VNG Realisatie

Handreiking uitvoering ENSIA verantwoording 2018

Versiebeheer

Versie	Wijzigingen	Datum
1.0	Eerste versie	september 2018
2.0	Kruisjestabel DigiD toegevoegd	oktober 2018
3.0	1. Suwinet normen versus BIG-vragen tabel in samenhang gebracht met SUWI keuzehulp instrument 2. Werkwijze verantwoording voor fuserende gemeenten toegevoegd	december 2018

Inhoudsopgave

Leeswijzer

In dit document wordt ingegaan op de uitvoering en organisatie van de horizontale en verticale verantwoording met ENSIA over het verantwoordingsjaar 2018. Het document geeft inzicht in onderliggende structuur van de tooling (www.ensia.nl), de diverse vragenlijsten en de wijze van verantwoording naar de raad en de verschillende toezichthouders. Ook worden aandachtspunten en tips gegeven hoe de verantwoording in samenhang met de interne en externe gemeentelijk betrokkenen georganiseerd kan worden.

Alle informatie over stelsels, de mijlpalen, uitvoering van de zelfevaluatie en het proces van verantwoorden is in één document opgenomen. U kunt via links in de inhoudsopgave naar het gewenste onderdeel in de handreiking klikken.

Heeft u bij het lezen van dit document vragen? Neem dan contact op via het centrale telefoonnummer 070 250 2400 of een mail sturen aan ensia@vng.nl.

ENSIA verantwoording 2018

ENSIA stelsel

ENSIA staat voor Eenduidig Normatiek Single Information Audit en is een uitvloeisel van de in 2013 door gemeenten omarmde resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente[1]'.

De uitgangspunten als volgt:

- De BIG (Baseline Informatieveiligheid Nederlandse Gemeenten) is het gemeentelijk basisnormenkader voor informatieveiligheid.
- ENSIA heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid.
- Gemeenten informeren hun eigen toezichthouder, de gemeente raad, over informatieveiligheid
- Gemeenten hebben in de resolutie opgeroepen om de verantwoordingslasten over informatieveiligheid te verminderen.
- Bij het afleggen van verantwoording wordt het principe van single information single audit toegepast.

De resolutie vormde de aanleiding voor de start van het project ENSIA. In 2018 hebben gemeenten zich voor het eerst verantwoord via de ENSIA systematiek over het verantwoordingsjaar 2017.

ENSIA zelfevaluatie en de BIG

De verantwoording over informatieveiligheid met ENSIA wordt gedaan door middel van een zelfevaluatie. Op www.ensia.nl is deze zelfevaluatie informatieveiligheid 2018 beschikbaar. Dit is een vragenlijst gebaseerd op de uitgangspunten van de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten). De vragen kunnen worden beantwoord met 'ja' of 'nee' door middel van bullets of ticketboxen (aan en/of uit vinken). In ENSIA

[1] https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid/brieven/resolutie-informatieveiligheid-randvoorwaarde-voor-de-professionele-gemeente

wordt uitgegaan vanuit het principe ‘comply or explain’ bij de onderbouwing van de antwoorden. Dit wil zeggen dat in principe aan het uitgangspunt wordt voldaan. Indien de gemeente niet aan het uitgangspunt voldoet, dan geeft de gemeente toelichting waarom een procedure of maatregel niet wordt gevolgd en op welke wijze de gemeente wel invulling geeft aan de betreffende norm of vereiste. De onderbouwing wordt ondersteund met benodigde documentatie. Bij elke vraag is een toelichting opgenomen met verwijzing naar wetsartikelen en/of een link naar een guidance en een suggestie voor documenten waarin de gevraagde eis aangetroffen kan worden. Het verdient aanbeveling om binnen het implementatieproject een heldere structuur voor documentatie op te zetten die voor betrokkenen transparant en toegankelijk is. Het op een gestructureerde wijze van verzamelen, ordenen en archiveren van documenten is relevant voor:
1. De beschikbaarheid van documentatie voor eigen oordeelsvorming.
2. Het (efficiënt) kunnen beantwoorden van aanvullende vragen vanuit eigen organisatie.
3. De ondersteuning van het auditproces voor verkrijgen van assurance op de collegeverklaring.

Het is mogelijk om in de ENSIA-tool verwijzingen (met links) op te nemen in het opmerkingenveld. Dit is geen verplichting.

Scoren en punten tellen met ENSIA

De BIG heeft betrekking op informatiebeveiliging in brede zin: op zowel fysieke (o.a. gebouwen, apparatuur en toegangscontrole) als logische beveiliging (processen en informatiesystemen). Het beantwoorden van de ENSIA zelfevaluatie leidt niet tot een score. Er wordt hoogstens wel of niet voldaan aan de BIG normen. De horizontale (gemeente brede) uitkomsten zijn een indicatie voor het voldoen aan de normen. De uitkomsten zijn een resultante van betrouwbaarheidseisen en – maatregelen die passen bij de eigen risicoanalyse en het risicodenken. Het verschilt dan ook per gemeente waar de accenten voor (door)ontwikkeling gelegd worden. Vanuit dit gezichtspunt een algehele score niet wenselijk.

Voor de verticale verantwoording ligt dit anders. Het ministerie van BZK (DGBRW) hanteert een telling in de formats voor de verantwoordingsdocumentatie:

- BAG, BGT en BRO rapportages kennen een maximale score van 200 punten
- Bij de BRP en PUN verantwoording wordt vanuit de kwaliteitsmonitor een score toegekend.

Horizontale en verticale verantwoording

Binnen het ENSIA stelsel wordt gesproken over horizontale en verticale verantwoording over informatieveiligheid. Horizontale verantwoording staat voor de interne verantwoording aan de eigen toezichthouder, de raad. Het gaat hierbij om een gemeentebreed beeld over de status van informatieveiligheid van een gemeente. Bij verticale verantwoording is sprake van de verantwoording over één stelsel (veelal basisregistraties) voor het verantwoordelijk ministerie.

In 2018 zijn de volgende stelsels opgenomen in de ENSIA systematiek:

Afkorting	Stelsel	Verantwoordelijk Ministerie
BRP	Basisregistratie Personen	BZK (RvIG)
PUN	Paspoortuitvoeringsregeling Nederland	BZK (RvIG)
BAG	Basisregistratie Adressen en Gebouwen	BZK (DGBRW)
BGT	Basisregistratie Grootschalige Topografie	BZK (DGBRW)
BRO	Basisregistratie Ondergrond	BZK (DGBRW)
DigiD	Digitale Identiteit	BZK (Logius)

GeVS Suwinet	Gezamenlijke elektronische Voorzieningen (GeVS) SUWI (Structuur Uitvoering Werk en Inkomen)	SZW

BIG over informatieveiligheid als basis

De zelfevaluatie ENSIA 2018/BIG is de hoofdvragenlijst voor uitvoering van de zelfevaluatie. Alle vragen over informatieveiligheid zijn opgenomen in deze vragenlijst. In 2017 hebben de gemeenten voor het eerst gebruik gemaakt van ENSIA als verantwoordingsinstrument. De veranderingen in de vragenlijst ten opzichte van 2017 zijn als volgt:

- De antwoorden op de vragen die u in 2017 hebt gegeven zijn beschikbaar gebleven. Deze worden getoond in een extra kolom bij de vragenlijst 2018.
- Er zijn nieuwe vragen geformuleerd (hier ziet u het ingediende antwoord van 2017 ook niet terug). De vervallen vragen (en antwoorden 2017) worden onderaan de hoofdstukken getoond.
- Uitbreiding loghistorie met:
    - Aanpassingen in gegeven antwoorden
    - Aanpassingen in het opmerkingenveld
    - Het inleveren van de vragenlijst
- Er is een geautomatiseerde Excel beschikbaar (onder het tabblad ‘invoeren’) waarmee makkelijk vragen op domeinen (via tags) zijn te selecteren.

Voor de stelsels[2] uit het overzicht hierboven zijn de informatiebeveiligingsvragen opgenomen in deze vragenlijst. Hoe verhoudt zich de BIG vragenlijst tot de separatie vragenlijsten?

- Voor Suwinet is het gehele normenkader opgenomen in de BIG vragenlijst. Er bestaat geen domeinspecifieke vragenlijst.
- Voor de BAG en BGT zijn de informatieveiligheidsvragen opgenomen in ENSIA. De overige vragen vanuit de stelselhouders over het gebruik zijn opgenomen in domeinspecifieke vragenlijsten.
- Voor de BRP en de PUN zijn de informatieveiligheidsvragen in ENSIA opgenomen. De overige vragen vanuit de stelselhouder worden via de Kwaliteitsmonitor (buiten ENSIA om) uitgevraagd. De uitkomsten vanuit ENSIA worden automatisch samengevoegd met de antwoorden uit de Kwaliteitsmonitor.
- Voor het DigiD normenkader zijn alle vragen in de separate vragenlijst opgenomen.

Onderstaand is een toelichting op deze stelsels opgenomen.

