Notitie Verantwoordingsstelsel ENSIA

Versie: 29 juni 2017, definitief

Inleiding

Doel van deze notitie is het bieden van een eenduidige beschrijving van het verantwoordingsstelsel ENSIA voor alle partijen en personen die betrokken zijn bij het ontwikkelen, invoeren en beheren van ENSIA.

Achtergrond

Het project ENSIA (Eenduidige Normatiek Single Information Audit) is een gezamenlijk project van het ministerie van Binnenlandse Zaken, gemeenten, het ministerie van SZW, het ministerie van I&M en de VNG. Het project 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). Uitgangspunt is dat aangesloten wordt op de gemeentelijke P&C-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan hier ook beter op sturen.

Het project is een resultaat van de resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" die in november 2013 tijdens de Buitengewone Algemene Ledenvergadering van De VNG is aangenomen.

In deze resolutie hebben de gemeenten het belang van informatieveiligheid erkend en de Baseline Informatieveiligheid Nederlandse Gemeenten (BIG) aangenomen als hét gemeentelijk basisnormenkader voor informatieveiligheid. De gemeenten hebben zich gecommitteerd aan de implementatie van de BIG in de eigen organisatie. Daarnaast informeert een college van B en W de gemeenteraad over informatieveiligheid in het jaarverslag. In de resolutie hebben de gemeenten ook een oproep gedaan aan de rijksoverheid en ketenpartners om de verantwoordingslast over informatieveiligheid te verminderen. Dit laatste vormde de aanleiding voor de start van het project ENSIA.

