Alles over ENSIA

UITVOERING

Wat is ENSIA?
ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent eenmalige informatieverstrekking en eenmalige IT-audit.

Het project ENSIA heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid, gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

ENSIA helpt gemeenten in één keer slim verantwoording af te leggen over informatieveiligheid gebaseerd op de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten). De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Inkomen (Suwinet) is samengevoegd en gestroomlijnd.

Uitgangspunt is het horizontale verantwoordingsproces aan de gemeenteraad. Dit vormt de basis voor het verticale verantwoordingsproces aan de nationale partijen die een rol hebben in het toezicht op informatieveiligheid.

Waarom ENSIA?
Tijdens de Buitengewone Algemene Ledenvergadering van de VNG van november 2013 is de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangenomen. Met het aannemen van de resolutie erkennen alle gemeenten het belang van informatieveiligheid en de BIG als het gemeentelijk basisnormenkader voor informatieveiligheid. In de resolutie hebben gemeenten afgesproken hun eigen toezichthouder, de gemeenteraad, in het jaarverslag te informeren over informatieveiligheid. Ook roepen de gemeenten in de resolutie op om de verantwoordingslasten over informatieveiligheid te verminderen. Dit vormde de aanleiding voor de start van het project ENSIA.

ENSIA is een initiatief van de VNG en de ministeries van BZK, I&M en SZW.

Wie is binnen de gemeente betrokken bij het uitvoeren van de ENSIA zelfevaluatie informatiebeveiliging?
Om het nieuwe verantwoordingsproces goed in te richten en de vragenlijsten voor zelfevaluatie in te vullen is betrokkenheid uit verschillende delen van de gemeente gewenst. Denk hierbij aan: portefeuillehouder, gemeentesecretaris, de verantwoordelijke personen Bedrijfsvoering (ICT/HR/Inkoop), Burgerzaken (BRP/PUN), Sociaal Domein

(Suwinet), DigiD, BAG-beheer en BGT-beheer. Per ledenbrief is aan het college van B&W gevraagd om een coördinator voor ENSIA aan te wijzen, zie https://vng.nl/files/vng/brieven/2017/20170321_ledenbrief_nieuw-verantwoordingsproces-informatieveiligheid.pdf.

Uit welke producten/onderdelen bestaat de ENSIA zelfevaluatie informatiebeveiliging?

- **Vragenlijst zelfevaluatie informatiebeveiliging**
  Met de ingevulde zelfevaluatievragenlijst en bijbehorende rapportages geeft het college van B&W aan in hoeverre de beheersmaatregelen aan de van kracht zijnde beveiligingsnormen voldoen. Bij het opstellen van deze vragenlijst is vastgesteld waar de normen van BRP, PUN, DigiD, Suwinet, BAG en BGT aansluiten op de BIG-normen en dus volstaan kan worden met vragen die gebaseerd zijn op de BIG-normen. Voor specifieke normen van BRP, PUN, DigiD, SUWInet, BAG en BGT zijn aanvullende vragen geformuleerd. De paragraaf informatiebeveiliging - met als onderdeel de collegeverklaring ENSIA - zijn onder meer gebaseerd op de zelfevaluatie.

- **Collegeverklaring ENSIA inzake informatiebeveiliging**
  Met deze verklaring geeft het college van B&W aan in hoeverre bij de gemeente de beheersingsmaatregelen voldoen aan de voor de ENSIA-verantwoording geselecteerde normen en - indien aan de orde - welke onderdelen daarvan zijn uitgezonderd. Ook wordt melding gemaakt van eventuele verbetermaatregelen die de gemeente gaat treffen. De collegeverklaring wordt gezamenlijk met het assurancerapport separaat van het jaarverslag aangeboden aan de gemeenteraad.[1]

- **Assurancerapport**
  Een bij de NOREA geregistreerde IT-auditor controleert de collegeverklaring en stelt een assurancerapport op. Deze werkzaamheden van de IT-auditor duiden we ook wel aan als de IT-audit. De IT-auditor verklaart in het assurancerapport dat de collegeverklaring een getrouw beeld geeft. Getrouw betekent dat de collegeverklaring met een redelijke mate van zekerheid juist en volledig is. Deze verklaring van getrouwheid geeft aanvullende zekerheid over de juistheid en volledigheid van de collegeverklaring.

