Proces verantwoorden ENSIA 2018

Toelichting en formats voor college en de raad

Inleiding

Introductie

Deze handreiking maakt onderdeel uit van de ondersteunende documentatie voor het ENSIA verantwoordingsproces over het jaar 2018. ENSIA staat voor Eenduidige Normatiek Single Information Audit en staat voor eenmalige informatieverstrekking en eenmalige IT-audit. Het project ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid. ENSIA neemt de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie.

De focus van ENSIA ligt op de horizontale verantwoording: binnen de gemeente, met een belangrijke rol voor de gemeenteraad. ENSIA structureert ook de verticale verantwoording richting de rijksoverheid voor:

- Basisregistratie Personen (BRP)
- Paspoortuitvoeringsregeling (PUN)
- Digitale persoonsidentificatie (DigiD)
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Ondergrond (BRO)
- Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI)

Met het gelijktrekken van tijdpaden voor verantwoording ligt het inmiddels ook meer voor de hand om op een meer gestructureerde wijze de rapportages te laten vaststellen en de raad hierover te informeren. Deze handreiking ondersteunt het voorbereidende proces op het vaststellen van de rapportages door het college en (vertrrouwelijk) aanbieden van de verantwoording aan de raad.

Deze handreiking is gericht op de rol van het college van B&W en de gemeenteraad bij het proces van verantwoorden. Daarbij ligt opnieuw de focus op de samenhang tussen horizontale en verticale verantwoording en de daarbij behorende processtappen.

Met dank aan

Dit docoment is uitgewerkt naar voorbeeld van het collegevoorstel zoals aangeboden aan het college van B&W in de gemeente Amsterdam voor de ENSIA verantwoording 2017. De raadsvoordracht is uitgewerkt naar een voorbeeld van Mijn Gemeente Dichtbij in 2017.

Hebt u vragen? Neem dan contact op met de ENSIA telefoon via 070-2502400 of mail via ensia@vng.nl.

VNG Realisatie
Nassaulaan 12 Den Haag | Postbus 30435, 2500 GK Den Haag
070 373 8008 | realisatie@vng.nl

Inhoudsopgave

VNG Realisatie
Nassaulaan 12 Den Haag | Postbus 30435, 2500 GK Den Haag
070 373 8008 | realisatie@vng.nl

1. Verantwoording

1.1. Taken college van B&W

Het college van B&W is eindverantwoordelijk voor informatieveiligheid en de verantwoording hierover. Het college verantwoord zich aan het eigen toezichtsorgaan, de raad, alsook aan de verschillende stelselhouders van het rijk.

1.1.1. Verantwoorden aan de raad

Jaarlijks legt het college van B&W verantwoording af aan de raad. Dit doet zij middels het jaarverslag. De verplichting komt voort uit de Gemeentewet[1]. In de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' is afgesproken de raad via dit middel te informeren over informatieveiligheid. Op deze wijze kan zij haar toezichthoudende functie uitoefenen. Het proces van het opstellen van het jaarverslag wordt geleid door de afdeling (concern)control of financiën in een gemeente. Indien in het jaarverslag van 2017 geen passage over informatieveiligheid is opgenomen, adviseren wij om vroegtijdig aan te sluiten bij het proces van totstandkoming van het jaarverslag om binnen de paragraaf bedrijfsvoering verantwoording af te leggen over informatieveiligheid.

1.1.2. Verantwoorden aan het rijk

Verantwoording afleggen aan het rijk over de verschillende stelsel is gebonden aan eisen. Zo dienen de verschillende specifieke rapportages te worden vastgesteld door het college, alvorens deze kunnen worden ge-upload in ENSIA. De verschillende rijksonderdelen eisen vervolgens dat de raad over de uitkomsten van de verticale verantwoording wordt geïnformeerd. De rapportages die het rijk ontvangt zijn opgesteld op basis van vaste formats en gaan vaak diep in op de (specifieke) materie binnen een basisregistratie, infrastructuur of koppeling waarover verantwoording wordt afgelegd. Deze (technische) rapportages zijn niet altijd even leesbaar en het betreft diepgaande informatie over een specifiek vakgebied.