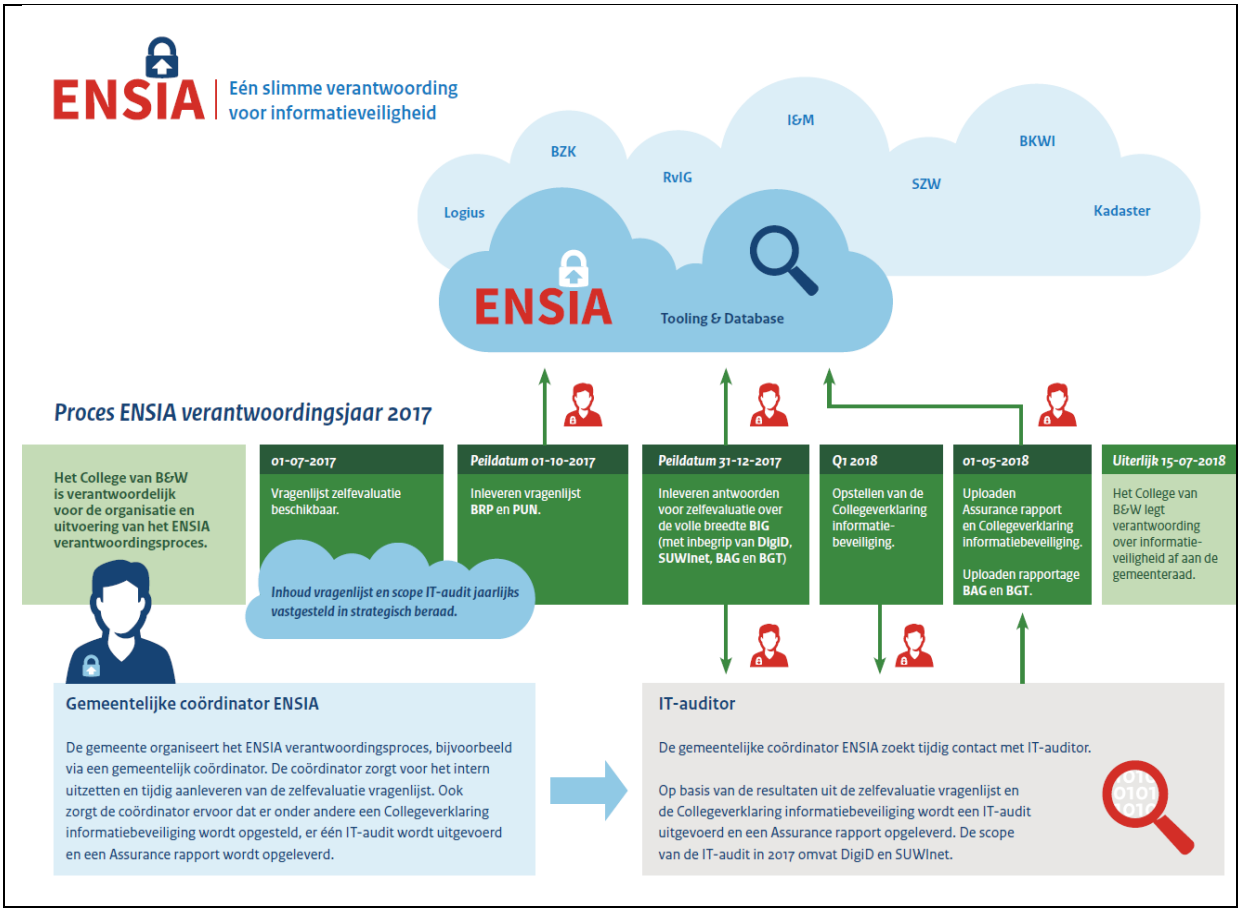
Versie historie

- Versie 29 juni 2016, vastgesteld in stuurgroep 12 juli 2016.
- Versie 21 november 2016, vastgesteld in de stuurgroep van 24 november 2016. Deze versie is aangepast aan voortschrijdend inzicht in de afgelopen maanden.
- Versie 16 december 2016: aangepast n.a.v. resultaten van de impactanalyse: redactieslag, aanpassing van het tijdpad, verdere uitwerking van bijlage 2 met detailafspraken over 2017 met nadere toelichting van de reikwijdte van de zelfevaluatie informatiebeveiliging, de Collegeverklaring informatiebeveiliging en de IT-audit. Besproken in de stuurgroep op 22 december 2016.
- Versie 16 maart 2017: aangepast n.a.v. herijking tijdpad en reikwijdte Collegeverklaring en IT-audit, herijkte formats Collegeverklaring (bijlage 2) en Assurancerapport (bijlage 3) na afstemming met NOREA, handreiking voor de paragraaf Informatieveiligheid in het jaarverslag (bijlage 5) toegevoegd en diverse aanpassingen op basis van voortschrijdend inzicht. Te bespreken in de stuurgroep op 23 maart.
- Versie 27 maart: vastgestelde versie. Oplegger en vragen aan de stuurgroep verwijderd, procesplaat toegevoegd op pagina 2.
- Versie 29 juni: n.a.v. diverse opmerkingen tekstaanpassingen ter verduidelijking doorgevoerd.

Het verantwoordingsstelsel ENSIA

De 'ENSIA verantwoording informatiebeveiliging' gaat uit van het principe van Single Information & Single Audit (SISA). Dit betekent eenmalige informatieverstrekking en eenmalige IT-audit.

De ENSIA werkwijze in het kort
Gemeenten voeren een zelfevaluatie informatiebeveiliging uit op basis waarvan het college van B en W in een paragraaf in het jaarverslag over de informatiebeveiliging rapporteert. Deze paragraaf omvat informatie over de informatiebeveiliging in brede zin en een verwijzing naar de zogenoemde Collegeverklaring ENSIA inzake informatiebeveiliging gericht op een aantal geselecteerde beveiligingsnormen van de BRP, PUN, BAG, BGT, DigiD en Suwinet. Een IT-auditor controleert de collegeverklaring en stelt een assurancerapport op. De ENSIA-tooling ondersteunt het uitvoeren van de zelfevaluatie en het beschikbaar stellen van relevante informatie aan de betrokken partijen met een toezichthoudende verantwoordelijkheid. ENSIA start in 2017 met een beperkte scope. ENSIA zal de komende jaren middels een groeipad worden doorontwikkeld. Jaarlijks maken vertegenwoordigers van gemeenten en betrokken departementen in het strategisch gremium ENSIA[1] daarover afspraken.



Afbeelding: procesplaat verantwoordingsstelsel ENSIA

[1] Voor 2017 maakt de stuurgroep ENSIA deze afspraken.

De gemeentelijke producten

- **Paragraaf Informatiebeveiliging in het jaarverslag / separate Rapportage Informatiebeveiliging**
  Het college van B en 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 ENSIA. De Collegeverklaring ENSIA maakt geen deel uit van het jaarverslag.[3] In bijlage 5 is een handreiking opgenomen voor het opstellen van de paragraaf Informatiebeveiliging. 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. In dit geval kan in het jaarverslag kort verwezen worden naar deze separaat uitgebrachte rapportage. Een aantal gemeenten kiest nu al voor deze behandeling omdat zij verwacht een grotere aandacht voor het onderwerp in de raadsbehandeling te krijgen. Een separate rapportage waarbij het College van B en W alle informatie over de informatiebeveiliging in samenhang aan de gemeenteraad voorlegt, verdient dan ook de voorkeur.

- **Collegeverklaring ENSIA inzake informatiebeveiliging**
  Met deze verklaring geeft het college van B en W aan in hoeverre bij de gemeente de beheersingsmaatregelen hebben voldaan 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. Zie de uitwerking van de Collegeverklaring ENSIA in bijlage 2. De Collegeverklaring ENSIA wordt gezamenlijk met het Assurancerapport separaat van het jaarverslag aan de gemeenteraad aangeboden.

- **Zelfevaluatie informatiebeveiliging**
  Met de ingevulde zelfevaluatievragenlijst geeft het college van B en 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 / separate Rapportage Informatiebeveiliging en de Collegeverklaring ENSIA zijn onder meer gebaseerd op de zelfevaluatie.

- **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. Zie de uitwerking van het Assurancerapport in bijlage 3.

[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.

Informatieverstrekking met behulp van de ENSIA-tooling
Via de ENSIA-tooling stellen gemeenten op digitale wijze rapportages en informatie beschikbaar over de zelfevaluatie, de Collegeverklaring ENSIA en het Assurancerapport aan de minister van BZK ten behoeve van het toezicht op de BRP, de PUN en DigiD en aan de minster van I&M ten behoeve van het toezicht op de BAG en de BGT. Verder bieden gemeenten via ENSIA transparantie aan de beheerder van de centrale omgeving van de GeVS[4] (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.

Samenwerkingsverbanden
Bij samenwerkingsverbanden blijft het college van B en W als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van informatie. Het is aan het college van B en W om hierover binnen de grenzen van het samenwerkingsverband afspraken te maken (zie nadere informatie in bijlage 4).

Verantwoording over gemeentelijke objecten
Een gemeente bepaalt op basis van eigen (risico-)afwegingen de reikwijdte van de jaarlijkse verantwoording over gemeentelijke objecten die onder de BIG vallen. Dit betreft objecten anders dan BRP, PUN, DigiD, Suwinet, BAG en BGT. Hierbij kan een gemeente een groeipad toepassen. Op termijn is denkbaar dat de verantwoordingssystematiek doorgroeit naar een collegeverklaring (in control statement) die zowel de hiervoor genoemde objecten als de overige gemeentelijke objecten omvat.