[1] Het opnemen van de ENSIA-verantwoordingsinformatie over informatiebeveiliging zal worden opgenomen met de Commissie Besluit begroting en verantwoording (BBV) die de regelgeving voor de jaarlijkse begrotings- en verantwoordingsstukken van gemeenten, provincies en waterschappen opstelt.

- **Paragraaf informatiebeveiliging in het jaarverslag /separate rapportage informatiebeveiliging**
  Het college van B&W neemt in het jaarverslag in de paragraaf bedrijfsvoering een aparte paragraaf op over informatiebeveiliging[2]. Deze paragraaf omvat informatie over de informatiebeveiliging in brede zin. Hierin rapporteert het college aan haar toezichthouder (de gemeenteraad) over informatiebeveiliging. Deze rapportage vloeit voort uit de afspraken in de gemeentelijke resolutie 'Informatiebeveiliging randvoorwaarde voor een professionele gemeente'. De gemeenteraad stelt de jaarstukken, waaronder het jaarverslag, vast. In de paragraaf informatiebeveiliging verwijst het college naar de collegeverklaring. De collegeverklaring maakt geen deel uit van het jaarverslag[3]. Gemeenten kunnen ervoor kiezen om een separate rapportage informatiebeveiliging aan de gemeenteraad te verstrekken. Deze rapportage omvat zowel de informatie over informatiebeveiliging in brede zin als de collegeverklaring ENSIA. Een aantal gemeenten kiest nu al voor deze behandeling omdat zij verwacht een grotere aandacht voor het onderwerp in de raadsbehandeling te krijgen. De assurancerapportage maakt geen onderdeel uit van de paragraaf informatiebeveiliging.

Hoe ziet de planning van het ENSIA-proces over het verantwoordingsjaar 2017 er uit?

De planning van de invoering ENSIA is als volgt:

1 juli – december 2017	Invullen en aanleveren zelfevaluatievragenlijst.
31 december 2017	Inleveren antwoorden voor zelfevaluatie over de volle breedte van de BIG (dus inclusief zelfevaluatie DigiD, Suwinet, BAG en BGT).
	<u>Voor horizontale verantwoording</u>
Jan - juli 2018	Opstellen paragraaf informatieveiligheid Opnemen in paragraaf bedrijfsvoering van het jaarverslag Jaarverslag bespreken in de raad
Voor 15 juli 2018	Het college van B&W legt verantwoording af over informatieveiligheid aan de gemeenteraad en stuurt de jaarstukken aan de minister van BZK.
	<u>Voor verticale verantwoording</u>
1 oktober 2017	Inleveren antwoorden zelfevaluatie informatieveiligheid BRP en PUN.

[2] Resolutie Informatieveiligheid, randvoorwaarde voor de professionele gemeente, BALV 29-10-2013: "Gemeenten zorgen voor verankering van informatieveiligheid op de gemeentelijke agenda, waarbij het college de gemeenteraad informeert. Dit gebeurt door middel van een aparte paragraaf informatieveiligheid in het jaarverslag."

[3] Om ongewenste samenloop met regelgeving voor accountants te voorkomen, is vooralsnog gekozen voor het niet opnemen van de door IT-auditor gecontroleerde Collegeverklaring in het jaarverslag.

Voor 1 mei 2018	Opstellen en uploaden collegeverklaring informatiebeveiliging.
Voor 1 mei 2018	Uitvoeren IT-audit en opstellen en uploaden assurancerapport.

