NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

HANDREIKING ENSIA voor IT-auditors (RE's)

Eénduidige Normatiek Single Information Audit voor gemeenten

Verantwoordingsjaar 2024 – versie 1.0
19 december 2024

1. Over deze handreiking ENSIA

Beheer
Deze handreiking is uitgegeven door NOREA, de beroepsorganisatie van IT-auditors in Nederland en is bedoeld als guidance-document voor de IT-auditors die zich bezighouden met het project Eénduidige Normatiek Single Information Audit (ENSIA) voor gemeenten.

In het kader van het afstemmen van verwachtingen wordt deze handreiking ook ter beschikking gesteld aan de ENSIA-coördinatoren van gemeenten.

De handreiking mag worden gebruikt en/of gedistribueerd, mits met bronvermelding.

Voor vragen en opmerkingen kunt u zich wenden tot:

NOREA
Postbus 242
2130 AE Hoofddorp
telefoon: 088 - 4960380
e-mail: norea@norea.nl

Meer informatie kunt u vinden op: www.norea.nl en/of www.ensia.nl

Deze ENSIA handreiking zal op basis van het ENSIA-proces 2024 (zelfevaluatie en verantwoording door gemeenten en uitgevoerde audit(s)) door de ENSIA-Werkgroep van NOREA worden geëvalueerd en zo nodig verbeterd. Het is de bedoeling om de handreiking op basis van ervaring en evaluatie jaarlijks als NOREA-handreiking (conform artikel 15 Reglement Beroepsbeoefening) vast te stellen.

Waar nodig zullen tussentijds en a tempo aanvullingen op de Handreiking gepubliceerd worden in de vorm van FAQ-teksten op de website van NOREA. Deze maken onverkort onderdeel uit van de Handreiking.

Deze versie vervangt de voorgaande versie(s) en is in zijn geheel van toepassing op de uitvoering van de werkzaamheden over het verslagjaar 2024.

Versiebeheer

Versie	Datum	Toelichting
Versie 0.9	30 oktober 2017	t.b.v. de ENSIA-training
Versie 0.91	16 november 2017	t.b.v. werkgroep ENSIA
Versie 0.92	21 november 2017	t.b.v. werkgroep ENSIA
Versie 0.93	23 november 2017	t.b.v. werkgroep ENSIA/ Vaktechnische Commissie / Bestuurlijk Overleg BZK – VNG – NOREA
Versie 0.94	5 december 2017	Incl. commentaar VC-NOREA /VNG/PWC
Versie 0.95 / Versie 1.0	15 december 2017 t/m 31 januari 2018	Enkele correcties en aanvullingen verwerkt
Versie 2.0	25 oktober 2018	Update t.b.v. audit 2018
Versie 2.3	26 september 2019	Update t.b.v. audit 2019
Versie 2.4	11 oktober 2019	Update t.b.v. audit 2019
Versie 2.5	14 oktober 2019	Update t.b.v. audit 2019 bespreekversie Werkgroep ENSIA/ VNG/ SZW/ BZK
Versie 2.6	23 oktober 2019	Versie ter vaststelling/ Addendum rond actualia separaat aangeboden
Versie 2.7	25 oktober 2019	Kleine redactionele aanpassingen
Versie 2.8	24 augustus 2020	Ter beoordeling Werkgroep ENSIA en VC
Versie 3.0	21 oktober 2020	Definitief: Update t.b.v. audit 2020
Versie 3.1	28 september 2021	Ter beoordeling Werkgroep ENSIA en VC
Versie 4.0	15 oktober 2021	Definitief: Update t.b.v. audit 2021
Versie 4.01	Mei 2024	Ter beoordeling Werkgroep ENSIA
Versie 4.02 – 4.05 / 0.51	Mei juni juli 2024	Ter beoordeling Werkgroep ENSIA
Versie 5.0	9 oktober 2024	Definitief: Update t.b.v. audit 2024 en afstemming VC
Versie 1.0	19 december 2024	Vaststelling bestuur

1.1 Aanleiding

Het project ENSIA (Eénduidige Normatiek Single Information Audit) is op 1 juli 2017 voor gemeenten van start gegaan. ENSIA is een gezamenlijk project van het ministerie van Binnenlandse Zaken (BZK), gemeenten, het ministerie van Sociale Zaken en Werkgelegenheid (SZW) en de Vereniging Nederlandse Gemeenten (VNG). Het project heeft tot doel invulling te geven aan de verantwoordelijkheid van gemeenten rond informatieveiligheid en domein specifieke aspecten.

1.2 Achtergrond

De kern van ENSIA is dat de gemeentelijke organisatie transparant is en verantwoording aflegt over de wijze waarop zij in control is op onder andere het thema 'informatieveiligheid'. Die verantwoording legt de gemeentelijke organisatie af aan haar eigen toezichthouder, in casu de gemeenteraad. Gemeenten hebben over dit principe in de algemene ledenvergadering van de VNG van november 2013 overeenstemming bereikt.

Gemeenten (College van B&W) leggen niet alleen verantwoording af aan de eigen toezichthouder (de Gemeenteraad). Van oudsher bestonden verantwoordingsverplichtingen ten aanzien van verschillende ministeries.

De gemeente kent een politieke- en een ambtelijke organisatie. De verantwoording over informatieveiligheid wordt geoperationaliseerd door de ambtelijke organisatie. In deze zin speelt de gemeentesecretaris, als ambtelijk verantwoordelijke, een belangrijke rol in de governance van ENSIA.

ENSIA integreert al deze typen verantwoordingen in één werkwijze en met één eenduidige taal: de BIO (voorheen BIG). Alle bestaande verantwoordingen zijn in goed overleg met de toezichthouders aangepast op ENSIA.

Voor alle verantwoordingen geldt dat waar mogelijk is, wordt aangesloten op de BIO. Daarnaast blijft de noodzaak om domein specifieke toezichtinformatie te blijven leveren. De verantwoording in ENSIA betreft in 2024:

- Basisregistratie Personen (BRP)
- Wet- en regelgeving Reisdocumenten (PUN en PNIK)
- Digitale persoonsidentificatie (DigiD)
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Ondergrond (BRO)
- de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)
- BIO versie 1.04zv

De onderdelen DigiD en Suwinet zijn onderdeel van de IT-audit. De ENSIA-rapportages van de gemeenten en de bijbehorende assurancerapporten worden conform gemaakte afspraken ter beschikking gesteld aan de betreffende toezichthouders (DigiD – Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Logius) / Suwinet – Ministerie van Sociale Zaken en Werkgelegenheid (BKWI)).

De reikwijdte van de Collegeverklaring over 2024 en daarmee de assurance-opdracht van de IT-auditor is ten opzichte van voorgaande jaren gewijzigd door de introductie van de toetsing op een vijftal normen op werking in het kader van de verantwoording over DigiD.

1.3 Toepassingsgebied ENSIA

ENSIA is alleen van toepassing op gemeenten[1]. De collegeverklaring gaat over DigiD en Suwi, waarbij de ENSIA-vragenlijst de in de vorige paragrafen genoemde aandachtsgebieden afdekt. Met ingang van 2017 is het DigiD-assessment voor gemeenten opgegaan in ENSIA. Daarnaast blijven in geval van nieuwe DigiD-aansluitingen de aansluitvoorwaarden van Logius ongewijzigd, waardoor binnen twee maanden na aansluiting ook voor gemeenten een regulier DigiD-assessment moet worden uitgevoerd.

[1] ENSIA is voor de BAG, BGT en BRO ook van toepassing op de waterschappen en de provincies. Het geheel valt vooralsnog buiten de reikwijdte van door IT-auditors uit te voeren assurance-werkzaamheden.

Daarna wordt de DigiD aansluiting opgenomen in de ENSIA verantwoording. Zie hiervoor website van Logius: https://logius.nl/diensten/digid/ict-beveiligingsassessments-digid/hoe-werkt-het .

Met Suwinet wordt alleen gerefereerd aan de gemeente als afnemer. Als afnemer kent Suwinet 'Suwi inkijk', 'Suwi inlezen', 'Digitaal Klantdossier (DKD) inlezen' en 'Wet gemeentelijke schuldhulpverlening' (WSG). Het Ketenoverleg heeft hiervoor als meest recente document de *Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2022* uitgebracht. Hierin is het vereiste, adequate niveau van informatiebeveiliging gebaseerd op het BIO normenkader zodat verantwoording op basis daarvan moet plaatsvinden. Voor het verantwoordingjaar 2024 zijn hierin geen wijzigingen in de verantwoordingsrichtlijn doorgevoerd.

In het kader van ENSIA zijn in overleg tussen stelselhouders nadere afspraken gemaakt omtrent het te hanteren normenkader alsmede het feit dat de verantwoording over het gebruik van Suwinet en de bijbehorende assurance zich richt op opzet en bestaan van de maatregelen per 31 december van het verslagjaar.[1]

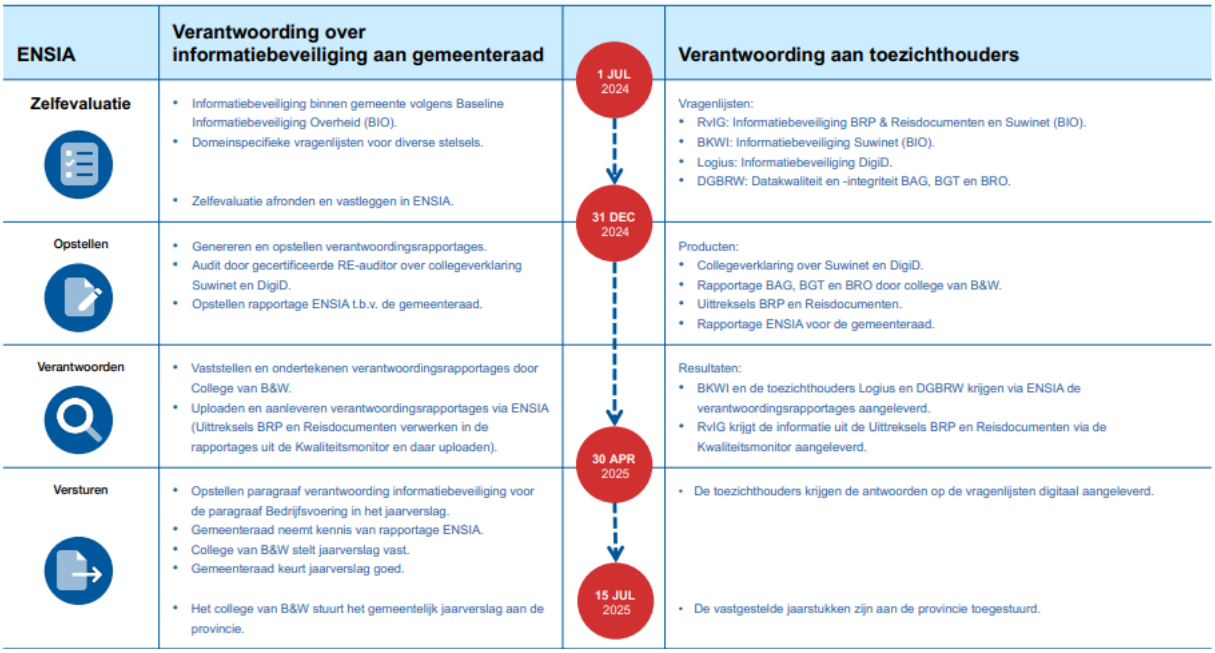
1.4 Werkwijze ENSIA

ENSIA ondersteunt zowel de verantwoording aan de gemeenteraad (voorheen aangeduid als het horizontale verantwoordingsproces) als de verantwoording aan de toezichthouders (voorheen aangeduid als het verticale verantwoordingsproces). Hieronder is het ENSIA-proces grafisch weergegeven. Meer informatie omtrent ENSIA en de werkwijze van de gemeenten is terug te vinden op www.ensia.nl. Het verantwoordingsproces gericht op de gemeenteraad vormt een belangrijke basis voor de IT-auditor en de gemeente:

Het verantwoordingsproces van de gemeente ziet er in hoofdlijnen als volgt uit:

[1] Zie ook NOREA Handreiking Suwi (in kader ENSIA) voor IT-auditors (RE) versie 1.0

Hierbij doorloopt de gemeenten voor 2024 in hoofdlijnen het weergegeven proces:



1.5 Toelichting zelfevaluatie en tool gemeenten

Via de online ENSIA tool is er een zelfevaluatie vragenlijst beschikbaar voor informatieveiligheid bij gemeenten over de volle breedte van de BIO met inbegrip van domein specifieke aspecten.

<u>Zelfevaluatie informatiebeveiliging</u>
Met de ingevulde zelfevaluatievragenlijst geeft het college aan in hoeverre de beheersingsmaatregelen aan de van kracht zijnde beveiligingsnormen voldoen.

<u>Zelfevaluatie en verantwoording domeinspecifieke aspecten BRP, PUN, BAG, BGT, BRO en AVG.</u>
Met de ingevulde zelfevaluatie domein specifieke vragenlijsten voor de BRP, PUN, BAG, BGT, BRO en BIO (algemeen) geeft het college aan in hoeverre de domein specifieke beheersingsmaatregelen (anders dan voor informatieveiligheid) zijn ingericht. Op basis van de zelfevaluatievragenlijsten voor de BAG, BGT en BRO, BRP en PUN alsmede BIO worden met behulp van de ENSIA-tooling de bestuurlijke rapportages voor de genoemde basisregistraties samengesteld, die als basis dienen voor de verantwoording door gemeenten.