1.1.3. Een efficiënte vorm van verantwoorden

In het eerste ENSIA jaar is daarom door veel gemeenten gekozen om de raad aanvullend via een (vertrouwelijke) separate rapportage te informeren. Hier zijn verschillende aanleidingen voor:

1) Informatie is het belangrijkste productiemiddel van elke gemeente. Een kort (openbaar toegankelijk) weergave in het jaarverslag geeft weinig diepgang en inzicht in de complexiteit en omvang over de status van informatieveiligheid.

[1] Artikel 160, eerste lid onder a, van de Gemeentewet geeft het college de bevoegdheid om het dagelijks bestuur van de gemeente te voeren. Informatiebeveiliging is hierin randvoorwaardelijk. In artikel 169, eerste en tweede lid, is geregeld dat het college en elk van zijn leden afzonderlijk verantwoording schuldig zijn aan de raad over het door het college gevoerde bestuur en het college geeft de raad alle inlichtingen die de raad voor de uitoefening van zijn taak nodig heeft.

2) Het risico bestaat dat de opname in het jaarverslag ertoe leidt dat de gemeenteraad onvoldoende toekomt aan het onderwerp informatieveiligheid.
3) Het rijk eist dat de raad over de specifieke rapportages van de verschillende stelsels wordt geïnformeerd.

Met het op één lijn brengen van data van verantwoording (een van de doelstellingen van ENSIA) is het nu mogelijk om de raad in één keer te informeren in plaats van alle rapportages op verschillende momenten ter kennisgeving aan te bieden. U biedt één rapportage vertrouwelijk ter informatie aan. De verticale rapportages over de stelsels voegt u als bijlage toe. U voldoet daarmee aan de vigerende wet- en regelgeving en bent in staat om de raad in begrijpelijke taal verslag te doen. Het is aan de raad om het onderwerp te agenderen en te bespreken.

2. Vaststelling college B&W

2.1. Instemmen, vaststellen en geheimhouding

In het voorstel voor het college (de oplegger) maakt u kenbaar wat u van het college vraagt. Zo dient het college in te stemmen met de uitkomsten van de collegeverklaring ENSIA en deze te ondertekenen. En u vraagt het college om in te stemmen met de uitkomsten van de rapportages voor de BAG, BGT (en de BRO). Hiermee worden de rapportages vastgesteld. De verantwoording over BRP en PUN heeft al eerder (voor 15 februari) separaat plaatsgevonden en wordt daarom niet meegenomen in deze oplegger voor het college.

En waarom onder geheimhouding? De informatie die u voorlegt aan het college bevat bedrijfskritische informatie. Informatie, die wanneer deze openbaar toegankelijk is, beveiligingsrisico's met zich meebrengen. Hiernaast is door de IT auditor in het assurancerapport (een van de bijlagen) aangegeven dat de informatie uit dit rapport alleen bestemd is voor de raad en de departementen die toezien op de veiligheid van DigiD en Suwinet.

Het proces van de collegeverklaring (of alleen de bijlagen) en het assurance rapport geheim verklaren vergt aandacht.

1. U neemt de grondslag (op basis waarvan u geheimhouding wenst) op in het collegevoorstel (WOB).
2. U geeft expliciet aan voor welke termijn de geheimhouding geldt.
3. Bij toezending van de geheime stukken aan de raad, dient de raad de geheimhouding te bekrachtigen. Let wel, indien u dit niet organiseert is de geheimhouding niet van kracht. De Gemeentewet[2] zegt hierover: "De krachtens het tweede lid opgelegde verplichting tot geheimhouding met betrekking tot aan de raad overgelegde stukken vervalt, indien de oplegging niet door de raad in zijn eerstvolgende vergadering die blijkens de presentielijst door meer dan de helft van het aantal zitting hebbende leden is bezocht, wordt bekrachtigd."
   U dient in het collegevoorstel de raad te vragen om de geheimhouding in haar vergadering te bekrachtigen.
4. Op de stukken aan de raad dient melding gemaakt te worden van de geheimhouding.