Afspraken over de ENSIA verantwoording en het groeipad
Jaarlijks maken vertegenwoordigers van gemeenten en betrokken departementen in het strategisch gremium ENSIA[5] 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. In de eerste jaren zal sprake zijn van een groeipad.

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

[5] Voor 2017 maakt de stuurgroep deze afspraken.

Middels het groeipad kan de ENSIA-systematiek met realistische jaarlijkse stappen doorgroeien naar een eindperspectief dat aansluit op de noodzaak en het ambitieniveau van gemeenten om het informatieveiligheidsbeleid zowel bestuurlijk als ambtelijk in de organisatie te borgen.

Uitgangspunt is dat in het eindperspectief de verantwoording over BRP, PUN, BAG en BGT op aspecten anders dan informatiebeveiliging, op hetzelfde moment wordt afgelegd als de verantwoording over informatiebeveiliging. Daarbij wordt waar mogelijk geharmoniseerd op taalgebruik, tooling en verantwoordingsafspraken. Afspraken hierover kunnen onderdeel zijn van het groeipad.

Afspraken over het jaar 2017
De stuurgroep ENSIA heeft besloten dat in het eerste jaar van ENSIA, verantwoording wordt afgelegd over de opzet en het bestaan van beheersmaatregelen en nog niet over de werking daarvan. Verder heeft de stuurgroep ENSIA besloten dat de zelfevaluatie in het eerste jaar betrekking heeft op BRP, PUN, DigiD, Suwinet, BAG en BGT en dat het gemeenten vrij staat om overige objecten in de zelfevaluatie te betrekken. Verder is in de stuurgroep afgesproken dat gemeenten er zorg voor dragen dat de noodzakelijke verantwoordingsinformatie via de ENSIA werkwijze wordt aangeleverd en zo invulling geven aan het single information single audit principe.

Over het verantwoordingsjaar 2017 richt de IT-audit zich op de DigiD-normen en een selectie van Suwinet normen. Een beperkt aantal normen zoals het informatiebeveiligingsbeleid en de betrokkenheid van het college van B en W bij informatiebeveiliging, hebben hierbij een generiek karakter. Met deze selectie van normen wordt ervaring opgedaan met het assuranceproces én is de inspanning om een goede 'guidance' te ontwikkelen relatief beperkt. Op basis van deze ervaring wordt de inrichting van de IT-audit over het verantwoordingsjaar 2018 aangepast. Eén en ander is verder uitgewerkt in bijlage 1.

Tijdpad ENSIA in 2017 en in het eindperspectief
In het verantwoordingsjaar 2017 is het nog niet mogelijk om de timing van de BRP/PUN kwaliteitsmonitor en de daarmee verband houdende wettelijke termijnen aan te passen op het voor ENSIA tijdspad. Met BRP/PUN zijn wel afspraken gemaakt om dit tijdspad en de onderliggende tooling op een zo kort mogelijke termijn op elkaar af te stemmen. In onderstaande tabel is weergegeven welke deadlines voor ENSIA en de kwaliteitsmonitor zullen gelden. In de kolom 'eindperspectief' is het uiteindelijk te realiseren beeld geschetst.

We moeten ons daarbij realiseren dat in de kwaliteitsmonitor nog alleen 'niet informatieveiligheids-issues' zijn opgenomen. Het betreft kwaliteitsaspecten die alleen binnen het werkveld 'burgerzaken' worden gehanteerd. Alle voor BRP/PUN geldende 'informatieveiligheidsissues' zijn opgenomen in de ENSIA vragenlijst. Een tussenstap is in 2017 daarom noodzakelijk.

Stap	2017	Eindperspectief
1. Afspraken maken over de verantwoording	uiterlijk 1 april 2017	1 april
2. Invullen van de zelfevaluatie vragenlijst	1 juli - 1 oktober 2017 voor BRP/PUN[6] 1 juli – 31 december 2017 voor alle andere vragen	1 juli – 31 december over opzet en bestaan per 31/12 en in de toekomst de werking over het kalenderjaar.
3. Afsluiten vragenlijst met peildatum 31 december	uiterlijk 31 december 2017	uiterlijk 31 december
4. - Opstellen van een Collegeverklaring. - Uitvoeren van een IT-Audit en het daarbij opstellen van een Assurancerapport. - Beschikbaar stellen van Collegeverklaring en Assurancerapport	uiterlijk 1 mei 2018	Uiterlijk 1 mei
5. Vaststellen van de jaarstukken door de gemeenteraad, toesturen van de jaarstukken aan de minister van BZK	uiterlijk 15 juli 2018	uiterlijk 15 juli[7]

Toelichting op de data van het proces in 2017:

- Deze data passen binnen bestaande wettelijke kaders van de stelsels die een onderdeel uitmaken van ENSIA.

Toelichting op de data in het eindperspectief:

1. Uitgangspunt is dat de verantwoording over informatiebeveiliging onderdeel wordt van de jaarlijkse verantwoordingscyclus bij gemeenten. De periode waarover in het jaarverslag verantwoording wordt afgelegd betreft daarbij het kalenderjaar. Voor de opzet en het bestaan van maatregelen is 31 december een logische datum. Het afleggen van verantwoording over de werking van maatregelen betreft het kalenderjaar.

2. Het geschetste tijdpad in de derde kolom is gericht op het eindperspectief ENSIA. Hierbij geldt:
    a. Waar nodig worden de bestaande wettelijke termijnen in lijn gebracht met het tijdpad in het eindperspectief.[8] Zo gelden op dit moment wettelijke termijnen bij BRP en PUN om de vragenlijst per 1 oktober te hebben ingevuld.
    b. De verantwoordingssystematiek groeit in de komende jaren stapsgewijs toe naar het eindperspectief, er is sprake van een groeipad. Zo heeft de stuurgroep besloten om het eerste jaar te starten met een verantwoording over opzet en bestaan en de werking op een later moment toe te voegen. Het groeipad kan, gezien de bestaande wettelijke termijnen, ook betrekking hebben op het tijdpad.