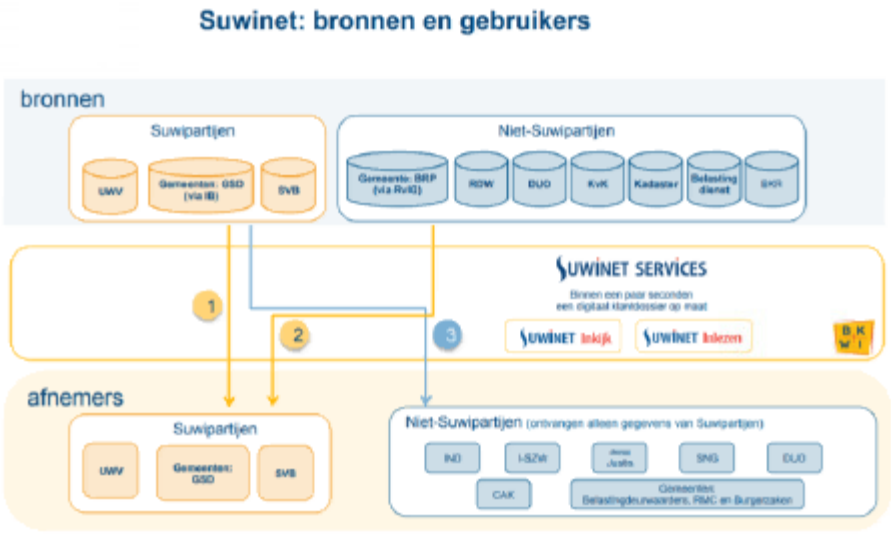
Suwinet

Suwinet is het systeem van informatie-uitwisseling in de keten van werk en inkomen. SUWI staat voor Structuur Uitvoeringsorganisatie Werk en Inkomen. Overheidsorganisaties kunnen gegevens van burgers en bedrijven digitaal bij elkaar opvragen en naar elkaar sturen. SUWI partijen zijn SVB, UWV en alle gemeenten. Het BKWI (als onderdeel van het UWV) beheert de web-toepassing. Voor een totaal overzicht van alle toepassingen en producten is de site van het BKWI een goede bron van informatie via www.bkwi.nl. De informatie/gegevens die in Suwinet vermeld staan komt van de **leveranciers (of bronnen)**. Leveranciers van de data in Suwinet zijn onder andere de Belastingdienst, BKR, DUO, GSD’s, Kadaster, KvK, RDW, SVB

[2] Met uitzondering van de BRO en DigiD. Voor de BRO is in 2018 met een domeinspecifieke (separate) vragenlijst opgenomen. Voor DigiD geldt dat de verantwoording op aansluitniveau is. Alle verantwoordingsvragen over DigiD zijn opgenomen in een separate vragenlijst.

en UWV.

De gegevens worden geraadpleegd door overheidsorganisaties. Waarbij de ‘grootverbruikers’ gemeentelijk sociale diensten, UWV en de Sociale Verzekeringsbank (SVB) zijn, maar ook IND, Bibob, deurwaarders, Zorginstituut NL, Inspectie SZW, RMC en Interventieteams zijn zogenaamde **afnemers (of gebruikers)** van Suwinet. Het inzien van de gegevens kan door de gegevens te raadplegen via een beveiligde webtoepassing (Suwinet Inkijk) of deze te gebruiken in een eigen bedrijfsapplicatie (Suwinet Inlezen (alle afnemers) of DKD-Inlezen (alleen voor UWV, SVB en gemeenten).



Overzicht Bronnen en gebruikers Suwinet (bron BKWI)

Het Suwinet wordt beschikbaar gesteld onder bepaalde condities, de SUWI verantwoordingsrichtlijn. Dit is de standaard voor het afleggen van de verantwoording over de beveiliging van Suwinet. De SUWI Verantwoordingsrichtlijn bevat het normenkader met de normen waaraan de beveiliging van de Gegevensuitwisseling elektronische Voorziening Suwinet (GeVS) aan moet voldoen. Er is een normenkader voor de beheerder, de leveranciers en een normenkader voor de afnemers. Voor gemeenten die niet voldoen aan het normenkader is een interventieprotocol door het ministerie van SZW opgesteld.

Wie welke gegevens mag inzien/gebruiken is geregeld in onderliggende wet- en regelgeving. De factsheet van de VNG[3] geeft een goede beschrijving wat wel en niet mag.

Suwinet voor uitvoering participatiewet

Geautoriseerde medewerkers bij de (I)GSD van gemeenten die belast zijn met de uitvoering van de wettelijke taken die vallen onder de P-wet, IOAW (Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers) en IOAZ (Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen) mogen gebruik maken van Suwinet. Suwinet wordt onder andere gebruikt in processen om de grondslag voor het toekennen of afwijzen van een uitkering te bepalen of voor re-integratie. In de onderlinge wet- en regelgeving wordt ook nadrukkelijk uitgesloten waar Suwinet niet voor mag worden gebruikt. Dit betreft raadpleging voor uitvoering van wetten anders dan de drie voornoemde wetten. Zo is het niet toegestaan Suwinet te gebruiken voor taken rondom schuldhulpverlening en de uitvoering van de WMO.

3 https://vng.nl/files/vng/2017-08_vng_factsheet_Suwinet_voor_gemeenten_v1.pdf

Suwinet voor burgerzaken

De gegevens die voor Burgerzaken beschikbaar zijn, betreffen de adresgegevens van iedereen die werkt of een uitkering ontvangt. Deze komen uit de loonaangifte die werkgevers en uitkeringsinstanties periodiek doen naar de Belastingdienst. De adresgegevens vanuit UWV mogen alleen gebruikt worden voor het bijhouden van adresgegevens in de Basisregistratie Personen BRP (de voormalige gemeentelijke basisadministratie (GBA)). Burgerzaken raadpleegt Suwinet bijvoorbeeld wanneer een natuurlijk persoon niet bekend is (of geen actuele registratie heeft) binnen de BRP. Een werkgever beschikt hier doorgaans wel over. Door de SUWI gegevens te raadplegen kan op deze wijze een actueel adres achterhaald worden (indien deze persoon een werkgever heeft gehad in de laatste 6 maanden).

Suwinet voor gemeentelijk gerechtsdeurwaarders

De gemeentelijk belastingdeurwaarder voert de heffing en de invordering van gemeentelijke belastingen met toepassing van de Algemene wet, de Invorderingswet 1990 en de Kostenwet invordering rijksbelastingen als waren die belastingen rijksbelastingen uit. Gemeentelijke belastingdeurwaarders mogen gebruik maken van Suwinet-Inkijk voor het leggen van loonbeslag. Het BKWI geeft hier het volgende criterium voor, namelijk 'waarvoor een getekend dwangbevel' aanwezig is. Gemeentelijk gerechtsdeurwaarders kunnen een beperkte set actuele UWV-gegevens raadplegen van BSN's waarvoor een getekend dwangbevel aanwezig is. Dit doen zij op basis van een zogenaamde whitelist. Wanneer iemand 'klant' is, wordt dit BSN doorgegeven worden aan BKWI en een paar minuten later kan de bevraging gedaan worden.

Een gemeentelijk gerechtsdeurwaarder kan voor meerdere gemeenten werkzaam zijn. De heffing, vordering en inning kan ook door een samenwerkingsverband worden uitgevoerd (met als onderlegger de Wgr).

Suwinet voor RMC contactgemeenten

De Regionale Meld- en Coördinatiepunt (RMC) contactgemeenten krijgen vanuit Ministerie van OCW geld om de RMC regelingen uit te voeren (waaronder het opsporen en weer naar onderwijs verleiden van vroegtijdig schoolverlaters (VSV). Medewerkers van RMC’s mogen Suwinet gebruiken voor hulp aan voortijdig schoolverlaters. In Nederland zijn 39 gemeenten die de RMC functie vervullen in de 39 regio's. Zij fungeren als contactgemeente. Deze regio’s zijn vastgesteld in de Uitvoeringsregeling Regionale Meld- en Coördinatiefunctie Voortijdig Schoolverlaten. De financiering vanuit OCW wordt gedaan op basis van aantal jongeren tussen 5 en 17 jaar woonachtig in de RMC regio. De autorisatie voor SUWI/RMC verloopt op het niveau van de RMC gemeente/uitvoerder.

Anders dan bij de SUWI levering voor Werk en Inkomen (participatiewet e.a.) hebben de gemeenten voor wat betreft de RMC uitvoering geen keuze om deze dienstverlening uit te besteden; het is immers een wettelijke regeling c.q. indeling vanuit het Rijk. De financiering voor uitvoering van de wettelijke taak verloopt centraal vanuit het Ministerie van OCW.

Daarmee kan een gemeente deel uitmakend van de RMC regeling, maar die zelf geen RMC contact gemeente is niet verantwoordelijk zijn, noch gehouden worden voor de uitvoering van deze regeling. Dit betekent dat voor wat betreft de SUWI RMC regeling alleen de contact gemeenten zich verantwoorden voor gebruik SUWI/RMC.

DigiD

DigiD staat voor digitale identiteit en is het standaardidentificatie- en authenticatiemechanisme bij

gegevensuitwisseling met de overheid via internet. Burgers kunnen met deze digitale identiteit inloggen op websites van de overheid en zorg. DigiD is in beheer bij de gemeenschappelijke beheerorganisatie van de overheid: Logius. Logius is een uitvoeringsorganisatie van het ministerie van BZK.

BRP en PUN

De Basisregistratie Personen (BRP) is onderdeel van het stelsel van basisregistraties van de Nederlandse overheid. Er zijn bijvoorbeeld basisregistraties voor gebouwen, rechtspersonen, ondernemingen en voertuigen. De Nederlandse overheid registreert persoonsgegevens in de BRP.

Alle overheidsinstellingen en bestuursorganen (zoals de Belastingdienst) zijn verplicht voor hun taken gebruik te maken van die gegevens. Het gaat daarbij onder andere om naam, geboortedatum, geboorteplaats, verblijfplaats en familierelaties. Met deze gegevens wordt bijvoorbeeld een paspoort en identiteitskaart verstrekt of wordt de hoogte van een studietoelage berekend. Voor het uitgeven van paspoorten hebben gemeenten m.b.t. wetgeving te maken met de Paspoortuitvoeringsregeling Nederland 2001 (PUN).

De Rijksdienst voor Identiteitsgegevens (RvIG) is de uitvoeringsorganisatie van het Ministerie van BZK op het gebied van persoonsgegevens en reisdocumenten voor het Koninkrijk der Nederlanden en beheert de BRP.