2.2. Opbouw collegevoorstel

In deze paragraaf is de opbouw van het collegevoorstel op basis van de ENSIA zelfevaluaties opgenomen. De horizontale verantwoording is vormvrij. Dit is een suggestie op basis van de ENSIA systematiek. Het is aan u om te bepalen wat u opneemt in een gemeentebrede (horizontale) rapportage. Uit de regiobijeenkomsten in januari 2019 bleek uit een peiling onder de bezoekers datveel ENSIA coordinatoren de verantwoording over

[2] Gemeentewet, artikel 25, lid 3

privacy te combineren met de verantwoording over informatieveiligheid. En op deze wijze de raad in een keer te informeren over zowel informatieveiligheid als privacy.

2.2.1. Inhoud collegevoorstel

In het voorstel aan het college vraagt u het college in te stemmen met:

1. De uitkomsten van de zelfevaluatie voor de aansluitingen DigiD en Suwinet.
2. De uitkomsten van de zelfevaluatie voor BAG, BGT (en BRO). Door in te stemmen met de uitkomsten legt het college verantwoording af over het gebruikt van de BAG, BGT <en BRO> aan de landelijk toezichthouder, het ministerie van BZK.
3. Indien er verbeterplannen zijn gemaakt, een functionaris te mandateren om toezicht te houden op de uitvoering van de verbetering binnen x termijn.
4. De collegeverklaring te ondertekenen. Met de collegeverklaring legt het college conform de ENSIA-methodiek verantwoording af over de informatiebeveiliging aan zowel de raad als aan de landelijke toezichthouders. In de verklaring verklaart het college dat de interne beheersingsmaatregelen van de gemeente in opzet en bestaan voldoen aan de normen voor DigiD en Suwinet, <behalve de in de (geheime/kabinet-)bijlagen genoemde uitzonderingen>.
5. Het opleggen van geheimhouding op de collegeverklaring en bijlage 1 DigiD en biljage 2 Suwinet van de collegeverklaring en het assurancerapport van de IT auditor op grond van artikel 25, tweede lid van de Gemeentewet, behoudens toezending van deze bijlagen en rapportage aan de landelijke toezichthouder. De geheimhouding wordt opgelegd in verband met de belangen genoemd in artikel 10, tweede lid, onder b en g van de Wet openbaarheid van bestuur. De geheimhouding wordt opgelegd voor onbepaalde duur.
6. De raad op grond van artikel 25, derde lid van de Gemeentewet te verzoeken de opgelegde geheimhouding op de collegeverklaring en bijlage 1 en 2 behorende bij de collegeverklaring ENSIA 2017 tijdens de eerstvolgende vergadering te bekrachtigen.
7. De bijgevoegde raadsvoordracht, waarin de raad gevraagd wordt om kennis te nemen van de verantwoording vanuit het ENSIA stelsel over het jaar 2018.

2.2.2. Onderbouwing besluit

Onderstaande tekst is een handreiking ter onderbouwing van de te nemen besluiten door het college. Zoals ook eerder aangegeven is de horizontale verantwoording vormvrij.

U kunt putten uit onderstaande suggestie:

> **Instemmen met:**
>
> Ad1. De uitkomsten van de zelfevaluatie ENSIA voor de aansluitingen DigiD en Suwinet
>
> Ad 3. In te stemmen met het mandateren van toezicht op uitvoering van de verbeteringen
>
> Ad 4. Ondertekening van de collegeverklaring

Naar aanleiding van een resolutie van de Buitengewone Algemene Ledenvergadering van de VNG, heeft de VNG samen met het rijk een nieuwe, efficiënte verantwoordingssystematiek ontwikkeld: de Eenduidige Normatiek Single Information Audit (ENSIA). Hiervoor zijn de verantwoordingssystematieken voor de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Inkomen (Suwinet) samengevoegd en gestroomlijnd. Dit betekent dat er niet voor alle onderdelen afzonderlijke audits (die elkaar deels overlappen) moeten worden uitgevoerd. Ook hoeven er geen afzonderlijke rapportages opgesteld te worden.

ENSIA helpt gemeenten in één keer slim verantwoording af te leggen over informatieveiligheid gebaseerd op de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten). Hiermee kan met één verklaring zowel horizontaal (van het college naar de raad) als verticaal (van het college naar de landelijke toezichthouders) verantwoording worden afgelegd. De verantwoordingssystematiek ENSIA is in 2017 ingevoerd.