<u>Zelfevaluatie DigiD en Suwinet</u>
De zelfevaluaties voor DigiD en Suwinet ondersteunen de interne beheersprocessen van de gemeente inclusief de verantwoordingen die daarover worden afgelegd. De Collegeverklaring is hier mede op gebaseerd. De Collegeverklaring inclusief de bijlagen DigiD en Suwinet vormt object van onderzoek van de IT-auditor. De auditor verstrekt het assurancerapport op basis van de uitgevoerde werkzaamheden.

Bij de beoordeling van deze zelfevaluaties wordt gebruik gemaakt van de door de gemeente uitgevoerde en gedocumenteerde werkzaamheden over de opzet en het bestaan van de beheersingsmaatregelen alsmede de werking van een vijftal maatregelen in het kader van de verantwoording over DigiD[1].

[1] Zie ook NOREA Handreiking DigiD-assessments 2024

2 Handreiking

Doel van deze handreiking is de IT-auditor een uniform toetsingskader te bieden voor het uitvoeren van een ENSIA-audit op basis van de beschikbare normen. Dit kader geldt voor controlejaar 2024. Deze handreiking dient te worden gelezen in samenhang met de NOREA Handreiking DigiD-assessment 2024 en NOREA Handreiking Suwi (in kader ENSIA) voor IT-auditors (RE's) versie 1.0 en eventuele gepubliceerde F.A.Q.'s.

ENSIA-ontwikkelingen en ervaringen uit de praktijk worden, indien nodig, vertaald in navolgende versies van deze handreiking en waar nodig de daarmee samenhangende handreikingen. De handreiking biedt een eenduidig en richtinggevend referentiekader voor de werkzaamheden van de IT-auditor om hiermee te voorkomen dat er grote verschillen ontstaan in zowel de mate van diepgang bij uitvoering van de IT-audits, als bij het beoordelen van afwijkingen. Het is daarom uitdrukkelijk niet de bedoeling van deze handreiking voor de audit andere of aanvullende vereisten op de geldende richtlijnen, standaarden of ten opzichte van bijvoorbeeld de NCSC-richtlijnen af te wijken[1].

Bij verschillen van inzicht is het primair aan de betrokken auditors om in overleg tot een oplossing te komen. (Vertegenwoordigers van) de NOREA werkgroep ENSIA, of de werkgroep DigiD kunnen daarbij eventueel als gesprekspartner deelnemen, altijd vanuit het perspectief van ENSIA (dus gericht op het geven van assurance). Voor substantiële meningsverschillen heeft de NOREA een procedure vastgesteld waarmee (via de Vaktechnische Commissie) een collegiaal standpunt wordt gegeven (zie ook hierna paragrafen over Opdrachtgerichte Kwaliteitsborging en Consultatie).

2.1 Opzet Handreiking 2024

Met ingang van het verantwoordingsjaar 2024 is voor een aangepaste opzet van de Handreiking gekozen. Tegen de achtergrond van de ontwikkelingen die bij de verschillende onder de Collegeverklaring, en daarmee de uitvoering van IT-audits, vallende stelsels is gekozen voor een onderverdeling in drie, separaat toepasbare, Handreikingen:

a. De onderhavige Handreiking specifiek gericht op het ENSIA-proces;
b. De NOREA Handreiking Suwinet voor gemeenten 2024, versie 1.0 (zie NOREA-website_
c. De NOREA Handreiking DigiD-assessments versie 2024 (zie NOREA-website: https://www.norea.nl/uploads/bfile/be186505-ac8e-46a6-9a9c-8713d6ed0403

2.2 Verantwoordingsproces

Verantwoordelijkheden gemeente

In het kader van het ENSIA-verantwoordingsproces gelden de navolgende specifieke verantwoordelijkheden voor de gemeente:

- De gemeente is verantwoordelijk voor het uitvoeren van de zelfevaluatie per assessmentplichtige DigiD-aansluiting waarvan de gemeente de houder is. Voor DigiD-aansluitingen die op naam staan van samenwerkingsverbanden waaraan de gemeente deelneemt, dienen de samenwerkingsverbanden zelfstandig de voorgeschreven DigiD-assessments per aansluiting te laten uitvoeren.
- Praktijk is dat de werkzaamheden in het domein werk en inkomen belegd kunnen zijn bij diverse samenwerkingsverbanden. Ongeacht de organisatie van de samenwerkingsverbanden blijft het gemeentebestuur verantwoordelijk voor het gebruik van Suwinet. De gemeente dient e.e.a. te betrekken in de zelfevaluatie. Zie bijlage 4 voor een nadere toelichting.
- Bij eventuele bevindingen in het kader van de zelfevaluatie dient de gemeente een verbeterplan op te stellen. Dit verbeterplan dient concrete verbetermaatregelen te omvatten voor alle hiervoor bedoelde bevindingen.

[1] De hier bedoelde aanpassingen vallen onder de gecombineerde verantwoordelijkheid van stelselhouders, stelselbeheerders en toezichthouders.

Verantwoordingsproces in detail
Het verantwoordingsproces begint met het invullen van de zelfevaluatie vragenlijst informatiebeveiliging 2024. De vragenlijst informatiebeveiliging is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO) aangevuld met domeinspecifieke aspecten.

Voor DigiD is omwille van de specifiek geldende normen, een aparte vragenlijst voor de zelfevaluatie beschikbaar. Per assessmentplichtige DigiD-aansluiting moet een vragenlijst worden ingevuld. In tegenstelling tot de andere verantwoordingen in ENSIA is DigiD namelijk te specifiek om in BIO-normen te kunnen worden vervat (vertaald).

Voor alle vragen geldt dat de gemeente de ondersteunende assurance-informatie (over opzet en bestaan (en vijftal normen werking DigiD) van de beheersingsmaatregelen) dient te verzamelen en gestructureerd toegankelijk dient te maken. Wat betreft de wijze van documentatie zijn aanwijzingen gegeven vanuit VNG-realisatie. Zie hiervoor: https://ensia.nl

De gemeente heeft tot en met **31 december 2024** de tijd om de vragenlijsten van de zelfevaluatie in te vullen en in te leveren. Inleveren kan pas als alle vragen beantwoord zijn. Voor verwerking van informatie en documentatie (inzake de werking van een vijftal maatregelen) DigiD zie Bijlage 3: ENSIA-specifieke aandachtspunten DigiD.

Ingeleverde vragenlijsten kunnen (in principe) niet meer worden gewijzigd. Indien bepaalde antwoorden toch nog veranderen dan dient de ENSIA-coördinator hiervoor contact op te nemen met de beheerder van het zelfevaluatietool (Beheerteam ENSIA). Door tussenkomst van de beheerder kunnen naderhand wijzigingen worden doorgevoerd. Het spreekt voor zich dat dit zeer terughoudend zal worden toegestaan.

In het kader van het invullen van de DigiD-vragenlijst per aansluiting dienen de uitkomsten door de ambtelijke organisatie van de gemeente te worden beoordeeld. Hierbij gaat het om de vragenlijst en de door de gemeente verzamelde ondersteunende assurance-informatie waaronder de ontvangen assurancerapporten. Deze beoordeling leidt tot de beantwoording in de ENSIA-tool en leidt tot een daartoe opgenomen rapportageformat 'Bijlage DigiD bij de Collegeverklaring ENSIA'.

Voor Suwinet geldt een vergelijkbaar proces waarbij op basis van de antwoorden in de ENSIA tool een specifieke Suwinet-bijlage bij de Collegeverklaring ENSIA' wordt gegenereerd. In tegenstelling tot DigiD worden bij Suwinet de van derden ontvangen assurancerapporten niet ter beschikking gesteld aan de toezichthouder.

Op basis van de uitkomsten van de zelfevaluatie in het kader van het verwerken van de antwoorden in de ENSIA-tool wordt door de gemeente de Collegeverklaring Informatiebeveiliging opgesteld. In de collegeverklaring wordt – mede vanwege de vertrouwelijke aard van de informatie – een samenvatting van de bevindingen op hoofdlijnen opgenomen.

De Collegeverklaring ENSIA en de hiervoor genoemde bijlagen bij de Collegeverklaring ENSIA vormen daarmee het object van controle voor de IT-auditor. Dit is de 'assertion based' benadering kenmerkend voor ENSIA. De IT-auditor zal zich daarbij mede richten op de inhoud van de Collegeverklaring en de door de gemeente verzamelde ondersteunende informatie ten behoeve van de assurance-werkzaamheden over de Collegeverklaring ENSIA, meer in het bijzonder de DigiD en Suwinet normen. Voor de validatie van deze opgeleverde informatie zal de IT-auditor ook eigen testwerk doen (re-performances/ aanvullende werkzaamheden waar nodig). De uitkomsten van de IT-audit legt de IT-auditor vast in een assurancerapport.

De gemeente levert vóór 1 mei 2025[1] het assurancerapport, de gewaarmerkte Collegeverklaring ENSIA met bijbehorende bijlagen bij de Collegeverklaring ENSIA en de ontvangen assurancerapporten inzake DigiD op aan de toezichthouder. Deze documenten kunnen tot deze datum met behulp van het ENSIA-tool ter beschikking gesteld worden.

[1] Voor het verantwoordingsjaar 2024 wordt vooralsnog uitgegaan van het gebruikelijke verantwoordingstraject.

Verantwoordelijkheden IT-auditor
De IT-auditor dient er voor te zorgen dat de betreffende documenten door hem gewaarmerkt zijn, zoals aangegeven in de formats voor collegeverklaring en assurancerapport (zie ook bijlage 5 over het waarmerken van stukken).

De IT-auditor dient bij de planning en uitvoering van de werkzaamheden rekening te houden met de doorlooptijd van de formele behandeling van de Collegeverklaring ENSIA (o.a. (voor-) bespreking met ambtelijk verantwoordelijken, portefeuillehouder(s) en collegebehandeling) Daarnaast dient rekening gehouden te worden met eventuele ondersteuning bij besprekingen met de raadscommissie(s) en gemeenteraad. Deze laatste hoeven de tijdige indiening van de volledige verantwoording via het ENSIA-tool niet in de weg te staan.

De IT-auditor kan eventueel erop toe te zien dat de gemeente de door hem gewaarmerkte documenten op de juiste wijze in de ENSIA-tool opneemt in het kader van het verantwoordingsproces. Dit kan bijvoorbeeld door de gemeente een schermprint te laten aanleveren van de upload in de ENSIA-tool.

Nadere informatie over het verantwoordingsproces is opgenomen in de Handleiding ENSIA-tool voor gemeenten (zie www.ensia.nl).

2.3 Wat verandert er voor de IT-auditor

Voor de IT-auditor verandert ten aanzien van zijn verantwoordelijkheid voor het goed voorbereiden en inrichten van zijn controle in principe niets. Met dien verstande dat elk audit project om een specifieke voorbereiding vraagt waarbij rekening wordt gehouden met het onderscheid tussen 'directe opdrachtenopdrachten' en 'attest-opdrachten'.

Bij de methode van 'directe opdrachten(zoals bij de DigiD assessments gebruikelijk) is de IT-auditor zelf in 'the lead' om zelf te komen tot een meting of evaluatie van het object van onderzoek aan de hand van de geldende criteria. Hierbij is voorbereiding in de vorm van het zelfstandig opvragen van stukken belangrijk.

Bij ENSIA betreft het een attest-opdracht op basis van de collegeverklaring en bijlagen ('attestation based audit'/ 'assertion based audit').Hierbij zijn de ingevulde vragenlijsten (de zelfevaluaties) in de ENSIA-tool en de door de gemeente gedocumenteerde ondersteunende assurance-informatie voor de IT-auditor een mogelijk startpunt die assurance-informatie biedt tijdens het veldwerk.

Op basis van de eigen risicoanalyse, zoals die voor elk audit project wordt uitgevoerd, stelt de IT-auditor zelfstandig o.b.v. risicoanalyse vast wat de diepgang van zijn werkzaamheden zullen zijn gegeven de veronderstelde kwaliteit van oplevering van de gegevensverzameling. Hierbij dient hij ook kennis te nemen van de andere onderdelen van het ENSIA-proces en de eventueel in samenhang daarmee uitgebrachte rapportages om eventuele aanvullende aandachtspunten voor zijn werkzaamheden te kunnen vaststellen. Hij zal nog eigen waarnemingen moeten uitvoeren om het aangeleverde materiaal te valideren

Het IT-audit project bestaat bij ENSIA met name ook uit het uitvoeren van procescontroles. De procescontroles geven de IT-auditor de mogelijkheid ook -en met name tussentijds- te beoordelen of de opgeleverde resultaten voldoen aan daaraan te stellen eisen. Daarbij valt te denken aan de authenticiteit van het aangereikte basismateriaal, de bruikbaarheid en de compleetheid van het aangereikte basismateriaal bij de onderscheiden onderdelen. In deze setting toetst de IT-auditor tussentijds en blijft objectief en onafhankelijk, terwijl de gemeente tijdig in de gelegenheid wordt gesteld verbeteringen door te voeren. De IT-auditor is daarbij niet inhoudelijk betrokken ter voorkoming van zelftoetsing. Bij DigiD worden ook technische testen op instellingen in de applicatie, platform en netwerk uitgevoerd, die herhaalbaar uitgevoerd moeten kunnen worden.

Ook het aspect van risico-inschatting is van belang. Op basis hiervan bepaalt de auditor met welke diepgang de controles van de -door de gemeente in het kader van de self-assessment beoordeelde normen- moeten plaatsvinden.

2.4 Formele aspecten van de assurance-opdracht

Een ENSIA-audit betreft een assurance-opdracht gericht op het geven van een oordeel met een redelijke mate van zekerheid, conform Richtlijn 3000 A (Attestopdracht). Het college van burgemeesters en wethouders komt met een collegeverklaring waarover de IT-auditor met redelijke mate van zekerheid een oordeel geeft. Beoogde gebruikers van deze collegeverklaring en het assurancerapport (oordeel) van de IT-auditor zijn de gemeenteraad en de departementen die toezien op de informatieveiligheid van DigiD en Suwinet. De uitvoering van de ENSIA audit dient in opdracht van het college plaats te vinden.

