NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

HANDREIKING Suwinet (in kader ENSIA) voor IT-auditors (RE's)

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 voor de IT-auditors die zich bezighouden met het project Eénduidige Normatiek Single Information Audit (ENSIA) voor gemeenten. Meer in het bijzonder betreft het geven van assurance over het gebruik van de Gezamenlijke elektronische Voorzieningen SUWINET (GeVS)[1] – hierna Suwinet - betrekking hebbende werkzaamheden van gemeenten en hun samenwerkingspartners in het kader van ENSIA.

In het kader van het afstemmen van verwachtingen wordt deze handreiking ook ter beschikking gesteld aan de ENSIA-gremia, de ENSIA-coördinatoren van gemeenten, VNG, samenwerkingsorganisaties, de stelselhouder Suwinet (Ministerie van Sociale Zaken en Werkgelegenheid (SZW)) en de stelselbeheerder / toezichthouder Suwinet (Bureau Keteninformatisering Werk en Inkomen (BKWI)).

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 handreiking zal op basis van het ENSIA-proces 2024 (zelfevaluatie en verantwoording door gemeenten en uitgevoerde audit(s)) in brede zin (ook samenwerkingspartners gemeenten) 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.

[1] https://www.bkwi.nl/producten/Suwinet-services/Suwinet-standaarden/ketenafspraken-ict-beheer/

Versiebeheer

Versie	Datum	Toelichting
Versie 0.1	28 mei 2024	Ten behoeve sub-groep Suwinet van de NOREA-werkgroep ENSIA
Versie 0.2	10 juni 2024	Ten behoeve van de NOREA Werkgroep ENSIA
Versie 0.3	juni 2024	Ten behoeve afstemming ENSIA-gremia
Versie 0.4	4 juli 2024	Ten behoeve afstemming ENSIA-gremia
Versie 0.5	16 juli 2024	Ten behoeve sub-groep Suwinet van de NOREA-werkgroep ENSIA
Versie 0.6	09 oktober 2024	Ten behoeve afstemming ENSIA-gremia
Versie 0.6a	3 december 2024	Ten behoeve Vaktechnische Commissie
Versie 1.0	19 december 2024	Vaststelling bestuur

1.1 Aanleiding

De Verantwoordingsrichtlijn GeVS 2022[1] beschrijft de scope en procedure van verantwoording voor alle partijen die gebruik maken van de GeVS. De Verantwoordingsrichtlijn GeVS 2022 geldt ook voor verantwoordingsjaar 2024.

Op grond van artikel 6.4 van de Regeling SUWINET dient zorg gedragen te worden voor de beveiliging van de gegevens die worden uitgewisseld aan de hand van de Gezamenlijke Elektronische Voorzieningen SUWINET (hierna: GeVS), ook aangeduid als Suwinet, tegen inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevensverwerking.

Daartoe zijn afspraken gemaakt over de informatiebeveiliging, over het te hanteren normenkader en de verantwoording over de naleving daarvan. Deze afspraken zijn vastgelegd in de Verantwoordingsrichtlijn Informatiebeveiliging GeVS[2]. Jaarlijks moeten afnemers van Suwinet-services zich verantwoorden over de informatiebeveiliging conform deze verantwoordingsrichtlijn. Voor gemeenten beperkt zich de ENSIA-verantwoording over Suwinet tot opzet en bestaan van de maatregelen voor het verantwoordingsjaar 2024.

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 domeinspecifieke aspecten.

In ENSIA-verband is door NOREA reeds een Handreiking opgesteld voor de door IT-auditors (RE's) uit te voeren werkzaamheden in het kader van het opstellen van de Collegeverklaring ENSIA en bijlagen in algemene zin. In deze Handreiking wordt nader ingegaan op de door IT-auditors (RE's) in het kader van het ENSIA-verantwoordingsproces uit te voeren werkzaamheden op grond van de specifieke afspraken op grond Verantwoordingsrichtlijn GeVS. De Handreiking kan worden toegepast bij werkzaamheden voor gemeenten en hun eventuele samenwerkingspartners. Zie voor nadere toelichtingen o.a. www.ensia.nl en www.norea.nl (Werkgroep ENSIA)[3].

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

[1] https://www.bkwi.nl/media/anpntl0w/verantwoordingsrichtlijn-informatiebeveiliging-gevs-2022.pdf

[2] Voor de goede orde: Documentnaam BKWI luidt "Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2022" en de titeltekst luidt "Verantwoordingsrichtlijn GeVS 2022". Beide worden in dit document naast elkaar gebruikt.

[3] De HANDREIKING Verantwoordingsrichtlijn Gezamenlijke elektronische Voorzieningen SUWI (GeVS) voor IT-auditors (RE's) is bedoeld als guidance-document voor de IT-auditors die zich bezighouden met het afgeven van assurance(-rapporten) bij verantwoordingen van partijen (anders dan gemeenten) die gebruik maken van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS).

gemeentesecretaris, als ambtelijk verantwoordelijke, een belangrijke rol in de governance van ENSIA. Zo wijst de gemeentesecretaris de ENSIA coördinator van de gemeente formeel aan.