[6] Deze stap is noodzakelijk geacht gegeven de bestaande wettelijke termijnen bij BRP en PUN om de vragenlijst per 1 oktober te hebben ingevuld

[7] Wettelijke termijn voor het aanleveren van het jaarverslag en de jaarrekening aan de minister van BZK

[8] In de stuurgroep ENSIA van 24 november 2016 is besloten dat de stuurgroep BZK, I&M en SZW verzoekt in beeld te brengen op welke termijn de wet- en regelgeving met het tijdpad voor het eindperspectief in overeenstemming kan worden gebracht.

3. Uitgangspunt is dat de verticale verantwoording wordt gebaseerd op de horizontale verantwoording. Het uiterlijk per 1 oktober invullen van de vragenlijst voor BRP/PUN past niet bij dit uitgangspunt. De IT-audit en de verantwoording in het jaarverslag aan de gemeenteraad zijn nog niet uitgevoerd en daarmee is het proces nog niet afgerond.

4. De Collegeverklaring ENSIA en het Assurancerapport dienen uiterlijk 1 mei beschikbaar te worden gesteld middels een upload met de ENSIA-tooling. De datum van 1 mei geeft voldoende ruimte voor het opstellen van de Collegeverklaring en het Assurancerapport en ligt vóór de start van de volgende jaarcyclus waarbij per 1 juli de zelfevaluatievragenlijst wordt opengesteld.

5. Consequentie van het beschreven tijdpad voor het eindperspectief is dat wet- en regelgeving in overeenstemming moet worden gebracht met dit tijdpad.

Bijlage 1 Detail Afspraken over de ENSIA verantwoording 2017

1. Inleiding

In deze bijlage zijn de voor het verantwoordingsjaar 2017 gemaakte afspraken over de ENSIA-verantwoording nader beschreven. Deze afspraken zijn gemaakt in de stuurgroep van het project ENSIA. Het betreft afspraken over te selecteren objecten, normen/vragen en over opzet en bestaan, rapportageperiode, rapportagemoment en de IT-audit. Na afronding van dit project gaan vertegenwoordigers van gemeenten en betrokken departementen jaarlijks in het in te richten strategisch gremium ENSIA afspraken maken over de de ENSIA-verantwoording.

In de eerste jaren zal sprake zijn van een groeipad. Middels het groeipad kan de ENSIA-systematiek met realistische jaarlijkse stappen doorgroeien naar een eindperspectief dat aansluit op de noodzaak en het ambitieniveau van gemeenten om het informatieveiligheidsbeleid zowel bestuurlijk als ambtelijk in de organisatie te borgen en daarbij te voldoen aan de eisen van BRP, PUN, DigiD, GeVS, BAG en BGT.

Uitgangspunt is dat in het eindperspectief de verantwoording over BRP, PUN, BAG en BGT op aspecten anders dan informatiebeveiliging, op hetzelfde moment wordt afgelegd als de verantwoording over informatiebeveiliging. Daarbij wordt waar mogelijk geharmoniseerd op taalgebruik, tooling en verantwoordingsafspraken. Afspraken hierover kunnen onderdeel zijn van het groeipad.

2. Normering

Voor het verantwoordingsjaar 2017 zijn in de volgende documenten de van kracht zijnde normen geformuleerd voor de objecten waarover verantwoording wordt afgelegd:

- BIG: Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten, versie 1.02, juni 2016
- GeVS: Specifiek Suwinet normenkader Afnemers, versie 1.0, 6-9-2016
- Digid: Het DigiD normenkader 2017
- BAG: BGT: Wet en regelgeving in ontwikkeling; vaststelling wordt verwacht zomer 2017
- BRP: Wet en regelgeving BRP
- PUN: Wet en regelgeving PUN

3. Reikwijdte zelfevaluatie informatiebeveiliging

Met de ingevulde zelfevaluatievragenlijst geeft het college van B en 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, 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 reikwijdte van de zelfevaluatie is in onderstaande figuur gearceerd aangegeven. 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 zijn de DigiD-vragen losgeweekt van de ENSIA vragenlijst. Matching met BIG-normen is daarom niet van toepassing.

BIG-hoofdstukken	**BRP**	**PUN**	**DigiD**	**Suwi-net**	**BAG**	**BGT**	**Selectie van overige gemeen-telijke objecten**
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							
DigiD-normen							

Figuur: Reikwijdte zelfevaluatie (gearceerd)

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).

4. Reikwijdte Collegeverklaring ENSIA inzake informatiebeveiliging en IT-audit

De Collegeverklaring ENSIA 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.

Het DigiD normkader 2.0

Als eerste is er de DigiD-norm met een andere scope dan de BIG en ook met een ander object van onderzoek. DigiD 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. Daarnaast is een deel van de DigiD-norm soms van toepassing op de gemeente en 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 meer 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.
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.
C.03	Vulnerability assesments (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 loggings- 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.

Nr	Beschrijving van de beveiligingsrichtlijn
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.