Doel van de ENSIA-audit is het verkrijgen van voldoende geschikte assurance-informatie om een oordeel met redelijke mate van zekerheid te verschaffen of de Collegeverklaring ENSIA inzake informatiebeveiliging van DigiD en Suwinet (inclusief de bijlage(n) bij de Collegeverklaring ENSIA DigiD en Suwinet waarnaar in de collegeverklaring wordt verwezen) van de gemeente, in alle van materieel belang zijnde aspecten, juist is. Hierbij zijn de eisen vanuit de regelgeving voor DigiD en Suwinet leidend.

De criteria voor een ENSIA IT-audit betreffen de normen inzake DigiD (Norm ICT-beveiligings-assessments DigiD versie 2024[1] en Suwinet voor gemeenten versie 1.0. De criteria worden ook in de collegeverklaring kenbaar gemaakt en zijn daarmee toegankelijk voor de gebruikers.

Het gaat om opzet en bestaan van de maatregelen per 31 december 2024 alsmede opzet, bestaan en werking van een aantal maatregelen (over een periode van 6 maanden – periode 1 juli – 31 december 2024) in het kader van DigiD-assessments[2]. Eventuele veranderingen / verbetermaatregelen in de periode tussen 31 december 2024 en de datum van afgeven van het assurancerapport dient het College in principe in de collegeverklaring toe te lichten[3]. De verbetermaatregelen / het verbeterplan betrekt de auditor in zijn onderzoek.

De NOREA beroepsorganisatie hanteert overigens het standpunt dat uitsluitend een herhaalde beoordeling van opzet en bestaan op den duur een schijnzekerheid impliceert als niet ook de werking in de beoordeling wordt betrokken. Het invoeringstraject daarvan vraagt echter de nodige voorbereidingstijd. Hiervoor wordt in het kader van de ENSIA-audit over 2024 een eerste stap gezet.

2.5 Ethische voorschriften en beroepsregels

De IT-auditor dient het Reglement Gedragscode ('Code of Ethics') na te leven. Bij een actieve betrokkenheid bij de inrichting van of uitvoering bij informatiebeveiliging is dit een risico ten aanzien van het fundamentele beginsel objectiviteit (inclusief onafhankelijkheid). Idem voor actieve betrokkenheid bij de uitvoering van de self-assessment die door het college moet worden uitgevoerd.

2.6 Pre-audit ENSIA

De ENSIA-vragenlijsten zijn vanaf 1 juli 2024 beschikbaar voor de gemeenten en zij hebben tot 31 december 2024 de tijd om de vragenlijsten in te vullen en op te leveren[4]. Inleveren kan pas als alle vragen zijn beantwoord. De IT-audit kan (pas) worden afgerond nadat de vragenlijsten zijn ingeleverd en de collegeverklaring is opgesteld door de gemeente. De gemeente heeft echter vaak de behoefte om tussentijds een terugkoppeling te ontvangen van de IT-auditor over de status van DigiD en Suwinet binnen de gemeente. Het advies is om een zogenaamde pre-audit of interim audit af te spreken en uit te voeren waarbij de IT-auditor DigiD en Suwinet-normen tussentijds toetst, het proces van oplevering beoordeelt en de uitkomsten rapporteert aan de gemeente. De gemeente wordt op

[1] Zie voor de testaanpakde Handreiking DigiD-assessment 2024 d.d. 1 juli 2024 (en eventuele aanvullende FAQ).

[2] Idem Zie NOREA-Handreiking DigiD assessments 2024 en Bijlage 3.

[3] Teneinde de uniformiteit en eenduidigheid van Collegeverklaringen te waarborgen kan e.e.a. ook in het verbeterplan van de gemeente (gebaseerd op de stand per 31 december) tot uitdrukking gebracht worden. De IT-auditor dient dan een paragraaf ter benadrukking van aangelegenheden op te nemen in het assurancerapport waarin hierop wordt gewezen.

[4] Zie ook Bijlage 3 en ENSIA-guidance voor verwerking informatie werking na 31-12-2024

deze wijze in de gelegenheid gesteld de nodige verbeteringen door te voeren alvorens de vragenlijsten definitief worden ingeleverd.

Het verdient aanbeveling om de bevindingen en aanbevelingen in het kader van de pre-audit ENSIA vast te leggen in een rapport of managementletter ten behoeve van de gemeente.

2.7 Opdrachtaanvaarding en continuering

Vereisten vanuit de Richtlijn Opdrachtaanvaarding zijn onverkort van toepassing. Het object van onderzoek betreft de Collegeverklaring en bijlagen waarin de informatiebeveiliging centraal staat. Competentie en capaciteit van het IT-auditopdrachtteam op dit terrein is dan ook een randvoorwaarde. Ervaring met het uitvoering van DigiD-assessments en/ of Suwi-audits alsmede kennis van het gemeentelijke domein zijn daarbij wenselijk.

2.8 Kwaliteitsbeheersing

Het Reglement Kwaliteitsbeheersing NOREA (RKBN) is van toepassing, dit komt ook tot uitdrukking in het assurancerapport.

Gegeven de aard van de opdracht, het maatschappelijke belang en mogelijk brede verspreidingskring van de Collegeverklaring en het assurancerapport (o.a. als gevolg van de Wet open overheid) dient voor ENSIA-audits expliciet een opdrachtgerichte kwaliteitsbeoordeling (OKB) overwogen te worden.

Overwegingen hierbij kunnen zijn (niet limitatieve opsomming):

a. Stelselgerelateerd: Grote wijzigingen in het ENSIA-stelsel zoals
    a. Toevoegen van stelsels die onder reikwijdte collegeverklaring en auditverplichting vallen;
    b. Aanpassingen in wijze verantwoorden één of meer stelsels die onder collegeverklaring / auditverplichting vallen;
    c. Aanpassingen in auditverplichting één of meer stelsels die onder collegeverklaring / auditverplichting vallen.
b. Klantgerelateerd: Aspecten als:
    a. Nieuwe klant voor auditorganisatie (eerstejaars audit);
    b. Ervaringen met klant uit voorgaande jaren;
    c. Grote wijzigingen bij klant:
        i. Overwegingen met betrekking tot personele wijzigingen bij klant;
        ii. Wijzigingen in organisatie met betrekking tot uitvoering van bedrijfsprocessen bij de klant (bijv. meer / minder uitbesteden);
c. In relatie tot organisatie auditor:
    a. Personele bezetting opdracht:
        i. Langdurige betrokkenheid;
        ii. Ervaring met (onderdelen van) ENSIA;
    b. Interne beleid kwaliteitsborging.

Hierbij is een eenduidig gedocumenteerde risico-inschatting van de audit-organisatie leidend. De auditor dient de overwegingen ter zake in het dossier vast te leggen. Zie verder ook NOREA Handreiking opdrachtgerichte kwaliteitsbeoordeling[1].

Een opdrachtgerichte kwaliteitsbeoordeling omvat in het algemeen een bespreking met de voor de opdracht verantwoordelijk professional, een onderzoek van informatie dat object van het onderzoek is en van het assurancerapport en in het bijzonder de juistheid daarvan. Het omvat ook het onderzoeken van geselecteerde dossierstukken die betrekking hebben op de belangrijke standpunten die het opdrachtteam heeft ingenomen en de eindoordelen en adviezen die zijn gevormd. De OKB moet zijn afgerond voordat het rapport wordt afgegeven.

[1] https://www.norea.nl/uploads/bfile/8112c9d2-1a37-4d11-aef6-b3ea2f3c7f53

2.9 Risico-inschatting

De IT-auditor dient zowel bij de opdrachtaanvaarding als tijdens de opdracht op basis van zijn inzicht risico's op afwijkingen van materieel belang in de informatie over het onderzoeksobject te identificeren en in te schatten. De schaal van inschatting is Hoog, Midden of Laag. Een veel gebruikte benadering hierbij is die van het audit controle risico (ACR) voor de bepaling van de auditstrategie. Daarbij is het audit controle risico een product van Interne Controle Risico (ICR), Inherente Risico (IHR) en Detectierisico (DR). De ENSIA-opdracht is gezien het feit dat het de decentrale overheid betreft en het feit dat de opdracht als complex wordt aangemerkt, te bestempelen als een opdracht met een gemiddeld tot hoog risico op afwijkingen van materieel belang.

De ACR van deze opdracht moet op een laag niveau gebracht worden om een oordeel met redelijke mate van zekerheid te kunnen afgeven. Dat wil zeggen dat voorkomen moet worden dat ten onrechte een foutief oordeel wordt afgegeven. Het betreft het:

- Inherent Risico: betreft een inschatting van de complexiteit van de te controleren objecten, in deze fase van release: DigiD en Suwinet;
- Interne Controle Risico: betreft een inschatting van de kwaliteit van de beheeromgeving van de gemeente bij de totstandkoming van de collegeverklaring op basis van de zelfevaluatie en het proces van zelfevaluatie;
- Detectierisico: is de resultante en stelt eisen aan de kwaliteit van de eigen auditorganisatie en de aard en omvang van de controlewerkzaamheden om fouten (tijdig) te ontdekken.

Omdat zowel ICR en IHR veelal Midden tot Hoog worden ingeschat zal het DR Midden tot Laag moeten zijn. Dit betekent dat hierop gerichte controlewerkzaamheden hier expliciet op ingericht moeten worden.

De auditor dient deze overwegingen ter zake vast te leggen in zijn dossier.

2.10 Het verkrijgen van assurance-informatie

De collegeverklaring komt tot stand door een self-assessment dat wordt uitgevoerd met behulp van de ENSIA tool betiteld als ' zelfevaluatie'. Dit kan door de IT-auditor worden gebruikt als startpunt voor zijn audit. In beginsel is hierin de beoordeling vastgelegd met betrekking tot de individuele normen/ vragen op basis van relevante assurance-informatie die door het college is verzameld[1]. Deze (assurance-)informatie omvat ook voor de IT-auditor assurance-informatie voor zijn oordeel.

Een professioneel kritische houding wordt van de IT-auditor verwacht bij het gebruik van deze informatie. Om zelfstandig tot een oordeel te komen zal de IT-auditor niet alleen de uitkomst van de self-assessment beoordelen maar ook de onderliggende documentatie toetsen en eigen (deel)waarnemingen uitvoeren t.a.v. de implementatie (bestaan) om zelfstandig te bepalen of in opzet en bestaan (bij DigiD ook werking van een aantal maatregelen) voldaan wordt aan de desbetreffende norm. De regels uit de Richtlijn Documentatie (NOREA 230) zijn hier onverkort van toepassing.

Gebruik van of steunen op de werkzaamheden van interne IT-auditors is mogelijk, met inachtneming van de vereisten zoals aangegeven in paragraaf 53-55 van Richtlijn 3000.

Onderdeel van de assurance-informatie is het verkrijgen van een schriftelijke bevestiging van de verantwoordelijke partij met een zo recent als mogelijke datum, voorafgaand aan de datum van het assurancerapport. Deze omvat: een (her)bevestiging van de collegeverklaring dat toegang is verschaft tot relevante informatie en personen; geen kennis is van zaken die op het oordeel een ander licht werpen; alsmede een bevestiging omtrent gebeurtenissen na de periode of het tijdstip waarop de opdracht betrekking heeft.

[1] Uitgangspunt is dat de zelfevaluatie is gebaseerd op / onderbouwd wordt door relevante documentatie. Deze dient door de gemeente op een systematische wijze vastgelegd en gedocumenteerd te worden.

2.11 Uitbesteding door gemeenten

Bij uitbesteding van werkzaamheden door gemeenten zijn de volgende situaties voorzien:

DigiD
Bij het beoordelen van uitbestede taken wordt aangesloten bij de in het kader van DigiD-assessments gebruikelijke werkwijze. Bij het beoordelen van uitbestede taken wordt uitgegaan van de 'carve-out methode'. Hierbij ontvangt de houder (gemeente) een DigiD-assurancerapport (DigiD-assessment) van de externe partij(-en). De IT-auditor van de houder voert daarbij geen onderzoek uit naar de juistheid van de oordelen die zijn vermeld in de rapportage van de derde partijen en neemt ook geen verantwoordelijkheid voor de in die rapportage vermelde oordelen.

Het college verwijst in de bijlage DigiD bij Collegeverklaring ENSIA naar de assurancerapporten van derden voor de desbetreffende onderdelen.

Binnen de ENSIA tooling zijn specifieke faciliteiten opgenomen om de betreffende documenten op te nemen en aan de toezichthouders ter beschikking te stellen.

Suwinet
Gemeenten blijven ook in het geval van uitbesteding en/ of samenwerking met andere organisaties bestuurlijk verantwoordelijkheid voor het gebruik van Suwinet gegevens ten aanzien van hun eigen inwoners en dienen daarover verantwoording af te leggen in ENSIA.

Dit betekent dat de IT-auditor zich met betrekking tot Suwinet ook een oordeel moet vormen over (de verantwoording en bijbehorende oordelen van IT-auditors over) de door de -in het netwerk geïdentificeerde- externe partijen uitgevoerde werkzaamheden en deze in zijn oordeelsvorming moet betrekken , hetzij via de inclusive (**), hetzij via de carve-out benadering waarbij de laatste benadering de voorkeur heeft.

Gebruik van of steunen op werkzaamheden van (interne) IT-auditors is mogelijk met inachtneming van de vereisten zoals aangegeven in paragraaf 53-55 van de Richtlijn 3000. Tevens zal de auditor daarbij aandacht moeten schenken aan de organisatie van de IT-audit (werkzaamheden), competentie van de verantwoordelijk IT-auditor en de geschiktheid van de uitgevoerde werkzaamheden in het kader van de ENSIA-audit.