Daarmee is 2018 het tweede jaar dat deze systematiek gebruikt wordt. De verklaring met bijlagen en de rapportages over het Geo-domein (BAG, BGT <en BRO>) zijn opgesteld aan de hand van landelijke modellen.

Met de voorliggende ENSIA-collegeverklaring geeft het college aan in hoeverre de beheersingsmaatregelen voldoen aan de normen die gelden voor DigiD en Suwinet en op welke onderdelen de gemeente niet voldoet aan deze normen. De collegeverklaring is opgesteld aan de hand van de uitkomsten van de zelfevaluaties die door de lijnverantwoordelijken zijn uitgevoerd, onder coördinatie van <noem functionaris>. Een gecertificeerde IT-auditor heeft de collegeverklaring gecontroleerd. Na vaststelling van de collegeverklaring zal de auditor zijn assurance rapport afgeven. De IT-auditor verklaart hierin dat de collegeverklaring een getrouw beeld geeft. De collegeverklaring wordt gezamenlijk met het assurance rapport aangeboden aan de gemeenteraad.

De zelfevaluaties van de DigiD-aansluitingen door de lijnverantwoordelijken leveren verbeterpunten op ten aanzien van:

- ..
- ...
- ..

De zelfevaluaties van de Suwinet-aansluitingen door de lijnverantwoordelijken leveren verbeterpunten op ten aanzien van:

- ..
- ...
- ..

In de bijlagen van de verklaring is per DigiD aansluiting en per Suwinet voorziening aangegeven op welke specifieke punten niet voldaan wordt aan het geldende normenkader. Naast de risico's die voortvloeien uit het niet voldoen aan het normenkader, bestaat er bij het niet-oplossen van de verbeterpunten nog het risico dat de landelijke toezichthouder de gemeente niet meer gebruik laat maken van deze voorzieningen. Dit heeft verregaande gevolgen voor de dienstverlening van de gemeente aan burgers en bedrijven.

Instemmen met:

Ad 2. De uitkomsten van de zelfevaluatie ENSIA voor de verantwoording over de BAG, BGT <en BRO>.

Binnen het ENSIA stelsel zijn voor het geo-domein BAG, BGT <en BRO> domeinspecifieke zelfevaluaties opgenomen over het gebruik van deze drie basisregistraties. De zelfevaluaties binnen het geo-domein zijn gekoppeld aan een puntenscore. In de bijlage is per stelsel een rapportage opgenomen met de bevindingen. Na vaststelling zullen de rapportages openbaar toegankelijk zijn via het ministerie van BZK.

De zelfevaluatie BAG door de lijnverantwoordelijken leveren een puntenscore op van .. .uit het maximaal aantal te behalen punten van .. De score is te beoordelen als… De zelfevaluatie levert verbeterpunten op ten aanzien van:

- ..
- ...
- ..

De zelfevaluatie BGT door de lijnverantwoordelijken leveren een puntenscore op van .. .uit het maximaal aantal te behalen punten van .. De score is te beoordelen als… De zelfevaluatie levert verbeterpunten op ten aanzien van:

- ..
- ...
- ..

<De zelfevaluatie BRO door de lijnverantwoordelijken leveren een puntenscore op van .. .uit het maximaal aantal te behalen punten van .. De score is te beoordelen als… De zelfevaluatie levert verbeterpunten op ten aanzien van:

- ..
- ...
- ..>

<Risico benoemen bij niet voldoen>.

De aansluitingen vallen onder <directies/portefeuilles>.