ENSIA integreert al deze typen verantwoordingen in één werkwijze en met één eenduidige taal: de BIO. 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 assurance-rapporten 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 niet gewijzigd.

1.3 Toepassingsgebied ENSIA

ENSIA is alleen van toepassing op gemeenten[1]. De collegeverklaring gaat over DigiD en Suwinet, waarbij de ENSIA-vragenlijst de in de vorige paragrafen genoemde aandachtsgebieden afdekt. Ook subserviceorganisaties en partners zoals Gemeenschappelijke Regelingen (hierna samenwerkingpartners) die diensten aan gemeenten leveren zijn hierbij betrokken.

Met ingang van 2017 is het DigiD-assessment voor gemeenten opgegaan in ENSIA voor wat betreft de reguliere aansluitingen.

In het kader van wet- en regelgeving rond Suwinet wordt alleen gerefereerd aan de gemeente als afnemer. Als afnemer kent Suwinet 'Suwinet inkijk', 'Suwinet inlezen', 'Digitaal Klantdossier (DKD) inlezen' en 'Wet gemeentelijke schuldhulpverlening' (WSG). Zie voor nadere toelichtingen hierop ook bijlage 3. Kern daarvan is dat gemeenten zich over het gebruik van Suwinet voor de gemeente verantwoorden ongeacht waar deze werkzaamheden worden uitgevoerd. Het is wenselijk dat samenwerkingspartijen van de gemeente verantwoording afleggen over het gebruik van Suwinet voor de gemeente en deze verantwoordingsinformatie laten voorzien van een assurance-rapport door een IT-auditor.

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 1.04 normenkader zodat verantwoording op basis daarvan moet plaatsvinden. In afwijking van de Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2022 is voor ENSIA bepaald dat gemeenten zich slechts over de opzet en het bestaan van de maatregelen per 31 december van het verslagjaar dienen te verantwoorden. Voor het verantwoordingjaar 2024 zijn hierin geen wijzigingen doorgevoerd.

[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.

1.4 Toepassing NOREA-Richtlijn 3000 (Herzien) 'Assurance-opdrachten door IT-auditors'

De NOREA-Richtlijn 3000 (Herzien) 'Assurance-opdrachten door IT-auditors' is onderverdeeld in richtlijnen voor attest-opdrachten (3000A) en directe-opdrachten (3000D).
De Verantwoordingsrichtlijn Informatiebeveiliging GeVS (versie 2022) gaat uit van het opstellen van de verantwoording door de verantwoordingsplichtige partij (gemeente en / of samenwerkingspartijen van gemeenten) en het afgeven van een oordeel daarbij door een IT-auditor (RE). In dat kader zijn de bepalingen van NOREA-Richtlijn 3000 onderdeel 3000A van toepassing.
In de praktijk worden opdrachten rond het afleggen van verantwoording door samenwerkingspartijen van gemeenten en het afgeven van een oordeel daarbij door een IT-auditor (RE) vaak uitgevoerd in de vorm van directe-opdrachten. In dat kader zijn de bepalingen van NOREA-Richtlijn 3000 onderdeel 3000D van toepassing.

In lijn met algemeen maatschappelijke ontwikkelingen, waarbij de verantwoordelijkheden van het management inclusief het afleggen van verantwoording over uitgevoerde werkzaamheden centraal staan, streeft het Ministerie van Sociale Zaken en Werkgelegenheid (stelselhouder Suwi) naar het toepassen van de uitgangspunten van de Verantwoordingsrichtlijn Informatiebeveiliging GeVS (versie 2022) binnen de gehele keten. Daarmee geldt ook dat samenwerkingspartijen van gemeenten zich zelfstandig dienen te verantwoorden en dat een IT-auditor (RE) daarbij een oordeel dient af te geven.

Het is de bedoeling dat alle samenwerkingspartijen van gemeenten uiterlijk over het verantwoordingsjaar 2025 voldoen aan de vereisten van de Verantwoordingsrichtlijn Informatiebeveiliging GeVS (versie 2022).
Het verantwoordingsjaar 2024 geldt daarbij als overgangsjaar waarbij de uitvoering van werkzaamheden door de IT-auditor volgens de richtlijnen voor attest-opdrachten (3000A) en directe-opdrachten (3000D) is toegestaan.

Hier is bij de verdere uitwerking van deze handreiking rekening gehouden.