Zie voor een nadere toelichting bijlage 4 "Overwegingen Audit in samenwerkingsverbanden Suwinet". Het gaat hierbij om overwegingen die betrokken kunnen worden bij het uitvoeren van de werkzaamheden in de samenwerkingsverbanden. Deze mogen echter geen afbreuk doen aan de fundamentele eisen die aan het uitvoeren van de werkzaamheden door de IT-auditor zijn gesteld.

Werkzaamheden auditor
Bij uitbesteding door de gemeente aan een externe partij (samenwerkingsverband / externe leverancier / combinatie van beide) heeft het de voorkeur dat de externe partij een assurancerapport (conform Richtlijn 3000 ,ISAE 3402 of vergelijkbaar) verzorgt dat betrekking heeft op de in het kader van ENSIA gestelde normen. In dit geval wordt de carve-out benadering gevolgd[1].

(**) Indien geen assurancerapport geleverd kan worden dan wordt in opdracht van de gemeente bij de externe partij onderzoek gedaan naar de naleving van de in het kader van ENSIA gestelde normen volgens de inclusive benadering. Dit kan door een door de gemeente ingeschakelde auditor worden gedaan. Dit kan ook de door de gemeente ingeschakelde ENSIA-auditor zijn. Voorwaarde hiervoor is dat de 'contractuele bepalingen' tussen de gemeente en de externe partij dit onderzoek mogelijk maken.

Bij de inclusive-benadering dient (ENSIA-) auditor van de gemeente hiervoor de vaktechnische verantwoordelijkheid te kunnen nemen. Hij dient dit – waar mogelijk in overleg met de auditor van de externe partij – te betrekken in de risicoanalyse, uitwerking van de controle-aanpak, bespreking van bevindingen, etc. en uitvoering van een dossierreview. De inspanning zal beperkter kunnen zijn indien

[1] Zie NOREA-Handreiking DigiD assessments 2024

de auditor van de externe partij werkzaamheden conform de ENSIA-normering en deze handreiking uitvoert en in de rapportage een bijlage opneemt van de uitgevoerde werkzaamheden naar analogie van wat bij een 3402-rapportage type 2 / rapportage conform SOC 2 (beide gericht op opzet bestaan en werking) vereist is[1].

De auditor dient de uitkomsten van de in dit kader uitgevoerde werkzaamheden te betrekken in zijn oordeelsvorming.

Het uiteindelijke streven moet zijn dat de externe partij(-en) een assurancerapport (conform Richtlijn 3000 (en idealiter 3000A) kan leveren. Een ISO 27001 - rapport is voor het doel van ENSIA onvoldoende.

Verbeterplannen
Hoewel de IT-auditor geen oordeel geeft over de toereikendheid (en uitvoering) van het verbeterplan van de gemeente naar aanleiding van eventuele bevindingen / tekortkomingen in het kader van de zelfevaluatie, is het wenselijk dat hij verifieert of de door de gemeente gesignaleerde bevindingen geadresseerd zijn, realistisch zijn en opgenomen in het verbeterplan. Eventuele bevindingen / tekortkomingen dienen onder de aandacht van de opdrachtgever gebracht te worden zodat deze, onder verantwoordelijkheid van het college, betrokken worden in de uitwerking van het verbeterplan en, waar nodig, de collegeverklaring.

2.12 Schriftelijke bevestiging (letter of representation)

Onderdeel van de assurance-informatie is het verkrijgen van een schriftelijke bevestiging van de verantwoordelijke partij (gemeente) zo dicht als praktisch uitvoerbaar is bij, maar niet na, de datum van het assurancerapport.

Deze omvat:
- Een herbevestiging van de collegeverklaring ENSIA;
- Een bevestiging dat toegang is verschaft tot relevante informatie en personen;
- Een bevestiging dat er geen kennis is van zaken die op het oordeel een ander licht werpen;
- Een bevestiging omtrent gebeurtenissen na de periode of het tijdstip waarop de opdracht betrekking heeft tot het moment van afgeven van de bevestiging die van invloed kunnen zijn op de collegeverklaring en de assurance die daarbij wordt afgegeven.

2.13 Het vormen van het oordeel

Bij het vormen van het oordeel worden de bepalingen uit het stramien voor assurance-opdrachten in acht genomen zoals deze zijn vastgelegd voor attest-opdrachten (assertion-based opdrachten).

De beantwoording van de vraag of voldoende en geschikte controle-informatie is verkregen voor het oordeel blijft daarbij onderwerp van professionele oordeelsvorming. Indien onvoldoende en/ of geen geschikte controle-informatie is verkregen brengt de IT-auditor dit tot uitdrukking in de strekking van het assurancerapport (beperking of oordeelonthouding).

Omdat in de collegeverklaring eventueel melding wordt gedaan van verbeterplannen en de IT-auditor hierover geen assurance verschaft (‘Ons oordeel heeft zich niet gericht op deze verbeterplannen en het beleggen en monitoren hiervan’) is het wèl van belang om de eventuele verbeterplannen expliciet in de paragraaf ter benadrukking van aangelegenheden te benoemen.

In die gevallen waarin naar de mening van de IT-auditor de collegeverklaring en bijbehorende bijlagen een getrouw beeld geven van de informatiebeveiliging (rond DigiD en Suwinet) bij de gemeente maar de informatiebeveiliging gebreken vertoont, die op grond van de oordeelsvorming van de IT-auditor dermate belangrijk zijn dat ze fundamenteel zijn voor het begrip van de gebruikers van de collegeverklaring, brengt de IT-auditor in het assurancerapport dit tot uitdrukking in een paragraaf ter benadrukking van aangelegenheden.

[1] Het gaat hierbij om de eisen die aan de inhoud van de betreffende bijlage worden gesteld en **niet** om de beoordeling van opzet, bestaan en werking.

2.14 Het opstellen van het assurancerapport

Voor de ENSIA-audit is gekozen voor een structuur voor het assurancerapport welke aansluit bij de door de NBA (Nederlandse Beroepsorganisatie van Accountants) op basis van de internationale IFAC-standaarden gehanteerde controle standaarden (COS) en daarmee ook op ontwikkelingen in internationaal verband. Hierbij is de Richtlijn 3000A leidend.

In bijlage 2 zijn de formats assurancerapporten opgenomen. Hieraan zijn voorbeeldteksten toegevoegd voor een oordeel met beperking/ oordeelonthouding. Daarnaast is in de formats assurancerapporten meer expliciet opgenomen op welk gebruik van Suwinet gegevens en welke DigiD aansluitingen het oordeel betrekking heeft.

Bij het door de IT-auditor ondertekende assurancerapport wordt ook de door de IT-auditor gewaarmerkte collegeverklaring en daarbij behorende bijlagen gevoegd. Deze set wordt door de gemeente gebruikt in het kader van het afleggen van verantwoording aan de toezichthouders (zie paragraaf 2.1 Verantwoordingsproces).

Nadere toelichting:
Bij assurancerapporten bij serviceorganisaties is het vereist dat bij het toetsen van de werking ook een bijlage wordt toegevoegd met een beschrijving van de uitgevoerde toetsingen van de interne beheersingsmaatregelen en de resultaten daarvan. De ENSIA-audit betreft een type 2 audit (opzet en bestaan aangevuld met toetsing op werking voor enkele DigiD-normen). Daarnaast is het doel en de doelgroep anders dan bij een ISAE3402-rapport.

Het opnemen van een bijlage met de beschrijving van uitgevoerde werkzaamheden is dan ook niet verplicht, doch optioneel.

Als gerapporteerd wordt binnen een samenwerkingsverband waarbij andere auditors gebruik willen maken van de rapportage en de uitgevoerde werkzaamheden, dan wordt aangeraden wel zo'n bijlage toe te voegen om de afstemming over de uitgevoerde werkzaamheden te faciliteren.

2.15 Overige rapportages

Het is wenselijk dat de IT-auditor (overige) bevindingen en aanbevelingen naar aanleiding van de uitgevoerde werkzaamheden die ten grondslag hebben gelegen aan het assurancerapport nader uitwerkt in een separate rapportage ten behoeve van de gemeente.

2.16 Documentatie

De IT-auditor dient tijdig opdrachtdocumentatie op te stellen die een vastlegging van de basis voor het assurancerapport verschaft. Richtlijn Documentatie (230) is onverkort van toepassing (inclusief 60 dagen termijn). Het dossier van de IT-auditor is zelfstandig leesbaar. Een integrale verwijzing naar de zelfevaluatietool gehanteerd door het college is niet toegestaan.

Evenmin is een vastlegging door de IT-auditor in de ENSIA-tool en / of andere door de gemeente ten behoeve van het verzamelen en vastleggen van assurance-informatie gebruikte systemen toegestaan aangezien deze geïnterpreteerd kunnen worden als een (goedkeurend) oordeel met betrekking tot het betreffende deelonderwerp / vraag.

2.17 Consultatie

Indien een auditor1 in het kader van de uitvoering van ENSIA-opdrachten bij meerdere klanten systematisch wil afwijken van Handreikingen / formats voorgeschreven door stelselhouder(s) / stelselbeheerder(s) / toezichthouder(s) of van de onderhavige Handreiking dient de auditor dit tijdig af te stemmen met NOREA.

[1] Hieronder te verstaan auditorganisatie en / of individuele auditor.

Op basis van een door de auditor concreet uitgewerkt voorstel zal onder verantwoordelijkheid van het bestuur van NOREA door ter zake deskundige leden een beoordeling plaatsvinden. Hierbij zullen, waar nodig, overige gremia binnen NOREA waaronder de Vaktechnische Commissie en het bestuur betrokken worden. Tevens zal, waar nodig, afstemming plaatsvinden met stelselhouder(s) / stelselbeheerder(s) / toezichthouder(s).

De uitkomsten van de beoordeling worden meegedeeld aan de auditor en zijn bepalend voor de verdere uitvoering van zijn werkzaamheden.

Waar nodig vindt communicatie in breder verband plaats. Denk daarbij aan alle bij de uitvoering van ENSIA-opdrachten betrokken auditors / alle leden NOREA (verantwoordelijkheid NOREA) en / of stelselhouder(s) / stelselbeheerder(s) / toezichthouder(s) en gemeenten en hun dienstverleners. (verantwoordelijkheid ENSIA-gremia).

De mogelijkheid tot afstemming staat ook open in het kader van de uitvoering van individuele opdrachten.

3 Tot slot

De ENSIA-audit maakt onderdeel uit van een breder overheidsinitiatief om de veiligheid van digitale dienstverlening te vergroten, maar is zeker niet het enige middel. Blijvende managementaandacht voor de risico's van digitale dienstverlening en het treffen van de juiste beheersingsmaatregelen is van groot belang. De IT-auditor betrekt deze context (de 'controle omgeving') wel bij zijn auditaanpak, maar voert daar in het kader van de ENSIA-audit geen specifiek onderzoek op uit.

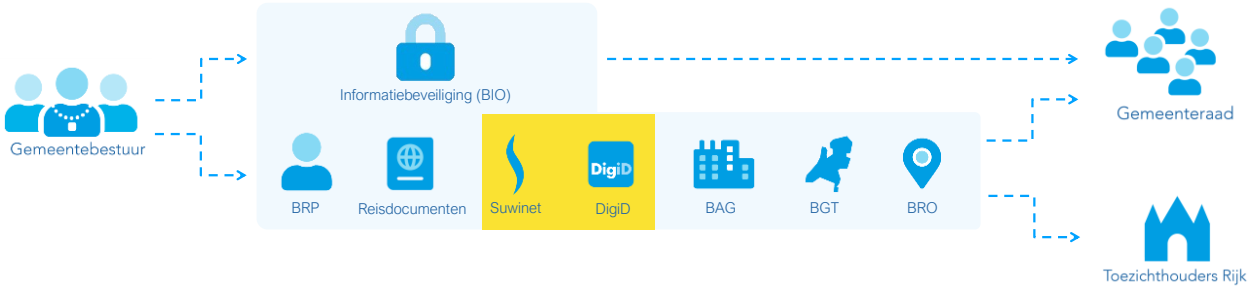
4 Bijlagen

[LOGO Gemeente]

4.1 Bijlage 1: Formats Collegeverklaringen en bijlagen

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente <gemeente>



Collegeverklaring informatiebeveiliging DigiD en Suwinet 2024

Gemeente <gemeente>

Doel en achtergrond verklaring

De aansluitingen die we als gemeente voor DigiD en Suwinet hebben, vereisen dat voorzieningen moeten zijn beveiligd en (privacygevoelige) data moet worden beschermd tegen onrechtmatig gebruik. De gemeente treft interne beheersingsmaatregelen om veilig gebruik te maken van deze aansluitingen.

Met deze verklaring geven wij, het College van Burgemeester en Wethouders, aan in welke mate de gemeente voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet. Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA[15] en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen gebaseerd op de door de toezichthouder geselecteerde eisen uit de 'Baseline Informatiebeveiliging Overheid' versie 1.04zv voor Suwinet en de 'Norm ICT-beveiligingsassessments DigiD versie 3.0' van Logius. De inhoud van deze collegeverklaring is getoetst door een onafhankelijke IT-auditor/RE.

Deze verklaring is bestemd voor de toezichthouders van DigiD en Suwinet, te weten Logius, en alsmede de stelselhouder: het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties en de toezichthouder van Suwinet, te weten het Ministerie van Sociale Zaken en Werkgelegenheid via het Bureau Keteninformatie Werk en Inkomen (BKWI).