Waarom moet in 2017 de zelfevaluatie voor BPR en PUN vóór 1 oktober worden aangeleverd?
Voor de BRP[4]/PUN[5] is wettelijk vastgelegd dat de verantwoordingsinformatie informatieveiligheid uiterlijk 30 september van het verantwoordingsjaar bekend moet zijn. Vanaf 2018 wordt toegewerkt naar één verantwoordingsmoment per jaar, te weten peildatum 31/12.

[3] Besluit BRP art. 47.1: De onderzoeken, bedoeld in artikel 4.3 van de wet, geschieden jaarlijks, uiterlijk op 30 september.

[4] Paspoortuitvoeringsregeling Nederland, art.94.1: De burgemeester of de gezaghebber voert voor 1 oktober van ieder jaar een controle uit op de toepassing van de beveiligingsmaatregelen, genoemd in de artikelen 90 tot en met 93, en de overige aspecten van het aanvraag- en uitgifteproces van reisdocumenten en informeert voor 1 november van ieder jaar de minister van Binnenlandse Zaken en Koninkrijksrelaties over de bevindingen van de controle.

Hoe verloopt de verantwoording over de domeinspecifieke vragen van de BAG, BGT, BRP en PUN?
Voor 2017 zijn in de ENSIA-tool alleen de domeinspecifieke vragen opgenomen ten behoeve van de verantwoording over de BAG en BGT. De ambitie is om vanaf 2018 ook de verantwoording over de domeinspecifieke vragen voor BRP en PUN op te nemen in de ENSIA-tool en gelijk te laten lopen met het verantwoordingsproces informatieveiligheid. De domeinspecifieke vragen BRP en PUN verlopen voor 2017 nog via de Kwaliteitsmonitor. Zie voor meer informatie over de Kwaliteitsmonitor: https://www.rvig.nl/actueel/nieuws/2017/04/05/vragenlijsten-zelfevaluaties-brp-en-pnik-2017-beschikbaar%5B2%5D.

Hoe komen de afspraken over de ENSIA-verantwoording tot stand?
Jaarlijks maken vertegenwoordigers van gemeenten en betrokken departementen in het strategisch beraad ENSIA afspraken over de inhoud van de ENSIA-verantwoording. Het betreft afspraken over te selecteren objecten, normen/vragen en over opzet/bestaan/werking, rapportageperiode, rapportagemoment en de IT-audit.

Wat is de reikwijdte van de zelfevaluatie informatiebeveiliging?
Met de ingevulde zelfevaluatievragenlijst geeft het college van B&W aan in hoeverre de beheersmaatregelen aan de van kracht zijnde beveiligingsnormen voldoen. Bij het opstellen van de zelfevaluatievragenlijst is vastgesteld waar de normen van BRP, PUN, Suwinet, BAG en BGT aansluiten op de BIG-normen en dus volstaan kan worden met vragen die gebaseerd zijn op de BIG-normen. Voor specifieke normen van BRP, PUN, Suwinet, BAG en BGT zijn aanvullende vragen geformuleerd. De reikwijdte van de zelfevaluatie is in onderstaande figuur gearceerd aangegeven.

BIG-hoofdstukken	**BRP**	**PUN**	**SUWI-net**	**BAG**	**BGT**
5 Beveiligingsbeleid					
6. Organisatie van de informatiebeveiliging					
7. Beheer van bedrijfsmiddelen					
8. Personele beveiliging					
9. Fysieke beveiliging					
10. Beheer van communicatie en bedieningsprocedures					
11. Toegangsbeveiliging					
12. Verwerving, ontwikkeling en onderhoud van Informatiesystemen					
13. Beheer van Informatiebeveiligings-incidenten					
14. Bedrijfscontinuïteitsbeheer					
15. Naleving					

De DigiD-norm kent een andere scope dan de BIG en ook een ander object van onderzoek. DigiD richt zich op de webpagina waarop zich een DigiD-snelkoppeling bevindt met een geheel eigen set van normen. Om die reden staan de DigiD-vragen los van de ENSIA vragenlijst. Matching met BIG-normen is daarom niet van toepassing.