Voor de <X-aantal> DigiD-aansluitingen van de gemeente XX zijn dit:

- DigiD-aansluiting <naam aansluiting en verantwoordelijk bedrijfsvoerings onderdeel>
- DigiD-aansluiting <naam aansluiting en verantwoordelijk bedrijfsvoerings onderdeel>

Voor de <aantal> Suwinet-aansluitingen zijn dit:

- Suwinet aansluiting Participatiewet, IOAZ en IOAW: <verantwoordelijk bedrijfsvoeringsonderdeel>
- Suwinet aansluiting Burgerzaken: <verantwoordelijk bedrijfsvoeringsonderdeel>
- Suwinet aansluiting Belastingdeurwaarders: <verantwoordelijk bedrijfsvoeringsonderdeel>
- Suwinet aansluiting RMC: <verantwoordelijk bedrijfsvoeringsonderdeel>

Voor het Geo-domein zijn dit:

- Basisregistratie Adressen en Gebouwen (BAG): <verantwoordelijk bedrijfsvoeringsonderdeel>
- Basisregistratie Grootschalige Topografie (BGT): <verantwoordelijk bedrijfsvoeringsonderdeel>
- Basisregistratie Ondergrond (BRO): <verantwoordelijk bedrijfsvoeringsonderdeel>

Instemmen met:

Ad 5. Het opleggen van geheimhouding op de collegeverklaring en bijlage 1 en 2 van de collegeverklaring en het assurancerapport van de IT auditor.

Ad 6. De raad te verzoeken de opgelegde geheimhouding op de collegeverklaring en bijlage 1 en 2 van de collegeverklaring ENSIA 2017 tijdens de eerstvolgende vergadering te bekrachtigen.

Ad 7. Kennisname ENSIA verantwoording 2018 door de raad.

Voorstel is dat op de collegeverklaring en de bijlagen 1 en 2 en het assurancerapport van de IT auditor geheimhouding wordt opgelegd op grond van artikel 25, tweede lid, van de Gemeentewet. Dit omdat in de bijlagen informatie is opgenomen over beveiligingsmaatregelen die de gemeente treft om de systemen en gegevens te beveiligen. Deze informatie kan kwaadwillenden helpen bij het doorbreken van de beveiliging, wat kan leiden tot grote schade voor de gemeente. Dit leidt tot onevenredige benadeling van de gemeente (artikel 10, tweede lid, onder g van de WOB) en kan de financiële belangen van de gemeente (artikel 10, tweede lid, onder b van de WOB) schaden.

De geheimhouding is niet van toepassing op toezending van de bijlagen aan de landelijke toezichthouders voor de DigiD- en Suwinetaansluitingen, die de bijlagen moeten ontvangen in het kader van het verticale toezicht.

De collegeverklaring en bijlagen maken onderdeel uit an de ENSIA verantwoording over 2018. Deze zal na instemming ter kennisname worden aangeboden aan de raad. Daarbij dient de door het college opgelegde geheimhouding op de bijlage 1 en 2 en het assurancerapport van de IT auditor behorende bij de collegeverklaring in de eerstvolgende vergadering te worden bekrachtigd door de raad.

3. Raadsvoordracht

In dit hoofstuk is een voorstel opgenomen voor het opstellen van een raadsvoordracht met informatie over de verantwoording informatieveiligheid. U kunt putten uit onderstaande suggestie.

Inleiding

<Neem als inleiding het informatiebeveilgingsbeleid in de gemeente als uitgangspunt. Geef aan wat hierover is opgenomen in het jaarverslag en benoem de doelstellingen/speerpunten/ambitie uit het informatiebeveiligingsbeleid, zoals zorgvuldig omgaan met informatie, betrouwbare en continue dienstverlening, vodoen aan vigerende wet- en regelgeving (bijvoorbeeld AVG), beheersen van risico's (governance, risk en compliance>.

Het college van burgemeester en wethouders legt over het jaar 2018 veranwoording af over de status van informatiebeveiliging. In 2017 hebben alle gemeenten voor de eerste keer de verantwoording aan hun eigen toezichthouder, de raad, en de toezichthouders van het rijk middels de ENSIA systematiek uitgevoerd. ENSIA staat voor Eenduidige Normatiek Single Information Audit. Voor de verantwoording aan de gemeenteraad sluit ENSIA aan op de gemeentelijke planning-en-controlcyclus. ENSIA neemt de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt. Vanuit deze horizontale (gemeente brede) zelfevaluatie wordt eveneens de verantwoording aan de stelselhouders bij het rijk afgeleid, de zogenaamde verticale verantwoording. Voor de uitvoering wordt gebruik gemaakt van zelfevaluaties.