Meer informatie over BRP en PUN is te vinden op de website van RvIG[4].

AVG

De Algemene verordening gegevensbescherming (AVG) is een privacywet die van toepassing is sinds 25 mei 2018 en geldt in de hele Europese Unie (EU). De wet bescherming persoonsgegevens (Wbp) geldt niet meer. De AVG is ook wel bekend onder de Engelse naam General Data Protection Regulation (GDPR).

In de AVG staat dat degene die persoonsgegevens verwerkt er voor moet zorgdragen dat dit veilig genoeg gebeurt. De data moeten volgens de wetgever beschermd zijn tegen verlies, enige vorm van onrechtmatige verwerking en onnodige verzameling.

Meer informatie over de AVG is te vinden op de website van de Autoriteit Persoonsgegevens (AP)[5].

BAG, BGT en BRO

De overheid kent een Stelsel van Basisregistraties waarin veel gebruikte overheidsgegevens worden vastgelegd. Er zijn 11 basisregistraties waarvan de volgende drie gericht zijn op het geo-informatiedomein. De rol van opdrachtgever en toezichthouder van deze drie basisregistraties is belegd bij het Directoraat Generaal Bestuur, Ruimte en Wonen (DGBRW) van het ministerie van BZK.

BAG

De Basisregistraties Adressen en Gebouwen (BAG) is een registratie waarin gemeentelijke basisgegevens over alle gebouwen en adressen in Nederland zijn verzameld. De BAG biedt een overzicht van vrijwel alle gebouwen in Nederland en een adressenbestand van hoge kwaliteit van heel Nederland. Gemeenten zijn bronhouder van de BAG.

---

[4] https://www.rvig.nl/
[5] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving

BGT

De Basisregistratie Grootschalig Topografie (BGT) is de uniforme, gedetailleerde digitale basiskaart van heel Nederland die alle overheidsinstanties vanaf 1 juli 2017 verplicht moeten gebruiken. Alle fysieke objecten zoals gebouwen, wegen, water en groen zijn in de BGT eenduidig vastgelegd. De BGT wordt gemaakt en beheerd door de zogenaamde bronhouders in medebewind. Dit zijn gemeenten, provincies, waterschappen, het Ministerie van Economische Zaken (Landbouw), het Ministerie van Defensie, Rijkswaterstaat en ProRail.

BRO

De Basisregistratie Ondergrond (BRO) bevat gegevens over de geologische en bodemkundige opbouw, de ondergrondse infrastructuur en gebruiksrechten.

Inrichting vragenlijsten

In de ENSIA tool zijn verschillende vragenlijsten beschikbaar. In onderstaand schema geeft aan op welke wijze de vragenlijsten zijn opgenomen in ENSIA.

De ENSIA zelfevaluatie informatiebeveiliging BIG 2018

De vragen in de BIG vragenlijst hebben allen betrekking op informatieveiligheid. De reikwijdte van de jaarlijkse verantwoording beslaat tenminste de objecten BRP, PUN, DigiD, Suwinet, BAG en BGT. Bij de beantwoording van de vragen wordt uitgegaan van het lokaal vastgestelde beveiligingsbeleid en de individuele risico-afwegingen die zijn opgesteld door de gemeenten. Op basis hiervan wordt de reikwijdte bepaald. Dit kan per gemeente verschillend zijn. De vragen zijn ingedeeld in hoofdstukken en sluiten aan bij de indeling van de tactische BIG[6]. De formulering van een control in de BIG is soms breed en omvat meerdere vragen. Voor ENSIA zijn vragen enkelvoudig geformuleerd en wordt een hoofdvraag waar nodig aangevuld met subvragen. In de toelichting wordt de vraag toegelicht, een verwijzing naar wetgeving gegeven (BRP, PUN, SUWI, BAG, BGT en AVG), een link naar de guidance van Suwinet en is een suggestie voor evidence/documentatie opgenomen. De verantwoording over de BRO is 2018 een proefjaar: er zijn geen informatieveiligheidsvragen over dit stelsel opgenomen in de ENSIA zelfevaluatie (BIG vragenlijst). Voor de beantwoording dient u een afweging te maken, waarbij u de situatie voor de stelsels die relevant bij enige vraag, laat meewegen bij de beantwoording. Het Suwinet stelsel neemt een bijzondere plaats in binnen de zelfevaluatie. Het normenkader afnemers Suwinet is in zijn geheel gemapt op en verwerkt in de BIG vragenlijst.

[6] Hoofdstuk 4 van de BIG is een beschrijvend hoofdstuk over risicobeoordeling en – afweging. Dit hoofdstuk is in ENSIA gebruikt voor de vragen over informatieveiligheid in relatie tot samenwerkingsverbanden.

De vragenlijst(en) voor de bestaande DigiD aansluiting(en)

Er is een scheiding aangebracht in de verantwoording op basis van de BIG en de DigiD-verantwoording. DigiD richt zich op de webpagina waarop zich een DigiD-snelkoppeling bevindt met een geheel eigen set van normen. De DigiD normen zijn uitgebreider zijn dan de BIG-normen. Daarnaast vindt de verantwoording over DigiD per DigiD aansluiting plaats. Dit maakt dat deze verantwoording niet te integreren is in de BIG vragenlijst en gekozen is om een separate vragenlijst voor DigiD in ENSIA op te nemen. Een van de eerste vragen in de vragenlijst DigiD is over hoeveel aansluitingen een gemeente zich gaat verantwoorden. Op basis hiervan maakt de ENSIA tool het juiste aantal vragenlijsten aan om hierna per aansluiting aan te geven of aan de normen worden voldaan.

Specifieke vragenlijsten

Bij het opstellen van de zelfevaluatievragenlijst is vastgesteld waar de normen van BRP, PUN, Suwinet, BAG en BGT aansluiten op de BIG-normen en daarmee 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. Voor de BAG, BGT en BRO zijn deze aanvullende vragen in ENSIA opgenomen. Voor de BRP en PUN wordt gebruik gemaakt van de kwaliteitsmonitor van RvIG. Deze zijn opgenomen in de specifieke vragenlijsten voor de voornoemde stelsels.

De domein specifieke vragenlijsten voor BAG, BGT en BRO

Naast de vragen over informatiebeveiliging in de ENSIA BIG vragenlijst zijn drie vragenlijsten opgenomen voor de geo-basisregistraties BAG, BGT en BRO. Het betreffen vragen over het gebruik van de BAG, BGT en BRO die verder gaan dan alleen informatieveiligheid. Deze zelfcontroles maken onderdeel uit van wetgeving BAG en BGT welke per 1 juli 2018 in werking treden. Voor de BRO geldt een proefjaar. In de nieuwe wetgeving is opgenomen dat voor de zelfcontroles wordt aangesloten bij de systematiek en het verantwoordingsproces van ENSIA.

Waar Staat Je Gemeente (WSJG)

Vanuit de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente[7]' is aangegeven dat gemeenten de lokale invulling rondom het thema van informatieveiligheid transparant maken voor burgers, bedrijven en (keten)partners. Deze transparantie wordt onder meer behaald door gebruik te maken van waarstaatjegemeente.nl. Deze openbare informatie vormt de basis voor jaarlijkse collegiale beoordeling (peer reviews). In 2018 zijn de vragen voor Waar Staat Je Gemeente (zie website www.waarstaatjegemeente.nl) voor de eerste maal in ENSIA opgenomen. Het betreft negen vragen, waarvan vier vragen ook in de BIG vragenlijst zijn opgenomen (en al beantwoord zijn). De vragen zijn beschikbaar via een separate vragenlijst.

Beheer, techniek en governance

Vanaf 1 juli 2018 is ENSIA in beheer genomen door VNG Realisatie. VNG Realisatie ondersteunt gemeenten bij het ENSIA verantwoordingsproces.

In deze nieuwe fase kent ENSIA een Regiegroep ENSIA onder leiding van een wethouder, waarvan het voorzitterschap bij de VNG ligt. De Regiegroep komt één keer per zes weken bij elkaar. De Stelselverantwoordelijkheid ligt bij het Ministerie van Binnenlandse Zaken (BZK). VNG is in de lead voor het beheer en coördinatie van de uitvoering. Ontwikkeling en implementatie liggen daarmee dicht bij elkaar in de nieuwe situatie. Naast de Regiegroep is tevens een partneroverleg, gebruikersoverleg en auditcommittee

[7] https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid/brieven/resolutie-informatieveiligheid-randvoorwaarde-voor-de-professionele-gemeente

ingericht. Deze overleggen vinden maandelijks plaats.

De ENSIA-tool (op www.ensia.nl) is in beheer bij ICTU, een onafhankelijke advies- en projectenorganisatie binnen de overheid. Een handleiding voor het gebruik van de tool is te downloaden vanuit de tool. De tool is ISO 27001 gecertificeerd en voldoet aan de laatste beveiligingsstandaarden. Momenteel wordt de ENSIA tool geaudit.

Planning en mijlpalen

Op 1 juli 2018 start het tweede jaar van verantwoording met ENSIA. Tot die tijd kan de gemeente zich voorbereiden. De zelfevaluatie moet vóór 31 december zijn ingeleverd. In het voorjaar van 2019 vindt verantwoording aan de gemeenteraad en de verticale toezichthouders plaats.