Een gemeente bepaalt op basis van eigen (risico-)afwegingen de reikwijdte van de verantwoording in de paragraaf informatiebeveiliging over de overige gemeentelijke objecten die onder de BIG vallen (informatie over de beveiliging in brede zin).

Wat is de reikwijdte van de collegeverklaring informatiebeveiliging en de IT-audit?
De collegeverklaring informatiebeveiliging en de IT-audit hebben betrekking op opzet en bestaan van de beheersingsmaatregelen per 31 december 2017 voor de gearceerde normen (controls) en objecten in de onderstaande tabellen.

DigiD normenkader 2.0
De DigiD-norm heeft een andere scope dan de BIG en een ander object van onderzoek. Deze richt zich op de webpagina waarop zich een DigiD-snelkoppeling bevindt, met een geheel eigen set van normen. Daarnaast moet een gemeente de DigiD-audit laten uitvoeren per aansluiting. Een deel van de DigiD-norm is soms van toepassing op de gemeente, soms op een leverancier en soms op beiden. Om die reden zijn de DigiD-vragen losgeweekt van de ENSIA-vragenlijst. Matching met BIG-normen is daarom niet van toepassing.

Nr	Beschrijving van de beveiligingsrichtlijn
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar.
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.

Nr	Beschrijving van de beveiligingsrichtlijn
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.
C.07	De logging- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.

Het Suwinet normenkader voor afnemers 1.0

De SUWInetnorm richt zich net zoals de BIG (generiek) op de bedrijfsvoering, met als focus de sociale keten binnen de gemeente. Omdat de Suwinetnorm maar eenmalig hoeft te worden uitgevraagd en omdat ze gematchd is op de BIG controls, zijn de Suwinetvragen in de ENSIA-vragenlijst verweven met de BIG-vragen.

BIG	**SUWInet**	**Overige objecten**
Generieke controls met specifieke objectgerichte aanvullingen		
5.1.1 Beleidsdocument voor informatiebeveiliging	x (B01)	
5.1.2 Beoordeling van het informatiebeleid	X	
6.1.1 Betrokkenheid van het college van B en W bij informatiebeveiliging	X	
6.1.2 Coördineren van informatiebeveiliging	x (B01, B03, B04)	
6.1.3 Toewijzing van verantwoordelijkheden voor informatiebeveiliging	x (B05)	
Objectgerichte controls		
8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	x	
10.1.3 Functiescheiding	x (B05)	
10.10.1 Aanmaken auditlogbestanden	x (C05)	
10.10.2 Controle van het systeemgebruik	x (C06)	
11.2.1 Registratie van gebruikers	x (U03)	
11.2.4 Beoordeling van toegangsrechten van gebruikers	x (U03, C04)	
11.5.2 Gebruikersidentificatie en -authenticatie	x (U03)	
12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen	x (U11)	

Bij de SUWInetnormen zijn tussen haakjes verwijzingen opgenomen naar het SUWInet specifieke normenkader voor afnemers. Dit normenkader omvat nadere toelichting op de SUWInet-normen.

VERANTWOORDING

Waarover en aan wie wordt er verantwoording afgelegd?
Gemeenten voeren een zelfevaluatie informatiebeveiliging uit op basis waarvan het college van B&W in een paragraaf in het jaarverslag over de informatiebeveiliging rapporteert. Deze paragraaf omvat informatie over de informatiebeveiliging in brede zin en de zogenoemde collegeverklaring informatiebeveiliging gericht op een aantal geselecteerde beveiligingsnormen van de BRP, PUN, BAG, BGT, DigiD en Suwinet.[6] Een IT-auditor controleert de collegeverklaring en stelt een assurancerapport op. De gemeenteraad stelt de jaarstukken vast.