In de zelfevaluatie is het vernieuwde DigiD normenkader zoals dat geldt vanaf 2017 verwerkt. Vanuit de zelfevaluatie wordt aan Logius in een voor hen verwerkbaar format per DigiD aansluiting informatie door de gemeente verstrekt. De in samenwerking met NOREA uitgewerkte guidance DigiD is uitgangspunt voor het uitvoeren van werkzaamheden door de gemeenten en de auditors. De gemeente stelt met ingang van 1 januari 2018 alle DigiD-rapportages (die op dit moment door de auditors aan Logius worden verstrekt) op en neemt een samenvatting (waarin in ieder geval alle geconstateerde afwijkingen van de DigiD-normen zijn opgenomen) van de DigiD-rapportages op in de Collegeverklaring. De IT-auditor geeft via een Assurancerapport zekerheid over de juistheid en volledigheid (getrouwheid) van de Collegeverklaring.

Het Suwinet normenkader voor afnemers 1.0
Als tweede is er de Suwinet-norm. Deze richt zich net zoals de BIG (generiek) op de bedrijfsvoering, met als focus de sociale keten binnen de gemeente, omdat de Suwinet-norm maar eenmalig hoeft te worden uitgevraagd en omdat ze gematchd zijn op de BIG controls, zijn de Suwinet-vragen 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)	

Figuur: Reikwijdte Collegeverklaring informatiebeveiliging en IT-audit (gearceerd)

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

Betreffende Suwinet gelden voor gemeenten alle van kracht zijnde aan de beveiliging van Suwinet gestelde normen van de BIG en het specifieke Suwinet normenkader afnemers.

De Inspectie SZW en de AP hebben in de afgelopen jaren ten behoeve van hun onderzoek de volgende onderwerpen geselecteerd:

1. Het informatiebeveiligingsbeleid en het beveiligingsplan Suwinet;
2. De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinet gegevens, applicaties, processen en infrastructuur en de rol van de security officer daarbij;
3. Het logische toegangsbeheer;
4. De aansluiting van niet-Suwi partijen en de toepassing van Suwinet-inlezen daarbij.

De 7 normen die de inspectie voor haar onderzoeken heeft geselecteerd, vormen een uitwerking van de eerste 3 onderwerpen. Voor 2017 is van belang dat het bereikte niveau van beveiliging wordt vastgehouden. De Suwinet beveiligingsnormen voor afnemers zijn het afgelopen jaar herijkt en daarbij is het Specifiek Suwinet normenkader Afnemers opgesteld. In de tabel hiervoor zijn de verwijzingen opgenomen naar dit normenkader opgenomen.

Verder is van belang dat invulling wordt gegeven aan de toezeggingen die UWV aan de AP heeft gedaan betreffende de controle op het gebruik van via Suwinet-Inlezen geleverde gegevens. UWV heeft aan de AP toegezegd medio 2016 van SNG, Amsterdam, Den Haag en Rotterdam een jaarrapportage te ontvangen over de uitgevoerde controles op het gebruik van Suwinet-Inlezen. Met ingang van het verantwoordingsjaar 2017 zal deze rapportage via ENSIA worden ingevuld. Conform het Suwinet specifieke normenkader afnemers betekent dit dat de eisen betreffende logging over het gegevensgebruik op medewerkersniveau, het opstellen van gebruiksrapportages en het op basis daarvan controleren van het gebruik op alle gemeentelijke applicaties van toepassing zijn waarin via Suwinet-Inlezen of DKD-Inlezen ingelezen gegevens worden verwerkt. Verder is, gezien het belang ervan, een norm toegevoegd voor het versleutelen van netwerkverbindingen.

Bijlage 2

Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet

Het college van burgemeester en wethouders van de gemeente <naam gemeente> legt met deze verklaring verantwoording af over geselecteerde informatiebeveiligingsnormen inzake DigiD en Suwinet op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.
Het doel van ENSIA is om de verantwoording over Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Gezamenlijke Elektronische Voorzieningen Structuur Uitvoeringsorganisatie Werk en Inkomen (Suwinet) te bundelen in één systematiek dat onder meer uitgaat van de Baseline Informatiebeveiliging Gemeenten (BIG). Naast deze verklaring is de zelfevaluatie van de BIG eveneens een onderdeel van de ENSIA systematiek.
ENSIA sluit aan op de gemeentelijke planning en control cyclus voor informatiebeveiliging. Hierdoor heeft het gemeentebestuur meer overzicht over de informatieveiligheid van de gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad en andere belanghebbenden.

Reikwijdte verklaring
Deze verklaring betreft de onderdelen van de ENSIA systematiek waarover assurance wordt gevraagd van een onafhankelijke IT auditor. Voor het jaar 2017 betreft dit DigID en Suwinet. De verklaring omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0 (de Norm v2.0) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.0). De normen staan op het openbare deel van de websites van het ministerie van BZK en het BKWI. De verklaring omvat niet de werking van de maatregelen over 2017.
Deze collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet.

Verklaring college
Het college verklaart dat bij gemeente <naam gemeente> op 31 december 2017 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigID en Suwinet, <alleen bij afwijkingen: met uitzondering van de hierna vermelde normen>.
..
De met de uitzonderingen samenhangende beoogde (aanvullende) beheersmaatregelen zijn in verbeterplannen opgenomen.

[Plaats, datum]

[College van B en W gemeente]

Bijlage 3

Assurance-rapport van de onafhankelijke IT-auditor

Aan: Opdrachtgever

Ons oordeel
Wij hebben de bijgevoegde Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet (hierna Collegeverklaring ENSIA 2017) van gemeente <naam gemeente> onderzocht.

Naar ons oordeel is bijgevoegde Collegeverklaring ENSIA 2017 van gemeente <naam gemeente>, in alle van materieel belang zijnde aspecten, juist.

De Collegeverklaring ENSIA 2017 omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigID (Norm ICT-beveiligingsassessments DigiD versie 2.0 (de Norm v2.0)) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.0). De normen DigiD en Suwinet staan op het openbare deel van de websites van het ministerie van BZK en het BKWI. Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel omtrent DigiD en Suwinet. De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel staan beschreven in de collegeverklaring.