In onderstaande tabel is een fasering voor het tweede verantwoordingsjaar weergegeven:

Fase	Start	Eind
Voorbereiding	1 juni 2018	1 juli 2018
Uitvoering zelfevaluatie	1 juli 2018	31 december 2018
Verantwoorden (verticaal en horizontaal)	1 januari 2019	15 juli 2019
Evaluatie	1 mei 2019	1 juni 2019

Planning

De planning voor de horizontale verantwoording ziet er als volgt uit:

De planning voor de verticale verantwoording ziet er als volgt uit:

Op bovenstaande platen is de planning voor de horizontale en verticale verantwoording uit elkaar getrokken. Omdat in de verantwoordingsfase verschillende documenten langs het college moeten gaan en de raad over alle uitkomsten geïnformeerd moet worden, zijn de mijlpalen in de planning van het Plan van Aanpak voor beide verantwoordingen nagenoeg gelijk. De verticale verantwoording kent echter een extra mijlpaal, zie hieronder:

Mijlpalen

- 1 juli 2018: Opening vragenlijst verantwoordingsjaar 2018
- 31 december 2018: Sluiting vragenlijst verantwoordingsjaar 2018
- 1 mei 2019: Uiterste aanleverdatum **verticale** verantwoordingsdocumentatie
- 15 juli 2019: Horizontale verantwoording via financieel jaarverslag gemeente aan BZK

Plan van aanpak

Ter ondersteuning en planning van de activiteiten is een format Plan van Aanpak opgesteld. U vindt dit format op de ENSIA site van VNG Realisatie[8] Het plan heeft tot doel om uitvoering van ENSIA in goede banen te leiden en de rollen en taken te organiseren. In dit plan komen de volgende voor de uitvoering relevante onderwerpen aan bod: beschrijving ENSIA 2018 en resultaten, activiteiten, planning, communicatie, organisatiestructuur en begroting. In het format zijn basisteksten, suggesties en vragen opgenomen die helpen om de aanpak te formuleren die het beste past bij uw gemeente. Per fase zijn de activiteiten uitgewerkt. Deze sluiten aan op de mijlpalen binnen het proces. Het Plan van Aanpak is opgesteld in een Word format. U kunt dit plan omzetten naar een schematische planning (bijvoorbeeld GANTT) om de voortgang van de verschillende activiteiten binnen het proces te bewaken.

Een belangrijk onderdeel voor een geslaagde uitvoering is om met betrokkenen (werk)afspraken te maken op welke wijze de aanlevering vanuit de verschillende domeinen, afdelingen, de FG, samenwerkingsverbanden en leveranciers tot stand komt.

[8] http://www.vngrealisatie.nl/sites/default/files/2018-07/180711%20Plan%20van%20aanpak%

Een paar tips:

1. Het verdient aanbeveling om interpretatie van de BIG vragen met elkaar (domeinen) te bespreken en waar nodig afstemming met de auditor te zoeken. Dit kost tijd, maar levert draagvlak op voor het ENSIA proces en versterkt kennisdeling over informatieveiligheid (over domeinen heen).
2. Zoek aanspreekpunten binnen de samenwerkingsverbanden waar diensten zijn uitbesteed. Het is efficiënt om hierbij afstemming te zoeken met andere gemeenten die bestuurlijk ook deel uitmaken van het samenwerkingsverband. Op deze wijze kan de verantwoording vanuit het samenwerkingsverband gecoördineerd plaatsvinden naar alle aangesloten gemeenten.
3. Bespreek het BIG principe ‘comply or explain’. Dit wil zeggen dat in principe aan het uitgangspunt wordt voldaan. Indien de gemeente niet aan het uitgangspunt voldoet, dan wordt een toelichting gegeven waarom een procedure of maatregel niet wordt gevolgd en op welke wijze de gemeente wel invulling geeft aan de betreffende norm of vereiste.
4. Spreek met elkaar af hoe de bewijslast (documenten, print screens, etc.) wordt georganiseerd zodat deze toegankelijk en raadpleegbaar is.
5. Communiceer regelmatig naar de betrokken stakeholders. Neem hen mee in het proces.

Uitvoeren zelfevaluatie

In dit hoofdstuk is de uitvoering van de zelfevaluatie uitgewerkt. Hoe gaat u te werk voor de algemene BIG vragen? Wat is een handige aanvliegroute voor de beantwoording van Suwinet vragen binnen de BIG vragenlijst? Waar moet u rekening mee houden bij de beantwoording van de DigiD vragenlijst(en)? Hoe werkt dat nu met de BRP en de PUN vragen en antwoorden in relatie tot de kwaliteitsmonitor, etc.

BIG principes

De beantwoording van de BIG vragenlijst is ééndimensionaal. Het antwoord is een Ja of een Nee en in een aantal gevallen is de mogelijkheid opgenomen om met een checkbox een verdieping op een bepaald domein aan te geven. Dit betekent dat een Ja of een Nee een afgewogen antwoord dient te zijn; één uitspraak over verschillende domeinen en afdelingen heen. Wanneer de conclusie is dat niet (of niet in zijn geheel) aan het BIG uitgangspunt wordt voldaan, dan dient te worden toegelicht waarom dit zo is. Wellicht wordt op alternatieve wijze invulling aan de norm te gegeven? Hierbij blijft het van belang om elke vraag met de juiste scope (voor de verschillende domeinen en afdelingen) te beantwoorden. De guidance in de toelichting en de verwijzing naar wetsartikelen helpen daarbij.

In het afgelopen jaar is ervaring opgedaan om tot één finaal antwoord in ENSIA te komen. Er zijn verschillende varianten de revue gepasseerd. De volgende werkwijzen zijn de meest voorkomende:

1. Vragenlijsten uitzetten bij verantwoordelijken. Individueel antwoorden en bewijsdocumentatie aanleveren en/of verwijzen. Antwoorden samenbrengen. Gezamenlijk bespreken met toelichting en het finale antwoord bepalen.
2. Vragenlijst gezamenlijk bespreken op onderwerp/domein. Antwoord bepalen met de werkgroep. Bewijsdocumentatie organiseren.
3. Niet voor alle vragen is het mogelijk tijdens een bijeenkomst tot één antwoord te komen. Veel ENSIA coördinatoren hebben die laatste slag voor 31 december gemaakt door de vragenlijst (en de verzamelde antwoorden) door te nemen met een collega (bijvoorbeeld de controller) om de antwoorden te controleren, een afweging te maken en definitief te maken. Met deze werkwijze wordt in elk geval aan het 4-ogen principe voldaan.

TIP: het is handig om bij een antwoord aan te geven wat de afwegingen zijn geweest tot het beantwoorden van een vraag met Ja of een Nee.

Zelfevaluatie ENSIA vanuit samenwerkingsverbanden

Bij samenwerkingsverbanden blijft het college van B en W als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van informatie (ongeacht de vorm van samenwerking). Vanuit gemeentelijk perspectief zijn er vele vormen van samenwerking. In relatie tot de scope voor ENSIA 2018 wordt in veel gemeenten samengewerkt op gebied van het domein Werk en Inkomen (ISD's) en op gebied van het opleggen en vorderen van gemeentelijke belastingen (belastingsamenwerkingen) en wordt veel ICT ondersteuning uitbesteed (Share Service Centra). De verantwoording vergt inzet en afstemming. In deze paragraaf wordt stapsgewijs de aandachtspunten weergegeven voor het verantwoordingsproces. Deze stappen zijn overigens ook geïntegreerd opgenomen in het Plan van Aanpak.

1. Voorbereidende werkzaamheden
   - Organiseer een aanspreekpunt bij het samenwerkingsverband (TBV)
   - Afstemming overleg structuur (met andere aangesloten gemeenten)
   - Update voortgang door te voeren verbeteringen 2017 (indien van toepassing)
2. Vragenlijsten uitzetten (zie ook het document 'Keuzehulp Suwinet verantwoording via www.vngrealisatie.nl/ensia) en afspraken maken over aanlevering van de antwoorden:
   - Tijdpad
   - Vorm (login ENSIA of andere wijze)
   - Organiseren van evidence en brondocumenten
   - TPM ja/nee
3. Antwoorden ontvangen en verwerken
   - Opnemen in ENSIA voor horizontale verantwoording
   - Opnemen voor IT audit. U kunt hierbij gebruik maken van het document 'Keuzehulp Suwinet verantwoording' via www.vngrealisatie.nl/ensia)
4. Voorbereiden audit
   Indien gebruik gemaakt wordt van een TPM steunt de auditor op de TPM die wordt afgegeven vanuit het samenwerkingsverband.
5. De eigen auditor zal contact opnemen met de auditor van het samenwerkingsverband voor verificatie. Indien geen gebruik gemaakt wordt van een TPM zal de auditor afspraken maken bij het samenwerkingsverband voor toetsing van de uitspraken in de opgestelde concept collegeverklaring. De documenten die dienen als bewijslast dienen gereed te staan voorafgaand aan de audit.
6. Verwerken van bevindingen met mogelijke uitkomst:
   - Aanpassen concept Collegeverklaring
   - Afstemmen en opstellen verbeterplan
7. Evaluatie ENSIA verantwoording 2018

Zelfevaluatie Suwinet met ENSIA

Verdeling van de vragen in BIG vragenlijst

Alle vragen die betrekking hebben op Suwinet zijn volledig gemapt op de BIG vragenlijst in ENSIA. Dit betekent dat het gehele normenkader Afnemers is verspreid over de verschillende vragen in de BIG vragenlijst 2018. Er is geen separate vragenlijst voor Suwinet. In het navolgende schema is de verdeling van het normenkader over de vragen in ENSIA zichtbaar gemaakt.