2 Handreiking

Doel van deze handreiking is de IT-auditor een uniform toetsingskader te bieden voor het uitvoeren van het onderzoek naar de bijlage Suwinet van de Collegeverklaring als verantwoordingsdocument (zie bijlage 1.1) alsmede de audit op door samenwerkingspartners op het gebied van Suwinet opgestelde verantwoordingen (zie bijlage 1.2) op basis van de beschikbare normen (zie bijlage 2). Dit kader geldt voor het verantwoordingsjaar 2024.
Deze handreiking dient te worden gelezen in samenhang met de NOREA Handreiking ENSIA voor IT-auditors (RE's) versie 5.0 – verantwoordingsjaar 2024 eventuele gepubliceerde F.A.Q.'s.

ENSIA-ontwikkelingen en ervaringen uit de praktijk worden, indien nodig, vertaald in navolgende versies van deze handreiking. 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 aanvullende vereisten op de geldende standaarden of aanvullende normen van bijvoorbeeld de Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2022 of NCSC-richtlijnen af te leiden.

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 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 ingenomen (zie ook paragraaf 2.7 Kwaliteitsbeheersing).

2.1 Verantwoordingsproces

Verantwoordelijkheden gemeenten / samenwerkingspartijen
In het kader van het ENSIA-verantwoordingsproces gelden de navolgende specifieke verantwoordelijkheden voor de betrokken partijen:

- 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 gemeenten dienen zich te verantwoorden over het eigen gebruik van Suwinetgegevens en de eventueel door de gemeente ingeschakelde samenwerkingspartijen. Zie bijlage 4 voor een nadere toelichting.
- Het verantwoordingsproces (vorm verantwoording / tijdstippen) van de samenwerkingspartijen kan per partij nader uitgewerkt worden maar dient erop gericht te zijn dat de opdrachtgevende gemeente(n) tijdig kunnen voldoen aan de verantwoordingsplicht in het kader van ENSIA. Het verdient aanbeveling dat de betrokken partijen (gemeente – samenwerkingspartij(-en) / samenwerkingspartijen onderling) hierover schriftelijk nadere afspraken maken.

Verantwoordingsproces gemeenten 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 alle vragen geldt dat de gemeente de ondersteunende assurance-informatie (over opzet en bestaan van de beheersmaatregelen) 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 via de zelfevaluatie tool te uploaden. Inleveren kan pas als alle vragen beantwoord zijn.

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 op Suwinet betrekking hebbende vragenlijst dienen de uitkomsten door de ambtelijke organisatie van de gemeente beoordeeld te worden. Het gaat hierbij om de vragenlijst en de door de gemeente verzamelde ondersteunende assurance-informatie waaronder van samenwerkingspartners ontvangen verantwoordingen en bijbehorende assurance-rapporten. Deze beoordeling leidt tot de beantwoording in de ENSIA-tool en leidt tot een daartoe opgenomen rapportageformat 'Suwinet-bijlage bij de Collegeverklaring ENSIA' (bijlage 1.1). Voor de goede orde wordt vermeld dat in tegenstelling tot DigiD bij Suwinet de van derden ontvangen assurance-rapporten niet ter beschikking worden 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, en voor deze Handreiking meer in het bijzonder de 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 assurance-rapport.

Het is wenselijk dat gemeenten van samenwerkingspartijen verantwoordingen conform de 'Suwinet-bijlage bij de Collegeverklaring ENSIA' (zie bijlage 1.2 voorbeeldrapportage) en bijbehorende assurance-rapporten (zie bijlage 5) tijdig ontvangen. Ook voor deze werkzaamheden geldt dat deze bij voorkeur 'assertion based' uitgevoerd worden.

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

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 assurance-rapport (hiervoor zijn de voorwaarden voor het electronisch ondertekenen van de stukken onverkort van toepassing – zie ook Handreiking ENSIA voor IT-auditors).

De IT-auditor dient bij de 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.

Bij de uitvoering van werkzaamheden voor samenwerkingspartijen dient de IT-auditor rekening te houden met de tussen de gemeente en samenwerkingspartijen gemaakte afspraken rond oplevering van verantwoordingsdocumenten en bijbehorende assurance-rapporten alsmede de doorlooptijd van de formele behandeling ervan door de bestuursorganen van deze partijen.

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).

2.2 Uitvoeren werkzaamheden door 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.

Bij ENSIA is de oplevering thans in de vorm van een attest-opdracht op basis van de Collegeverklaring ENSIA en bijlagen (in het bijzonder bijlage 1 Suwinet) danwel Suwinet-verantwoording van een samenwerkingspartij van de gemeenten ('attestation based audit'/ 'assertion based audit'). Hierna wordt gerefereerd aan de Suwinet-verantwoording.

Hoewel de Suwinet-verantwoording het object van controle vormt, zijn de ingevulde vragenlijsten (de zelfevaluaties) in de ENSIA-tool (gemeenten) en de door de betrokken organisaties (gemeenten en samenwerkingspartners) gedocumenteerde ondersteunende assurance-informatie voor de IT-auditor het basismateriaal waar elke IT-auditor vanuit kan gaan en assurance-informatie vormt tijdens het veldwerk.