Reikwijdte en diepgang verklaring

De aansluitingen die we als gemeentelijke organisatie voor DigiD en Suwinet hebben, vereisen dat onze voorzieningen moeten zijn beveiligd en dat (privacygevoelige) data moet worden beschermd tegen onrechtmatig gebruik. Hiervoor stellen de stelselhouders een aantal informatiebeveiligingsnormen verplicht. De gemeentelijke organisatie moet interne beheersingsmaatregelen treffen om te voldoen aan deze gestelde normen teneinde gebruik te mogen (blijven) maken van deze aansluitingen.

De zelfevaluatie ENSIA gaat over de opzet en het bestaan van deze beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD en Suwinet op 31 december 2024. Voor DigiD wordt het door Logius vastgestelde Norm ICT-beveiligingsassessments DigiD versie 3.0 gehanteerd. Daarbij zijn normen getoetst op werking.

Voor Suwinet de Verantwoordingsrichtlijn GeVS 2022 (tevens geldend voor het verslagjaar 2024) waarin zijn opgenomen de geselecteerde eisen uit de 'Baseline Informatiebeveiliging Overheid' versie 1.04zv. Deze Verantwoordingsrichtlijn betreft opzet, bestaan en werking van de interne beheersingsmaatregelen. In het kader van de zelfevaluatie ENSIA zijn geen werkzaamheden uitgevoerd met betrekking tot de werking van deze maatregelen.

- Onderstaande tekst weghalen indien niet van toepassing

[15] ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Overheid (BIO), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten (PUN, PNIK), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO), de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

[Als gevolg van de uitbesteding aan serviceorganisaties door de gemeente is een aantal van de interne beheersingsmaatregelen belegd bij serviceorganisaties. Hiervan hebben wij als gemeente een verantwoording voorzien van een oordeel van een onafhankelijke IT-auditor/RE van de serviceorganisaties ontvangen.]

Collegeverklaring en samenvattend beeld van de auditbevindingen

Verklaring / Conclusie

Het college van Burgemeester en Wethouders van de <gemeente> verklaart dat de gemeentelijke organisatie op 31 december 2024 [voldoet][niet voldoet] aan alle geselecteerde normen inzake DigiD en Suwinet.

Samenvattend beeld

Deze collegeverklaring betreffende de gemeentelijke organisatie en de serviceorganisaties dekt de geslecteerde normen inzake DigiD en Suwinet af. Het detailoverzicht van normen en of we hier als gemeente aan voldoen, is opgenomen in de volgende bijlagen:

- Bijlage 1 DigiD met kenmerk [gemeentelijk kenmerk]
- Bijlage 2 Suwinet met kenmerk [gemeentelijk kenmerk]

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
<tabel met digid.aansluitingen>	[Ja] [Nee]	[Ja] [Nee] [Niet van toepassing]
Suwinet voor SUWI-taken	[Ja] [Nee] [Niet van toepassing]	[Ja] [Nee] [Niet van toepassing]
Suwinet voor niet-SUWI-taken	[Ja] [Nee] [Niet van toepassing]	[Ja] [Nee] [Niet van toepassing]

Namens het College van B&W <gemeente>

[Naam], [functie]

[Plaats], [datum]

Bijlage 1 DigiD - <aansluitingnaam> - <aansluitnummer>

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting <aansluitingnaam> met aansluitnummer <aansluitnummer>

<gemeente> biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting <aansluitingnaam> voor authenticatie wordt gebruikt:

- <omschrijving functionaliteit>.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Naam: <naam webapplicatie>.
- Versie: <versie>.

Deze webapplicatie is extern benaderbaar via [de/het] volgende internetadres[sen]:

- <URL>.
- <URL>.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting <aansluitingnaam>. De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de “Norm ICT-beveiligingsassessments DigiD versie 3.0” van Logius.

Deze webapplicatie betreft < type webapplicatie>. De webapplicatie wordt onderhouden door <beheerorganisatie>.

DigiD-aansluiting <aansluitingnaam> bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze webapplicatie op draait, wordt beheerd door <leverancier> met beheervorm <beheervorm>.

➢ Verwijder onderstaande alinea als er geen gebruik wordt gemaakt van een Identity Broker.
[Voor het afhandelen van het authenticatieverzoek van de gebruiker maakt <gemeente> gebruik van authenticatiedienst van <identity broker>.]

<gemeente> heeft de DigiD web-omgeving uitbesteed aan:

- <leverancier>.
- <leverancier>.
- <leverancier>.

Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie(s). Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie(s). De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

De DigiD-webomgeving moet aan het gehele normenkader voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier(s) van de gemeente valt voor de periode:

Aansluithouder	
Oordeelsdatum:	<oordeelsdatum>
Controleperiode:	<controleperiode>

De overige normen worden afgedekt door onderstaande assurancerapportage(s) (AR)van de (toe)leverancier(s):

Applicatieleverancier	
Naam applicatieleverancier:	<leverancier>
Referentie/rapportnummer:	AR: <rapportnummer> Sub-AR: <rapportnummer>
Oordeelsdatum:	AR: <oordeelsdatum> Sub- AR: < oordeelsdatum >
Controleperiode:	AR: < controleperiode > Sub- AR: < controleperiode >
Naam RE-auditor	AR: <naam RE-auditor> Sub- AR: < naam RE-auditor >
Ondertekend door RE-auditor:	AR: <Ja/Nee> Sub-TPM AR <Ja/Nee>

Hostingleverancier	
Naam hostingleverancier:	<leverancier>
Referentie/rapportnummer:	AR: <rapportnummer> Sub- AR: <rapportnummer>
Oordeelsdatum:	AR: <oordeelsdatum> Sub- AR: < oordeelsdatum >
Controleperiode:	AR: < controleperiode > Sub- AR: < controleperiode >
Naam RE-auditor	AR: <naam RE-auditor> Sub- AR: < naam RE-auditor >
Ondertekend door RE-auditor:	AR: <Ja/Nee> Sub- AR: <Ja/Nee>

- Verwijder de onderstaande tabel als er geen gebruik wordt gemaakt van een Identity Broker. De AR betreft de AR van de Identity Broker. De sub- AR betreft de AR van de toeleverancier van de Identity Broker (alleen in het geval er sprake is van carve-out).

Identity Broker	
Naam Identity Broker:	<leverancier>
Referentie/rapportnummer:	AR: <rapportnummer> Sub- AR: <rapportnummer>
Oordeelsdatum:	AR: <oordeelsdatum> Sub- AR: < oordeelsdatum >
Controleperiode:	AR: < controleperiode > Sub- AR: < controleperiode >
Naam RE-auditor	AR: <naam RE-auditor> Sub- AR: < naam RE-auditor >
Ondertekend door RE-auditor:	AR: <Ja/Nee> Sub- AR: <Ja/Nee>

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de assurancerapportages (AR) van onze serviceorganisatie(s) het gehele normenkader afdekken. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk [kenmerk assurancerapport].

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm inclusief de normen die getoetst zijn bij de bovengenoemde leveranciers.

- Verwijder de kolommen met Identity Broker als er geen gebruik wordt gemaakt van een Identity Broker.
- Verwijder de kolom “Oordeel sub- AR” als de serviceorganisatie geen toeleverancier heeft.

		Aansluithouder	Applicatieleverancier		Hostingleverancier		Identity Broker		
DigiD-norm	**Toetsing op**	**Oordeel**	**Oordeel AR**	**Oordeel sub- AR**	**Oordeel AR**	**Oordeel sub- AR**	**AR**	**Oordeel sub-TPM**	**Totaaloordeel**
B.01 Informatiebeveiligingsbeleid	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
B.05 Contractmanagement	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/TV.01 Identificatie en authenticatie	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
	Werking	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/WA.02 Webapplicatiebeheerproces	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
	Werking	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing

		Aansluithouder	Applicatieleverancier		Hostingleverancier		Identity Broker		
DigiD-norm	**Toetsing op**	**Oordeel**	**Oordeel** AR	**Oordeel sub-** AR	**Oordeel** AR	**Oordeel sub-** AR	AR	**Oordeel sub-TPM**	**Totaaloordeel**
U/WA.03 Automatische data-invoercontrole	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Niet van toepassing	Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/WA04. Normaliseren uitvoer	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Niet van toepassing	Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/WA.05 Cryptografie/ Privacybevordering	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/PW.02 Garanderen webprotocollen	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/PW.03 Configureren webserver	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/PW.05 Toegang tot beheermechanismen	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/PW.07 Hardening van platformen	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Niet van toepassing	Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/NW.03 DMZ	*Opzet en bestaan*	Voldoet Voldoet niet	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet	Voldoet Voldoet niet	Voldoet Voldoet niet	Voldoet Voldoet niet	Voldoet Voldoet niet	Voldoet Voldoet niet

		Aansluithouder	Applicatieleverancier		Hostingleverancier		Identity Broker		
DigiD-norm	**Toetsing op**	**Oordeel**	**Oordeel** AR	**Oordeel sub-** AR	**Oordeel** AR	**Oordeel sub-** AR	AR	**Oordeel sub-TPM**	**Totaaloordeel**
		Niet van toepassing		Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing
U/NW.04 Protectie- en detectiemechanismen	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/NW.05 Scheiding beheer- en productieomgeving	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
U/NW.06 Hardening van netwerken	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
C.03 Vulnerability-assessments	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
C.04 Penetratietesten	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
C.06 Signaleringsfuncties	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Niet van toepassing	Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
C.07 Monitoringfuncties	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Niet van toepassing	Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing

		Aansluithouder	Applicatieleverancier		Hostingleverancier		Identity Broker		
DigiD-norm	**Toetsing op**	**Oordeel**	**Oordeel** AR	**Oordeel sub-** AR	**Oordeel** AR	**Oordeel sub-** AR	AR	**Oordeel sub-TPM**	**Totaaloordeel**
	Werking	Voldoet Voldoet niet Niet van toepassing	Niet van toepassing	Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
C.08 Wijzigingenbeheer	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
	Werking	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
C.09 Patchmanagement	*Opzet en bestaan*	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing
	Werking	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing	Voldoet Voldoet niet Niet van toepassing

➢ De bovenstaande tabel is geautomatiseerd gevuld met de antwoorden uit de vragenlijst. Controleer iedere cel zorgvuldig.

- Op deze pagina kan de gemeente in overleg met auditor beperkingen of bijzonderheden met betrekking tot de oordelen uit de zelfevaluatie opnemen. Als er geen beperkingen of bijzonderheden zijn, dan moet deze pagina verwijderd worden.

[Beperkingen of bijzonderheden:

…
…
]

Bijlage 2: Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de Verantwoording informatiebeveiliging Suwinet per 31-12-2024 <gemeente> . Onderwerp van de verantwoording is het gebruik van Suwinet. Deze ventantwoording heeft betrekking op de Verantwoordingsrichtlijn GeVS 2022 die is gebaseerd op geselecteerde controls uit de Baseline Informatieveiligheid Overheid (BIO), meer in het bijzonder de in het kader van ENSIA geselecteerde controls.

Suwinet-gegevens worden ten behoeve van de dienstverlening door <gemeente> verwerkt. Hierbij is de eventuele aanwezigheid van IT-serviceorganisaties in aanmerking genomen.

➢ Alleen indien er een serviceorganisatie is, anders weglaten

[Het bestuur / de directie van <gemeente> is als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van Suwinet en legt hierover verantwoording af. <organisatienaam> heeft een deel van de [Suwinet taken] [en] [of] [niet-SUWI-taken] uitbesteed aan [naam serviceorganisatie(s)] [en] [of] [naam gemeente(n)]. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie[s] [en] [of] [[naam gemeente(n)]]. In de navolgende tabellen is opgenomen of het onderzoeken over het al dan niet voldoen aan deze maatregelen is uitgevoerd door de IT-auditor van deze serviceorganisatie[s]. De controls die betrekking hebben op de taken die belegd zijn bij de serviceorganisatie(s) maken geen onderdeel uit van de zelfevaluatie van <gemeente>, tenzij sprake is van een gedeelde norm.

De zelfevaluatie ENSIA voor Suwinet is toegepast op dat deel van het gebruik en normenkader dat niet onder uitbesteding aan onze serviceorganisatie[s] valt. De overige normen worden afgedekt door onderstaande assurancerapportage[s] (AR) van onze serviceorganisatie[s] [en] [of] [[naam andere gemeente(n)]].

➢ De volgende tabellen zijn optioneel en kunnen verwijderd worden indien niet van toepassing:

[

Leverancier 1	
Naam serviceorganisatie:	[Naam]
Referentie/rapportnummer:	[Nummer]
Rapportagedatum:	[Datum]
Naam RE-auditor:	[Naam]
Ondertekend door RE-auditor:	[Ja] [Nee]

Leverancier 2	
Naam serviceorganisatie:	[Naam]
Referentie/rapportnummer:	[Nummer]
Rapportagedatum:	[Datum]
Naam RE-auditor:	[Naam]
Ondertekend door RE-auditor:	[Ja] [Nee]

]

Gebruik van Suwinet voor SUWI-taken

Voor de volgende taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	AR
Participatiewet (Pw)	[Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	 [Ja] [Nee] [Ja] [Nee]
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	[Niet van toepassing] [Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	 [Ja] [Nee] [Ja] [Nee]
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	[Niet van toepassing] [Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	 [Ja] [Nee] [Ja] [Nee]
Wet gemeentelijke schuldhulpverlening (Wgs)	[Niet van toepassing] [Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	 [Ja] [Nee] [Ja] [Nee]
Uitvoeren bijzonder bijstand	[Niet van toepassing] [Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	 [Ja] [Nee] [Ja] [Nee]
Uitvoeren bezoldiging zelfstandigen	[Niet van toepassing] [Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	 [Ja] [Nee] [Ja] [Nee]
Sociale recherche	[Niet van toepassing] [Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	 [Ja] [Nee] [Ja] [Nee]

Gebruik van Suwinet voor niet-SUWI-taken

Voor de volgende niet-SUWI-taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	AR
Hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC) <naam RMC-gemeente>[16]	[Niet van toepassing] [Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente][17]	 [Ja] [Nee] [Ja] [Nee]
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	[Niet van toepassing] [Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	 [Ja] [Nee] [Ja] [Nee]

[16] Alleen de regiogemeente moet verantwoorden en niet de aangesloten gemeente.
[17] Hier gemeenten vermelden waarvoor RMC-gemeente informatie verwerkt.