Scope voor beantwoording vragen Suwinet in ENSIA

IN ENSIA/BIG VRAAG	Norm	IT AUDIT	SUWI
BIG 5.1.1.a	B.01	x	x
BIG 5.1.1.b	B.01	x	x
BIG 5.1.2.a	C.01	x	x
BIG 6.1.1.a	B.01	x	x
	C.01	x	x
BIG 6.1.2.a	B.01	x	x
	B.04	x	x
BIG 6.1.3.a	B.05	x	x
BIG 6.1.7.a	B.04		x
BIG 6.1.8.a	C.01		x
	C.08		x
BIG 6.2.1.h	B.03		x
BIG 6.2.3.a	U.01		x
BIG 7.1.1.a	B.06		x
BIG 7.2.1.a	U.06		x
BIG 7.2.1.b	U.06		x
BIG 7.2.2.a	U.06		x
BIG 8.2.2.a	Notitie Verantw	x	x
BIG 8.3.1.b	U.02		x
BIG 10.1.1.b	U.10		x
BIG 10.1.2.a	C.03		x
BIG 10.1.3.a	B.05		x
BIG 10.1.3.b	B.05	x	x
BIG 10.1.3.c	B.05	x	x
BIG 10.1.4.a	U.09		x
BIG 10.8.1.a	U.07 en U.08		x
BIG 10.8.1.b + c	U.07 en U.08		x
BIG 10.8.4.a	U.08		x
BIG 10.8.5.a	U.05		x
BIG 10.10.1.a	C.05	x alleen Inlezen	x
BIG 10.10.1b	C.05	x alleen Inlezen	x
BIG 10.10.2.a	C.06	x	x
BIG 11.2.1.a	U.02	x	x
	U.03	x	x
BIG 11.2.1.b	U.02	x	x
	U.03	x	x
BIG 11.2.3.a	U.03		x
BIG 11.2.4.a	C.04	x alleen Inkijk	x
BIG 11.4.2.c*	C.07		x
BIG 11.4.6.a	U.11		x
BIG 11.5.2.a	U.03	x alleen Inlezen	x
BIG 11.5.2.b	U.03	x alleen Inlezen	x
BIG 11.6.1.a	U.04		x
BIG 11.7.2.a	U.12		x
BIG 11.7.2.b	U.12		x
BIG 12.3.1.a	U.11	x	x
BIG 15.2.1.a	B.02		x

De BIG vragenlijst gebruikt andere bewoordingen dan in het SUWI normenkader worden gebruikt. Hier zijn door gemeenten veel vragen aan VNG Realisatie over gesteld. Met name over de diepgang van de beantwoording van de vragen in ENSIA (‘als gemeente zijn wij toch niet verantwoordelijk voor wat het BKWI doet?) en met welke scope de vragen uit ENSIA dienen te worden beantwoord. De evaluatie over 2017 is aanleiding geweest om voor de verticale verantwoording 2018 (IT audit vragen) aan de tweedelijns toezichthouder (ministerie SZW) een ondersteunend document op te stellen. Dit document heet de ‘Keuzehulp Suwinet verantwoording’. Dit document is afgestemd met NOREA en het ministerie van SZW. In dit document is voor de IT audit vragen opgenomen met welke scope u de BIG vragen die betrekking hebben op Suwinet dient te beantwoorden. De scope voor de beantwoording (en vervolgens de IT audit), wordt bepaald door de wijze waarop de gegevens van Suwinet worden gebruikt in de organisatie:

- Suwinet-Inkijk
- Suwinet-Inlezen
- DKD-Inlezen

Het document kunt u vinden op de site www.vngrealisatie.nl/ensia onder downloads.

Het schema hiernaast toont hoe het normenkader Suwinet voor Afnemers is verdeeld over de BIG vragenlijst in ENSIA. U vindt dit schema ook terug in Bijlage 1.

Stappenplan

Onderstaand stappenplan ondersteunt u bij de voorbereiding op de IT audit en de verwerking van de antwoorden van (de verschillende type) Suwinet bevraging(en).

1. **Inventariseer waar Suwinet wordt gebruikt voor Participatiewet/IOAZ/IOAW uitvoering.**
    i. Intern
    ii. Uitbesteed via een samenwerkingsverband (incl. gemeenschappelijke regeling)

De gemeente legt in beide gevallen verantwoording af via ENSIA, dus ook voor gebruik van Suwinet door een samenwerkingsverband. Indien Suwinet wordt gebruikt vanuit bijvoorbeeld een ISD, maak dan afspraken met de samenwerkende gemeenten en de ISD over het beantwoorden van de informatieveiligheidsvragen uit ENSIA. Houdt hierbij rekening dat de ICT diensten die betrekking hebben op het gebruik Suwinet ook nog kunnen worden geleverd door een Shared Service Centrum (SSC). Dit SSC zal dan ook dienen te worden betrokken bij de verantwoording.

2. **Inventariseer van welke Suwinet aansluitingen voor niet-SUWI partijen uw gemeente gebruikt maakt.**

I. RMC

Alleen indien uw gemeente RMC contactgemeente is, verantwoordt u zich over de levering van gegevens. Hierbij kan mogelijk gebruik gemaakt worden van een uitbestede dienst in een samenwerkingsverband. Ook dan dient alleen de contactgemeente zich te verantwoorden (en te voldoen aan het normenkader).

II. Gemeentelijke gerechtsdeurwaarders

De gemeente verantwoordt zich alleen indien deze levering daadwerkelijk wordt afgenomen. Dit is niet bij elke gemeente het geval. Let wel: het is mogelijk dat de gemeente deze dienst heeft uitbesteed, bijvoorbeeld aan een belastingsamenwerking. De gemeente dient zich ook dan te verantwoorden over de informatieveiligheid van dit gebruik. Maak in deze situatie afspraken met de samenwerkende gemeenten en het samenwerkingsverband over het beantwoorden van de vragen in ENSIA.

III. Burgerzaken

Indien de gemeente van deze levering gebruik maakt zal zij zich verantwoorden over deze levering. Beantwoord de vragen uit ENSIA met de afdeling Burgerzaken.

3. **Inventariseer voor alle Suwinet aansluitingen op welke wijze van de gegevens gebruik gemaakt wordt.**
    a. Suwinet-Inkijk
    b. Suwinet-Inlezen
    c. Suwinet-DKD Inlezen (alleen voor uitvoering P-wet)

Het type aansluiting en gebruik (Inkijk of Inlezen) bepaalt de toepasselijkheid en scope van de beantwoording van de BIG vragen op basis van het Suwinet normenkader Afnemers. Hiervoor gebruikt u het document ‘Keuzehulp Suwinet verantwoording’ vanaf de ENSIA site van VNG Realisatie.

4. **Opdrachtverstrekking aan IT auditor**

Neem in de opdrachtbevestiging aan de auditor op wat de scope is voor de audit van de Collegeverklaring. Ofwel, op welke type Suwinet leveringen de collegeverklaring betrekking heeft (en bestaande DigiD aansluitingen).

5. **Verwerk de antwoorden op de vragen in ENSIA** voor de horizontale verantwoording en verticale verantwoording. Voor de verticale verantwoording geldt dat de IT auditor alleen de antwoorden zal toetsen die betrekking hebben op de Suwinet aansluitingen (dus niet op de horizontale beantwoording van de vragen in ENSIA). Het kan is goed mogelijk dat het horizontale antwoord (gemeentebreed) op een BIG vraag Nee is, maar dat u de vragen voor de IT audit met Ja beantwoord (verticaal), omdat u voor het specifieke onderdeel Suwinet voldoet.

Slechts een deel van de antwoorden Suwinet (alleen de IT audit vragen) worden door de IT auditor beoordeeld voor assuranceverlening op de collegeverklaring. Indien uw gemeente diensten met betrekking tot Suwinet heeft uitbesteed, maak dan afspraken over de wijze waarop de IT audit plaatsvindt. Bijvoorbeeld door het afgeven van een TPM vanuit het samenwerkingsverband of het aanstellen van eenzelfde IT auditor.

6. **Oormerk de antwoorden en evidence van de verschillende Suwinet leveringen** (zie stap 1 en 2) die betrekking hebben op de IT audit. Op deze wijze maakt u het de auditor mogelijk de IT audit gericht uit te voeren.

7. **Stel de concept Collegeverklaring op**. Hier vult u de benodigde gegevens aan. De collegeverklaring heeft een vaste opmaak en inrichting. Het is niet toegestaan tekstuele aanpassingen in het format aan te brengen (vormvast format). Het format wordt ter beschikking gesteld via de tool ENSIA.nl, zodra deze definitief is vastgesteld voor het verantwoordingsjaar 2018.

8. **Hierna volgt de voorbereiding op de audit**. Stem de werkzaamheden met de auditor en het samenwerkingsverband af. U hebt sowieso de antwoorden op de vragen nodig voor de horizontale verantwoording van ENSIA. Geeft uw samenwerkingsverband (ISD) een TPM af, dan zal de IT auditor van de gemeente contact opnemen met de auditor van het samenwerkingsverband. De TPM die wordt afgegeven door de auditor vanuit het samenwerkingsverband valt namelijk binnen de verantwoordelijkheid van de auditor van de gemeente, anders gesteld de beheersingsmaatregelen van het samenwerkingsverband vallen binnen de werkzaamheden van de auditor (inclusive methode). De auditor van de gemeente steunt op de afgegeven TPM door het samenwerkingsverband.

   Indien er geen TPM afgegeven wordt door het samenwerkingsverband, bereidt dan de audit zo goed mogelijk voor. Denk hierbij aan toegankelijkheid van evidence ten aanzien van autorisaties, logging, controle van logging en opvolging van bevindingen. De evidence waarover u kunt afstemmen met het samenwerkingsverband omvat op hoofdlijnen:

   I. Aansluitbeleid/informatiebeveiligingsbeleid
   II. Evaluaties aansluitbeleid/informatiebeveiligingsbeleid
   III. Incidentmanagementproces (beveiligingsincidenten)
   IV. Autorisatiematrix en –proces (nieuwe medewerkers/wijzigingen/beëindigingen)
   V. Review van autorisatiematrix en -proces
   VI. Loggingrapportages
   VII. Monitoring van loggingrapportages
   VIII. Rapportages over IAA aan management en bijbehorende follow-up

Zie ook het eerder genoemde document ‘Keuzehulp Suwinet verantwoording’.