Op basis van de eigen risicoanalyse, zoals die voor elke 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 verantwoordingsproces/ de verantwoordingsprocessen 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.

De opdracht bestaat met name 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 relevantie en betrouwbaarheid van het aangereikte basismateriaal bij de onderscheiden onderdelen. In deze setting toetst de IT-auditor tussentijds en blijft objectief en onafhankelijk, terwijl de opdrachtgever / betrokken organisatie tijdig in de gelegenheid wordt gesteld verbeteringen door te voeren. De IT-auditor is daarbij niet inhoudelijk betrokken ter voorkoming van zelftoetsing.

Ook het aspect van risico-inschatting is van belang. Op basis hiervan bepaalt de auditor de timing en met welke diepgang de verschillende werkzaamheden moeten plaatsvinden.

2.3 Formele aspecten van de assurance-opdracht

Een ENSIA- of Suwinet-audit betreft een assurance-opdracht gericht op het geven van een oordeel met een redelijke mate van zekerheid, conform Richtlijn 3000 A (Attestopdracht). De verantwoordelijke partij komt met een Suwinet-verantwoording waarover de IT-auditor met redelijke mate van zekerheid een oordeel geeft. Beoogde gebruikers van deze Suwinet-verantwoording en het assurance-rapport (oordeel) van de IT-auditor zijn de organen die toezien op de informatieveiligheid van Suwinet. De uitvoering van de audit dient in opdracht van het verantwoordelijk management plaats te vinden.

Doel van de audit is het verkrijgen van voldoende geschikte assurance-informatie om een oordeel met redelijke mate van zekerheid te verschaffen of de Suwinet-verantwoording, in alle van materieel belang zijnde aspecten, juist is. Hierbij zijn de eisen vanuit de regelgeving voor Suwinet leidend.

De criteria voor een IT-audit inzake de Suwinet-verantwoording betreffen de normen inzake zoals in deze Handreiking neergelegd. De criteria worden ook in de Suwinet-verantwoording kenbaar gemaakt en zijn daarmee toegankelijk voor de gebruikers.

Het gaat om opzet en bestaan van de maatregelen per 31 december 2024[1]. Eventuele veranderingen / verbetermaatregelen in de periode tussen 31 december 2024 (c.q. datum vaststellen Suwinet-verantwoording) en de datum van afgeven van het assurance-rapport dient het verantwoordelijk management in principe in de Suwinet-verantwoording toe te lichten[2]. Deze verbetermaatregelen / het verbeterplan zijn geen onderdeel van het onderzoek van de IT-auditor.

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.

2.4 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.

2.5 'Pre-audit'

De ENSIA-vragenlijsten zijn vanaf 1 juli beschikbaar voor de gemeenten en zij hebben tot 31 december de tijd om de vragenlijsten in te vullen en op te leveren. Inleveren kan pas als alle vragen zijn beantwoord. De afronding van de IT-audit vindt (pas) plaats 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 Suwinet binnen de gemeente. E.e.a. is onverkort ook van toepassing bij de samenwerkingspartijen. Het advies is om een zogenaamde 'pre-audit' of interim audit af te spreken en uit te voeren waarbij de IT-auditor Suwinet-normen tussentijds toetst, het proces van oplevering beoordeelt en de uitkomsten rapporteert aan de opdrachtgever. De opdrachtgever wordt op deze wijze in de gelegenheid gesteld de nodige verbeteringen door te voeren alvorens de vragenlijsten / verantwoording definitief worden ingeleverd.

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

2.6 Opdrachtaanvaarding en continuering

Vereisten vanuit de Richtlijn Opdrachtaanvaarding zijn onverkort van toepassing. Het onderzoek heeft betrekking op informatiebeveiliging. Competentie en capaciteit van het IT-audit opdrachtteam op dit terrein is dan ook een randvoorwaarde. Ervaring met het uitvoering van Suwinet-audits alsmede kennis van het gemeentelijke domein in brede zin zijn daarbij wenselijk.

2.7 Kwaliteitsbeheersing

Het Reglement Kwaliteitsbeheersing NOREA (RKBN) is van toepassing, dit komt ook tot uitdrukking in het assurance-rapport. Gegeven de aard van de opdracht, het maatschappelijke belang en mogelijk brede verspreidingskring van de Collegeverklaring en het assurance-rapport (o.a. als gevolg van de Wet open overheid) dient voor de op Suwinet-verantwoording gerichte audits expliciet een opdrachtgerichte kwaliteitsbeoordeling (OKB) overwogen te worden.

Overwegingen hierbij kunnen zijn (niet limitatieve opsomming):

a. Stelselgerelateerd: Grote wijzigingen in Suwinet zoals:
    a. Toevoegen van applicaties / aanpassing in wet- en regelgeving die onder de reikwijdte van Suwinet vallen;

[1] 31 december 2024 peildatum voor gemeenten, peildatum voor samenwerkingspartijen tussen partijen nader overeen te komen

[2] 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 assurance-rapport waarin hierop wordt gewezen.

        b. Aanpassingen in wijze verantwoorden;
        c. Aanpassingen in auditverplichting.
    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 assurance-rapport 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.

