvB), welke in gebruik is door gemeenten. Bij VvB gaat het om een vrijwillig vergelijking van de gemeente met andere gemeenten over bedrijfsvoeringissues. Het gebruik van VvB voor het uitwisselen van (verantwoording)informatie over informatieveiligheid stelt extra eisen aan de applicatie. Vanuit ICTU, IBD en KING is aangegeven dat:

- Er zijn een aantal beveiligingseisen vastgesteld: HTTPS met HSTS, two-factor authenticatie en jaarlijkse pentest.
- Een Pentest op platform ensia.nl is uitgevoerd. Penetratietest heeft enkele blokkerende bevindingen opgeleverd. Deze bevindingen worden onder coördinatie van ICTU door de leverancier opgepakt.
- Het is niet noodzakelijk om e-herkenning te gebruiken voor de authenticatie.

Aandachtspunten

- Er is een bewerkersovereenkomst (tussen KING-ICTU-TOTTA) voor Vensters voor Bedrijfsvoering. Voor ENSIA zou dit nog moeten worden gemaakt.
- Er heeft geen baselinetoets BIG plaatsgevonden.
- Mogelijk moeten er nog meer maatregelen worden genomen op basis van de BIG, de beveiligingsrichtlijn voor webapplicaties (NCSC) en de standaarden conform de *pas-toe-of-leg-uit* lijst van het forum standaardisatie.

3.2 Communicatie

De hoofdlijnen van ENSIA en het bijbehorende verantwoordingsproces zijn redelijk bekend bij de relevante stakeholders van de gesproken gemeenten. Men baseert zich op informatie afkomstig van VNG. Vooral de mensen vanuit de ICT zijn goed op de hoogte. Bij de bestuurders en college is ENSIA minder bekend. Raadsleden zijn gedurende de impactanalyse niet gesproken.

Raad en college worden door CISO's geïnformeerd over informatieveiligheid. Hoewel bewustwording en aandacht voor privacy toeneemt, is het bewustzijn over Informatieveiligheid bij het bestuur nog niet op het gewenste niveau. De betrokkenheid van portefeuillehouders is afhankelijk van de kennis en achtergrond. Dit geldt ook voor de raad. Projectleiders ervaren de betrokkenheid van de raad als beperkt. CISO's krijgen nauwelijks reacties op hun berichtgeving naar de raad. Hoewel alle relevante stakeholders. waaronder burgemeester, CISO en portefeuillehouder, de communicatie richting de raad en college belangrijk vinden, lijkt er sprake van m.n. ad hoc communicatie.

Aandachtspunten:

- Verwachting is dat er op strategisch niveau zware druk komt te liggen. VNG/KING zal hier alert op moeten zijn en een bewustwordingscampagne richting bestuurders en directie moeten organiseren. Factsheets en bezoeken door visitatiecommissie kunnen daar positief bijdragen.
- Voor een succesvolle uitrol volgende jaar is goede PR wenselijk. Via gemeentesecretarissen, commissies van VN en branche-organisaties.
- Communicatie voor proceseigenaren van stelsels binnen de gemeente.

[1] Security en privacy, communicatie, organisatie, personeel, administratieve organisatie, financieel,informatievoorziening, juridisch en technologie.

- Aandacht voor informatieveiligheid wordt door betrokkenen gepositioneerd in het domein van bedrijfsvoering, wanneer informatieveiligheid in het domein van veiligheid in het algemeen, privacy of dienstverlening wordt gepositioneerd zou het mogelijk meer aandacht krijgen.

3.3 Organisatie

3.3.1. Impact op werkprocessen

Er wordt geen of nauwelijks impact op de werkprocessen verwacht. Op het gebied van stelsels hebben gemeenten alle noodzakelijke processen al ingericht. Op het gebied van ICT en audit kunnen kleine aanpassingen nodig zijn.

3.3.2. Organisatieverandering

Gemeenten verwachten niet dat een verandering van organisatie nodig is a.g.v. implementeren van ENSIA. De invoering van ENSIA kan mogelijk wel effect hebben op de organisatie als gevolg van de externe druk die ontstaat om de BIG in te voeren. Daar waar gemeenten aan het begin staan van de implementatie van de BIG, is het mogelijk dat ENSIA indirect wel organisatieverandering tot gevolg heeft. Denk hierbij bijvoorbeeld aan de invulling van de rol van de CISO of de positie van de CISO in de organisatie.

Sommige gemeenten zijn voornemens ENSIA volgend jaar projectmatig op te pakken. Andere gemeenten hebben nog geen beeld hoe ze het volgend jaar willen organiseren. In elk van de gemeenten is in ieder geval een rol voor de CISO weggelegd in het realiseren van ENSIA. Als projectleider of in de aansturing van de projectleider.

3.3.3. Opdrachtgeverschap

Als intern opdrachtgever voor ENSIA wordt genoemd de portefeuillehouder in het college van B&W die de gemeentesecretaris opdracht geeft ENSIA te implementeren.

3.4 Personeel

3.4.1. Benodigde kennis

Medewerkers die ENSIA-vragen moeten beantwoorden, hebben over het algemeen de nodige kennis als het gaat om stelsel specifieke (DigiD, BAG/BGT, SuwiNet etc) vragen. Het beantwoorden van generieke BIG-informatiebeveiligingsvragen van tactisch, - strategisch aard is voor hen wel een uitdaging. Het is belangrijk dat de juiste mensen de juiste vragen ontvangen.

Aanpassing van functieprofielen kan wenselijk zijn. Dit is niet in elk HR-systeem mogelijk. Om aan te sluiten op HR21 is het van belang om informatieveiligheid jaarlijks in een taakgesprek met een medewerker te bespreken. Extra opleiding is niet noodzakelijk. Bewustwording via ENSIA zal maar beperkt effect hebben, aangezien slechts een beperkt aantal mensen bij het invullen van de vragenlijst is betrokken. Diverse gemeenten zijn voornemens separaat awareness campagnes informatieveiligheid te houden.

ENSIA vereist wel gedragsverandering van medewerkers – het realiseren van informatieveiligheid is een gezamenlijke verantwoordelijkheid.

Sommige gemeenten willen parallel aan ENSIA ook een nieuw ISMS-systeem uitrollen. Invullers hebben veelal geen kennis van ISMS-systemen; dit kan vertragend werken.

3.4.2. Impact op werkdruk

Er wordt op lange termijn een gunstig effect op de werklast van het personeel verwacht. Er is geen nieuw werk toegevoegd; wat medewerkers doen, doen ze al.

Bovenstaande geldt echter niet voor de eerste jaar. Verwachting is dat het in ieder geval volgend jaar meer tijd gaat kosten. Dat ligt volgens CISO's niet aan de implementatie van ENSIA maar aan de mate waarin de BIG is geïmplementeerd. Hierdoor is tijdens de uitrol volgend jaar mogelijk tijdelijk inzet van extra resources nodig. Deze extra inzet is volledig afhankelijk van het volwassenheidsniveau van de desbetreffende gemeente voor wat betreft BIG-invoering. Hoe verder een bepaalde gemeente met de invoering van BIG is, hoe minder is de benodigde extra inzet in komende jaren.

3.5 Administratieve organisatie

De verwachting van betrokken gemeenten is dat de invoering van ENSIA beperkt dan wel geen impact zal hebben op hun administratieve organisatie. Mocht zo'n aanpassing wel noodzakelijk zijn, dan is dat volgens hen niet te wijten aan ENSIA maar de invoering van de BIG. Gemeenten zijn van mening dat ENSIA goed aansluit bij bestaande taken. Een volledigheidscheck op de werkinstructies zal wel nodig zijn.

Wat opvalt is dat bijna alle gesproken gemeenten parallel aan ENSIA-uitrol ook overwegen een ISMS-systeem aan te schaffen en uit te rollen. Gedachte hierbij is dat met de inrichting van ISMS, administratieve organisatie zelf gaan ontstaan.

3.6 Financieel (Business Case)

Geen enkele gemeente had een business-case of is voornemens om een business-case op te stellen. Het idee van een business case speelt niet bij gemeenten. In de gesprekken heeft KING gevraagd naar verwachtte kosten en materiële dan wel immateriële baten.

3.6.1. Kosten

Over het algemeen gaat men er vanuit dat de invoering van ENSIA geen noemenswaardige extra kosten met zich mee brengt. De realisatie zal onderdeel vormen van regulier werk; het zijn m.n. interne uren, die veelal niet worden doorbelast. Pilotgemeenten hebben voor ENSIA voor 2017 geen kosten geraamd.

Mogelijk zijn er wel extra kosten t.b.v. de audit. Hoewel ten tijde van onze gesprekken met de gemeenten de gehele audit-cyclus nog niet was doorgelopen, had men het gevoel dat de auditlasten waren verdubbeld en daardoor ook de auditkosten mogelijk zouden gaan stijgen. Gesuggereerd is dat het financieel zou gaan om een verdubbeling van de kosten die nu voor een Digid-audit door gemeenten moeten worden betaald. De daadwerkelijke hoogte wordt mede bepaald door de mate waarin er al dan niet reeds een SUWI-audit werd gedaan en de mate waarin er met TPM's wordt gewerkt. Overige financiële reserveringen die zijn genoemd, hadden niet zo zeer te maken met ENSIA-invoering maar vooral met BIG-invoering, ISMS-aanschaf en invoering etc.

3.6.2. Baten

Gesproken vertegenwoordigers van de gemeenten hadden geen zicht over de mogelijke materiële baten van de ENSIA-invoering. Alle gemeenten zagen immateriële baten: bewustwording, bijdrage aan BIG-invoering, door beantwoording vragen overzicht over je eigen verbeterpunten, helpt om informatieveiligheid richting raad en bestuur te positioneren, vergroting efficiency van verticale verantwoording, procesverbetering en imagoverbetering.

Aandachtspunt

- Om auditkosten te besparen is geopperd een pre-audit door iemand met auditkennis te laten doen (kan niet dezelfde persoon zijn die de daadwerkelijke audit doet), zodat je weet of je klaar bent voor de audit. Tevens is voorgesteld dat gemeenten elkaar onderling zouden toetsen. Beide zouden gemeenten geld kunnen schelen.

3.7 Informatievoorziening [Evaluatieprotocol]

3.7.1. Vragenlijst

De ENSIA-vragenlijst zoals in de tool opgenomen omvat ongeveer 70 procent van de BIG-normen. Daarnaast zijn domein-specifieke vragen opgenomen. De gemiddelde vragenlijst voor gemeenten bevat tussen de 250 en 300 vragen.

De ENSIA-vragenlijst wordt door zowel pilot als niet-pilotgemeenten in het algemeen positief beoordeeld. Doordat de beantwoording van de vragen elk jaar op het voorgaande jaar voortbouwt verwacht men dat het elk jaar makkelijker wordt. Desalniettemin zijn er kritische opmerkingen geplaatst t.a.v. aanscherpen van vraagstelling, uitbreiding van toelichting, afkortingen, kunnen toevoegen van evidence in tool, het uit elkaar halen van generieke en domeinspecifieke vragen en/of vragen op strategisch, tactisch en operationeel niveau. Tevens zijn opmerkingen over de domein-specifieke vragen gemaakt. De in de impactanalyse opgehaalde opmerkingen over de vragenlijst zijn teruggekoppeld aan ICTU en IBD ter verdere aanscherping van de vragenlijst.