<Alleen bij afwijkingen: passage zonder paragraafkop over beperkingen bij het onderzoek.
Zoals in de collegeverklaring ENSIA 2017 is aangegeven wordt aan de volgende normen niet voldaan:
- >

De basis voor ons oordeel
Wij hebben onze assurance-opdracht met betrekking tot de Collegeverklaring ENSIA 2017 verricht in overeenstemming met Richtlijn 3000 (Herzien) 'Assuranceopdrachte door IT-auditors' van NOREA. Deze assurance-opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Onze verantwoordelijkheden voor de assurance-opdracht betreffende de Collegeverklaring ENSIA 2017'.

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

Wij vinden dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor ons oordeel.

Beperking in gebruik en verspreidingskring
Dit assurancerapport is bestemd voor gebruikers van de Collegeverklaring ENSIA 2017. De Collegeverklaring ENSIA 2017 is opgesteld voor de gemeenteraad en voor de departementen die toezien op de veiligheid van DigiD en Suwinet. Doel van de Collegeverklaring ENSIA 2017 is om de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet te informeren over het in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigID en Suwinet. Ons assurancerapport is derhalve uitsluitend bestemd voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet en dient niet te worden verspreid aan of te worden gebruikt door anderen.

Verantwoordelijkheden van het college van burgemeester en wethouders gemeente <naam gemeente>
Het college van burgemeester en wethouders is verantwoordelijk voor het opstellen van de Collegeverklaring ENSIA 2017. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet dienen voldoende inzicht te hebben om deze collegeverklaring, samen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die zelf

worden uitgevoerd, te beschouwen wanneer zij de risico's van afwijkingen van materieel belang in relatie tot DigiD en Suwinet inschatten.
De criteria waarvan bij het maken van deze verklaring gebruik werd gemaakt, hielden in dat:

- de risico's die het bereiken van de geselecteerde normen DigID en Suwinet in gevaar brengen, werden geïdentificeerd en
- de onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de vermelde interne beheersingsdoelstellingen niet zouden verhinderen.

Het college van burgemeester en wethouders is ook verantwoordelijk voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de Collegeverklaring ENSIA 2017 mogelijk te maken zonder afwijkingen van materieel belang als gevolg van fraude of fouten.

Onze verantwoordelijkheden voor de assurance-opdracht betreffende de collegeverklaring ENSIA 2017. Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van een assurance-opdracht dat wij daarmee, met een redelijke mate van zekerheid voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel. Een redelijke mate van zekerheid wil zeggen dat onze assurance-opdracht is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens onze assurance-opdracht niet alle materiële fouten en fraude ontdekken.

Wij passen het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van de ethische voorschriften, professionele standaarden en andere wet- en regelgeving.

Afwijkingen kunnen ontstaan als gevolg van fraude of fouten en zijn materieel indien redelijkerwijs kan worden verwacht dat deze, afzonderlijk of gezamenlijk, van invloed kunnen zijn op de beslissingen die gebruikers op basis van de Collegeverklaring ENSIA 2017 nemen. De materialiteit beïnvloedt de aard, timing en omvang van onze assurance-werkzaamheden en de evaluatie van het effect van onderkende afwijkingen op ons oordeel.

Wij hebben deze assurance-opdracht professioneel kritisch uitgevoerd en hebben waar relevant professionele oordeelsvorming toegepast in overeenstemming met de Richtlijn 3000 (Herzien) 'Assuranceopdrachten door IT-auditors' van NOREA.

Onze assurance-opdracht bestond onder andere uit:

- het verkrijgen van kennis omtrent de Collegeverklaring ENSIA 2017 en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen;
- het op basis van deze kennis inschatten van de risico's dat de Collegeverklaring ENSIA 2017 onjuistheden van materieel belang bevat;
- het reageren op de ingeschatte risico's, waaronder het ontwikkelen van een algehele aanpak, en het bepalen van de aard, de tijdsfasering en de omvang van verdere procedures;
- het uitvoeren van verdere procedures die duidelijk zijn gekoppeld aan de gesignaleerde risico's, waarbij gebruik wordt gemaakt van een combinatie van inspectie, waarnemingen ter plaatse en inwinnen van inlichtingen en
- het evalueren van de toereikendheid van de assurance-informatie.

Plaats en datum

... (naam IT-auditeenheid)

... (naam IT Auditor RE)

Bijlage 4. De invulling van verantwoordelijkheden in samenwerkingsverbanden

Wat is de aanleiding?
Eind 2013 is in de BALV de resolutie 'Informatieveiligheid randvoorwaarde voor een professionele gemeente aangenomen. In de resolutie hebben gemeenten afgesproken de BIG (Baseline Informatie veiligheid Gemeenten) te hanteren als gezamenlijk normenkader. Gemeenten zullen zich in het jaarverslag gaan verantwoorden over informatieveiligheid aan de eigen toezichthouder (horizontale verantwoording). Gemeenten hebben gevraagd aan Min BZK om de bestaande verantwoordingen op het vlak van informatieveiligheid te stroomlijnen. In de huidige situatie hebben gemeenten te maken met minimaal vijf verantwoordingen op het vlak informatieveiligheid. Deze verschillen qua diepgang, timing en gevraagde assurance, terwijl zij steeds hetzelfde thema belichten.