2.8 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 op de Suwinet-verantwoording gerichte 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: Suwinet;
- Interne Controle Risico: betreft een inschatting van de kwaliteit van de beheeromgeving van de opdrachtgever bij de totstandkoming van de Suwinet-verantwoording;
- 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 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.

2.9 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

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

normen/ vragen op basis van relevante assurance-informatie die door het college is verzameld[1]. Deze (assurance-)informatie omvat ook voor de IT-auditor een basis 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 uitvoering 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 voldaan wordt aan de desbetreffende norm.

Bij werkzaamheden rond een Suwinet-verantwoording van een samenwerkingspartij zal de IT-auditor niet alleen het proces van tot stand brengen van de Suwinet-verantwoording 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 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 assurance-rapport. Zie ook paragraaf 2.11.

2.10 Uitbesteding door partijen

Partijen, in het bijzonder gemeenten, blijven ook in het geval van uitbesteding en/ of samenwerking met andere organisaties bestuurlijk verantwoordelijkheid voor het gebruik van Suwinet gegevens en dienen daarover verantwoording af te leggen in een Suwinet-verantwoording.

Dit betekent dat de IT-auditor zich met betrekking tot Suwinet ook een oordeel moet vormen over de door de -in het netwerk geïdentificeerde- externe partijen uitgevoerde werkzaamheden en deze in zijn oordeelsvorming moet betrekken, hetzij via de inclusive (zie **), 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 op de Suwinet-verantwoording gerichte audit.

Zie voor een nadere toelichting bijlage "Overwegingen ENSIA IT-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.

<u>Werkzaamheden auditor</u>
Bij uitbesteding door de gemeente aan een externe partij (samenwerkingsverband / externe leverancier/ combinatie van beide) heeft het de voorkeur dat de externe partij een assurance-rapport (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.

(**) Indien geen assurance-rapport geleverd kan worden dan wordt in opdracht van de opdrachtgever 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 opdrachtgever ingeschakelde auditor worden gedaan. Voorwaarde hiervoor is dat de 'contractuele bepalingen' tussen de gemeente

[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.

en de externe partij / contractuele bepalingen externe partijen onderling dit onderzoek mogelijk maken.

De (ENSIA-) auditor van de gemeente dient 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 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 assurance-rapport (conform Richtlijn 3000 , ISAE 3402 of vergelijkbaar) kan leveren. Een ISO 27001 - certificering is voor het doel van ENSIA-doeleinden onvoldoende.

Verbeterplannen
De IT-auditor geeft geen oordeel over de toereikendheid (en uitvoering) van het verbeterplan van de opdrachtgever naar aanleiding van eventuele bevindingen / tekortkomingen in het kader van het verantwoordingsproces bij de opdrachtgever gesignaleerde bevindingen.. 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 Suwinet-verantwoording.

2.11 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 assurance-rapport.

Deze omvat:
- Een herbevestiging van de Suwinet-verantwoording;
- 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 Suwinet-verantwoording en de assurance die daarbij wordt afgegeven.

2.12 Het vormen van het oordeel

Bij het vormen van het oordeel worden de bepalingen uit het stramien voor assurance-opdrachten en Richtlijn 3000 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 assurance-rapport (beperking of oordeelonthouding).

Omdat in de Suwinet-verantwoording 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 wel van belang om de eventuele verbeterplannen expliciet in de paragraaf ter benadrukking van aangelegenheden te benoemen.

[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.

In die gevallen waarin naar de mening van de IT-auditor de Suwinet-verantwoording een getrouw beeld geven van de informatiebeveiliging bij de opdrachtgever 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 assurance-rapport dit tot uitdrukking in een paragraaf ter benadrukking van aangelegenheden. Zie hiervoor Richtlijn 3000 paragraaf 77b.

2.13 Het opstellen van het assurance-rapport

Voor de audit van de Suwinet-verantwoording is gekozen voor een structuur voor het assurance-rapport 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 5 zijn de formats assurance-rapporten opgenomen. Hieraan zijn ook voorbeeldteksten toegevoegd voor een oordeel met beperking / afkeurend oordeel en de oordeelonthouding. Deze formats zijn in het bijzonder bestemd voor toepassing bij het afgeven van assurance bij verantwoordingen van samenwerkingspartijen van gemeenten. In de formats assurance-rapporten is meer expliciet opgenomen op welk gebruik van Suwinet gegevens het oordeel betrekking heeft.

Bij het door de IT-auditor ondertekende assurance-rapport 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 assurance-rapporten bij serviceorganisaties is het vereist dat bij het toetsen van de bestaan / werking ook een bijlage wordt toegevoegd met een beschrijving van de uitgevoerde toetsingen van de interne beheersmaatregelen en de resultaten daarvan. 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.