Wensen t.a.v. de doorontwikkeling van de vragenlijst zijn slechts in beperkt aantal gesprekken aan de orde gekomen. Als suggesties voor doorontwikkeling zijn genoemd: DigiD-specifieke vragen verwijderen, meer ruimte voor ‘zoeklichten’ en toevoegen van financiële audits.

Aandachtspunten

- Hoe om te gaan met als iets in het ene stelsel wel is ingericht en in het andere stelsel niet? Bij vragen die meerdere domeinen dekken kan het antwoord per domein anders zijn
- De wens om generieke beveiligingsvragen los te koppelen van de stelsel-specifieke vragen zou nader moeten worden bekeken. Juist de confrontatie met informatieveiligheidsvragen die een medewerker niet direct kan beantwoorden, zou bewustwording kunnen creëren.
- Voor wat betreft de omvang geeft één projectleider aan de omvang van de vragenlijst zoals deze nu is wel als het maximale te beschouwen dat kan worden gevraagd.

3.7.2. Tool

De tool wordt in het algemeen als positief beoordeeld. Werken met de tool is eenvoudig, overzichtelijk en de tool is makkelijk toegankelijk.[2]

Aandachtspunten zijn:

- Bij navigatie onderscheid maken tussen strategische, tactische en operationele vragen.
- Vanuit het perspectief van het makkelijk kunnen vullen van de vragenlijst is een verdere opsplitsing in tags en mogelijkheden van toewijzing wenselijk. Evenals het uit elkaar trekken van vragen op ICT en stelsel-niveau. Anderzijds kan juist het inzicht in verschillen van beantwoording en de onmogelijkheid om vragen te beantwoorden, een proces van gedeelde verantwoordelijkheid en beeld van informatieveiligheid creëren. Hierdoor zou organisatie-breed bewustzijn van informatieveiligheid kunnen toenemen. Het is goed om nog een keer kritisch te kijken naar de inrichting van de vragenlijst vanuit de doelstelling van het project.
- Beheermodule verbeteren door toekennen rechten op het niveau van een stelsel. Ook waren er projectleiders die de voorkeur gaven aan het per vraag kunnen toewijzen aan medewerkers.
- Verbetering dashboardfunctie gewenst is, zodat zichtbaar is hoever een medewerker is met de aan hem toegewezen vragen óf hoever het beantwoorden van de vragen gerelateerd aan één stelsel is gevorderd.

3.7.3. Invulproces

De pilot werd gecoördineerd door een ***projectleider***, meestal een CISO. De projectleider moet intern voldoende mandaat, kennis van vakgebied en natuurlijk evenwicht hebben. "Van belang is dat het een medewerker van de gemeente is die deze rol invult, zodat het rendement in huis blijft." "Als een CISO maar vier of acht uur per week heeft is het moeilijk om de rol van CISO echt goed te kunnen invullen." In de pilotgemeenten waren zowel fulltime als parttime CISO's betrokken.

Sommige gemeenten hebben een ***kick-off*** georganiseerd voor medewerkers die de ENSIA-vragenlijst zouden gaan invullen; soms werd management hier ook voor uitgenodigd. Met de kick-off werd gezamenlijkheid gecreëerd. Een gemeente wil volgend jaar aan het begin van het implementatietraject een presentatie voor zowel college als raad houden. In de meeste gemeenten zijn ***managers*** in beperkte mate betrokken. Tijdens een van de groepsinterviews gaven alle betrokken managers aan volgend jaar tijdens de transitie betrokken blijven en in ieder geval bij de kick-off aanwezig zijn. "Managers zullen de ENSIA-aspecten in eigen teams moeten bespreken, ook als mensen zelf geen vragen hoeven in te vullen."

In iedere gemeente waren er tussen de 10 en 15 personen betrokken bij het ***beantwoorden*** van de vragenlijst. Voor projectleiders was het niet altijd makkelijk om te bepalen wie welke vraag moet beantwoorden. Het inventariseren en beleggen van de vragen bij medewerkers nam voor CISO wel wat tijd in beslag. Een gemeente geeft aan: "Invullers zijn niet altijd dezelfde mensen als voorheen. Voorheen lag de nadruk op inhoud, nu meer vanuit bedrijfsvoering." De meeste projectleiders hebben alle betrokken een user-id gegeven. Daarbij bleek dat het niet voor alle mensen even makkelijk was om de vragen te beantwoorden. Dit had te maken met de generieke vragen die meerdere stelsels raken. De scope was niet voor alle invullers helder. In een gemeente heeft de CISO alles ingevuld en daarbij collega's betrokken, dat beviel hem goed. In een andere gemeente is het invullen echt een groepsproces geweest. Een projectleider uit weer een andere gemeente heeft zich voorgenomen om volgend jaar interviews met mensen te plannen om hen te

[2] De in de impactanalyse opgehaalde opmerkingen over de tool zijn teruggekoppeld aan ICTU.

helpen de vragenlijst in te vullen. In een gemeente werd gebruikgemaakt van een ISMS. De vragen zijn uit ENSIA geëxporteerd en uitgezet via ISMS bij invullers. In deze gemeente heeft alleen de coördinator de ENSIA-tool gebruikt.

Gemeenten maken de inschatting dat het beantwoorden van de vragen zelf niet de uitdaging is. De uitdaging ligt meer op het terrein van ***organisatorische complexiteit*** en indien nodig samenstellen van ontbrekende ***documentatie*** als bewijsmateriaal. De verwachting is dat gemeenten deze documentatie nu niet op orde hebben. Gemeenten zouden deze documentatie zelf moeten verzamelen dan wel opstellen en hier geen externe medewerkers voor aan moeten trekken. Het gaat immers niet in de eerste plaats om het op orde hebben van het papierwerk, maar om het op orde krijgen van de eigen informatieveiligheid. Eén gemeente merkt op: "Beantwoording van de vragen zal niet hetzelfde kwaliteitsniveau hebben als voorheen." Dit is te wijten aan de overgang van de verantwoording per domein naar een integrale verantwoording over de domeinen heen.

3.7.4. Rapportage uit de ENSIA-Tooling

Na uploaden door de gemeente wordt de zelfevaluatievragenlijst bevroren. Wijziging van de vragenlijst is dan alleen nog mogelijk door de centrale administrator van ICTU. De tool biedt verschillende soorten rapportages.

De rapportage voor horizontale verantwoording bevatte op het moment van de impactanalyse een integrale lijst met ingevulde vragen en antwoorden. Gedurende de impactanalyse is door de IBD-vertegenwoordiger een weging aan de keycontrols gehangen. Hierdoor kan een rapportage worden gemaakt met top 3 wat gaat goed en top 3 wat gaat beter. Tevens is de mogelijkheid gecreëerd om een rapportage per BIG-hoofdstuk en per verantwoordingstelsel uit te draaien. De weging is nog niet getoetst bij gemeenten. Voor gemeenten is deze weging niet helder: welke normen zijn wel en welke niet meegenomen en hoe dat is gewogen. CISO: "*Als ik dit rapporteer aan de wethouder, dan kan ik de eventuele vragen niet beantwoorden. Omdat ik niet weet hoe die score is samengesteld. Als de scores niet bevallen en mensen willen uitleg, wat dan*?"

Niet alle gemeenten hadden op het moment van gesprek de rapportages al bekeken. Eén gemeente had net ontdekt dat er rapportages waren. Een andere gemeente beschouwt de rapportages als niet echt geweldig. De rapportage uit de tooling is in geen enkele gemeente voorgelegd aan portefeuillehouder of raad.

Aandachtspunten
- Het is wenselijk om de weging van antwoorden te toetsen bij gemeenten
- Wellicht is het zinvol om een rapportage zowel voor management als college B&W/raad te maken. zij kijken immers vanuit verschillende behoeften? Vanuit perspectief van horizontale verantwoording lijkt het zinvol om te onderzoeken welk type rapportage een raad zou willen ontvangen, bijvoorbeeld via raadslid.nu.

3.7.5. Samenwerkingsverbanden

Veel gemeenten werken samen in een of meerdere samenwerkingsverbanden. In de pilot zijn geen samenwerkingsverbanden betrokken. Pilotgemeenten, die in een samenwerkingsverband werken, hebben voor slechts één gemeente in dat samenwerkingsverband de ENSIA-tool ingevuld. Het beeld is dat de ENSIA-Tool gemeenschappelijke regelingen onvoldoende ondersteunt. Vragen over organisatie heen(keten) kan complexiteit opleveren.

Aandachtspunten
- Toetsing van werking van ENSIA-tool in samenwerkingsverbanden heeft niet plaatsgevonden
- Invullen door SSC voor meerdere gemeenten moet ook voor meerdere gemeenten eenvoudig bruikbaar zijn; wellicht mogelijk om met soort TPM te werken?
- Idee om tool ook ter beschikking te stellen aan SSC zodat vragen over jaren heen worden vastgelegd. Dit zou dan zonder mogelijkheid van horizontale en verticale rapportage zijn.

3.7.6. Audit

Het auditproces bij gemeenten was ten tijde van de impactanalyse nog in volle gang. Geen van de projectleiders hadden, op het moment van het interview, het auditrapport gezien. Uit de gesprekken blijkt dat gemeenten heel verschillend zijn ge-audit. Bij de ene gemeente keek de auditor in detail, meer zwart/wit; andere gemeenten geven aan dat er werd meegedacht. De positie en planning van de audit in het verantwoordingsproces was niet helder. Het kostte veel tijd om evidence ter onderbouwing van de beantwoording te verzamelen, dan wel indien noodzakelijk aan te passen of te creëren: aantal documenten loopt uiteen van 25 voor alleen keycontrols tot 157 documenten in andere gemeente. Door het toenemen van het aantal audit-vragen verwachten gemeenten dat de kosten omhoog zullen gaan (verdubbeling van kosten van Digid-audit). Een ander zorgpunt is hoe auditors oordelen als er op het ene domein onvoldoende wordt gescoord en op andere domeinen voldoende – is dan alles onvoldoende? Gemeenten verwachten dat er voldoende capaciteit in markt is; de introductie van ENSIA creëert markt. Tot slot is het, vanwege de onduidelijkheden in het auditproces, voor gemeenten nog te vroeg om aan te geven of deze audit een verbetering is t.o.v het huidige proces.

Aandachtspunten voor gemeenten t.a.v. de audit:
- Ontwikkelen van guidance voor auditors zodat gemeenten op vergelijkbare wijze worden ge-audit
- Begin vroeg met de zelfevaluatie, zodat je verbeteringen tussentijds kunt doorvoeren
- Vroegtijdig meerdere offertes vragen voor auditors;
- Bij samenwerkingsverbanden wordt aangeraden om gezamenlijk een auditor te zoeken. Dit voorkomt dat de ene gemeente positief oordeel krijgt waar in een andere gemeente de auditor op basis van zelfde informatie een ander oordeel krijgt;
- Uitvoeren van pre-audits – dan weet je of je er goed voor staat en wat je nog moet aanpassen;
- Organiseren van peer review op zelfevaluatie – onderling toetsen scheelt geld dat anders aan auditor moet worden besteed.
- Het inhuren van consultants om de documentatie op orde te brengen is minder passend in een traject waar het om leren leren gaat; het is belangrijker om het proces te verbeteren (risico documenten wel en proces niet op orde);
- Gekozen auditor eventueel toegang geven tot de ingevulde zelfevaluatie.