Min BZK heeft in samenwerking met betrokken departementen en VNG het project ENSIA gestart en (Eenduidige Normatiek Single Information Audit) heeft tot doel om het horizontale verantwoordingsproces rond informatieveiligheid bij gemeenten in te richten op basis van een zelfevaluatie (met als basis de BIG). De betrokken departementen vervolgens krijgen vanuit dit proces de voor hen relevante informatie. De zelfevaluatie leidt tot een gemeentelijke collegeverklaring informatiebeveiliging die door een IT auditor wordt onderzocht. De departementen 'steunen' als het ware op de resultaten van dit verantwoordingsproces.

Kern van het geheel is de eigen verantwoordelijkheid van het gemeentebestuur voor de inrichting van deze informatieveiligheid. Die verantwoordelijkheid is eenduidig zolang de diverse relevante processen zich binnen de gemeentelijke organisatie afspelen. De praktijk is echter dat gemeenten voor een aantal taken de samenwerking opzoekt. En natuurlijk geldt ook in die situatie dat uiteindelijk de gemeentelijk bestuurder verantwoordelijkheid kent voor de processen die in die samenwerking worden afgehandeld. De vraag ligt voor hoe aan die verantwoordelijkheid invulling te geven en hoe dat vervolgens moet landen in de ENSIA verantwoording.

De WGR en informatieveiligheid
(Inter) gemeentelijke samenwerkingen zijn geënt op Wet Gemeenschappelijke regelingen (WGR). De wet beschrijft een aantal mogelijke juridische mogelijkheden om samenwerkingen vorm te geven. En beschrijft daarbij op de hoofdlijn de wijze waarop per construct verantwoording moet/kan worden afgelegd. De wet gaat bij geen enkele beschreven samenwerking in op het thema informatieveiligheid en laat de invulling daarvan over aan de samenwerkende partijen die daarover al dan niet afspraken (wensen te) maken. De wijze waarop die verantwoording vorm krijgt, is ook afhankelijk van de specifieke juridische constructie van het samenwerkingsverband. Een openbaar lichaam (als zelfstandig rechtspersoon) heeft daartoe andere mogelijkheden dan bijvoorbeeld een BV of stichting. Een centrumgemeenteconstructie kent ook weer zijn eigen beperkingen in het afleggen van verantwoording. De wet geeft verder weinig kapstokken om aan die verantwoordelijkheid invulling te geven.

Handreiking Informatieveiligheid en intergemeentelijke samenwerking
In deze handreiking is al het volgende opgenomen:

- *Een portefeuillehouder binnen het college van B en W is verantwoordelijk voor de (prioritering van) beveiliging van informatie binnen de bedrijfs(werk)processen. Deze verantwoordelijkheid wijzigt niet op het moment dat de gemeente besluit om een bepaalde dienst of taak uit te besteden of samen met andere gemeenten (intergemeentelijk) uit te voeren. De gemeente blijft als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van informatie. Het is aan de portefeuillehouder om hierover binnen de grenzen van het samenwerkingsverband afspraken te maken. In de handreiking informatieveiligheid en intergemeentelijke samenwerking worden aanzetten gegeven hoe die verantwoording invulling te geven. https://vng.nl/files/vng/publicaties/2015/20150731_informatieveiligheid-en-intergemeentelijke.pdf. In dit rapport wordt ingegaan op publiekrechtelijke samenwerkingsvormen (openbaar lichaam, centrumgemeente), privaatrechtelijke samenwerkingsvormen en ketens. In het rapport wordt het volgende al behandeld: afspraken over de BIG, aanvullende afspraken tov de BIG, afleggen van verantwoording en audits. Er is dus al het een en ander verwoord als het gaat over de gemeentelijke verantwoordelijkheid bij*

samenwerking.

Om invulling te geven aan de specifieke verantwoordelijkheid rond (intergemeentelijke) informatieveiligheid suggeren de bij ENSIA betrokken auditors de volgende aanvulling op deze handreiking:

- *Bij publiekrechtelijke en privaatrechtelijke samenwerkingsvormen is het uitgangspunt dat de gemeente voor de bij de samenwerkingsvorm ondergebrachte activiteiten verantwoordelijk blijft voor het aantoonbaar voldoen aan de BIG (c.q. de beveiligingsafspraken). De verantwoording van de gemeente over het voldoen aan de BIG omvat derhalve ook de activiteiten van de samenwerkingsvormen voor de gemeente. De gemeente laat zich door de samenwerkingsvorm informeren over het voldoen van de ondergebrachte activiteiten aan de BIG (c.q. beveiligingsafspraken) en de gemeente stelt de juistheid en volledigheid van de ontvangen verantwoording van de samenwerkingsvorm vast. De gemeente kan dit zelf doen of de samenwerkingsvorm vragen hiervoor een auditor in te schakelen.*

Kern van deze aanvulling is dat de gemeenten binnen het samenwerkingsverband afspreken hoe zij zich wil laten informeren over de gerealiseerde informatieveiligheid en op welke wijze deze informatie landt in de zelfevaluatie. De ontwikkelde tool biedt daarvoor beperkte functionaliteit. Als met het samenwerkingsverband een vorm van gebruik van TPM's is ingericht, kunnen gemeenten daar (desgewenst) uiteraard op steunen.

- *Bij ketens heeft iedere deelnemer een zelfstandige verantwoordelijkheid. Iedere deelnemer van de keten legt verantwoording af over het voldoen aan de BIG en laat deze verantwoording **desgewenst** van zekerheid voorzien door een auditor. De ketenpartners/ ketenregisseur stelt vast dat er niets tussen de wal en het schip valt en dat de verantwoordingen de gehele keten afdekken.*

Kern van deze aanvulling is dat aanvullend op de reguliere verantwoording van een ketenpartner wordt bewaakt dat alle in de keten betrokken partijen voldoen aan de gemaakte afspraken. Concreet betekent dit dat binnen de keten in ieder geval de afspraak moet bestaan dat voldaan wordt aan BIG (of vergelijkbare baseline).