2.14 Overige rapportages

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

2.15 Documentatie

De IT-auditor dient tijdig opdrachtdocumentatie op te stellen die een vastlegging van de basis voor het assurance-rapport 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 opdrachtgever ten behoeve van het verzamelen en vastleggen van assurance-informatie gebruikte systemen niet toegestaan aangezien deze geïnterpreteerd kunnen worden als een (goedkeurend) oordeel met betrekking tot het betreffende deelonderwerp / vraag.

2.16 Consultatie

Indien een auditor[1] in het kader van de uitvoering van op Suwinet-verantwoording gerichte 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.

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 / stelselbeheerder / toezichthouder.

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 op Suwinet-verantwoordingen gerichte opdrachten betrokken auditors / alle leden NOREA (verantwoordelijkheid NOREA) en / of stelselhouder / stelselbeheerder / toezichthouder 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 op een Suwinet-verantwoording gerichte 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 beheersmaatregelen 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 op een Suwinet-verantwoording gerichte audit geen specifiek onderzoek op uit.

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

Bijlagen

Bijlage 1: Verantwoordingsmodellen

Bijlage 1.1 Bijlage bij Collegeverklaring ENSIA

Bijlage 2: Gebruik van Suwinet maakt onderdeel uit van de Collegeverklaring ENSIA. Deze vormt onderdeel van het object van onderzoek door de IT-auditor. Op dit onderdeel is deze Handreiking van toepassing.

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>[12]	[Niet van toepassing] [Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente][13]	 [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]

[12] Alleen de regiogemeente moet verantwoorden en niet de aangesloten gemeente.
[13] 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 beheersmaatregelen 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]]

]

Bijlage 1.2 Verantwoording gebruik Suwinet <organisatienaam>

Verantwoording gebruik Suwinet <organisatienaam> kan gebruikt worden als verantwoording door samenwerkingspartners van gemeenten in het kader van de door de gemeente op te stellen Collegeverklaring ENSIA. Hiervan maakt de verantwoording over het gebruik Suwinet onderdeel uit (bijlage 2). De Verantwoording gebruik Suwinet vormt het object van onderzoek door de IT-auditor waarop deze Handreiking van toepassing is.

Verantwoording gebruik van Suwinet <organisatienaam>

Dit document vormt Verantwoording informatiebeveiliging Suwinet per 31-12-2024 <organisatienaam> . 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 <organisatienaam> 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 <organisatienaam> 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-SUWINET-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 evaluatie van <organisatienaam>, tenzij sprake is van een gedeelde norm.

De evaluatie 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 assurance-rapportage[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>[14]	[Niet van toepassing] [Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente][15]	 [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]

[14] Alleen de regiogemeente moet verantwoorden en niet de aangesloten gemeente.
[15] 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 beheersmaatregelen 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]]

]

Bijlage 2: Normenkader GeVS 2022 versie 1.0

Bijgaande tabel is ontleend aan de Verantwoordingsrichtlijn GeVS 2022 en geeft in hoofdlijnen het actuele normenkader weer. Dit normenkader verwijst naar de geselecteerde BIO-normen.

Hoofdstuk	Nummer	Normen
5. Informatiebeveiligings-beleid	5.1.1.	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
5. Informatiebeveiligings-beleid	5.1.2	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
6. Organiseren van informatiebeveiliging	6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.
6. Organiseren van informatiebeveiliging	6.1.2	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
7. Veilig personeel	7.2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
9. Toegangsbeveiliging	9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
9. Toegangsbeveiliging	9.2.2	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
9. Toegangsbeveiliging	9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
9. Toegangsbeveiliging	9.2.6	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
10. Cryptografie	10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en Geïmplementeerd.
12. Beveiliging bedrijfsvoering	12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.
12. Beveiliging bedrijfsvoering	12.1.2[16]	Wijzigingsbeheer: Veranderingen in de organisatie, bedrijfs-processen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.
12. Beveiliging bedrijfsvoering	12.1.4[17]	Scheiding van ontwikkel-, test- en productieomgevingen: Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of

[16] In overleg met Domeingroep / VNG / NOREA toegevoegd als GITC-norm voor de inleesapplicatie

[17] Idem

		veranderingen aan de productieomgeving te verlagen.
12. Beveiliging bedrijfsvoering	12.4.1[18]	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
12. Beveiliging bedrijfsvoering	12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	14.2.2[19]	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework.
18. Naleving	18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