9. **De auditor vormt hierna zijn oordeel** met betrekking tot assurance verlening.

Zelfevaluatie DigiD met ENSIA

Doelstelling en scope DigiD-assessment

Het ministerie van BZK heeft een algemene doelstelling voor het DigiD-assessment geformuleerd: ‘Het verschaffen van aanvullende zekerheid over de opzet en het bestaan in een DigiD- webomgeving van een aantal beveiligingsmaatregelen die zijn gebaseerd op een selectie uit de actuele ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC en die gericht zijn op enerzijds de preventie van het optreden van bedreigingen vanaf internet en anderzijds de detectie en de incident response indien deze bedreigingen zich toch manifesteren.’ Het DigiD-assessment via ENSIA is van toepassing op bestaande actieve aansluitingen waarvan de contracten met Logius op naam staan van de gemeente (niet van een samenwerkingsverband o.i.d.).

Het DigiD-assessment beperkt zich tot het beoordelen van de opzet en het toetsen van het bestaan van de beheersmaatregelen. Met ‘opzet’ wordt de beschrijving van het stelstel van informatiebeveiligings- en beheersingsmaatregelen bedoeld. Het ‘bestaan’ is gedefinieerd als ‘het daadwerkelijk functioneren van een stelsel van informatiebeveiligings- en beheersingsmaatregelen, conform beschrijving op of rond een peildatum’.

Het kan voorkomen dat bij het uitvoeren van de audit wel voldaan is aan de opzet van beheersingsmaatregel (de maatregel is beschreven), maar dat het bestaan niet kan worden beoordeeld. Bijvoorbeeld omdat in de onderzochte periode de relevante gebeurtenis zich niet heeft voorgedaan. In dat geval wordt dit weergegeven als ‘voldoet’ in het assurance-rapport en voorzien van een toelichting.

Praktische tip
Maak zo snel mogelijk afspraken met uw leverancier/serviceorganisatie over het ontvangen van de TPM, waarbij 15 oktober 2018 de streefdatum is.

Alleen assessmentplichtige aansluitingen vallen binnen de ENSIA-zelfevaluatie

Gemeenten hebben een verantwoordingsplicht met ENSIA voor wat betreft de actieve aansluitingen. Nieuwe aansluitingen vallen buiten de ENSIA-zelfevaluatie, daarvoor geldt de bestaande aansluitprocedure. Assessmentplichtige DigiD aansluitingen zijn **actieve bestaande** DigiD-aansluitingen die per 1 mei 2019 actief zijn. Dit roept de vraag op wanneer een DigiD-aansluiting als een nieuwe aansluiting wordt gekenmerkt. Dat ligt aan het moment waarop de betreffende DigiD-aansluiting is geactiveerd. De activatiedatum is dus van belang om te bepalen wanneer een nieuwe DigiD-aansluiting onder het reguliere regime gaat vallen. Onderstaande voorbeelden maken dit duidelijk:

Voorbeeld 1:
Een bestaande DigiD-aansluiting wordt naar verwachting niet meer gebruikt en afgesloten voor 1 mei 2019. Deze aansluiting valt in de vrijstellingsperiode en hoeft niet te worden verantwoord richting Logius. In het de ENSIA-systematiek telt deze aansluiting niet mee; er hoeft geen DigiD-vragenlijst te worden ingevuld voor deze aansluiting.

Voorbeeld 2:
Een nieuwe DigiD-aansluiting is geactiveerd op 2 februari 2018. De assessmentplicht voor een nieuwe aansluiting is twee maanden na activatie, in dit geval dus per 2 april 2018, met een vrijstelling voor 12 maanden (tot 2 april 2019). De vrijstellingsdatum van 2 april valt **in** de ‘reguliere audit periode’, die loopt van 1 januari tot 1 mei 2019, en daarmee valt de betreffende DigiD-aansluiting onder de ENSIA-systematiek. Dit betekent: uiterlijk voor 1 mei 2019 een assessment-rapportage indienen over 2018.

Voorbeeld 3:
Een nieuwe DigiD-aansluiting is geactiveerd op 15 april 2018. De assessmentplicht voor een nieuwe aansluiting is twee maanden na activatie, in dit geval dus per 15 juni 2018 met een vrijstelling voor 12 maanden (tot 15 juni 2019). De vrijstellingsdatum van 15 juni valt **buiten** de ‘reguliere audit periode’, die loopt van 1 januari tot 1 mei 2019, en daarmee valt de betreffende DigiD-aansluiting niet onder de ENSIA-verantwoordingsplicht. Dit

betekent: niet opnemen in de collegeverklaring, geen audit door de auditor en vrijstelling voor een jaar; uiterlijk voor 1 mei 2020 een assurancerapport indienen over 2019.

Er zijn ook gedeactiveerde DigiD-aansluitingen. Dat zijn aansluitingen die bijvoorbeeld niet voldoen aan de assessmentplicht of op verzoek van de gemeente zelf zijn gedeactiveerd. Om bestaande gedeactiveerde aansluitingen te activeren moet eerst een assessmentrapport worden ingediend. Daarbij ontvangt u een brief van Logius waarin de vrijstellingsperiode staat aangegeven. Op basis daarvan kunt u bepalen of uw aansluiting wel of niet binnen de ENSIA-systematiek valt.

Samengevat: alleen voor bestaande actieve DigiD-aansluitingen geldt de verantwoordingsplicht vanuit ENSIA. Bestaande aansluitingen zijn vroegere aansluitingen, aansluitingen die actief zijn geworden tussen 1 november 2017 en 1 maart 2018 én die nog actief zijn op 1 mei 2019. Aansluitingen geactiveerd na 1 maart 2018 worden geclassificeerd als nieuwe aansluitingen en vallen vanwege de vrijstellingsperiode buiten de scope van de ENSIA verantwoordingsplicht. Dat laatste geldt ook voor bestaande aansluitingen die niet meer actief zijn op 1 mei 2019 of eerder. Ook voor deze aansluitingen geldt dat de ENSIA verantwoordingsplicht vervalt. Indien uw gemeente geen ENSIA assessmentplichtige DigiD aansluitingen heeft, maakt DigiD ook geen onderdeel uit van de op te stellen en te auditen collegeverklaring. Bovenstaande casuïstiek geldt bij het indienen van ‘groene’ assessmentrapportages, waarvan Logius vaststelt dat de gemeente voldoet aan de gestelde normen. Indien sprake is van een situatie waarin niet aan alle normen is voldaan, dan komt de gemeente terecht in een regulier verbetertraject, zie www.logius.nl voor de betekenis hiervan. Het verbetertraject gaat buiten ENSIA en de ENSIA tool om.

Gebruik van meer dan één DigiD-aansluiting

De ENSIA-zelfevaluatie dient te worden ingevuld per DigiD-aansluiting. Dit omdat u zich als aansluithouder per aansluiting dient te verantwoorden. U verantwoordt zich in één Collegeverklaring over al uw assessmentplichtige DigiD-aansluitingen. Wel stelt u per DigiD-aansluiting de bijlage 1 op. De auditor stelt één assurancerapport op over alle assessmentplichtige DigiD-aansluitingen (en Suwinet).

Uitbesteding van de DigiD applicatie

Gemeenten kiezen zelf of ze de taken in het DigiD-domein uitbesteden of niet. Veel gemeenten kiezen voor maximaal ontzorgen en nemen de DigiD-applicatie af bij een serviceorganisatie. Dat kan een SAAS-oplossing zijn, maar de combinatie van een hosting- en applicatieleverancier komt ook voor. Bij dit laatste kan het voorkomen dat meerdere leveranciers participeren binnen de applicatie en daarmee ook elk verantwoordelijk zijn voor het afdekken van een deel van de te toetsen normen. Een aantal (veelal) grotere gemeenten heeft gekozen voor een eigen webserver en nemen alleen applicatiediensten af. Er is, ongeacht de vorm van samenwerking een minimaal aantal van zes normen waar de gemeente altijd zelf aan dient te voldoen. Het is van belang om per DigiD-aansluiting te weten welk model wordt gehanteerd en hoe zich dit verhoudt tot de te verantwoorden normen door partijen.

De meest voorkomende varianten zijn:

- Zowel hosting, applicatiebeheer als de implementatie zijn in handen van de gemeente.
- Hosting bij de gemeente en applicatiebeheer bij de leverancier, die geen verantwoordelijkheid heeft voor de implementatie.
- Hosting bij de gemeente en applicatiebeheer bij de leverancier, die bepaalde verantwoordelijkheid heeft voor de implementatie en beheerrechten heeft in de productieomgeving.
- Uitbesteding van applicatiebeheer en hosting onder aansturing van de gemeente (geen SAAS-

omgeving) aan één of twee leveranciers.

- Volledige uitbesteding als SAAS-oplossing, waarbij wijzigingenbeheer volledig onder de leverancier valt met betrokkenheid van een gebruikersgroep. Ook andere varianten en vormen van ketensamenwerking zijn mogelijk.

Het DigiD-assessment is gebaseerd op een normenset (webrichtlijnen NCSC). Bij het uitvoeren van het DigiD-assessment moet per norm worden bepaald welke partij verantwoordelijk is voor een norm.

Ruwweg wordt deze indeling aangehouden:

- Normen waarvoor de aansluithouder/gemeente verantwoordelijk is;
- Normen waarvoor de serviceorganisatie/leverancier verantwoordelijk is;
- Normen waarvoor beiden een gedeelde verantwoordelijkheid hebben.