3.7.7. Geschiktheid voor benchmark?

Het nut van benchmarking met de ENSIA-tool wordt heel uiteenlopend beoordeeld vanuit verschillende beelden die men bij benchmarken heeft:
- Vergelijken op hoofdlijnen of de volledige vragenlijst
- Een openbare vergelijking (waar.staat.je. gemeente.nl) of binnen de tool
- Op gemeentenaam of anoniem (bijv. vergelijken met gemeenten van vergelijkbare grootte)
- Vanuit rol van bestuurder of vanuit rol van medewerker
- Op termijn of vanaf 2017

Pilotgemeenten zijn positiever over benchmarken dan de niet-pilotgemeenten. Vanuit pilotgemeenten is het beeld dat portefeuillehouders wel openbaar zouden willen vergelijken op

hoofdlijnen ongeacht hoe men scoort op de benchmark. Op medewerkersniveau is men meer terughoudend en denkt men eerder aan anoniem benchmarken. Men is nog volop bezig om de BIG te implementeren en er valt nog voldoende te leren door implementatie in de eigen organisatie. Vergelijken met andere organisaties voegt daar in huidige fase niet veel aan toe.

Gemeenten zijn zich er van bewust dat zij, op termijn, de toegezegde transparantie ook na moeten komen. " Men zal wel rekening moeten houden met het verschil tussen bestuurlijke informatie die openbaar moet zijn en de technisch inhoudelijke informatiebeveiligingsissues waarmee men terughoudend moet zijn met openbaarmaking."

3.7.8. Implementeerbaarheid

Doordat de ENSIA-vragen met bijbehorend proces en governance grotendeels zijn gebaseerd op de BIG, is het stadium van BIG-Invoering in een gemeente mede bepalend voor de mate waarin de desbetreffende gemeente in staat is om ENSIA te implementeren. Uit de gesprekken blijkt dat de meeste gemeenten voor wat betreft BIG-invoering nog lang niet zo ver zijn; dit geldt ook voor de pilotgemeenten zelf. Vooral voor kleine gemeenten kan dit lastig zijn.

Anderzijds stelt een van de projectleiders van een G32-gemeenten dat ENSIA op huidige manier voor grotere gemeenten niet goed gaat werken en meer geschikt is voor toezichthouders. Voor kleine gemeenten vindt hij het beter geschikt. Kans op succes bij kleine gemeenten acht hij dan ook veel groter. Dit met name door beperkte coördinatielast als gevolg overzichtelijkheid van de organisatie bij kleine gemeenten.

Het ontbreken van de implementatie van de BIG heeft niet zo zeer impact op de beantwoording van de ENSIA-vragen zelf, maar wel op de tijdige verzameling dan wel samenstelling van bewijsmateriaal die nodig is voor een succesvolle audit – aangezien het gaat om een grotere hoeveelheid vragen. Als een gemeente eerder een risico-analyse heeft gemaakt en aan de slag is gegaan met informatieveiligheid zal een groot deel van de gevraagde documentatie reeds aanwezig zijn.[3]

Gemeenten beschouwen vragenlijst en tool zelf als goed implementeerbaar. Echter voor samenwerkingsverbanden zijn tool en vragenlijst noch organisatorische impact in de pilot getest.

Gemeenten is gevraagd hoe zij aankijken tegen de implementatie van ENSIA in 2017. Alle gemeenten zijn in principe voorstander voor uitrol in 2017. Ze hebben voldoende vertrouwen dat ze het kunnen. Voornaamste argumenten voor een uitrol in 2017 is de angst om momentum te missen, dat uitstel tot afstel leidt, om te leren en verwachtte bijdrage die ENSIA gaat leveren voor BIG implementatie (als stok achter de deur; resolutie is al in 2013 aangenomen). Gemeenten hebben wel twijfels of het de overige gemeenten lukt om volgend jaar alles op tijd af te hebben. Suggesties voor een meer gefaseerde uitrol in 2017 zijn: in 2017 alleen de huidige gebruikelijke audit en pas daarna ENSIA uitrol of het verkleinen van scope door bijvoorbeeld in eerste jaar alleen key-controls uit rollen. Deze zijn zo belangrijk die zou elke gemeente ook echt op orde moeten hebben. In ieder geval is het belangrijk om stappenplan voor gemeenten op te stellen. Gemeenten beschouwen het commitment van de verticale toezichthouders als een cruciale randvoorwaarde voor de uitrol.

[3] Als een gemeente besluit om bepaalde BIG maatregelen niet of later te implementeren, dan zal een ENSIA vraag negatief worden beantwoord, maar is dan toch goed uitlegbaar. Als een gemeente in ENSIA slecht scoort omdat ze nog maar net gestart zijn met de BIG dan is er niets aan de hand. Als ze maar een goede planning hebben dan kunnen ze dat uitleggen. Onderbouwen met documentatie is wel makkelijker met implementatie van BIG.

Bovenstaande antwoorden moeten worden bezien in het licht van ervaringen van gemeenten die merendeels (vijf van de zeven pilotgemeenten) al een aantal jaar zijn betrokken bij de ontwikkeling van de BIG zelf en aansluitend ENSIA. Dit levert mogelijk een vertekening in positieve zin op.

3.7.9. Risico's

Gemeenten signaleren de volgende risico's bij de implementatie van het ENSIA- gedachtengoed en de ENSIA-tool:

- Het door de gemeente uitvoeren van een gap-en risico-analyse is van belang voor de opzet, inrichting en uitvoering van ENSIA. Het per hoofdstuk implementeren van de BIG is niet de oplossing voor informatieveiligheid
- Als het invullen van de vragenlijst als het doel c.q. een invuloefening wordt gezien, levert het schijnzekerheid op
- "Beperkt beschikbaarheid van CISO (als informatieveiligheidsadviseur en overall coördinator) in combinatie met beperkt bevoegdheden is zeker een risico voor de succesvolle uitrol"
- Spanningsveld tussen dienstverlening en informatieveiligheid.
- Werkdruk van medewerkers of bezuinigingstaakstelling kan er voor zorgen dat mensen die kennis en ervaring de invulling van vragenlijst niet kunnen doen c.q. andere verantwoordingen voorrang krijgen.
- Informatieveiligheid als sluitstuk is onacceptabel risico.
- Het kan zijn dat als men denkt dat gaat onze auditlasten verminderen, dat het vertaald wordt naar afslanking c.q. mensen verdwijnen.

Het is van belang om bij de implementatieondersteuning rekening te houden met deze risico's.

3.7.10. KING/VNG Ondersteuning

Gemeenten is gevraagd welke behoefte aan ondersteuning zij gedurende de implementatie van KING of VNG verwachten dan wel wat voor andere gemeenten zinvolle ondersteuning zou kunnen zijn.

Het blijkt dat gemeenten niet stil hebben gestaan bij het feit dat het gaat om een extern gehoste webapplicatie. Gemeenten nemen stilzwijgend aan dat zaken zoals: security, hosting, technisch en functioneel beheer, doorontwikkeling van deze applicatie buiten hen om door landelijke partijen goed is geregeld.

Gemeenten hebben behoefte aan ondersteuning op het terrein van intern draagvlak, betrokkenheid van de bestuur en raad, bewustwording van alle stakeholders, coaching /begeleiding en indien nodig een snel antwoord op hun vragen. Diverse gemeenten benadrukten het belang van aandacht voor strategisch draagvlak. Hoe kunnen gemeentesecretarissen, wethouders en raadsleden meer bewust worden van het belang van informatieveiligheid? De visitatiecommissie heeft hierin zeker geholpen, maar er is nog steeds meer nodig. "Bestuur meenemen, vreemde ogen dwingen". Vwb bestuurlijke ondersteuning: "Eerder door VNG dan door KING".

Voorbeelden van mogelijke ondersteuningsproducten die zijn genoemd zijn:

- Regiobijeenkomsten voor algemene toelichting en netwerkvorming
- Procesondersteuning voor de inrichting en organisatie op locatie bij gemeenten
- Stappenplan voor gemeente (vgl Digid-stappenplan)
- Ondersteuning bij werking van de tool, vergelijk ondersteuning van ICTU tijdens pilot
- Ondersteuning bij de interpretatie van de vragenlijst. "Hoe moet ik deze vraag interpreteren?" (functioneel inhoudelijke ondersteuning)

- Centraal aanspreekpunt dat vragen verzamelt en antwoorden terugkoppelt.
- Communicatie gericht op de diverse doelgroepen binnen gemeenten (raad, portefeuillehouder, CISO, invullers)
- Gebruikmakend van doelgroep-specifieke kanalen (Vereniging van Gemeentesecretarissen (VGS), VIAG, raadslid.nu)
- Informatie vanuit stelsels richting domeinmedewerkers én vanuit ENSIA
- Communicatie, guidance-richtlijnen voor auditors

3.7.11. ISMS systemen

In vrijwel alle gesprekken met gemeenten is het gebruik van ISMS aan de orde geweest. ISMS is een Informatie Security Management System. Met een dergelijk systeem kan workflow worden bijgehouden, acties worden toegewezen en vastgelegd en voortgang worden bewaakt. (Voor meer informatie zie www.ibdgemeenten.nl). D.m.v. een import en exportfunctie kunnen vragen uit de ENSIA-tool worden ingelezen in het ISMS systeem; en de antwoorden geëxporteerd in de ENSIA-tool.
Twee betrokken gemeenten gebruiken ISMS. Via ISMS kunnen ENSIA vragen aan medewerkers worden uitgezet en voortgang worden bewaakt; het is niet nodig om medewerkers toegang te geven tot ENSIA. Twee gemeenten zijn bezig met een aanbestedingstraject voor ISMS en twee gemeenten oriënteren zich op het aanschaffen. Zij hebben het beeld dat ISMS het proces makkelijker en overzichtelijker kan maken. "Je krijgt een beter beeld van uitgezette acties." "Met 6 systemen lukt het nog wel in Excel, maar met 60 systemen heb je echt een ISMS nodig." Een van de gemeenten heeft besloten om geen gebruik te maken van een ISMS-systeem, omdat men van mening is dat aandacht voor informatieveiligheid verankerd moet zijn in de manier van werken.

Belangrijk voor de bruikbaarheid van ISMS is de mogelijkheid van een import en exportfunctie vanuit de ENSIA-tool naar ISMS. Een van de ISMS-leveranciers heeft dit nu geregeld. Voor alle ISMS-leveranciers wordt begin december een voorlichtingsbijeenkomst georganiseerd.

Aandachtspunt
- het gebruik van een ISMS-systeem kan ondersteunend werken, maar is geen voorwaarde voor implementatie van ENSIA.

3.8 Juridisch

De invoering van ENSIA heeft juridisch gezien geen directe impact op de gemeenten.