Via de ENSIA-tooling stellen gemeenten op digitale wijze rapportages en informatie beschikbaar over de zelfevaluatie, de collegeverklaring en het assurancerapport aan de minister van BZK. Dit ten behoeve van het toezicht op de BRP, de PUN en DigiD. Aan de minister van I&M ten behoeve van het toezicht op de BAG en de BGT. De minister van I&M dient de rapportages die in het kader van het toezicht op BAG en BGT zijn aangeleverd te publiceren op www.basisregistratiesienm.nl. Verder bieden gemeenten via ENSIA transparantie aan de beheerder van de centrale omgeving van de GeVS[7] (BKWI) ten behoeve van het jaarlijks opstellen van een totaaloverzicht van de beveiliging van de GeVS. Deze rapportage wordt uitgebracht aan het ketenoverleg GeVS en de minister van SZW. De Inspectie SZW houdt onafhankelijk signalerend toezicht op het functioneren van het stelsel werk en inkomen. Als de inspectie daartoe aanleiding ziet, kan de inspectie onderzoek doen naar de beveiliging van Suwinet bij gemeenten. Om de daarbij door de inspectie gevraagde informatie aan te leveren, kunnen gemeenten putten uit de via de ENSIA-tooling beschikbare verantwoordingsinformatie.

Komt er een samenvatting van de ENSIA zelfevaluatie informatiebeveiliging op waarstaatjegemeente.nl?
Dat is wel de ambitie voor de toekomst. Echter voor het verantwoordingsjaar 2017 komt er nog geen rapportage over de informatieveiligheid op www.waarstaatjegemeente.nl

De vragenlijst informatieveiligheid, zoals deze afgelopen jaren op Waarstaatjegemeente stond, is op 3 april opnieuw gepubliceerd. Deze vragenlijst heeft betrekking op de huidige situatie in 2017. Sluitingsdatum hiervoor is 1 september 2017.

[6] Voor de verantwoording over 2017 zijn de DigiD-normen en een beperkt aantal Suwinormen geselecteerd.

[7] GeVS staat voor Gezamenlijke Elektronische Voorzieningen SUWI, en wordt veelal aangeduid als Suwinet.

ENSIA-TOOL

Waaruit bestaat de ENSIA-tool?

Vragenlijsten

In de ENSIA-tool zijn drie vragenlijsten opgenomen voor de verantwoording over de informatiebeveiliging. Eén vragenlijst is gebaseerd op de BIG, met inbegrip van de specifieke normen over informatiebeveiliging van de BRP, PUN, BAG, BGT en Suwinet. Daarnaast is er de vragenlijst DigiD, welke per aansluiting moet worden ingevuld. De tool is gebaseerd op Vensters voor Bedrijfsvoering.

Rapportages

De gehele ENSIA-rapportage is bedoeld voor de horizontale verantwoording over informatiebeveiliging. Er is mogelijkheid om de rapportages te selecteren op de verschillende BIG-hoofdstukken en op stelselniveau.

Upload veld verantwoordingsdocumenten

Om de ENSIA-zelfevaluatie informatiebeveiliging af te ronden moet er ook een collegeverklaring informatiebeveiliging en een assurancerapport worden geüpload.

In de tool zijn *formats* opgenomen voor de collegeverklaring ENSIA inzake informatiebeveiliging DigiD en SUWInet en het assurancerapport van de onafhankelijke IT-auditor.

Is het mogelijk om de zelfevaluatie informatiebeveiliging via de ENSIA-tool te bekijken?

Dat is nog niet mogelijk. Van augustus 2016 tot en met december 2016 vond er een ENSIA-pilot plaats met zeven gemeenten. De pilot richtte zich onder andere op het toetsen van de vragenlijst voor zelfevaluatie, de tool en het doorlopen van het ENSIA-verantwoordingsproces. De resultaten van de pilot zijn verwerkt in de vragenlijst en de tool. Eind april/begin mei zal een laatste test plaatsvinden, gericht op gewijzigde functionaliteiten. Begin juni zal de vragenlijst beschikbaar worden gesteld via de websites www.kinggemeenten.nl en www.ensia.nl.