[18] Idem

[19] Idem

Bijlage 3: Testaanpak bij de te onderzoeken normen relevant voor Suwinet

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
5. Informatiebeveiligingsbeleid			
5.1.1 Beleidsregels voor informatiebeveiliging	Criterium BIO: Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. Doelstelling: Richting geven aan en handhaven van beveiliging van de Suwinet aansluiting en de gegevens die worden getransporteerd en ervoor te zorgen dat aansluiting van de gemeente op Suwinet aantoonbaar aan de vereiste beveiligingsvoorwaarden voldoet. *Risico:* *Het risico bestaat dat de bescherming van de aansluiting op Suwinet, in tegenstelling tot bescherming van haar eigen ICT omgeving, onvoldoende aandacht krijgt.*	5.1.1.1 Er is een informatiebeveiligingsbeleid opgesteld door de gemeente. Dit beleid is vastgesteld door het College van B&W van de gemeente, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen en bevat ten minste de volgende punten: a) De strategische uitgangspunten en randvoorwaarden die de gemeente hanteert voor informatiebeveiliging en in het bijzonder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid. b) De gemeente van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden. c) De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers. d) De gemeenschappelijke betrouwbaarheidseisen en normen die op de gemeente van toepassing zijn. e) De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd.	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: De gemeente moet beschikken over een Suwinet informatiebeveiligingsbeleid (eventueel als onderdeel van het algehele informatiebeveiligingsbeleid). Het informatiebeveiligingsbeleid betreft het beleid aangaande de bescherming van de eigen informatiehuishouding in relatie tot de eigen delen van Suwinet en de via Suwinet beschikbaar gestelde gegevens. Diepgang: Opzet en bestaan Test aanpak: Inspectie van het informatiebeveiligingsbeleid. Deze dient inzicht te geven in de in 5.1.1.1 genoemde type maatregelen voor de beveiliging van de eigen delen van Suwinet (bijv. organisatorische-, technische- en beheersingsmaatregelen). Stel vast dat het beleid is vastgesteld door het College van B&W van de gemeente (het dagelijks bestuur).

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
		f) De bevordering van het beveiligingsbewustzijn.	Stel vast dat het beleid is gepubliceerd en gecommuniceerd aan medewerkers en relevante partijen zoals bijvoorbeeld subserviceorganisaties. Interview de verantwoordelijke functionarissen.
5.1.2 Beoordeling van het informatie-beveiligingsbeleid	Criterium BIO: Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is. Doelstelling: Bewerkstellingen dat de getroffen beveiligingsmaatregelen continue voldoen aan het juiste beveiligingsniveau. *Risico:* *De getroffen beveiligingsmaatregelen kunnen ontoereikend zijn in relatie tot aangescherpte wetgeving, verandering van risicoklasse van gegevens en de toegepaste technologieën.*	5.1.2.1 Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: Het Suwinet informatiebeveiligingsbeleid (eventueel als onderdeel van het algehele informatiebeveiligingsbeleid) dient actueel te zijn en periodiek* te worden beoordeeld en zo nodig te worden bijgesteld bij grote wijzigingen of aan de hand van externe ontwikkelingen. **Note: hiervoor geldt dat de periodiciteit aansluit bij de (bestaande) bestuurs- en P&C-cycli. Voor overheidsorganisaties geldt doorgaans dat dit een periode van 4 jaar is.* **Note: sluit hierbij aan op het voor de gemeente vastgestelde beleid ten aanzien van periodieke beoordeling van het (specifieke Suwinet) beveiligingsbeleid.* Diepgang: Opzet en bestaan

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			Test aanpak: Inspectie van het informatiebeveiligingsbeleid. Stel minimaal jaarlijks vast dat het beleid aantoonbaar actueel is en conform de (bestaande) bestuurs- en P&C-cycli is bijgesteld. Beoordeel hierbij ook of er sprake is van significante (beleids-) wijzigingen die van invloed zijn op het (eventueel tussentijds) bijstellen van het informatiebeveiligingsbeleid. Interview de verantwoordelijke functionarissen.
6. Organiseren van informatiebeveiliging			
6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	Criterium BIO: Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. Doelstelling: Het voorkomen dat risico's optreden als gevolg van het ontbreken van coördinatie op het gebied van activiteiten aangaande de bescherming van de eigen delen van Suwinet. *Risico:* *Het risico bestaat dat door gebrek aan coördinatie van activiteiten niet op beveiligingsincidenten wordt geacteerd en dat door wijzigingen nieuwe kwetsbaarheden ontstaan.*	6.1.1.1 Het Coilege van B&W van degemeente heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar gemeente. 6.1.1.2 De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten. 6.1.1.3 De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd. 6.1.1.4 Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit de verschillende delen van de gemeente met relevante rollen en functies. Controle technische functiescheiding (CTFS) is hierbij van belang waar van toepassing waar het gaat om het onderscheiden van verantwoordelijkheid. Diepgang: Opzet en bestaan.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			Test aanpak: Inspecteer het informatiebeveiligingsbeleid en stel minimaal jaarlijks vast dat taken, bevoegdheden en verantwoordelijkheden (CTFS) ten aanzien van de IB functie t.a.v. Suwinet formeel zijn vastgesteld en stel vast dat deze functie en onderliggende rol(-len) ook als zodanig zijn ingericht* en beschreven. **Note: idealiter zijn bovenstaande documenten onderdeel van een ingerichte AO/IB. Het gaat onder meer om de Suwinet gebruikersbeheerder(s), de security officer(s) Suwinet en Suwinet gemandateerde(n).* Zie ook 12.4.1. Incidentmanagementproces (als onderdeel van het informatiebeveiligingsbeleid) Interview de verantwoordelijke functionarissen.
6.1.2 Scheiding van taken	Criterium BIO: Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de gemeente te verminderen. Doelstelling: Ervoor zorgen dat de juiste taken en verantwoordelijkheden binnen de onderkende rollen juist worden uitgevoerd met inachtneming van de juiste functiescheiding voor zover de organisatiegrootte dit toelaat.	6.1.2.1 Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen* waarnemen of voorkomen. * **Note: o*nder bedrijfsmiddelen worden in dit verband de Suwinet gegevens met name begrepen.	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd (in de vorm van bijvoorbeeld een RACI-matrix*).