De ENSIA-tool is gebaseerd op de onlineapplicatie *CViews* van het bedrijf *Totta Research*. *Totta Research* is hostingpartner waar alle data straks wordt bewaard. Juridische aanscherping is wenselijk t.a.v. de volgende aspecten:
- Contract-technische afspraken tussen ICTU als serviceprovider en de Totta Research als hostingpartner/softwareleverancier (Underpinning Contract)
- SLA tussen Serviceprovider en gebruikersorganisatie (gemeenten en eventueel toezichthouders).
- Wat gebeurt er als de gemeente de zelfevaluatie heeft geüpload, maar de verticale toezichthouder deze niet heeft ontvangen.
- Eigenaarschap van de gegevens
- Het moeten opnemen van de collegeverklaring in het jaarverslag moet mogelijk een weerslag krijgen in regelgeving rondom jaarverslag of Comptabiliteitswet. Dit is nog een uitzoekpunt.

3.9 Technologie

Gemeenten hebben nauwelijks opmerkingen gemaakt over de achterliggende technologie. Ze nemen stilzwijgend aan dat de dienstverlener hier voldoende bij stil heeft gestaan. Gemeenten en ICTU gaven aan dat deze tool in ieder geval geen impact zal hebben op het gemeentelijke IT-landschap en daarmee gemeentelijke IT-Architectuur. Pilot-gemeenten hebben voldoende vertrouwen dat de ENSIA-tool ook gaat werken voor overige gemeenten; vraag is of de opgeleverde tool ook voldoende dekking biedt voor samenwerkingsverbanden. Op dat terrein valt in de tool een en ander te verbeteren vond men.

ICTU die momenteel acteert als ontwikkelaar en beheerder van de tool, had op het gebied van technologie volgende antwoorden:

- *Projectarchitectuur:* Er is geen P(S)A. ICTU-architect is aan het begin betrokken geweest, deze had geen opmerkingen over een noodzaak van een PSA. Bewust is gekozen voor bestaande techniek uit te markt.
- *Sourcecode:* ENSIA-tool is geen open source. Source code is niet beschikbaar voor ICTU. Eventuele aanpassingen in de code gaat via ICTU naar leverancier.
- *Koppelingen:* Koppeling met ISMS kan handig zijn. Excelexport is mogelijk.
- *Procesmodellen:* Geen procesmodellen aanwezig.
- *Webrichtlijnen:* Deze richtlijnen zijn bedoeld om websites zo breed mogelijk toegankelijk te maken. ICTU heeft via www.gewoontoegankelijk.nl een geautomatiseerde scan gedaan. Voor de ENSIA-tool zijn er 11 aandachtpunten. Het grootste gebrek is dat niet overal alternatieve teksten achter bv. knoppen of formulieropties zijn geprogrammeerd zodat deze voor blinden raadpleegbaar zijn. ICTU streeft om vóór implementatie verbeterpunten te hebben gerealiseerd en een goede toegankelijkheidsverklaring te hebben ontvangen. (https://www.digitoegankelijk.nl/onderwerpen/toegankelijkheidsverklaring)
- ENSIA is wel berekend op grootschalig gebruik.

Vanuit gemeenten bezien is het wenselijk dat er een gebruikersgroep wordt geformeerd om functionele wensen t.a.v. doorontwikkeling tooling groepsgewijs te toetsen. Wat technisch mogelijk is, is vanuit gemeentelijk perspectief niet altijd wenselijk.

4 IMPACT OP TOEZICHTHOUDERS

4.1 LOGIUS | DigiD

4.1.1. Algemeen

Logius bemoeit zich niet met inhoud van de vragen. Gebruikelijke werkwijze is: uitvoeren van een controle op de ingeleverde stukken en bij tekortkoming het geven van tijd om alsnog ontbrekende stukken aan te vullen. Verder geeft Logius ook geen advies aan desbetreffende gemeente, wat ze wel doen is de procesbegeleiding. In de huidige situatie gaat ongeveer 70% van de DigiD verantwoordingen niet in keer goed. Dit betekent veel interventie door Logius.

4.1.2. Standpunt voor uitrol in 2017

Logius denkt dat ENSIA zal zorgen voor meer bewustwording en control bij de gemeenten. Om momentum ook niet te missen is Logius voorstander van het uitrol in 2017. Logius vindt het belangrijk dat de gemeenten tijdens de uitrol en transitie goed worden gefaciliteerd. Specifieke aandachtspunten hierbij zijn: TPM's, verbetertrajecten en meerdere aansluitingen. Een andere voorwaarde die ze aan deze uitrol stellen is dat ze de informatie die ze nu krijgen (uiterst in de periode tussen 1 jan-1 mei) via ENSIA blijven ontvangen.

4.1.3. Security

Informatiebeveiligingseisen aan de tool zijn belangrijk en de tool moet zelf ook voldoen aan informatiebeveiligingsnormen.

4.1.4. Communicatie

Logius heeft behoefte aan een door KING/VNG samengestelde Communicatieplan over ENSIA.
Logius hanteert identieke communicatie aan alle aansluithouders, daar past geen ENSIA-specifieke communicatie in. De communicatie richting alle aansluithouders ziet er als volgt uit:

- FAQ op website
- Eind november 2016 mail naar contactpersonen (meestal CISO): "Let op verantwoording komt eraan!"
- Herinnering in januari dat iedereen auditrapport moet aanleveren
- 7 mei melding van "in gebreke stellingen"

4.1.5. Organisatie en personeel

Er wordt geen impact op de organisatie of personeel van Logius verwacht. Impact op de administratieve organisatie is ook minimaal en zal volgens Logius m.n. gaan over kleine aanpassingen in logistiek en andere brievenbus.

4.1.6. Informatievoorziening | Evaluatieprotocol

Gesproken personen van Logius hebben toegang tot de ENSIA-tool, maar hebben de ENSIA-vragenlijst en de ENSIA-rapporten nog niet bekeken of bestudeerd. Dit vinden ze ook niet relevant. *Wat wel belangrijk voor hen is, is een op de NOREA-standaarden gebaseerde auditverklaring. Oordeel van auditors is voor Logius leidend.* ENSIA-gebaseerde auditverklaring hebben ze ook nog niet gezien. Met andere woorden Logius heeft nog geen beeld wat ze gaan krijgen.

Auditverklaring

- De periode tussen 1 januari en 1mei ziet Logius als ideaal om auditverklaringen te ontvangen. In de beleving van Logius ontstaat bij upload op 1 oktober, in de periode vanaf 1 oktober tot 1 januari een ongecontroleerd vacuüm. Vraag is hoe hiermee om te gaan? Tussentijdse freeze zien ze als een mogelijke oplossing.

- In de huidige situatie worden TPM's meegenomen in de audit; elke aansluithouder stuurt zijn auditrapport met TPM's aan Logius toe. TPM is beperkt houdbaar. Hoe ENSIA met TPM's omgaat is voor Logius niet duidelijk.
- In de huidige situatie heeft men ook te maken met een "Lead-auditrapport" en onderlinge audit-rapporten die onder supervisie van een Lead-auditor door meerdere auditors is samengesteld. Hoe dit proces in de nieuwe situatie gaat lopen is niet helder.

4.1.7. Financieel | Businesscase

Kosten:
Verwachting is dat de invoering van ENSIA voor Logius geen extra kosten met zich meebrengt.

Baten:
- Als huidige verhouding van 70% van de verantwoordingen, met tekorten waar interventie noodzakelijk is, tegenover 30% goed verandert naar 30%-70% dan is het doel bereikt.
- ENSIA is zeer goed voor de bewustwording van gemeenten over Informatieveiligheid, hierdoor zal ook het vertrouwen van Logius in de kwaliteit van de verantwoordingen stijgen.
- Als single audit de informatiebehoefte van de Logius dekt dan zijn ze 100% voorstander van de invoering. Gedachtengoed vindt men prima.
- Doordat de gemeenten nu bewuster met beveiliging omgaan, zullen ze noodgedwongen hele jaar door onafgebroken bezig zijn met informatiebeveiliging. Hierdoor zullen de gemeenten beter in control zijn. Kwaliteit zal omhooggaan.

4.1.8. Aandachtspunten

- *Meerdere aansluitingen* – in vragenlijst kan nu slechts voor 1 aansluiting worden beantwoord, terwijl het van belang is dat gemeente invullen per aansluiting. Ook moet er per aansluiting een auditrapport worden opgesteld.
- *Nieuwe aansluitingen*: Als gemeente nieuwe aansluiting doet moet er binnen 2 maanden auditrapport zijn, daarna jaar vrijstelling. Huidige ENSIA voorziet dat niet. Zou dit er wel of niet in moeten worden opgenomen? Hoe om te gaan met wijzigingen in aansluiting
- Er zijn vaak *serviceorganisaties*. Een andere auditor stelt auditrapport op over serviceorganisatie. Het bewijs moet richting Logius. Er zijn 5 a 6 normen waarop gemeenten direct worden getoetst. Leadauditeur kijkt hiernaar – maar moet ook naar TPM's met onderliggende rapporten kijken.
- *Ontvangen van rapportage* Logius wil niet in tool kijken – is het mogelijk om automatische melding te krijgen van het uploaden door gemeenten?
- Volledigheid: wie checkt op 1 oktober of alle gemeenten hun upload hebben gedaan? Voor BZK/Logius is 1 mei is een belangrijkere datum, dan moet het Auditrapport beschikbaar zijn. Mocht het auditrapport er niet zijn, wie gaat dat escaleren, rappelleren.
- Als de rapporten door fouten in de systeem niet in database zit dan kan dat een issue worden. Wel geüpload maar niet ontvangen door verticale toezichthouder. Wie is hiervoor verantwoordelijk? Hoe kun je dit oplossen?
- *Escalatieladder* Formeel gezien moet elke structurele wijziging voor Digid worden voorgelegd aan de DigiD-afnemersraad (bestuurlijk) en klankbordgroep (ambtelijk). Escalatieladder voor Digid is x oplossen in 1 maand, x oplossen in twee of 6 maanden. NB dit is v.w.b. implementatietijdpad lastig. 60% van afnemers is gemeenten. Logius stelt dat als er geen geharmoniseerde escalatieladder is, Logius de eigen escalatieladder hanteert.

4.2 SZW | BKWI | SUWINET

4.2.1. Algemeen

Via de gezamenlijke elekronische voorzieningen SUWI (GeVS) wisselen UWV, SVB en gemeentelijke Sociale Diensten gegevens met elkaar uit voor taken op het gebied van werk en inkomen. Daarnaast zijn ook een aantal andere partijen aangesloten. De GeVS wordt in de praktijk veelal aangeduid met Suwinet. Het Bureau Keteninformatisering Werk en Inkomen (BKWI) is een afzonderlijk organisatieonderdeel van UWV en de beheerder van de centrale omgeving van de GeVS.