Het overzicht van de normen maakt onderdeel uit van de Collegeverklaring en is opgenomen in de notitie verantwoordingsstelsel ENSIA 2018. Het normenkader en de toelichting voor de auditors wordt beschikbaar gesteld via de site van NOREA[9], www.norea.nl.

Bijlage 2[10] bevat een overzicht van de meest voorkomende verdeling van normen over de verschillende partijen. Een apart aandachtspunt daarbij vormen de normen waarvan de serviceorganisatie/leverancier aanneemt dat ook de aansluithouder/gemeente verantwoordelijk is (ook wel de '*user control considerations*' genoemd). Dit omdat de normen bij de serviceorganisatie alleen geen voldoende zekerheid bieden voor de beheersing van de DigiD-beveiligingsrisico's. Over deze normen dient goede afstemming te bestaan tussen de partijen. Het overzicht in bijlage 2 geeft inzicht in de normen waarvoor mogelijk zowel de aansluithouder/gemeente als de serviceorganisatie/leverancier verantwoordelijk zijn.

De tabel in bijlage 2 bevat, naast de kolom voor de aansluithouder, twee kolommen: hostingpartij en softwareleverancier. Het komt voor dat een gemeente gebruik maakt van twee leveranciers, een voor de hosting en een voor applicatiebeheer. Veelal wordt dit door dezelfde leverancier uitgevoerd, in dat geval worden alle normen van de serviceorganisatie/leverancier ondergebracht in één TPM. Indien gebruik gemaakt wordt van twee verschillende partijen, zullen twee TPM's opgeleverd worden.

Praktische tip:
Breng voor uw situatie per DigiD-aansluiting de verdeling van de activiteiten in kaart en daarop gebaseerd de verdeling van de normen.

TPM's als onderdeel van DigiD-verantwoording

De leverancier of serviceorganisatie kan een deel van de vragen beantwoorden vanuit een TPM (Third Party Mededeling of memorandum). Deze dient aan te sluiten op de vragen uit de ENSIA- tool. Het is belangrijk

[9] https://www.norea.nl/download/?id=3941
[10] Nog niet gereed bij de publicatie van deze versie

om tijdig afspraken te maken met uw leverancier over de inhoud van de TPM (volgens het *carve-out model*). Deze zullen afhankelijk zijn van de diensten die u afneemt. Het is wenselijk dat gemeenten uiterlijk 15 oktober 2018 over de TPM beschikken. Dit zodat de gemeenten tijdig de TPM inhoudelijk beoordelen en vaststellen welke normen door de TPM zijn afgedekt. U kunt voor bestaande aansluitingen niet de bestaande TPM (over de DigiD-aansluiting in 2017) gebruiken. TPM's mogen niet worden herbruikt. De TPM over 2018 dient gebaseerd te zijn op versie 2 van het DigiD-normenkader.

Praktische tip
Indien bij uw gemeente sprake is van een nieuwe DigiD-aansluiting, achterhaal de activatiedatum en bepaal of de betreffende DigiD-aansluiting binnen of buiten de ENSIA-verantwoording valt. Achterhaal tevens of de DigiD aansluitingen van uw gemeente nog actief zijn per 1 mei 2019. Let op bij geactiveerde (van voorheen gedeactiveerde) aansluitingen, raadpleeg in die gevallen de begeleidende brief van Logius.

Op de juiste wijze verantwoordingsdocumenten aanleveren

Naar aanleiding van de eerste ervaringen in 2017 zijn de verantwoordingsdocumenten (collegeverklaring en de bijlage Suwinet en DigiD) gewijzgd (o.a. tekstueel vereenvoudigd). Met het publiceren van deze versie van de handreiking zijn deze documenten nog niet definitief vastgesteld en daarom nog niet beschikbaar. Wij informeren u verder over het verantwoordingsproces en het invullen van de formats voor de verantwoording.

Zelfevaluatie BAG, BGT en BRO met ENSIA

De informatieveiligheidsvragen voor de BAG en BGT zijn opgenomen in de BIG vragenlijst 2018. Dit betreft een zeer beperkt aantal vragen. Er zijn geen vragen over de BRO opgenomen in de BIG vragenlijst. Aanvullende vragen die buiten informatieveiligheid vallen, zijn opgenomen in drie separate vragenlijsten. De verantwoording over het jaar 2018 is voor de BAG en BGT verplicht. Voor de BRO geldt een proefjaar.

Zelfevaluatie BRP en PUN met ENSIA

Net als afgelopen jaar zijn de informatieveiligheidsvragen voor de BRP en PUN opgenomen in ENSIA. Het inlevermoment voor de vragen is verschoven van 1 oktober in 2017 naar 31 december in 2018. Als gevolg van intreden van nieuwe wetgeving (harmonisatie met ENSIA proces van het stelsel) geldt geen 1 oktober inleverdatum meer voor de BRP en PUN. Direct na 31 december worden de antwoorden overgeheveld naar de kwaliteitsmonitor. In de kwaliteitsmonitor zijn de domeinspecifieke/aanvullende vragen opgenomen voor de verantwoording naar RvIG/BZK. Hierna volgt u het proces vanuit de kwaliteitsmonitor.

Werkwijze ENSIA voor bestuurlijk fuserende gemeenten

Indien uw gemeente bestuurlijk fuseert naar een nieuw op te richten gemeente, of wanneer de gemeente wordt ingevoegd bij een bestaande gemeente is de volgende werkwijze van toepassing:

Voor Suwinet geldt:

Gemeenten die rechtsopvolging vinden in een nieuwe gemeente worden vrijgesteld van de verantwoordingsverplichtingen in het jaar van de gemeentelijke herindeling (in dit geval het verantwoordingsjaar 2018). Over het daaropvolgende jaar (in dit geval het 2019) is de nieuwe gemeente weer gehouden aan de verantwoordingsverplichtingen. Daarbij geldt dat indien een nieuwe gemeente in haar eerste jaar niet voldoet aan de SUWI-normen, normherstel niet eerst aan de gemeenteraad wordt gelaten, maar meteen geëscaleerd wordt naar de 2e stap in het, escalatieprotocol SUWI. Dit om het risico

op langdurige niet-naleving te beperken.

Voor DigiD geldt:
Wanneer bestaande DigiD aansluitingen worden afgesloten voor 1 mei van enig jaar hoeft hierover geen verantwoording te worden afgelegd aan Logius. Voor de meeste fusiegemeenten geldt dat bestaande DigiD aansluitingen op naam van de op te heffen gemeente worden opgezegd. Een nieuwe aansluiting op naam van de nieuw te vormen gemeente valt buiten de scope van ENSIA. Een nieuwe aansluiting wordt binnen 2 maanden na activatiedatum ge-audit, waarna bij goedkeuring een vrijstellingsperiode van 12 maanden volgt.

Voor BRP/PUN geldt:
Voor de BRP en PUN geldt dat verantwoording wordt afgelegd in het jaar voorafgaand aan de fusie. Het uittreksel wordt vastgesteld door het college waarin de gemeente rechtsopvolging vindt. Gemeenten zijn uitgesloten van de steekproef.

Voor BAG/BGT geldt:
Verplichting tot verantwoording voorafgaand aan de fusie blijft van kracht. De rapporten worden vastgesteld door het college waarin de gemeente rechtsopvolging vindt.

Voor ENSIA geldt:
De gemeente dient aan te geven welke gegevens vanuit een van de oorspronkelijke gemeenten de data uit ENSIA in het opvolgende jaar getoond gaan worden. Hiernaast dient de nieuwe ENSIA coördinator aangemeld te worden. Hierna kunnen alle rechten opnieuw worden toegekend.

Horizontale verantwoording

Aansluitend op het proces van de zelfevaluatie volgt het proces van verantwoorden. De eerstelijns verantwoording is de interne verantwoording aan de raad; het eigen toezichthoudend orgaan. We noemen dit de horizontale verantwoording. De wijze waarop het horizontale verantwoordingsproces wordt vormgegeven is vormvrij. De verantwoording over informatieveiligheid komt voort uit de resolutie uit 2013. Met aanname van de resolutie hebben gemeenten afgesproken zich te verantwoorden naar de raad via het jaarverslag. De ervaring van 2017 leert dat de verantwoording via het jaarverslag zodanig op hoofdlijnen is dat veel gemeenten gekozen hebben om de raad met een (vertrouwelijke) separate rapportage over informatieveiligheid te informeren. Op deze wijze hebben veel gemeenten ook direct de rapportages voor de tweedelijns toezichthouders (ministeries) opgenomen als bijlage. In dit hoofdstuk wordt de werkwijze en de stappen voor de horizontale verantwoording beschreven.

Interne balans opmaken over uitkomsten zelfevaluatie

Na het inleveren van de vragenlijsten uiterlijk 31 december is het tijd om de balans op te maken. Via de ENSIA tool zijn er verschillende manieren om de vragenlijsten uit te draaien. Het is nu aan de gemeente om de antwoorden te gaan aggregeren en op basis van de risico-analyse te gaan bepalen welke verbeteringen moeten worden doorgevoerd of wordt besloten om geen verbeteringen door te voeren, maar dan ook de risico's te aanvaarden.

Naast de export mogelijkheden kunt u in ENSIA een interne verantwoording/management rapportage ENSIA genereren. In het format zijn de algemene beschrijvingen opgenomen. De inrichting is op basis van de BIG hoofdstukken. Er is een omschrijving van het hoofdstuk opgenomen. Hierna volgt de mogelijkheid om aan te geven waar in het afgelopen jaar aandacht aan is geschonken, wat goed is gegaan en voor welke onderdelen verbetering wenselijk is. Dit rapport biedt een handzaam overzicht.