De scope van ENSIA is als volgt:

- Implementatie Baseline Informatiebeveiliging Gemeenten (BIG)
- Basisregistratie Personen (BRP)
- Paspoortuitvoeringsregeling Nederland (PUN)
- Digitale persoonsidentificatie (DigiD)
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Ondergrond (BRO)
- Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Een verkorte weergave van de uitkomsten treft u aan in deze voordracht.

Activiteiten in 2018

<Beschrijf de belangrijkste inzet/activiteiten van afgelopen jaar. Beschrijf de belangrijkste beheersmaatregelen die in het afgelopen jaar hebben bijgedragen aan de doelstellingen>.

Resultaten in 2018

<Beschrijf het gemeentebrede beeld uit de zelfevaluatie ENSIA. In welke mate zijn de eerder genoemde doelstellingen gerealiseerd? Beschrijf welke doelstellingen zijn gerealiseerd en welke nog aandacht behoeven. NB: omschrijf dit omzichtig.>

Resultaten zelfevaluatie BIG

Onderwerpen uit de BIG zijn:

- Beveiligingsbeleid
- Interne organisatie en externe partijen
- Beheer van bedrijfsmiddelen
- Personele beveiliging
- Fysieke beveiliging
- Beheer van Communicatie- en bedieningsprocessen
- Toegangsbeveiliging
- Informatiesystemen
- Informatiebeveilgingsincidenten
- Bedrijfscontinuïteit
- Naleving

Resultaten per stelsel

Vanuit de uitgevoerde zelfevaluaties is vanuit de ENSIA systematiek ook verantwoording afgelegd aan het rijk. Met onderstaande uitwerking informeren wij u per stelsel over de uitkomsten. De rapportages zijn als biljage (vertrouwelijk) opgenomen bij deze voordracht.

<Houd rekening in uw rapportage indien de raad al eerder over de resultaten van de BRP & PUN/PNIK zijn geïnformeerd.>

Domein	**Bevindingen en door te voeren verbeteringen**	**Status**
Basisregistratie Personen (BRP)	<score en eindoordeel> <wel/niet steekproef> <resultaten steekproef indien bekend>	
Paspoortuitvoeringsregeling Nederland (PUN)	<score en eindoordeel> <wel/niet steekproef> <resultaten steekproef indien bekend>	

Domein	Bevindingen en door te voeren verbeteringen	Status
Digitale persoonsidentificatie (DigiD)	<aantal aansluitingen en gebruik> <geef aan of er bevindingen geconstateerd zijn> <Door te voeren verbeteringen aangeven (hoofdlijn)> <geef aan dat de zelfevaluatie is getoetst door een IT auditor en verwijs naar bijlage met collegeverklaring, de bijlage DigiD en assurancerapport (vertrouwelijk)>	
Basisregistratie Adressen en Gebouwen (BAG)	<geef aan welke score behaald is ten opzichte van het totaal te behalen aantal punten> <geef door te voeren verbeteringen aan>	
Basisregistratie Grootschalige Topografie (BGT)	<geef aan welke score behaald is ten opzichte van het totaal te behalen aantal punten> <geef door te voeren verbeteringen aan>	
<Basisregistratie Ondergrond (BRO)>	<proefjaar>	
Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).	<geef aan op welke wijze gebruik gemaakt wordt van Suwinet en benoem partners> <geef aan of er bevindingen geconstateerd zijn> <Door te voeren verbeteringen aangeven (hoofdlijn)> <geef aan dat de zelfevaluatie is getoetst door een IT auditor en verwijs naar bijlage met collegeverklaring, de bijlage DigiD en assurancerapport (vertrouwelijk)>	

Resultaatafspraken

<Opgestelde verbeterplannen, beleggen van doorvoeren van de verbetering in de organisatie, planning>

Meer informatie

Heeft u behoefte aan toelichting op de informatie uit deze handreiking, neemt u dan contact op met een van de procesbegeleiders uit het team ENSIA bij VNG Realisatie. Zij zijn dagelijks telefonisch te bereiken via 070-250 2400 of per e-mail via ensia@vng.nl.

VNG Realisatie
Nassaulaan 12 Den Haag | Postbus 30435, 2500 GK Den Haag
070 373 8008 | realisatie@vng.nl