Naast ENSIA-project loopt op dit moment het programma : Borging Veilige Gegevensuitwisseling via SuwiNet (BVGS) om een aantal verbetermaatregelen te nemen betreffende de bescherming van persoonsgegevens bij de gegevensuitwisseling via Suwinet. BVGS en ENSIA dienen gezien de overlap en afhankelijkheden in samenhang te worden gerealiseerd. Het borgen van de samenhang tussen ENSIA en GEVS is een belangrijk aandachtspunt. Men is dan ook alert op de samenhang tussen de twee trajecten. Zodoende worden de voor Suwinet herijkte beveiligingsnormen al meegenomen in ENSIA

4.2.2. Standpunt voor uitrol in 2017

Belang van ENSIA voor de BKWI/SZW is dusdanig groot dat men ENSIA volgend jaar graag uitgevoerd/uitgerold hebben.

4.2.3. Security

Er zijn geen bijzondere security wensen.

4.2.4. Communicatie

BKWI/SZW is betrokken bij de ontwikkeling van ENSIA en zo bekend met ENSIA en het bijbehorende horizontale en verticale verantwoordingsproces. Er is geen specifieke communicatiebehoefte.

4.2.5. Organisatie en personeel

Alle afnemers van de GeVS gaan jaarlijks informatie aan BKWI ter beschikking stellen op basis waarvan BKWI een totaalrapportage over de beveiliging van de GeVS opstelt. Voor Gemeenten zal deze informatie via ENSIA aan BKWI ter beschikking worden gesteld.

Voor Suwinet worden de normenkaders herijkt en geoperationaliseerd, bijvoorbeeld door het beheer te beleggen en sommige processen opnieuw te definiëren. Het betreft hier een dynamisch proces dat continue moet worden bewaakt/beheerd en onderhouden. Speciaal voor ENSIA is het Suwinet normenkader voor afnemers naar voren gehaald. Het normenkader beheer wordt opgesteld en doorvertaald naar de organisatie BKWI. Er wordt impact op de administratieve organisatie en personele inzet van BKWI verwacht. De precieze aard en omvang is nog niet bekend. Hiervoor wordt een impactanalyse uitgevoerd.

4.2.6. Informatievoorziening | Evaluatieprotocol

- BKWI heeft de ENSIA-tool gezien, is bekend met de inhoud van de vragen en zijn hierover tevreden.
- BKWI heeft de concept ENSIA-Suwi-Rapportage gevuld met dummy-gegevens bekeken. BKWI is niet de tevreden over de rapportagemogelijkheden. Deze rapportage heeft voor BKWI geen toegevoegde waarde. Suggestie van BKWI is “GeVS-transparantie-rapportage” uitsluitend ter

beschikking te stellen aan gemeenten zelf. Dan kan deze door de CISO met (management van) Sociale Zaken, het werkplein of GR worden besproken.

- BKWI heeft rapportages met de resultaten van de zes pilot gemeenten niet gezien.
- BKWI wenst export van ENSIA-gegevens om zelf de totaalrapportage over de beveiliging van de GeVS op te stellen. De totaalrapportage is hooguit een trendanalyse, bijvoorbeeld er zijn meer dan 30% van de gemeenten die NEE hebben geantwoord op vraag X; dat kan vervolgens (mogelijk) relevante stuurinformatie zijn voor SZW of Inspectie SZW. BKWI wil nadrukkelijk niet in (zelfs de schijn van) een Toezichthoudersrol terecht komen.Met ENSIA verwacht SZW, als vervanging van de huidige incidentele onderzoeken van de Inspectie SZW, over te gaan naar een structurele oplossing waarbij gemeenten in hun planning & control-cyclus vaststellen of ze aan de gestelde beveiligingseisen voldoen.
- BKWI/SZW zou zich kunnen vinden in eindtijd zelfevaluatie 31/12. Opleveren aan SZW (verticale rapportage/collegeverklaring en auditverklaring) zou op 15 maart moeten gebeuren (zo gebeurt het nu ook). In Suwi-regeling staat dat samenvattende rapportage uiterlijk 15/3 moet zijn aangeleverd.
- *Harmoniseren van escalatieladders* is een belangrijke punt, hiervoor loopt een traject met andere beleidsdirecties en toezichthouders van de ministeries. Het verschil tussen escalatieladders DigiD en Suwi is groot. Onderlinge bereidheid om escalatieladders te stroomlijnen is in een half jaar erg verbeterd.

4.2.7. Financieel | Businesscase

Voor SZW is de Business Case niet relevant. In stuurgroep is ook besloten om niet naar BC te kijken. Over de nut en noodzaak van ENSIA heeft SZW geen twijfel.

ENSIA draagt in de beleving van BKWI sterk bij, aan het overzicht over alle gemeenten en daarmee over de gehele SuwiNet-keten heen. Met ENSIA ontstaat standaardisatie in het verantwoordingstraject; dit wordt gezien als een zeer grote efficiency slag.

4.2.8. Aandachtspunten

- Een punt van aandacht voor BKWI en SZW is dat de governance en het beheer van ENSIA nog moeten worden ingericht.
- Het borgen van de samenhang tussen ENSIA en GEVS is een belangrijk aandachtspunt.

4.3 BZK | RvIG | BRP-PUN

4.3.1. Algemeen

BZK/RviG beschouwt de rapportage, vraagstelling en inrichting van de tool als zeer belangrijk; deze moeten goed zijn. Echter, twee van de drie gesproken vertegenwoordigers van BZK en RvIG waren pas aan het einde van de ENSIA-traject erbij betrokken. Hierdoor hadden ze niet voldoende beeld van ENSIA-vragen. Derde geïnterviewde was alleen aan het begin vanuit beleidsperspectief erbij betrokken en hierdoor had ze geen beeld over de resultaten van de pilot. Twee andere vertegenwoordigers van BZK/RvIG die wel betrokken waren voor de operationele kant van het project, waren tijdens de gesprekken niet aanwezig. Vanwege bovengenoemde redenen had geen van de geïnterviewde zicht of alle RvIG gerelateerde must-vragen in de vorm van KeyControls wel of niet in ENSIA-tool staan.

Opvallend is dat een van geïnterviewden geen beeld had waarom ze elke keer bij ENSIA overleggen werd uitgenodigd en wat er precies van haar werd verwacht.

4.3.2. Standpunt voor uitrol in 2017

BZK ziet *BRP-Monitor* als een kwaliteit stimulerend instrument dat een goede bijdrage levert aan de integriteit van gegevens. Vraag is of ENSIA deze rol ook kan vervullen? De BRP-monitor is destijds bij 19 gemeenten getoetst en vragen worden elk jaar verder aangescherpt. Daarom wil BZK de BRP-monitor pas in ENSIA opnemen als deze zich bewezen heeft.

BZK/RviG heeft een afwachtende houding en pleit voor een gefaseerde uitrol in 2017.

4.3.3. Organisatie en personeel

Huidige kwaliteitsmonitor (eigen instrument van RviG) blijft naast ENSIA bestaan. Impact op eigen organisatie is verwaarloosbaar. Provincies zijn nu nog niet betrokken. Naar mate er meer niet-informatieveiligheid vragen erbij komen, zal de provincie moeten worden betrokken. Voor nu goed dat dit niet zo is.

4.3.4. Informatievoorziening | Evaluatieprotocol

Geïnterviewden kunnen geen oordeel geven de ENSIA-Tool en het bijbehorende proces van horizontale en verticale verantwoording. Geen van de geïnterviewden heeft de verticale rapportage gezien of heeft een beeld van de kwaliteit van de rapportages en de bruikbaarheid hiervan voor de verticale verantwoording.

Er is tijdens de Pilot geen contact geweest met de invullers uit de pilot gemeenten, hierdoor is er geen beeld hoe de gemeenten BRP/PUN vragen ervaren hebben. Er zijn heel veel vragen die met –Ja of met –Nee kunnen worden beantwoord. RvIG vindt dat er ook nuances mogelijk moeten zijn. Goed doorlopen van een proces hoeft niet te betekenen dat de resultaten ook goed zijn.

4.3.5. Financieel | Businesscase

RvIG geeft geen beeld erbij over de mogelijk kostenimpact op hun organisatie.
Mogelijke baten zijn:

- Vergroten van bestuurlijke aandacht op informatiebeveiliging.
- ENSIA zal als een kwaliteit stimulerend instrument positief bijdragen aan de integriteit van gegevens.

4.4 I&M | BAG-BGT

4.4.1. Algemeen

De ENSIA-vragenlijst bevat twee vragen over informatieveiligheid die van belang zijn voor BAG/BGT. Deze hebben betrekking op de Back-up en Uitwijk. Deze vragen zijn onderdeel van de Keycontrols en onderhavig aan het auditproces. In de ENSIA-tool is een separate vragenlijst opgenomen met beleidsinhoudelijke vragen; de BAG/BGT-vragenlijst. Deze vragenlijst wordt door het ministerie van I&M zelf geëvalueerd. Zie bijlage 1 voor informatie over aanpak en ervaring met deze vragenlijst welke uit gesprekken in het kader van impactanalyse naar voren is gekomen.

4.4.2. Standpunt voor uitrol in 2017

I&M hecht aan uitrol van ENSIA in 2017 en gaat mee in het tijdpad dat voor ENSIA wordt gekozen.

4.4.3. Informatievoorziening | Evaluatieprotocol

Voor I&M is een auditverklaring niet per se noodzakelijk. Informatie in de vorm van een rapport vanuit ENSIA is goed genoeg (v.w.b. ENSIA-BIG-compartiment). Een natte handtekening of waarmerk is niet noodzakelijk. Zo'n rapport is al gedefinieerd en staat in ENSIA.

Voor wat betreft harmonisatie van escalatiekanalen inzake informatiebeveiliging gaat I&M mee in de nog uit te werken escalatieladder. Deze hebben voor I&M alleen betrekking op twee BIG-normen t.a.v. back-up en uitwijk. (Voor I&M is in afgelopen 3 jaar slechts in 1 gemeente een issue geweest). I&M gaat ervanuit dat de behoeften vanuit de andere stelsels scherper zijn dan de behoeften vanuit I&M. De escalatieladder heeft geen betrekking op BAG/BGT-vragenlijsten.

5 EVALUATIE O.B.V. PRESTATIE-INDICATOREN

5.1 Business Case

Uit de gesprekken met gemeenten blijkt dat gemeenten niet naar ENSIA kijken vanuit een financiële businesscase. In de stuurgroep is eveneens aangegeven dat een financiële businesscase niet van belang is. Bij betrokkenen uit alle doelgroepen van gemeenten en toezichthouders is er draagvlak voor het achterliggende idee van ENSIA: de horizontale verantwoording als basis voor de verticale verantwoording en uitvragen d.m.v. één vragenlijst en één tool.

Gemeenten zien weinig directe kosten m.u.v. de auditkosten. Het beeld is dat de omvang van het aantal vragen dat wordt ge-audit wordt verdubbeld. Gemeenten zien baten in:

- Bevordert de governance
- Positioneert informatieveiligheid
- Bevordert bewustwording over informatieveiligheid door hele organisatie heen
- Stimuleert en/of versnelt BIG-implementatie
- Bevordert samenwerking tussen afdelingen
- Bevordert samenhang in informatieveiligheid
- Positioneert CISO

5.2 Effect op Werkprocessen, Organisatie en Informatie voorzieningen

Pilotgemeenten geven aan de impact op werkprocessen, organisatie, personeel en informatievoorziening beperkt te vinden (zie paragraaf 3.3, 3.4 en 3.5).