Raad informeren

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. In de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' is afgesproken om de raad via dit middel te informeren over informatieveiligheid. Op deze wijze kan zij haar toezichthoudende functie vervullen. 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, dan 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.

Zoals eerder vermeld hebben veel gemeenten gekozen voor een (vertrouwelijke) separate rapportage aan de raad. Een dergelijke rapportage zal vaak breder informatie bieden dan alleen ENSIA. Het format 'rapporteren over informatieveiligheid' geeft een handreiking op basis waarvan u de inhoud van een gemeente brede rapportage kunt opstellen (www.vngrealisatie.nl/ensia). De management rapportage (via de ENSIA tool (na inleveren)) biedt u inhoudelijk eveneens een goede basis. De rapportages bieden een mooi handvat om gelijktijdig de verticale rapportages aan te bieden. Op deze wijze informeert u in één keer de raad volledig. U biedt de rapportage vertrouwelijk ter informatie aan. Het is aan de raad om het onderwerp te agenderen en te bespreken.

Verticale verantwoording

De verticale verantwoording betreft de verantwoording aan de tweedelijnstoezichthouders. De verantwoording is ‘vormvast’, ofwel u werkt op basis van sjablonen waar inhoudelijk geen aanpassingen op zijn toegestaan. In dit hoofdstuk worden de stappen en de werkwijze toegelicht. Voor alle documenten die u aan de verticale toezichthouders verstrekt geldt dat u de raad hierover dient te informeren. Het verdient aanbeveling om dit ineens te doen met alle verantwoordingsstukken. U informeert de raad met een vertrouwelijke separate rapportage over informatieveiligheid en neemt de verschillende vastgestelde rapportages voor Suwinet, DigiD, BAG, BGT, (BRO), BRP en PUN op als bijllagen. U vergroot daarmee de kans dat de raad dit stuk (en de bijlagen) ook zal agenderen en bespreken.

Collegeverklaring en assurance Suwinet en DigiD

Voor Suwinet en DigiD geldt dat de zelfevaluatie getoetst wordt door de IT auditor. Het ‘object van onderzoek’ is de collegeverklaring. De formats van deze documenten zijn beschikbaar in ENSIA zodra deze definitief zijn vastgesteld. U vult de collegeverklaring aan. Deze is vormvast en dat betekent dat er geen ruimte is voor aanpassingen of andere ‘dichterlijke vrijheden’. Naar aanleiding van de ervaringen in 2017 geven we graag mee dat u in de collegeverklaring alleen aangeeft of al dan niet aan de normen voor Suwinet en/of DigiD wordt voldaan (format). U noemt hier niet de normen van Suwinet of DigiD waaraan niet voldaan wordt. De details over de normen DigiD en Suwinet neemt u namelijk op in de bijlagen. De auditor toetst de collegeverklaring en 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.

U upload voor 1 mei in ENSIA de benodigde stukken:

Suwinet	DigiD
Collegeverklaring	Collegeverklaring
Bijlage 2 Suwinet	Bijlage 1 DigiD
Assurancerapport	Assurancerapport
	TPM's (indien van toepassing)

Vaststelling BAG, BGT en BRO

Na inleveren van de vragenlijsten voor BAG, BGT en BRO (proefjaar) voor 31 december 2018 kunt u de rapportages in ENSIA gaan genereren. U vult deze rapportages aan en laat deze door het College vaststellen. De vaststellingdatum door het College neemt u op in de rapportages. U informeert hierna de raad. In de eerste alinea van dit hoofdstuk is aangegeven dat met het aanbieden van een separate (vertrouwelijke) rapportage de kansen vergroot worden om het onderwerp op de agenda van de raad geplaatst te krijgen.

Proces verantwoording BRP en PUN

De antwoorden op de informatiebeveiligingsvragen uit de BIG vragenlijst worden na de sluiting op 31 december 2018 overgeheveld naar de kwaliteitsmonitor. De resultaten uit ENSIA worden automatisch samengevoegd. Het is vanaf 3 januari 2019 mogelijk om vanuit de kwaliteitsmonitor (bij Burgerzaken) een uittreksel en een managementrapportage te genereren. Dit proces en het verdere verantwoordingsproces speelt zich af buiten ENSIA om. De afdeling Burgerzaken is goed op de hoogte van de processen. Op hoofdlijnen verloopt het verantwoordingsproces als volgt:

- Gemeenten zijn vrij om een toelichting te schrijven in aanvulling op het uittreksel.
- Het uittreksel wordt ondertekend door het college van B&W
- Gemeenten sturen het uittreksel van de rapportage voor 14 februari 2019 aan de minister van BZK en de Autoriteit Persoonsgegevens.

Let op dit is een afwijkende datum ten opzichte van de overige verticale verantwoording waar voor 1 mei 2019 geldt. Na aanlevering wordt door het CBS een steekproef bepaald van 35 gemeenten om een controle uit te voeren op de zelfevaluatie ENSIA en de vragenlijst BRP bij Burgerzaken.

Vragen

VNG Realisatie is het eerste aanspreekpunt voor gemeenten. Als u een vraag heeft kunt u contact opnemen via het centrale telefoonnummer 070 250 2400 of een mail sturen aan ensia@vng.nl. Daarnaast is allerhande informatie te vinden op de website https://www.vngrealisatie.nl/ensia.

Als VNG Realisatie de vraag niet zelf kan beantwoorden zal zij contact opnemen met de tweede lijn bijv. ICTU als het gaat om technische vragen over de ENSIA tool of een stelselhouder als het gaat om de domeinspecifieke vragenlijsten of verantwoording.

Bijlagen

1. Verdeling Suwinet over de BIG vragenlijst
2. Notitie verantwoordingsstelsel (nog niet vastgesteld)
3. Kruisjestabel bij Normenkader DigiD

Verwijzingen

NOREA handreiking 2018 via www.norea.nl (nog niet gepubliceerd, verwachting oktober 2018)
Escalatieprotocol Suwinet via VNG Realisatie (www.vng.nl/ensia nog niet gepubliceerd)
Verantwoordingsformats Collegeverklaring en bijlagen (nog niet vastgesteld, hangt samen met notitie verantwoordingsstelsel, op nader tijdstip te downloaden via ensia.nl)

Bijlage 1

Verdeling Suwinet over de BIG vragenlijst

IN ENSIA/BIG VRAAG	Norm	IT AUDIT	SUWI
BIG 5.1.1.a	B.01	x	x
BIG 5.1.1.b	B.01	x	x
BIG 5.1.2.a	C.01	x	x
BIG 6.1.1.a	B.01	x	x
	C.01	x	x
BIG 6.1.2.a	B.01	x	x
	B.04	x	x
BIG 6.1.3.a	B.05	x	x
BIG 6.1.7.a	B.04		x
BIG 6.1.8.a	C.01		x
	C.08		x
BIG 6.2.1.h	B.03		x
BIG 6.2.3.a	U.01		x
BIG 7.1.1.a	B.06		x
BIG 7.2.1.a	U.06		x
BIG 7.2.1.b	U.06		x
BIG 7.2.2.a	U.06		x
BIG 8.2.2.a	Notitie Verantw	x	x
BIG 8.3.1.b	U.02		x
BIG 10.1.1.b	U.10		x
BIG 10.1.2.a	C.03		x
BIG 10.1.3.a	B.05		x
BIG 10.1.3.b	B.05	x	x
BIG 10.1.3.c	B.05	x	x
BIG 10.1.4.a	U.09		x
BIG 10.8.1.a	U.07 en U.08		x
BIG 10.8.1.b + c	U.07 en U.08		x
BIG 10.8.4.a	U.08		x
BIG 10.8.5.a	U.05		x
BIG 10.10.1.a	C.05	x alleen Inlezen	x
BIG 10.10.1b	C.05	x alleen Inlezen	x
BIG 10.10.2.a	C.06	x	x
BIG 11.2.1.a	U.02	x	x
	U.03	x	x
BIG 11.2.1.b	U.02	x	x
	U.03	x	x
BIG 11.2.3.a	U.03		x
BIG 11.2.4.a	C.04	x alleen Inkijk	x
BIG 11.4.2.c*	C.07		x
BIG 11.4.6.a	U.11		x
BIG 11.5.2.a	U.03	x alleen Inlezen	x
BIG 11.5.2.b	U.03	x alleen Inlezen	x
BIG 11.6.1.a	U.04		x
BIG 11.7.2.a	U.12		x
BIG 11.7.2.b	U.12		x
BIG 12.3.1.a	U.11	x	x
BIG 15.2.1.a	B.02		x

Bijlage 3

Kruisjestabel DigiD 2018

Norm	*Omschrijving norm*	*Aansluithouder /gemeente*	*Hosting partij*	*Applicatie leverancier*	*Saas leverancier*
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.	X	X	X	X
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 de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.	X	X	X	X
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	X		X	X
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze wordt verwerkt.			X	X
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.			X	X
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	X	X	X	X
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.		X	X	X
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.		X	X	X

Norm	*Omschrijving norm*	*Aansluithouder /gemeente*	*Hosting partij*	*Applicatie leverancier*	*Saas leverancier*
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen. Daarnaast wordt het beheer uitgevoerd conform het operationeel beleid voor platformen.		X		X
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar.		X		X
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 is gepositioneerd.		X		X
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.		X		X
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.		X		X
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.	X	X		X
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd. Dit op de ICT-componenten van de webapplicatie (*scope*).		X		X
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (*scope*).		X	X	X
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief, efficiënt, effectief en beveiligd ingericht.		X		X

Norm	*Omschrijving norm*	*Aansluithouder /gemeente*	*Hosting partij*	*Applicatie leverancier*	*Saas leverancier*
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt en geanalyseerd) en de bevindingen worden gerapporteerd.		X		X
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	X	X	X	X
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings-)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.		X		X