Taak	Organisatie	AR
Adresonderzoek door Burgerzaken	[Niet van toepassing] [Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	 [Ja] [Nee] [Ja] [Nee]

Naleving BIO-maatregelen

➢ Indien geen afwijkingen van de maatregelen de volgende tekst opnemen:
[Zoals in de Verantwoording vermeld, voldoet <gemeente> aan alle interne beheersingsmaatregelen inzake Suwinet op 31 december 2024 in opzet en bestaan aan de geselecteerde controls.]

➢ Bij afwijkingen van de normen betreffende SUWI-taken de volgende tekst opnemen:
[Met uitzondering van de volgende maatregelen voldoen de interne beheersingsmaatregelen voor de SUWI-taken op 31 december 2024 in opzet en bestaan aan de doelstellingen uit de verantwoordingsrichtlijn GeVS 2022:

Organisatie	SUWI-taak	BIO-maatregel	Applicatie
[Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	Participatiewet (Pw)	[Maatregel]	[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie]] [DKD-Inlezen met [naam inleesapplicatie]]
[Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	[Maatregel]	[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie]] [DKD-Inlezen met [naam inleesapplicatie]]
[Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	[Maatregel]	[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie] [DKD-Inlezen met [naam inleesapplicatie]]
[Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	Wet gemeentelijke schuldhulpverlening (Wgs)	[Maatregel]	[Wgs-Inkijk] [WGS-Inlezen met [naam inleesapplicatie]
[Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	Uitvoeren bijzonder bijstand	[Maatregel]	[Suwinet-Inkijk] [DKD-Inlezen met [naam inleesapplicatie]
[Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	Uitvoeren bezoldiging zelfstandigen	[Maatregel]	[Wgs-Inkijk] [WGS-Inlezen met [naam inleesapplicatie]
[Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	Sociale Recherche	[Maatregel]	[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie] [DKD-Inlezen met [naam inleesapplicatie]]

]

➢ Bij afwijkingen van de normen betreffende niet-SUWI-taken:

[Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de niet-SUWI-taken in opzet en bestaan aan alle geselecteerde normen:

Organisatie	Niet-SUWI-taak	BIO-maatregel	Applicatie
[Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	Hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC)	[Maatregel]	[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie]]
[Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	[Maatregel]	[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie]]
[Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	Adresonderzoek door Burgerzaken	[Maatregel]	[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie]]

]

4.2 Bijlage 2: Formats assurance-rapporten

4.2.1 Goedkeurend oordeel

ASSURANCE-RAPPORT

Inzake de Collegeverklaring ENSIA 20XX
van de gemeente <naam gemeente>
en de bijlagen 1 DigiD en 2 Suwinet
waarnaar in de Collegeverklaring verwezen wordt

(Bestemd voor gemeente <naam gemeente>,
Logius, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties,
BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid)

Uniek identificatienummer IT-auditor

Assurance-rapport van de onafhankelijke IT-auditor

Aan: <opdrachtgever>

Assurance over de Collegeverklaring ENSIA 20XX van de gemeente <naam gemeente> en de bijlagen 1 DigiD en 2 Suwinet waarnaar in de Collegeverklaring wordt verwezen

Ons oordeel
Ingevolge uw opdracht hebben wij de bijgevoegde collegeverklaring ENSIA 20XX inzake Informatiebeveiliging van DigiD en Suwinet (hierna: collegeverklaring), inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> onderzocht.

Naar ons oordeel is bijgevoegde collegeverklaring, inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente>, in alle van materieel belang zijnde aspecten, juist.

De basis voor ons oordeel
Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht, de NOREA Richtlijn 3000A "Assurance-opdrachten door IT-auditors (Attest-opdrachten)" en de NOREA Handreiking ENSIA voor IT-auditors (RE's) versie 5.0 d.d. 1 juli 2024. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Verantwoordelijkheden van de IT-auditor'.

Wij zijn onafhankelijk van <naam gemeente> en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA.

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

Object van onderzoek
Met de collegeverklaring geeft het college van Burgemeester en Wethouders, aan in welke mate de gemeente voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet. De collegeverklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen gebaseerd op de 'Norm ICT-beveiligingsassessments DigiD versie 3.0' van Logius voor DigiD en de door de toezichthouder geselecteerde eisen uit de 'Baseline Informatiebeveiliging Overheid' versie 1.04zv voor Suwinet. Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

Betreffende DigiD gaat de verantwoording over de opzet, het bestaan van de interne beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD op 31 december 2024 alsmede de werking van de maatregelen U/TV.01; U/WA.02; C.07; C.08 en C.09 gedurende de periode 1 juli – 31 december 20XX.

Betreffende Suwinet gaat de verantwoording over de opzet en het bestaan van de interne beheersingsmaatregelen per 31 december 20XX.

Scope
De scope van ons onderzoek bestond uit de hierna genoemde DigiD aansluitingen en Suwinet gegevensverwerkingen:

Onderzochte DigiD aansluitingen:

Aansluitnummer	Aansluitnaam

Onderzochte gegevensverwerkingen Suwinet:
<TABEL OVERNEMEN UIT BIJLAGE 2 COLLEGEVERKLARING>

Wij hebben geen onderzoek uitgevoerd naar hierboven niet genoemde DigiD aansluitingen en gegevensverwerkingen Suwinet en doen daar derhalve ook geen uitspraak over.

<Alleen bij uitzonderingen: passage zonder paragraafkop over beperkingen bij het onderzoek. Zoals in de collegeverklaring is aangegeven wordt nog niet aan alle normen inzake DigiD en/of Suwinet voldaan>.

<indien van toepassing:
Benadrukking aangelegenheden
Wij hebben vastgesteld dat de op de uitzonderingen gerichte beheersingsmaatregelen in verbeterplannen zijn opgenomen, zijn belegd en worden gemonitord. Ons onderzoek heeft zich niet gericht op de juistheid, volledigheid en uitvoering van de verbeterplannen. Ons oordeel is niet aangepast als gevolg van deze aangelegenheid.>

Beoogde gebruikers en doel
Ons assurance-rapport is bestemd voor gebruikers van de collegeverklaring. De collegeverklaring is opgesteld voor de gemeenteraad en voor de departementen en aangewezen uitvoeringsinstanties die toezien op de veiligheid van DigiD en Suwinet. Doel van de collegeverklaring is om de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet te informeren over het voldoen aan de geselecteerde normen DigiD en Suwinet.

Ons assurance-rapport mag enkel worden gebruikt door de beoogde gebruikers voor het doel waarvoor het is opgesteld en dient niet te worden verspreid aan of te worden gebruikt door anderen of voor een ander doel.

Beschrijving van de verantwoordelijkheden

Verantwoordelijkheden van het college van gemeente <naam gemeente>
- Het college van burgemeester en wethouders van gemeente <naam gemeente> is verantwoordelijk voor het opstellen van de collegeverklaring.

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

Verantwoordelijkheden van de IT-auditor
Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van ons onderzoek dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel.

Ons onderzoek is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens ons onderzoek niet alle materiële afwijkingen als gevolg van fraude of fouten ontdekken.

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

Onze assurance-opdracht bestond onder andere uit:
- het verkrijgen van kennis omtrent de collegeverklaring
- en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen;
- het op basis van deze kennis identificeren en inschatten van de risico's dat de collegeverklaring onjuistheden van materieel belang als gevolg van fraude of fouten bevat;
- het in reactie op deze risico's bepalen en uitvoeren van assurance-werkzaamheden en het verkrijgen van assurance-informatie die voldoende en geschikt is als basis voor ons oordeel;
- het evalueren of de collegeverklaring in overeenstemming is met de onderliggende beheersingsmaatregelen en uitgevoerde werkzaamheden; en
- het evalueren van de uitkomsten van onze werkzaamheden.

Plaats en datum
... (naam IT-auditeenheid)
... (naam IT Auditor RE)

4.2.2 Oordeel met beperking

ASSURANCE-RAPPORT

Inzake de Collegeverklaring ENSIA 20XX
van de gemeente <naam gemeente>
en de bijlagen 1 DigiD en 2 Suwinet
waarnaar in de Collegeverklaring verwezen wordt

(Bestemd voor gemeente <naam gemeente>,
Logius, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties,
BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid)

Uniek identificatienummer IT-auditor

Assurancerapport van de onafhankelijke IT-auditor

Aan: <opdrachtgever>

Assurance over de Collegeverklaring ENSIA 20XX van de gemeente <naam gemeente> en de bijlagen 1 DigiD en 2 Suwinet waarnaar in de Collegeverklaring wordt verwezen

Ons oordeel met beperking
Ingevolge uw opdracht hebben wij de bijgevoegde collegeverklaring ENSIA 20XX inzake Informatiebeveiliging van DigiD en Suwinet (hierna: collegeverklaring), inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> onderzocht.

Naar ons oordeel is, uitgezonderd de <gevolgen>[18] <mogelijke effecten>[19] van de <aangelegenheid> <aangelegenheden> beschreven in de paragraaf 'De basis voor ons oordeel met beperking', bijgevoegde collegeverklaring, inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente>, in alle van materieel belang zijnde aspecten, juist.

De basis voor ons oordeel met beperking
<Instructie voor de auditor: beschrijving van de aangelegenheid / aangelegenheden welke aanleiding heeft / hebben gegeven tot het oordeel met beperking.>

Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht, de NOREA Richtlijn 3000A "Assurance-opdrachten door IT-auditors (Attest-opdrachten)" en de NOREA Handreiking ENSIA voor IT-auditors (RE's) versie 5.0 d.d. 1 juli 2024. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Verantwoordelijkheden van de IT-auditor'.

Wij zijn onafhankelijk van <naam gemeente> en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA.

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

Object van onderzoek
Met de collegeverklaring geeft het college van Burgemeester en Wethouders, aan in welke mate de gemeente voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet. De collegeverklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen gebaseerd op de 'Norm ICT-beveiligingsassessments DigiD versie 3.0' van Logius voor DigiD en de door de toezichthouder geselecteerde eisen uit de 'Baseline Informatiebeveiliging Overheid' versie 1.04zv voor Suwinet. Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

Betreffende DigiD gaat de verantwoording over de opzet, het bestaan van de interne beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD op 31 december 2024 alsmede de werking van de maatregelen U/TV.01; U/WA.02; C.07; C.08 en C.09 gedurende de periode 1 juli – 31 december 20XX.

Betreffende Suwinet gaat de verantwoording over de opzet en het bestaan van de interne beheersingsmaatregelen per 31 december 20XX.

Scope

[18] Tekst bij fouten van materiele maar niet diepgaande aard.

[19] Tekst bij onvoldoende geschikte controle informatie van materiele maar geen diepgaande aard.

De scope van ons onderzoek bestond uit de hierna genoemde DigiD aansluitingen en Suwinet gegevensverwerkingen:

Onderzochte DigiD aansluitingen:

Aansluitnummer	Aansluitnaam

Onderzochte gegevensverwerkingen Suwinet:
<TABEL OVERNEMEN UIT BIJLAGE 2 COLLEGEVERKLARING>

Wij hebben geen onderzoek uitgevoerd naar hierboven niet genoemde DigiD aansluitingen en gegevensverwerkingen Suwinet en doen daar derhalve ook geen uitspraak over.

<Alleen bij uitzonderingen: passage zonder paragraafkop over beperkingen bij het onderzoek. Zoals in de collegeverklaring is aangegeven wordt nog niet aan alle normen inzake DigiD en/of Suwinet voldaan>.

<indien van toepassing:

Benadrukking aangelegenheden

Wij hebben vastgesteld dat de op de uitzonderingen gerichte beheersingsmaatregelen in verbeterplannen zijn opgenomen, zijn belegd en worden gemonitord. Ons onderzoek heeft zich niet gericht op de juistheid, volledigheid en uitvoering van de verbeterplannen. Ons oordeel is niet aangepast als gevolg van deze aangelegenheid.>

Beoogde gebruikers en doel

Ons assurance-rapport is bestemd voor gebruikers van de collegeverklaring. De collegeverklaring is opgesteld voor de gemeenteraad en voor de departementen en aangewezen uitvoeringsinstanties die toezien op de veiligheid van DigiD en Suwinet. Doel van de collegeverklaring is om de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet te informeren over het voldoen aan de geselecteerde normen DigiD en Suwinet.

Ons assurance-rapport is derhalve uitsluitend bestemd voor de gemeenteraad en de departementen en aangewezen uitvoeringsinstanties die toezien op de veiligheid van DigiD en Suwinet en dient niet te worden verspreid aan of te worden gebruikt door anderen of voor een ander doel.

Beschrijving van de verantwoordelijkheden

Verantwoordelijkheden van het college van gemeente <naam gemeente>

- Het college van burgemeester en wethouders van gemeente <naam gemeente> is verantwoordelijk voor het opstellen van de collegeverklaring.

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

Verantwoordelijkheden van de IT-auditor

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van ons onderzoek dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel.

Ons onderzoek is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens ons onderzoek niet alle materiële afwijkingen als gevolg van fraude of fouten ontdekken.