Om ENSIA tot een succes te maken is van belang dat er een CISO is aangesteld die voldoende tijd beschikbaar heeft, dan wel mensen om zich heen heeft om hem bij het werk te ondersteunen. Tevens is de positie van de CISO van belang. Het is handig als er een directe lijn is met een portefeuillehouder, dan wel dat de relatie met de manager zodanig is dat in overleg de portefeuillehouder kan worden geïnformeerd (zie www.ibdkinggemeenten voor functieprofiel en tips van IBD).

De mate van impact op werkprocessen, organisatie en personeel is afhankelijk van de implementatie van de BIG. In gemeenten waar de implementatie op de BIG flink op streek is, zal de implementatie van ENSIA minder impact op de organisatie hebben, dan in gemeenten waar de implementatie nog moet beginnen. De implementatie van BIG is overigens geen noodzakelijke voorwaarde, maar helpt wel. De vragenlijst ENSIA beslaat ongeveer 70 procent van de BIG-vragen.

Verschillende pilotgemeenten geven aan geen effect zien op de organisatie of organisatieverandering nodig te vinden. Mogelijk is het oordeel afhankelijk van hetgeen in ENSIA wordt benadrukt en de wijze waarop het wordt aangepakt.

1. Vanuit perspectief van invullen van vragenlijst is het mogelijk om vragenlijst als CISO grotendeels zelf in te vullen. Domeinspecialisten worden gevraagd om op inhoudelijke vragen de antwoorden te geven. Er is nauwelijks sprake van organisatieverandering.
2. Wanneer het invullen van de zelfevaluatievragenlijst mede wordt ingestoken vanuit leren leren en meer projectmatig (over de domeinen heen) wordt aangepakt lijkt men wel organisatieverandering te zien. Door in gezamenlijkheid de vragenlijst te bekijken worden

issues geconstateerd die in verschillende domeinen op verschillende manieren worden opgepakt. Hierdoor kan een meer integrale aanpak van informatieveiligheid over de domeinen worden ontwikkeld en ontstaat een meer gedeeld gevoel van verantwoordelijkheid en integraal beeld van informatieveiligheid over de domeinen heen. over de domeinen heen.

De systemen van gemeenten worden door de implementatie van ENSIA niet geraakt. Veel gemeenten zijn bezig met de oriëntatie of aanschaf van een ISMS-systeem. Een ISMS-systeem lijkt te kunnen helpen, maar is geen noodzakelijke voorwaarde voor de implementatie van ENSIA.

Benchmarken wordt door gemeenten wisselend beoordeeld. Voor 2017 lijkt dit nog niet wenselijk (er valt nog genoeg te leren), op termijn kan benchmarking zeker toegevoegde waarde leveren en is passend bij ontwikkeling naar meer transparantie.

De invoering van ENSIA heeft bij de toezichthouders nauwelijks effect op organisatie of werkprocessen. Uitzondering hierop is BKWI.

5.3 Gemiddelde doorlooptijd van implementatie

Met de gemiddelde doorlooptijd van implementatie wordt verwezen naar het aansluiten en inregelen van ENSIA in de gemeente, uitgaande van beschikbaarheid van de tool. CISO's geven aan dat het invullen van de vragenlijst vrij eenvoudig te doen is. Binnen een week zou een gemeente in principe de zelfevaluatievragenlijst kunnen opleveren. Voor de directe coördinatie wordt de inschatting gemaakt dat dit de CISO gedurende de invultijd (half jaar) een aantal uur per week kost. Invullers uit de diverse domeinen geven aan dat het invullen van de vragenlijst hen ongeveer evenveel tijd kost als met de huidige uitvraag vanuit de Rijksoverheid.

Projectleiders verwachten dat de meeste tijd nodig is voor enerzijds het doorvoeren van procesverbetering n.a.v. het invullen van de vragenlijst en anderzijds afstemming, het verzamelen van documentatie en onderbouwen van de beantwoording van de vragen mede afhankelijk van de audit. Daarom verwachten zij dat het evenveel, dan wel meer tijd kost dan nu. De tijd c.q. inspanning dat dit kost is met name afhankelijk van de mate waarin de BIG reeds is geïmplementeerd. Betrokken pilotgemeenten zijn reeds langer met BIG bezig.

Het kunnen invullen van de zelfevaluatievragenlijst gedurende een lange periode wordt door gemeenten gewaardeerd omdat dit het mogelijk maakt om tussentijds verbeteringen in beleid en werkprocessen door te voeren.

Deze prestatie-indicator speelt geen rol bij de verticale toezichthouders.

5.4 Behoefte aan implementatie-ondersteuning, collectieve aanpak en inrichting/planning van de ondersteuning

Gemeenten vinden het moeilijk om aan te geven welke ondersteuning zij bij de implementatie nodig hebben. De gemeenten die hebben meegedaan aan de pilot zijn van mening dat het hen zelf volgend jaar wel zal lukken om zelfevaluatie te realiseren. Zorgen worden m.n. geuit t.a.v. CISO's die weinig uren hebben, kleinere gemeenten, werkdruk, het organiseren van het interne proces en betrokkenheid van portefeuillehouder en raad. Ondersteuningsinstrumenten die zijn genoemd zijn:

- Regiobijeenkomsten voor algemene toelichting en netwerkvorming
- Procesondersteuning voor de inrichting en organisatie op locatie bij gemeenten
- Stappenplan (vgl Digid-stappenplan)
- Ondersteuning bij werking van de tool, vergelijk ondersteuning van ICTU tijdens pilot

- Ondersteuning bij de interpretatie van de vragenlijst. "Hoe moet ik deze vraag interpreteren?"
- Communicatie gericht op de diverse doelgroepen binnen gemeenten (raad, portefeuillehouder, CISO, invullers)
- Gebruikmakend van doelgroep-specifieke kanalen (Vereniging van Gemeentesecretarissen (VGS), VIAG, raadslid.nu)
- Informatie vanuit stelsels én vanuit ENSIA
- Communicatie, guidance-richtlijnen voor auditors

Vanuit verticale toezichthouders zijn opmerkingen over de ondersteuning gemaakt. Logius heeft aangegeven geen communicatie over ENSIA te doen. Logius heeft een identieke communicatie naar alle afnemers, daar past geen ENSIA-communicatie in. Met RvIG is niet over ondersteuning gesproken. BKWI en SZW participeren in het programma BVGS; een implementatieprogramma loopt in 2017 door. I&M heeft aangegeven over de BAG/BGT-vragenlijst via de eigen communicatiekanalen direct met BAG/BGT- betrokkenen te willen communiceren. De CISO zou in deze communicatie geen rol hebben.

Aandachtspunten:
- Met oog op implementatie in 2017 is het van belang om een gezamenlijk, dan toch in ieder geval afgestemde, aanpak voor de communicatie richting gemeenten te ontwikkelen.
- Er heeft in het kader van de impactanalyse geen gesprek plaatsgevonden over een mogelijke taakverdeling van ondersteuning tussen IBD, VNG, ICTU, BZK en KING.

5.5 De wijze van organiseren van het verantwoordingsstelsel

Voor het realiseren van een goed functionerend verantwoordingsstelsel is het van belang dat zowel de horizontale verantwoording als de verticale verantwoording goed is ingericht. En dat de verticale verantwoording is gestroomlijnd. T.a.v. dit onderwerp heeft KING de volgende zaken gesignaleerd.

Horizontale verantwoording
- Tijdens het uitvoeren van de impactanalyse is een discussie ontstaan over de inleverdatum 1 oktober vanuit het perspectief van auditors. In een aantal gesprekken met gemeenten is de vraag voorgelegd of gemeente voorkeur heeft voor 1/10 of 31/12.[4] Voor gemeenten is 31 december een datum die aansluit bij de jaarcyclus. Het jaarverslag gaat immers over het hele jaar. Gemeenten zien een risico als wordt gekozen voor het één uploaden per 1 oktober en de rest op 31 december – hoe wordt door auditor dan omgegaan met verschillen die in deze periode ontstaan?
- De rapportages voor horizontale verantwoording zijn nog in ontwikkeling. Deze rapportages zijn voor gemeenten nu niet direct bruikbaar in de verantwoording. Er is waardering voor het wegen van de indicatoren, waardoor als het ware een samenvatting kan worden gemaakt. De weging lijkt nog onvoldoende bij gemeenten getest c.q. bekend.
- Portefeuillehouders zijn wisselend betrokken; de betrokkenheid van de raad afhankelijk van achtergrond van raadsleden; behoefte van raad onbekend, GS slechts 1 keer gesproken. Om de horizontale verantwoording te laten slagen is het van belang hen ook meer te betrekken. De tool biedt de mogelijkheid om leesrechten toe te kennen, suggestie is om deze ook aan de portefeuillehouder te geven.
- Informatieveiligheid is in de meeste gemeenten gepositioneerd in het domein van bedrijfsvoering. In het licht het vergroten van betrokkenheid van college en raad zou kunnen

[4] In stuurgroep d.d. 24 november 2016 is besloten dat de looptijd van het invulproces zal lopen van 1 juli t/m 31 december.

worden gekeken of informatieveiligheid gepositioneerd zou kunnen worden in het domein van privacy, bedrijfsvoering of veiligheid. Deze domeinen krijgen van nature meer bestuurlijke aandacht.

- T.a.v. opnemen van een collegeverklaring in het jaarverslag is opgemerkt dat hiervoor mogelijk in juridische zin iets moet worden geregeld – vanuit de impactanalyse is dit aspect niet verder onderzocht.
- Gemeenten hadden ten tijde van de impactanalyse, m.u.v. rapportage BAG/BGT die de gemeente zelf uitdraait, geen zicht op hetgeen toezichthouders ontvangen. Vanuit de verantwoordelijkheid van de gemeente voor deze rapportage is het wenselijk dat de gemeente inzicht heeft in de eigen domein-specifieke 'rapportage'.
- Door het ontbreken van rapportages en auditverslagen zijn er nauwelijks gesprekken met portefeuillehouders gevoerd. De horizontale werking van ENSIA is in de pilot feitelijk onvoldoende getoetst.