Binnen ENSIA is vooralsnog de afspraak dat minimaal BRP, PUN, BAG, BGT SUWI en DigiD in de zelfevaluatie betrokken zijn. De evaluatie betreft het voldoen aan de volle breedte van de BIG op dit vlak. De audit in 2017 spitst zich toe op een beperkt aantal normen.

De verantwoordelijkheid van gemeenten betreft uiteraard alle vormen van samenwerking. Voorstelbaar is dat de focus voor gemeenten allereerst ligt bij die samenwerkingsverbanden die binnen de scope van ENSIA vallen.

Bijlage 5. Handreiking Paragraaf Informatiebeveiliging in het jaarverslag van gemeenten / separate Rapportage Informatiebeveiliging

Met de VNG resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' van november 2013 hebben gemeenten afgesproken om de informatiebeveiliging op orde te krijgen en te houden. In deze resolutie is onder meer afgesproken dat de gemeente in het jaarverslag een aparte paragraaf opneemt over informatiebeveiliging. Met deze paragraaf verantwoordt een college van B en W zich aan de gemeenteraad over informatiebeveiliging in brede zin ('horizontale verantwoording'). Dit betreft onder meer gemeentelijke doelstellingen en afspraken over informatiebeveiliging. Daaronder zijn de afspraken die gemaakt zijn voor de ENSIA verantwoording informatiebeveiliging ('verticale verantwoording'). Over (het nakomen van) de ENSIA afspraken doet de gemeente ook een specifieke uitspraak in de 'Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en SUWInet)'[9]. De IT-auditor doet een uitspraak over de juistheid en volledigheid van de Collegeverklaring ENSIA.

De (sub-)paragraaf Informatiebeveiliging wordt opgenomen in de paragraaf Bedrijfsvoering van het jaarverslag (als onderdeel van de jaarstukken, naast de jaarrekening). Om gemeenten te faciliteren de paragraaf Informatiebeveiliging op eenduidige wijze op te stellen, volgt hierna een format met de ingrediënten daarvan.

Gemeenten kunnen ervoor kiezen om een separate Rapportage Informatiebeveiliging aan de Raad 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. In dat geval kan in het jaarverslag kort verwezen worden naar deze separaat uitgebrachte rapportage. Een separate rapportage waarbij het College van B en W alle informatie over de informatiebeveiliging in samenhang aan de gemeenteraad voorlegt, verdient dan ook de voorkeur.

[9] Over het verantwoordingsjaar 2017 richt de IT-audit zich op de DigiD-normen en een selectie van Suwinet-normen (zie bijlage 1). Hierbij is een groeipad voorzien.

Paragraaf Informatiebeveiliging in het jaarverslag óf separate Rapportage Informatiebeveiliging

IB beleid, doelstellingen en afspraken
Bestuurlijke beschrijving van de belangrijkste gemeentelijke doelstellingen van het informatiebeveiligingsbeleid, waaronder onder meer: "zorgvuldig omgaan met informatie", "betrouwbare en continue dienstverlening", "voldoen aan wet- en regelgeving (privacy)" en "beheersen van risico's" (Governance, Risk en Compliance).
Beschrijf hier ook specifieke doelstellingen zoals:

- de ambities om te voldoen aan de BIG als basisnormenkader voor de IB maatregelen.
- het nakomen van de afspraken over de 'ENSIA verantwoording'.

Algemeen beeld en resultaten afgelopen periode
Beschrijving van de (belangrijkste) activiteiten / resultaten die in het afgelopen jaar hebben bijgedragen aan het behalen van de doelstellingen. "In 2017 heeft de gemeente .."

"Disclaimer"
Wellicht verstandig om iets op te nemen over de illusie van 100% veiligheid.

Beheersmaatregelen IB
Geef een overzicht van de belangrijkste maatregelen die bijdragen aan het realiseren van de IB doelstellingen:

- Organisatie en TBV's, awareness
- Organisatorische en technische maatregelen
- Information Security Management System (ISMS) / PDCA

Realisatie doelstelling IB Beleid (effectiviteit beheersmaatregelen en risico's)
Geef aan in welke mate de afgesproken doelstellingen voor 2017 zijn gerealiseerd (in hoever beheersmaatregelen effectief zijn in relatie tot realiseren van het IB Beleid en welke (*specifieke) doelstellingen en risico's nog aandacht behoeven (en waarvoor nog maatregelen getroffen moeten worden). Let wel, hier wel omzichtig zijn met wat je naar buiten brengt.
Geef aan hoe dit is getoetst. Onder meer met de ('brede') Zelfevaluatie Informatiebeveiliging en eventueel andere instrumenten (ISMS). Geef ook aan wat de reikwijdte is van de Zelfevaluatie Informatiebeveiliging.

Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en SUWInet
Bij een paragraaf Informatiebeveiliging in het Jaarverslag wordt hier een verwijzing naar een separate Collegeverklaring ENSIA opgenomen. Bij een separate Rapportage Informatiebeveiliging wordt hier de Collegeverklaring ENSIA opgenomen.

Incidenten
Rapportage (privacy) incidenten / datalekken en de afhandeling daarvan.

Meerjaren perspectief
Beschrijving van aandachtspunten, doelstellingen en resultaatafspraken (planning) volgende periode.

De stappen en het tijdspad voor het implementeren van de BIG. Beschrijf per stap de reikwijdte (systemen en ICT-beheerprocessen[10]).

[10] Bijvoorbeeld Logische Toegangsbeveiliging (LTB).