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

Onze assurance-opdracht bestond onder andere uit:

- het verkrijgen van kennis omtrent de collegeverklaring
- en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen;
- het op basis van deze kennis identificeren en inschatten van de risico's dat de collegeverklaring onjuistheden van materieel belang als gevolg van fraude of fouten bevat;
- het in reactie op deze risico's bepalen en uitvoeren van assurance-werkzaamheden en het verkrijgen van assurance-informatie die voldoende en geschikt is als basis voor ons oordeel;
- het evalueren of de collegeverklaring in overeenstemming is met de onderliggende beheersingsmaatregelen en uitgevoerde werkzaamheden; en
- het evalueren van de uitkomsten van onze werkzaamheden.

Plaats en datum

... (naam IT-auditeenheid)

... (naam IT Auditor RE)

4.2.3 Afkeurend oordeel

ASSURANCE-RAPPORT

Inzake de Collegeverklaring ENSIA 20XX
van de gemeente <naam gemeente>
en de bijlagen 1 DigiD en 2 Suwinet
waarnaar in de Collegeverklaring verwezen wordt

(Bestemd voor gemeente <naam gemeente>,
Logius, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties,
BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid)

Uniek identificatienummer IT-auditor

Assurancerapport van de onafhankelijke IT-auditor

Aan: <opdrachtgever>

Assurance over de Collegeverklaring ENSIA 20XX van de gemeente <naam gemeente> en de bijlagen 1 DigiD en 2 Suwinet waarnaar in de Collegeverklaring wordt verwezen

Ons afkeurend oordeel
Ingevolge uw opdracht hebben wij de bijgevoegde collegeverklaring ENSIA 20XX inzake Informatiebeveiliging van DigiD en Suwinet (hierna: collegeverklaring), inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> onderzocht.

Naar ons oordeel is, bijgevoegde collegeverklaring, inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente>, vanwege het belang van de <aangelegenheid> <aangelegenheden> beschreven in de paragraaf 'De basis voor ons afkeurend oordeel" niet in alle van materieel belang zijnde aspecten, juist.

De basis voor ons afkeurend oordeel
<Instructie voor de auditor: beschrijving van de aangelegenheid / aangelegenheden welke aanleiding heeft / hebben gegeven tot het afkeurend oordeel.>

Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht, de NOREA Richtlijn 3000A "Assurance-opdrachten door IT-auditors (Attest-opdrachten)" en de NOREA Handreiking ENSIA voor IT-auditors (RE's) versie 5.0 d.d. 1 juli 2024. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Verantwoordelijkheden van de IT-auditor'.

Wij zijn onafhankelijk van <naam gemeente> en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA.

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

Object van onderzoek
Met de collegeverklaring geeft het college van Burgemeester en Wethouders, aan in welke mate de gemeente voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet. De collegeverklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen gebaseerd op de 'Norm ICT-beveiligingsassessments DigiD versie 3.0' van Logius voor DigiD en de door de toezichthouder geselecteerde eisen uit de 'Baseline Informatiebeveiliging Overheid' versie 1.04zv voor Suwinet. Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

Betreffende DigiD gaat de verantwoording over de opzet, het bestaan van de interne beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD op 31 december 2024 alsmede de werking van de maatregelen U/TV.01; U/WA.02; C.07; C.08 en C.09 gedurende de periode 1 juli – 31 december 20XX.

Betreffende Suwinet gaat de verantwoording over de opzet en het bestaan van de interne beheersingsmaatregelen per 31 december 20XX.

Scope
De scope van ons onderzoek bestond uit de hierna genoemde DigiD aansluitingen en Suwinet gegevensverwerkingen:

Onderzochte DigiD aansluitingen:

Aansluitnummer	Aansluitnaam

Onderzochte gegevensverwerkingen Suwinet:
<TABEL OVERNEMEN UIT BIJLAGE 2 COLLEGEVERKLARING>

Wij hebben geen onderzoek uitgevoerd naar hierboven niet genoemde DigiD aansluitingen en gegevensverwerkingen Suwinet en doen daar derhalve ook geen uitspraak over.

<Alleen bij uitzonderingen: passage zonder paragraafkop over beperkingen bij het onderzoek. Zoals in de collegeverklaring is aangegeven wordt nog niet aan alle normen inzake DigiD en/of Suwinet voldaan>.

<*indien van toepassing:*
Benadrukking aangelegenheden
Wij hebben vastgesteld dat de op de uitzonderingen gerichte beheersingsmaatregelen in verbeterplannen zijn opgenomen, zijn belegd en worden gemonitord. Ons onderzoek heeft zich niet gericht op de juistheid, volledigheid en uitvoering van de verbeterplannen. Ons oordeel is niet aangepast als gevolg van deze aangelegenheid.>

Beoogde gebruikers en doel
Ons assurance-rapport is bestemd voor gebruikers van de collegeverklaring. De collegeverklaring is opgesteld voor de gemeenteraad en voor de departementen en aangewezen uitvoeringsinstanties die toezien op de veiligheid van DigiD en Suwinet. Doel van de collegeverklaring is om de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet te informeren over het voldoen aan de geselecteerde normen DigiD en Suwinet.

Ons assurance-rapport is derhalve uitsluitend bestemd voor de gemeenteraad en de departementen en aangewezen uitvoeringsinstanties die toezien op de veiligheid van DigiD en Suwinet en dient niet te worden verspreid aan of te worden gebruikt door anderen of voor een ander doel.

Beschrijving van de verantwoordelijkheden

Verantwoordelijkheden van het college van gemeente <naam gemeente>
- Het college van burgemeester en wethouders van gemeente <naam gemeente> is verantwoordelijk voor het opstellen van de collegeverklaring.

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

Verantwoordelijkheden van de IT-auditor
Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van ons onderzoek dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel.

Ons onderzoek is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens ons onderzoek niet alle materiële afwijkingen als gevolg van fraude of fouten ontdekken.

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

Onze assurance-opdracht bestond onder andere uit:
- het verkrijgen van kennis omtrent de collegeverklaring
- en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen;
- het op basis van deze kennis identificeren en inschatten van de risico's dat de collegeverklaring onjuistheden van materieel belang als gevolg van fraude of fouten bevat;
- het in reactie op deze risico's bepalen en uitvoeren van assurance-werkzaamheden en het verkrijgen van assurance-informatie die voldoende en geschikt is als basis voor ons oordeel;
- het evalueren of de collegeverklaring in overeenstemming is met de onderliggende beheersingsmaatregelen en uitgevoerde werkzaamheden; en
- het evalueren van de uitkomsten van onze werkzaamheden.

Plaats en datum
... (naam IT-auditeenheid)

... (naam IT Auditor RE)

4.2.4 Oordeelonthouding

ASSURANCE-RAPPORT

Inzake de Collegeverklaring ENSIA 20XX
van de gemeente <naam gemeente>
en de bijlagen 1 DigiD en 2 Suwinet
waarnaar in de Collegeverklaring verwezen wordt

(Bestemd voor gemeente <naam gemeente>,
Logius, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties,
BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid)

Uniek identificatienummer IT-auditor

Assurancerapport van de onafhankelijke IT-auditor

Aan: <opdrachtgever>

Assurance over de Collegeverklaring ENSIA 20XX van de gemeente <naam gemeente> en de bijlagen 1 DigiD en 2 Suwinet waarnaar in de Collegeverklaring wordt verwezen

Onze oordeelonthouding
Wij hebben de opdracht gekregen om bijgevoegde collegeverklaring ENSIA 20XX inzake Informatiebeveiliging van DigiD en Suwinet (hierna: collegeverklaring), inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> te onderzoeken.

Wij geven geen oordeel over de juistheid van de, bijgevoegde collegeverklaring, inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente>. Vanwege het belang van de <aangelegenheid> <aangelegenheden> beschreven in de paragraaf 'De basis voor onze oordeelonthouding' zijn wij niet in staat geweest om voldoende en geschikte assurance-informatie te verkrijgen om daarop ons oordeel te kunnen baseren bij de collegeverklaring, inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente>.

De basis voor onze oordeelonthouding
<Instructie voor de auditor: beschrijving van de aangelegenheid / aangelegenheden welke aanleiding heeft / hebben gegeven tot de oordeelonthouding.>

Object van onderzoek
Met de collegeverklaring geeft het college van Burgemeester en Wethouders, aan in welke mate de gemeente voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet. De collegeverklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen gebaseerd op de 'Norm ICT-beveiligingsassessments DigiD versie 3.0' van Logius voor DigiD en de door de toezichthouder geselecteerde eisen uit de 'Baseline Informatiebeveiliging Overheid' versie 1.04zv voor Suwinet. Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

Betreffende DigiD gaat de verantwoording over de opzet, het bestaan van de interne beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD op 31 december 2024 alsmede de werking van de maatregelen U/TV.01; U/WA.02; C.07; C.08 en C.09 gedurende de periode 1 juli – 31 december 20XX.

Betreffende Suwinet gaat de verantwoording over de opzet en het bestaan van de interne beheersingsmaatregelen per 31 december 20XX.

Scope
De scope van ons onderzoek bestond uit de hierna genoemde DigiD aansluitingen en Suwinet gegevensverwerkingen:

Onderzochte DigiD aansluitingen:

Aansluitnummer	Aansluitnaam

Onderzochte gegevensverwerkingen Suwinet:
<TABEL OVERNEMEN UIT BIJLAGE 2 COLLEGEVERKLARING>

Wij hebben geen onderzoek uitgevoerd naar hierboven niet genoemde DigiD aansluitingen en gegevensverwerkingen Suwinet en doen daar derhalve ook geen uitspraak over.

<Alleen bij uitzonderingen: passage zonder paragraafkop over beperkingen bij het onderzoek. Zoals in de collegeverklaring is aangegeven wordt nog niet aan alle normen inzake DigiD en/of Suwinet voldaan>.

<*indien van toepassing:*
Benadrukking aangelegenheden
Wij hebben vastgesteld dat de op de uitzonderingen gerichte beheersingsmaatregelen in verbeterplannen zijn opgenomen, zijn belegd en worden gemonitord. Ons onderzoek heeft zich niet gericht op de juistheid, volledigheid en uitvoering van de verbeterplannen. Ons oordeel is niet aangepast als gevolg van deze aangelegenheid.>

Beoogde gebruikers en doel
Ons assurance-rapport is bestemd voor gebruikers van de collegeverklaring. De collegeverklaring is opgesteld voor de gemeenteraad en voor de departementen en aangewezen uitvoeringsinstanties die toezien op de veiligheid van DigiD en Suwinet. Doel van de collegeverklaring is om de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet te informeren over het voldoen aan de geselecteerde normen DigiD en Suwinet.

Ons assurance-rapport is derhalve uitsluitend bestemd voor de gemeenteraad en de departementen en aangewezen uitvoeringsinstanties die toezien op de veiligheid van DigiD en Suwinet en dient niet te worden verspreid aan of te worden gebruikt door anderen of voor een ander doel.

Beschrijving van de verantwoordelijkheden

Verantwoordelijkheden van het college van gemeente <naam gemeente>
- Het college van burgemeester en wethouders van gemeente <naam gemeente> is verantwoordelijk voor het opstellen van de collegeverklaring.

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

Verantwoordelijkheden van de IT-auditor
Onze verantwoordelijkheid is het geven van een oordeel over de collegeverklaring, inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> op basis van onze audit, verricht in overeenstemming met Nederlands recht, waaronder de NOREA Richtlijn 3000A "Assurance-opdrachten door IT-auditors (Attest-opdrachten)" en NOREA Handreiking ENSIA voor IT-auditors (RE's) versie 5.0 d.d. 1 juli 2024. Vanwege het belang van de <aangelegenheid><aangelegenheden> beschreven in de paragraaf 'De basis voor onze oordeelonthouding' zijn wij niet in staat geweest om voldoende en geschikte assurance-informatie te verkrijgen om daarop ons oordeel te kunnen baseren bij de, collegeverklaring, inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> als geheel.

Wij zijn onafhankelijk van <naam gemeente> en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA>.

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

Plaats en datum
... (naam IT-auditeenheid)
... (naam IT Auditor RE)

4.3 Bijlage 3: DigiD-specifieke aandachtspunten ENSIA

In afwijking van de NOREA-handreiking DigiD assessments 2024 gelden voor gemeenten die DigiD-aansluithouder zijn de volgende aandachtspunten:

1. 3000A-systematiek wordt gehanteerd voor gemeenten, in tegenstelling tot serviceorganisaties en andere typen aansluithouders. Hierbij beoordeelt de auditor de wijze waarop de gemeente het van de auditor ontvangen assurancerapport heeft betrokken in de ENSIA-verantwoording.
2. Rapportages zijn, in tegenstelling tot de NOREA Handreiking DigiD-assessments, conform de ENSIA 2024 rapportage templates[20].
3. Gemeenten delen de rapportages inzake DigiD via de ENSIA-tool, in tegenstelling tot andere typen aansluithouders die rechtstreeks een assurancerapport verstrekken aan Logius.
4. De controle periode voor de toetsing van de werking voor enkele maatregelen is voor gemeenten een vaste periode van 1 juli tot en met 31 december.
5. De controleperiode voor serviceorganisaties (en sub-serviceorganisaties) is uiteraard ook minimaal 6 maanden. Rekening houdend met de wensen van gemeentelijke aansluithouders om voldoende gelegenheid te hebben om de ENSIA tooling in te vullen, zal het assurancerapport voor gemeenten uiterlijk 15 oktober gereed moeten zijn. Dit betekent voor serviceorganisaties die DigiD webapplicaties leveren aan gemeenten dat de controle periode in de praktijk 1 april- 30 september zal zijn.

[20] TPM's / assurancerapporten van serviceorganisaties volgen 3000 D inclusief daarvoor gepubliceerde rapportage templates.