Verticale verantwoording

- Tijdens het uitvoeren van de impactanalyse is een discussie ontstaan over de inleverdatum 1 oktober vanuit het perspectief van auditors. Idee is uitgesproken om deze datum te verschuiven naar 31 december. Verticale toezichthouders zitten hier verschillend in; voor RvIG is 1 oktober een wettelijke datum, voor I&M is 1 oktober een wenselijke datum, BKWI en Logius hebben een voorkeur voor 31 december.
- Wat willen toezichthouders van gemeente ontvangen – ook dit verschilt per toezichthouder (zie tabel). Toezichthouders (I&M, RvIG) hebben aangegeven tevreden te zijn over de rapportage die zij krijgen. BKWI was nog in gesprek met ICTU over de data-export. Logius geeft aan er vanuit te gaan hetzelfde te ontvangen als voorheen, namelijk een separaat auditrapport Digid. Toezichthouders hebben voor de beoordeling van de rapportage een rapportage met dummygegevens ontvangen, niet een met pilotgegevens ingevulde rapportage. Bij data-export is voor gemeenten op dit moment niet precies duidelijk wat er met de gegevens gebeurt noch zijn juridische (?) kaders opgesteld wat er met deze informatie door de toezichthouder mag worden gedaan.
- Uitgaande van de inleverdatum van de evaluatievragenlijst op 1 oktober verwachten verticale toezichthouders op vier verschillende momenten de rapportages van gemeenten

Samengevat leiden bovenstaande constateringen tot onderstaand overzicht:

	Inleverdatum zelfevaluatie	Soort rapportage	Ontvangst rapportages	Toelichting
I&M	1 oktober	rapportage, incl. bestuurlijke managementsamenvatting, d.d. van vaststelling door B&W opgenomen in rapport, staafdiagram	1 december	
BKWI	31 december	export van alle gegevens om zelf te bewerken (mogelijkheid om toelichting van gemeenten op te vragen)	15 maart	
Logius	31 december (collegeverklaring ook 31 dec)	auditrapport (Digid-deel)	1 mei	ongecontroleerd vacuüm bij upload 1 oktober
RvIG	1 oktober (wettelijke datum)	Ruwe data in spreadsheet	1 november	

- Het moment in het proces waarop de verticale toezichthouder de rapportage krijgt is op dit moment niet duidelijk: als zelfevaluatie is gevuld, collegeverklaring is opgesteld of auditrapport is afgerond en geüpload?
- Het is op dit moment nog niet duidelijk hoe toezichthouders de rapportages krijgen. Krijgen toezichthouders toegang tot tool? Sturen van automatisch bericht aan toezichthouder als gemeente rapportage heeft geüpload? Is er een rol voor ICTU, gemeente, toezichthouder?
- Bij wie ligt de verantwoordelijkheid als gemeente rapportage zegt te hebben gestuurd, maar toezichthouder deze niet heeft ontvangen?
- Vanuit auditors is aangegeven dat normen waaraan de antwoorden moeten worden getoetst ontbreken. Zij zijn voornemens deze op te stellen. Vraag is of de basis hiervan niet ligt bij de verticale toezichthouders. In hoeverre hebben toezichthouders een gezamenlijk beeld over een gedeelde norm?
- Toezichthouders hebben uitgesproken hun escalatieladders te willen harmoniseren. Hierover heeft in oktober 2016 een eerste gesprek plaatsgevonden. De escalatieladder van Digid heeft de scherpste normen. I&M heeft aangegeven mee te zullen gaan in escalatieladder vwb informatieveiligheidsaspecten, omdat I&M er vanuit gaat dat de normen voor andere toezichthouders (aangezien het persoonsgegevens bevat) strenger zullen zijn dan de behoefte van I&M zelf. Planning over het afronden van een geharmoniseerde escalatieladder ontbreekt.
- Alle transitieplannen van toezichthouders zijn gereed maar moeten nog onderling worden afgestemd.
- Vanuit het perspectief van de impactanalyse, rekening houdend met het nog doorlopen van de pilot tot 13 december is het op dit moment (17 november) niet vast te stellen of de zelfevaluatie voldoende garantie voor verticale verantwoording aan toezichthouders biedt. Toezichthouders lijken hier wel vertrouwen in te hebben.

Aandachtspunten voor verticale toezichthouders

- Vanuit Digid-stelsel is aangegeven dat niet is gekeken naar de vragenlijst. Dit is risico
- Zijn er gedeelde beelden wanneer wordt voldaan aan een bepaalde norm die vanuit meerdere stelsels wordt gevraagd?
- Is het mogelijk om tot een gedeeld tijdpad en proces te komen t.a.v. volgorde van activiteiten t.b.v. verticale verantwoording?

Beheer

ICTU vervult in opdracht van BZK de rol van dienstverlener zowel richting toezichthouders als richting de gemeenten. De ENSIA-tool is gebaseerd op de onlineapplicatie CViews van het bedrijf Totta Research (Totta). Totta is hostingpartner waar alle data straks wordt bewaard. De contacten met Totta lopen via ICTU.

ICTU is verantwoordelijk voor functioneel- en, technisch beheer en ontwikkeling. Applicatiebeheer en 1e lijn Helpdesk functies worden rechtsreeks door ICTU vervuld. Technisch beheer, waaronder hosting van de applicatie en databasebeheer, is uitbesteed aan Totta. Bij het oplossen van issues en beantwoorden van de functioneel inhoudelijke vragen van gebruikers werkt ICTU nauw samen met IBD-deskundigen. Deze samenwerking is gebaseerd op functioneel inhoudelijke aspecten van beheer en ontwikkeling. Technische beheer en ontwikkeling doet ICTU zelf.

IBD, BZK, toezichthouders en pilotdeelnemers leveren input voor de ontwikkeling van de tool. ICTU zorgt in overleg met betrokkenen voor een passend ontwerp/oplossing en de daadwerkelijke realisatie. IBD is leidend als het gaat om de inhoud van de vragenlijst en vervult voor ICTU de rol

van 2e Lijn Helpdesk voor inhoudelijke vragen. De afweging van keuzes t.a.v. ontwikkeling van de tool ligt in de eerste plaats bij het Ministerie van BZK.

Aandachtspunten:
- Eigenaarschap van tool, gegevens en afgeleide rapportages moet nog worden uitgewerkt
- Ontwerp en inrichting beheer moet nog worden uitgewerkt
- Groepsbetrokkenheid van gemeenten bij de ontwikkeling van de tool: het is wenselijk dat er een gebruikersgroep wordt geformeerd om functionele wensen t.a.v. doorontwikkeling tooling groepsgewijs te toetsen. Wat technisch mogelijk is, is vanuit gemeentelijk perspectief niet altijd wenselijk.
- Structurele dekking voor beheer vanaf 2018 moet nog worden gerealiseerd

5.6 De vraag hoe externe audit vorm kan worden gegeven

Het auditproces bij gemeenten was ten tijde van de impactanalyse nog in volle gang. Geen van de projectleiders hadden, op het moment van het interview, het auditrapport gezien. Op verzoek van ADR hebben auditors evaluatieformulieren ingevuld, welke op 21 november in het Assurance-overleg zijn besproken.[5] Hieruit komt het volgende, grotendeels gedeelde beeld van gemeenten en auditors, naar voren:

- Scope, reikwijdte en normering zijn niet duidelijk: wat wordt er precies ge-audit (zelfevaluatie, collegeverklaring, collegeverklaring in jaarverslag) en tegen welke normen vindt deze audit plaats.
- De positie en de planning van de audit in het verantwoordingsproces is onduidelijk.
- Wat zijn de normen van verticale toezichthouders t.a.v. de gedeelde BIG-normen? Het zou goed zijn als auditors hun gedeelde auditnormen hiervan kunnen afleiden. Hierdoor zou een eenduidige “ENSIA-taal” kunnen ontstaan.
- Guidance bij vragen levert onvoldoende informatie voor onderbouwing van antwoorden
- Auditors hebben op verschillende manieren de audit uitgevoerd (grote diversiteit in uitvoering)
- Er bestaat onduidelijkheid over de audit-rapportage – wat omvat dit precies?
- Vanuit auditors is aangegeven dat het belangrijk is om een aantal vaktechnische producten voor borgen van eenduidige uitvoering en kwaliteit van audits te ontwikkelen. De ervaringen van gemeenten bevestigen dit.
- Gemeenten verwachten dat er voldoende capaciteit in de markt is (vraag creëert markt); auditors maken zich zorgen over de capaciteit als alles in Q1 zou moeten worden uitgevoerd.
- Gemeenten verwachten dat de kosten voor de audit omhoog gaan vanwege de verdubbeling van het aantal te toetsen normen (verdubbeling van kosten van DigiD-audit). Aangezien normen, rapportages, proces et cetera nog niet volledig zijn uitgelijnd kunnen auditors dit niet bevestigen noch ontkennen. Vanuit gemeentelijk perspectief is het wenselijk dat auditkosten niet verder toenemen. Dit was immers een van de oorspronkelijke doelstellingen van ENSIA.
- Gemeenten noch auditors kunnen op dit moment bevestigen dat ENSIA een verbetering is t.o.v. de huidige praktijk.

Om ENSIA in 2017 te implementeren zullen deze issues moeten worden opgelost.

[5] KING is bij deze bespreking aanwezig geweest, maar heeft geen vragen gesteld in het kader van de impactanalyse

6 CONCLUSIES EN AANBEVELINGEN

Alles in ogenschouw nemend concludeert KING dat:

1. Alle betrokken stakeholders enthousiast zijn voor het idee van ENSIA
2. De snelheid en eenvoud van implementatie door gemeenten m.n. afhangt van de mate waarin de gemeente de BIG heeft geïmplementeerd;
3. De beelden van verticale toezichthouders over verantwoordingsproces, normen, tijdpad en rapportage op dit moment niet eenduidig zijn;
4. Auditors de scope, reikwijdte en normering van de audit verschillend interpreteren en producten voor het borgen van eenduidige uitvoering en kwaliteit van audits ontbreken;
5. Aangezien de verantwoordingsprocessen ten tijde van de impactanalyse nog niet waren doorlopen, kan geen uitspraak worden gedaan over de bijdrage van ENSIA aan het horizontale of verticale verantwoordingsproces, dan wel vermindering van de auditlast;
6. ENSIA in de huidige vorm door gemeenten niet per 1 april 2017 kan worden geïmplementeerd.

In het licht hiervan beveelt KING het Ministerie van BZK aan om in 2017 te starten met de implementatie van ENSIA onder de volgende voorwaarden:

1. De periode van het vullen van de vragenlijst te verschuiven van 1 april tot 1 oktober naar 1 juli tot 31 december;
2. t.b.v. het realiseren van de horizontale verantwoording over informatieveiligheid, maar de verticale verantwoording en audit te beperken tot DigiD en Suwi;
3. Verticale toezichthouders te vragen om gezamenlijk een eenduidig verantwoordingsproces, tijdspad, normen en eisen aan auditrapport te formuleren;
4. Auditors te vragen om - op basis van door verticale toezichthouders vastgestelde normen – een eenduidige scope, reikwijdte en normering van de audit te bepalen en producten voor het borgen van eenduidige uitvoering en kwaliteit van audits te ontwikkelen;
5. In 2017 nog niet te benchmarken (op termijn is dit wel wenselijk);
6. Een groeipad te formuleren voor ENSIA de komende jaren;
7. Voor een succesvolle implementatie door gemeenten per 1 juli 2017 is het noodzakelijk dat bovengenoemde aanbevelingen uiterlijk 1 april 2017 (drie maanden voor start uitrol) zijn gerealiseerd;
8. 2017 te beschouwen als een gezamenlijk leerjaar.

7 BIJLAGEN

7.1 BIJLAGE 1 VRAGENLIJST BAG/BGT

7.1.1. Algemeen

In deze bijlage zijn ervaringen opgenomen van zowel het Ministerie van Infrastructuur en Milieu (I&M) als gemeenten t.a.v. de beleidsinhoudelijke vragenlijst BAG/BGT. Het gaat hier om bijvangst die in gesprekken naar voren is gekomen. De vragenlijst zelf is niet door KING in impactanalyse betrokken.