INFORMATIE EN CONTACT

Uitvoering ENSIA
KING ondersteunt gemeenten bij het inrichten van het verantwoordingsproces en de implementatie van ENSIA. Meer informatie vindt u op https://www.kinggemeenten.nl/implementatie-ensia-het-kort. Voor vragen over implementatie en ondersteuning kunt u contact opnemen met KING via ensia@kinggemeenten.nl.

Inhoud verantwoording/inhoud informatiestelsels
Heeft u vragen over de verantwoording/inhoud van de BRP, PUN, DigiD, BAG, BGT of Suwinet? Neem dan contact op met de betreffende toezichthouder of uitvoerder.

BRP en PUN: www.rvig.nl
DigiD: www.logius.nl
BAG en BGT: www.basisregistratiesienm.nl
Suwinet: www.vng.nl/suwinet

Algemene vragen over de tooling en het project ENSIA kunt u mailen naar ensia@ictu.nl

Veranderingen verantwoording informatiebeveiliging op hoofdlijnen

Oude situatie (2016)	ENSIA-situatie in 2017
Niet alle gemeenten verantwoorden zich bestuurlijk in het openbaar over informatieveiligheid Bij verantwoordingsactiviteiten wordt niet aangesloten bij de P&C-cyclus van gemeenten	Er wordt aangesloten bij gemeentelijke P&C-cyclus. Informatieveiligheid krijgt daarmee meer politieke/bestuurlijke aandacht en wordt beter meegenomen in organisatiebrede afwegingen rond mensen, middelen en risicobeheersing.
Er zijn verschillende vragenlijsten/verantwoordingen over informatieveiligheid (BRP, PUN, DigiD, BAG, BGT en SUWInet) die op verschillende momenten, verspreid binnen de gemeente worden uitgezet	Zelfevaluatie Informatieveiligheid en zelfevaluatie DigiD assessment wordt door middel van één tool uitgevraagd.
Nationale toezichthouders stellen veel dezelfde vragen aan gemeenten.	Dubbelingen uit de vragenlijsten zijn verminderd. De zelfevaluatie Informatieveiligheid BIG bevat 15 % minder vragen dan in de oude situatie. Gemeenten worden in staat gesteld om de verplichte audit DIGID en SUWI goed voor te bereiden.
Gemeenten dienen zich op meerdere momenten in het jaar te verantwoorden	2017 is een overgangsjaar en zijn er twee momenten van 'verantwoorden' informatieveiligheid: peildatum 1/10: BRP, PUN peildatum 31/12: DigiD, SUWInet, BAG en BGT Vanaf 2018 wordt toegewerkt naar één peildatum, te weten 31/12. Voor 15 juli 2018 legt het College van B&W verantwoording af over informatieveiligheid aan gemeenteraad.
Er zijn meerdere audits (SUWInet, DigiD)	Er is één IT-audit. De reikwijdte van de audit voor 2017 betreft SUWInet en DigiD
Uitvraag voor de verantwoording over niet-informatieveiligheidsaspecten (domeinvragen) vindt op andere momenten plaats en doormiddel van verschillende tools.	Het verantwoordingsjaar 2017 is een overgangsjaar voor ENSIA. Voor het verantwoordingsjaar 2018 is het de ambitie om ook de uitvraag voor de verantwoording over domeinspecifieke aspecten van de BRP en PUN te laten verlopen via de ENSIA-tool. En het moment van uitvraag te harmoniseren met de uitvraag voor verantwoording

	over informatieveiligheid.
Informatieveiligheid heeft geen vaste plek in het jaarverslag.	Het gemeentebestuur legt verantwoording af over de informatieveiligheid aan de gemeenteraad. Conform de Resolutie Informatieveiligheid is de ambitie om informatieveiligheid als vast onderdeel op te nemen in het jaarverslag.