4.4 Bijlage 4: Overwegingen ENSIA IT-Audit in samenwerkingsverbanden Suwinet

De uitgangspunten
De Verantwoordingsrichtlijn GeVS 2022 is volledig gebaseerd op de BIO. De gemeente geeft in de collegeverklaring aan in hoeverre wordt voldaan aan dit normenkader. Suwi-regelgeving vraagt van het gemeentebestuur een door een IT-auditor (RE) afgegeven assurance op de collegeverklaring. De Suwi-regelgeving steunt sterk op het principe van de horizontale verantwoording.

Praktijk is dat gemeenten in een aantal gevallen de werkzaamheden in het domein werk- en inkomen hebben belegd buiten de gemeente. Dit kunnen diverse vormen van samenwerkingsverbanden zijn. Deels werken deze onder mandaat, deels op basis van delegatie.

Ongeacht de organisatie van de samenwerkingsverbanden blijft het gemeentebestuur verantwoordelijk voor het gebruik van SUWI. SZW verwacht van gemeenten dat zij ook in het geval samenwerking de bestuurlijke verantwoordelijkheid blijven nemen. De verantwoordings-systematiek gaat dan ook uit van het principe dat gemeenten verantwoording afleggen aan de toezichthouder. De daarvoor relevante informatie moeten zij bij eventuele samenwerkingsverbanden ophalen en verwerken. Binnen de ENSIA-tooling zijn daarvoor mogelijkheden gecreëerd.

In de praktijk blijken de afspraken tussen samenwerkingsverbanden en gemeenten zich vooral te richten op financiële performance en correcte afhandeling van werkprocessen. Het onderwerp informatieveiligheid is niet in alle gevallen belegd in de afspraken tussen gemeenten en samenwerkingsverbanden. Wel zullen in het kader van de AVG verwerkersovereenkomsten beschikbaar zijn.

Zorgpunten
Als Suwi taken zijn uitbesteed aan een samenwerkingsverband, dienen de deelnemende gemeenten dit mee te nemen in hun rapportage in de ENSIA tool. In het ideale geval kan dit worden vormgegeven doordat het samenwerkingsverband compliancy t.a.v. de Suwinet normen aantoont op basis van een daarop gericht assurancerapport (TPM). Alhoewel dit in een aantal gevallen al gebeurt, is dat echter nog niet overal het geval.

Aangezien elke gemeente (ook) verantwoordelijk is voor het Suwinet gebruik door een samenwerkingsverband, dient invulling te worden wordt gegeven aan de voor SUWI relevante normen bij het samenwerkingsverband en de vertaling daarvan in de collegeverklaring ENSIA.

De audit in uitvoering
De meest pragmatische werkwijze lijkt dat de IT-auditor blijft werken vanuit gemeentelijk perspectief, dus:

- Zich een beeld vormt van de wijze waarop de gemeentelijk coördinator de totstandkoming van de collegeverklaring heeft vormgegeven en kan steunen op de gemeentelijke organisatie.
- Zich een beeld vormt van de wijze waarop de informatie vanuit samenwerkingsverbanden in de gemeentelijke zelfevaluatie is verwerkt.
- De aansluiting tussen collegeverklaring en onderliggende zelfevaluatie toetst.
- Met de gemeentelijk coördinator en samenwerkingsverband afstemt welke gemeenten mogelijk gebruik maken van een andere auditor.
- Concreet: Eén auditor neemt de lead voor het toetsen van de Suwi normen bij het samenwerkingsverband in de vorm van een Richtlijn 3000-opdracht (TPM). Vooraf dienen de werkzaamheden met de collega-auditoren worden afgestemd. Afsluitend aan de werkzaamheden rapporteert de IT-auditor hierover aan zijn collega-auditoren bij de deelnemende gemeenten.

Zie NOREA Handreiking Suwi (in kader ENSIA) voor IT-auditors (RE's) voor gedetailleerde toelichtingen op de uit te voeren werkzaamheden.

4.5 Bijlage 5: Waarmerken stukken en digitaal ondertekenen

Het assurancerapport moet een kenmerk (nummer) hebben van de auditorganisatie, de bijlage DigiD verwijst immers naar een kenmerk van het assurancerapport (een nieuwe versie van het assurancerapport vereist een nieuw kenmerk). Een assurancerapport wordt uitgebracht op briefpapier van de auditorganisatie.

Het waarmerken van de stukken door de IT-auditor dient aan een aantal vereisten te voldoen. Deze omvatten:

- Het eenduidig identificeren van het assurancerapport (door toekennen uniek identificatienummer en dateren) door de IT-auditor (en de auditorganisatie). Dit geschiedt standaard bij het ondertekenen van het assuranceapport.
- Het eenduidig identificeren van de verantwoordelijke IT-auditor (en de auditorganisatie). Dit geschiedt standaard bij het ondertekenen van het assurancerapport.

Betrouwbaarheidseisen aan de handtekening van een IT-auditor (RE)

DigiD

Met ingang van het jaar 2023 accepteert Logius twee vormen van elektronische handtekeningen in assessmentrapporten:

- De gekwalificeerde elektronische handtekening met een EUTL-certificaat.
- De geavanceerde elektronische handtekening met een EUTL-certificaat

EUTL staat voor European Union Trusted List en is een Europees middel dat wordt gebruikt om de identiteit van de uitgever van de elektronische handtekening te verifiëren. In de eigenschappen van de elektronische handtekening is voor iedereen te zien of de uitgever van het certificaat op de EUTL staat. Dit geeft een hoge betrouwbaarheid.

Let op: 'Assurance rapporten die worden uitgegeven na 2023, ten behoeve van de inleverperiode van 1 januari tot 1 mei 2025, moeten zijn voorzien van een elektronische handtekening met een EUTL-certificaat.

ENSIA

Op basis van nader overleg tussen alle direct betrokken partijen is besloten deze beleidslijn onverkort te volgen voor ENSIA.

In de praktijk betekent dit dat alle documenten los van elkaar ondertekend moeten zijn met een elektronische handtekening.

Ter toelichting: Dit betekent dat het assurancerapport, de Collegeverklaring en de bijlage DigiD en Suwi voorzien moeten zijn van een elektronische handtekening.

Aandachtspunt voor aansluithouders en IT-auditors

Voor een goede werking van het geheel is het van groot belang dat de aansluithouders de door de IT-auditor aangeleverde, van een elektronische handtekening voorziene stukken (PDF/a – format) onveranderd aanleveren. De stelselhouders zullen hiervoor waar nodig nog nadere aanwijzingen geven (zie website Logius en website BKWI).

4.6 Bijlage 6: Begrippenkader

Aansluitbeleid	Onder aansluitbeleid wordt verstaan het beleid aangaande de bescherming van de eigen informatiehuishouding van de gemeente in relatie tot de eigen delen van Suwinet en de via Suwinet ter beschikbaar gestelde gegevens (bron: Specifiek Suwinet-normenkader Afnemers d.d. 1.01.2017)
Afnemer	De partij die de Suwigegevens gebruikt voor de uitvoering van haar wettelijke taken (de gemeente).
Applicatieleverancier	Een organisatie die een webapplicatie levert en die conform gemaakte afspraken verantwoordelijk is voor het onderhoud en de eventuele doorontwikkeling aan de software.
Bestaan	Het functioneren van een stelsel van informatiebeveiligings- en beheersingsmaatregelen conform beschrijving op of rond een peildatum.
BIG	Baseline Informatiebeveiliging Nederlandse Gemeenten (gebaseerd op BIR – Baseline Informatiebeveiliging Rijksdienst. De BIG is vervangen door BIO.
BIO	Baseline Informatibeveiliging Overheid
Carve out methode	Bij de carve-out methode wordt in een assurancerapport (zoals een DigiD assessment) een verwijzing opgenomen naar het assurancerapport (de TPM) van een leverancier. De auditor van het assurance- rapport en de auditor van de leverancier houden ieder zelfstandig hun vaktechnische verantwoordelijkheid. De eerste auditor dient wel vast te stellen dat de scope van beide rapportages in voldoende mate op elkaar aansluit.
Hosting leverancier	Een organisatie die conform gemaakte afspraken ICT-infrastructuur inclusief internettoegang aanbiedt waarop een webapplicatie kan worden uitgevoerd en kan worden aangeboden aan gebruikers.
Houder DigiD aansluiting	De organisatie die bij Logius staat geregistreerd als de verantwoordelijke voor een specifieke DigiD aansluiting. Iedere DigiD aansluiting wordt gekenmerkt door een uniek aansluitnummer. Per aansluitnummer is er een houder.
Inclusive methode	Bij de inclusive methode worden alle beheersingsmaatregelen in een assurance rapport overgenomen en er wordt dus niet verwezen naar de van derden verkregen assurancerapporten (TPM's) waar eventueel gebruik van is gemaakt. De auditor van het assurancerapport is vaktechnisch volledig verantwoordelijk en voert indien nodig een dossierreview uit voor een assurancerapport waarvan de resultaten worden overgenomen.
IT-serviceorganisatie	In het Suwinet control framework wordt gesproken over een 'IT-serviceorganisatie'. In het kader van de IT-audit Suwinet dient onder deze term te worden verstaan: 'de externe of interne leverancier die de IT-systemen beheert waarin de Suwi-gegevens van de gebruikersorganisatie (gemeenten) worden verwerkt. Met nadruk wordt opgemerkt dat de softwareleverancier van de applicatie waarin de Suwi-gegevens worden verwerkt, hier NIET mee wordt bedoeld. De essentie is dat de auditor de gegevensstroom volgt en in kaart brengt welke diensten de IT-serviceorganisatie verleend en hoe deze diensten verleend worden. Hiervoor kan de IT auditor gebruik maken van de overeenkomst met de service verlener (DVO/SLA), technische handleidingen van de applicatie en/of informatie verzamelen.

Opzet	De beschrijving van een stelsel van informatiebeveiligings- en beheersingsmaatregelen.
Penetratietest	Dit is een specifieke vorm van een vulnerability-assessment. Het is een proces waarbij met behulp van technische hulpmiddelen specifieke componenten of specifieke delen van de ICT-infrastructuur op zwakheden gecontroleerd worden. (NCSC) In de context van het DigiD assessment wordt met een penetratietest een technisch beveiligingsonderzoek bedoeld dat vanaf het internet wordt uitgevoerd door een (ervaren) penetratietester en waarbij scantools worden ingezet en aanvullende handmatige onderzoeks-werkzaamheden worden uitgevoerd.
SAAS leverancier	Een organisatie die een webapplicatie als online dienst aanbiedt waarbij de klanten de software niet hoeven aan te schaffen. De aanbieder draagt zorg voor onderhoud en doorontwikkeling van (de software van) de applicatie, hosting en applicatiebeheer.
Third Party Mededeling (TPM)	Een TPM is een assurancerapport dat betrekking heeft op een leverancier (serviceorganisatie) waarbij de doelgroep van het rapport een andere is dan de serviceorganisatie en de assurance wordt gegeven door een onafhankelijke auditor. Hierbij wordt opgemerkt dat de aanduiding Third Party Mededeling of TPM geen grondslag kent in de regelgeving van NOREA. In dit document is daarom telkens verwezen naar de term assurancerapport onder opname van de term TPM aangezien deze term in de praktijk nog veel wordt gebruikt door alle bij ENSIA betrokken organisaties.
User control considerations (UCC)	In de UCC paragraaf in een assurancerapport (TPM) worden beheersingsmaatregelen (controls) beschreven waarvan de betreffende leverancier aangeeft dat de gebruikersorganisatie (bijvoorbeeld een gemeente) deze moet hebben ingericht teneinde het stelsel van beveiligings- en beheersingsmaatregelen bij de leverancier optimaal te laten functioneren.
Vulnerability assessment	Dit is een proces waarbij met behulp van technische hulpmiddelen wordt nagegaan in hoeverre in de ICT-componenten kwetsbaarheden voorkomen waarvan ongeautoriseerden gebruik zouden kunnen maken (NCSC). In de context van het DigiD assessment wordt een (bij voorkeur geautomatiseerde) scan bedoeld die vanaf een intern netwerksegment zo dicht mogelijk bij de server wordt uitgevoerd op bekende kwetsbaarheden en ontbrekende patches.

4.7 Bijlage 7: Afkortingenlijst

BAG	:	Basisregistraties Adressen en Gebouwen
BIG	:	Baseline Informatiebeveiliging Nederlandse Gemeenten
BIO	:	Baseline Informatiebeveiliging Overheid
BGP	:	Bruto Gemeentelijk Product = rekenfactor gebaseerd op Verklaringsmodel Lokale Economie
BGT	:	Basisregistratie Grootschalige Topografie, digitale kaart waarop gemeenten infrastructuur op éénduidige wijze moeten vastleggen
BRP	:	Basisregistratie Personen
BRO	:	Basis Registratie Ondergrond
BZK	:	(ministerie van) Binnenlandse Zaken en Koninkrijksrelaties
DigiD	:	Digitale Identiteit (voor overheidsdiensten en zorgverleners)
DKD	:	Digitaal Klant Dossier (in beheer bij het Inlichtingenbureau)
ENSIA	:	Eenduidige Normatiek Single Information Audit
GeVS	:	Gezamenlijke elektronische Voorziening Suwinet
ISAE	:	International Standard on Audit Engagements (ook wel NV COS)
NCSC	:	Nationaal Cyber Security Centrum
PUN	:	Paspoort Uitvoeringsregeling Nederland
SOS	:	Security Officer Suwinet
Suwi(net)	:	Netwerk voor gegevensuitwisseling tussen overheidsorganisaties op basis van de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen
SZW	:	Ministerie van Sociale Zaken en Werkgelegenheid
VNG	:	Vereniging van Nederlandse Gemeenten
VNGR	:	VNG-Realisatie