7.1.2. Standpunt voor uitrol in 2017

I&M gaat zo veel mogelijk met de ENSIA-traject mee, maar hebben voor BAG en BGT eigen formele besluitvormingslijnen. Op 24 november zijn de resultaten uit de pilot voor BAG/BGT-vragenlijst geëvalueerd – resultaten zijn KING onbekend.

7.1.3. Communicatie

I&M heeft geen communicatie issues, ze hebben voldoende kanalen om een en ander richting beheerders te communiceren. Aanspreekpunten voor I&M zijn de BAG/BGT-beheerders, hier ZIJN ook directe communicatielijnen mee. Er is ook communicatie via Kadaster. Daarnaast steunt I&M op het door de ENSIA-stuurgroep vastgestelde communicatieplan en de afspraken over communicatie die in de ENSIA-werkgroep *Implementatie en Communicatie* worden gemaakt. Sturen van een mail aan alle BAG-beheerders en hun informeren over ENSIA en wat er komende periode van hen wordt verwacht behoort ook tot de mogelijkheden.

7.1.4. Informatievoorziening | Evaluatieprotocol

ENSIA-Vragen:

- Totstandkoming vragenlijst:
    - Besproken in BAG/BAO-overleg - bestuurlijk
    - Agenda-overleg – gemeentegroep (AO BAG en pilotgemeenten ENSIA)
    - Twee keer uitgebreid besproken; 24 november 3e bespreking evaluatie pilot
    - Vragenlijst is pilot in gegaan.
- Het is een bewuste keuze van I&M om vragenlijsten van BAG en BGT zoveel mogelijk naar elkaar toe te trekken.
- In de BAG/BGT-vragenlijst zijn verantwoordingen en verbeterplannen opgenomen op verzoek van de gemeenten zelf.
- Aan pilotgemeenten is evaluatieformulier gestuurd t.b.v. BAG/BGT-vragenlijst. In ENSIA opgenomen vragen zijn momenteel *semi definitief*. Er worden geen grote wijzigingen op de inhoud van de gekozen *vragen verwacht*. Eventuele aanpassingen worden op aangeven van I&M door ICTU doorgevoerd. Of er een wijziging op de inhoud van de vragen plaats gaat vinden, is afhankelijk van de evaluatie op 24 november.
- Er is een onderscheid tussen informatiebeveiliging en beleid. Van alle BAG/BGT vragen zijn er slecht twee gerelateerd aan informatieveiligheid (Back-up en Uitwijk) en daardoor in de KeyControls/ENSIA lijst staan. Rest zijn stelsel specifieke beleidsvragen die niet door CISO maar door desbetreffende beheerder kunnen worden beantwoord.
- ICTU heeft tegen I&M gezegd dat wellicht direct toegang tot de BAG/BGT-vragenlijst in ENSIA-tool voor BAG/BGT-beheerders zou moeten komen.

Escalatieladder:

- Minister is het hoogste escalatieniveau. De toezichthouder I&M en de kwaliteitsmanager Kadaster werken samen. De toezichthouder bepaalt of er wordt geëscaleerd.
- Voor informatieveiligheidsvragen gaat I&M mee met harmonisatie van escalatiekanalen. Deze hebben voor I&M alleen betrekking op twee BIG-normen t.a.v. back-up en uitwijk. Er is geen escalatieladder t.a.v. BAG/BGT-vragenlijsten.

Rapportage:

- College rapporteert aan de minister over de beleidsinhoudelijke BAG en BGT-compartimenten. Dit is een wettelijke verplichting.
- Rapportage aan minister: Totaal vragenlijst, bestuurlijke management samenvatting en een staafdiagram, groen rood (resultaat in één oogopslag.) Bestuurlijke managementsamenvatting is bedoeld om te zien of de gemeente zelf in de gaten heeft welke risico's men loopt.

Tijdspad:

- Huidige proces: Vragenlijsten staan per 1/4 open voor beantwoording; definitieve antwoorden worden uiterlijk 1/10 geüpload naar de database bij ICTU. Gemeente heeft tot 1/12 om de rapportage voor zowel BAG als BGT op te stellen en deze voor I&M te uploaden. Betreft de wettelijk verplichte rapportages aan de minister.
- Er zijn geen inlevermomenten in wet opgenomen.
- Nieuwe wetgeving gaat per 1 januari 2018 in.
- Beschikbaarheid van geüploade vragen aan I&M per 1/10 vindt men noodzakelijk. Aan de uiterste inleverdatum van 1-12 voor de rapportages BAG en BGT wil I&M vasthouden.
- I&M wil graag zicht op wat men wanneer krijgt, bijvoorbeeld op 1 oktober. Wil niet tot april daaropvolgend jaar wachten.

Verantwoording/Audit:

- Ingevulde vragenlijsten zijn voor de toezichthouder onderdeel van de uitvoering van de toezicht en handhaving taak I&M; m.n. fase 1 de informatiefase. Beelden vanuit de formele vragenlijsten worden gecombineerd met de beelden vanuit het operationeel kwaliteitsmanagement, zodat men zicht krijgt op hoe het bij gemeente loopt. Als er problemen zijn met meer dan vijf gemeenten, dan is dat veel. Kwaliteitsmanagers van Kadaster hebben adviesfunctie t.a.v verbetering.
- I&M is nadrukkelijk van de externe audit (inspecties) afgestapt. Voor I&M leverden inspecties niets op.
- Het is absoluut niet de bedoeling dat gemeenten voor de BAG en BGT-vragenlijsten extra kosten gaan maken voor een externe audit.

7.1.5. Ervaringen van gemeenten met BAG/BGT-vragenlijst

Communicatie

Pilotgemeenten hebben de communicatie over pilot ENSIA-traject in relatie tot BAG/BGT als zeer verwarrend beschouwd. Voor pilottrekkers (CISO'S) was lastig dat er directe communicatie met domeinspecialisten plaatsvond.

Impact op werkprocessen

Gemeenten verwachten dat de beantwoording van de BGT-vragen impact zal hebben op de werkprocessen. Dat komt, doordat men dingen moeten inrichten die eigenlijk nog niet zijn ingericht (verwijzingen naar brondocumenten die niet bestaan – wel in BAG, maar niet in BGT).

Vragenlijst
Gemeenten gaven aan dat vragen, vanwege open karakter, op meerdere manieren te beantwoorden waren, te makkelijk manier en weinig waarde toevoegend. Ook werd opgemerkt dat de normenset van de BGT is gebaseerd op oude BAG. ICT-vragen vond men wel lastig om te beantwoorden. Open vragen werden niet door iedereen gewaardeerd. Gemeenten vonden het lastig dat de vraagstelling van de BAG/BGT-vragenlijst een ander format en andere wijze van vragen had dan de ENSIA-vragenlijst. Door gemeenten werd gevraagd of de vragenlijst wel bij gemeenten is getoetst en gesuggereerd om de vragenlijst nog in het GEO-beraad te laten toetsen.

7.2 BIJLAGE 2 GERAADPLEEGDE ORGANISATIES EN PERSONEN

Organisatie	Datum gesprek	Gesproken met
ICTU	6 oktober	Daniel van Geest
Gemeente Edam-Volendam	13 oktober	• Anna Steur-Bootsman • Arjen van Veen • Gerard Kwakman • Ilja Koning • Kees Springer • Nico Tol • Niek Slagter • Remco Rekoert
Gemeente Arnhem	18 oktober	• Chris Deben [CISO] • Simon Does [CIO] – niet aanwezig • Ron Borst [IT-Auditor/ENSIA 35oordinator] • Albert ten Broeke • Desmond Olde-Velthuis • Dirk Grosman • Guillaume Bardet – niet aanwezig • Hans Jansen • Harrie Kierkels • Helma Wieringa • Ingrid Veldhoen • Jan van Alebeek • John Jacobs • Theo Arends
Gemeente Zeewolde	26 oktober	• Rein Zijlstra [Wethouder] • Arno Murrer [Loco-gemeentesecretaris] • Chris Deben [CISO] • Anneke van der Veen [Zeewolde | Burgerzaken] • Alexander van Beers [Meerenzicht | Informatisering & Automatisering] • Rene Heijink [Zeewolde | BGT] • Rob van den Heuvel [Zeewolde | BAG] • Jacqueline Spelhofen-Miset [Meerinzicht |Teamcoördinator HRM] • Kasper Herrewijn [Meerinzicht | Teamcoördinator FG&I (Facilitair, Gebouwen & Inkoop)
Gemeente Vugt	1 november	• Margareth van Hees | Coördinator SUWI • Ilse | BAG • Jeroen | BGT • Patrick | Facilitair • Tim | W&I • Mana | PUN • Anneke | BRP-PUN • Bob • René | ADV • Berry | CISO-Controller
Gemeente Haaren	1 november	• Terence van Gestel [CISO, Haaren, Boxtel, St-Michel] • Jan (CISO Velthoven) • Britt van de Loo [b.vd.loo@MijnGemeenteDichtbij.nl]; Burgerzaken • Wim de Kort [W.d.Kort@Haaren.nl]; • Ron Rutjes [R.Rutjes@MijnGemeenteDichtbij.nl]; • Willian Timmermans [W.Timmermans@MijnGemeenteDichtbij.nl]; • Mari Steenbakkers • [M.Steenbakkers@MijnGemeenteDichtbij.nl];

		• Gerdien Sommers [G.Sommers@MijnGemeenteDichtbij.nl]; • Marc van Dijk [Ma.v.Dijk@MijnGemeenteDichtbij.nl]; • Christel van Rooij [C.v.Rooij@MijnGemeenteDichtbij.nl]; • Bode-SMG [Bode@sint-michielsgestel.nl]; • Frans de Kruijf [f.d.kruijf@MijnGemeenteDichtbij.nl]
Gemeente Het Bildt	8 november	• Gerrit Krol | Burgemeester • Aart van Tuijl | Projectleider-CISO
Gemeente Zaandam	10 november	• Rita Visscher | Portefeuillehouder • Linda Goedhart| CISO
Gemeente Den Bosch	15 november	• Arjan Kieboom
Gemeente Tiel	15 november	• Youri Lammerts van Bueren , CISO
LOGIUS	2 november	• Jorik van het Hof • Rein During
RviG	7 november	• Mandy Van Tol | RvIG • Enry Brouwer | RvIG (Afwezig) • Diana van Driel | BZK + Coördinatie Reisdocumenten • Aart Verloop | BZK (Afwezig) • Esther Petray | BZK
BKWI-Suwinet-SZW	9 november	• Hilko Batterink | BKWI • Jasmijne Schouten | BKWI • Anton Slijkhuis | Min. SZW
I&M	16 november	• Alex van de Ven | alex.vande.ven@minienm.nl • Noud Hooyman | noud.hooyman@minienm.nl

KWALITEITS
INSTITUUT
NEDERLANDSE
GEMEENTEN

KWALITEITSINSTITUUT
NEDERLANDSE GEMEENTEN

NASSAULAAN 12
2514 JS DEN HAAG

POSTBUS 30435
2500 GK DEN HAAG

T 070 373 80 08
F 070 363 56 82

INFO@KINGGEMEENTEN.NL
WWW.KINGGEMEENTEN.NL