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
	<u>Risico:</u> *Onduidelijke taken en verantwoordelijkheden en het ontbreken van juiste functiescheiding kunnen leiden tot:* *- misbruik van bevoegdheden,* *- te ruim toegekende bevoegdheden,* *- over het hoofd zien van en/of tot implementatie van tegenstrijdige beveiligingsmaatregelen.*		**Note: RACI staat voor Responsible, Accountable, Consulted en Informed. Idealiter onderdeel van een ingerichte AO/IB.* **Note: de taken, verantwoordelijkheden en bevoegdheden van de betrokken Suwinet functionarissen zijn beschreven in (een) autorisatiematrix(ces), daarbij is rekening gehouden met conflicterende rollen zoals:* • *t.a.v. invoerende en controlerende taken;* • *Beheer Suwinet versus Security officer Suwinet;* • *Beheerder(s) Suwinet/ Security officer Suwinet versus medewerkers met Suwinet inkijk en SUWINET-inlezen rechten;* • *Autoriseren van toewijzing van toegang tot Suwinet gerelateerde gegevens;* • *Controleren van rechtmgebruik van Suwinet gerelateerde gegevens;* • *Controleren van de actualiteit van de gebruikersadministratie;* • *Melding van incidenten gerelateerd aan Suwinetgegevens;* De gedocumenteerde rollen zijn door het College van B&W dagelijks bestuur/ de directie (dit kan per gemeente verschillen) onderkend, goedgekeurd en van toepassing verklaard. Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de gemeente te verminderen. Het gaat hierbij om de verantwoordelijkheden van lijnmanagement, security management, maar ook bijvoorbeeld informatiemanagement en control. <u>Diepgang:</u> Opzet en bestaan

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			Test aanpak: Inspecteer de relevante functie/taakbeschrijvingen van met name de sleutelfunctionarissen, de autorisatiematrix en het autorisatiebeheerproces, en stel vast dat deze voldoen aan bovenstaande aandachtspunten. Stel vast dat functionarissen benoemd zijn en actief invulling geven aan hun rol. Doe een deelwaarneming om de opzet en het bestaan van de beheersingsmaatregelen te kunnen vaststellen. Interview de verantwoordelijke functionarissen.
7. Veilig personeel			
7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Criterium BIO: Alle medewerkers van de gemeente en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de gemeente, voor zover relevant voor hun functie. Doelstelling: Het bewustmaken van gebruikers van Suwinet gegevens *Risico:* *Indien gebruikers van Suwinet gegevens zich niet of onvoldoende bewust zijn van de*	7.2.2.1 Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen. 7.2.2.2 Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: a) De gemeente moet beschikken over een procedure die zorg draagt voor het adequaat houden van het bewustzijn onder de medewerkers ten aanzien van informatiebeveiliging/ het werken met (privacy) gevoelige data. Dit kan worden bereikt door

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
	(hoge) vertrouwelijkheid, bestaat het risico dat deze gegevens onvoldoende worden beschermd.	7.2.2.3 Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.	bewustwordingssessies, trainingen, social engineering, etc. b) De gemeente moet in dit kader waarborgen scheppen die ervoor zorgen dat gebruikers hun gebruikersidentificaties niet delen met andere gebruikers. Bij voorkeur is dit opgenomen in de gedragsregels. <u>Diepgang:</u> Opzet en bestaan van maatregelen rond bewustzijn, opleiding en training ten aanzien van informatiebeveiliging. <u>Test aanpak:</u> Stel vast op basis van inspectie dat in een procedure / informatiebeveiligingsplan is vastgelegd dat periodiek (bij voorkeur meerdere malen per jaar, doch minimaal jaarlijks[20]) aandacht wordt besteed aan bewustwording van informatiebeveiliging waarbij expliciet aandacht wordt besteed aan Suwinet gerelateerde onderwerpen. Stel vast dat deze bewustwordingswerkzaamheden daadwerkelijke ten uitvoer zijn gebracht. Interview de verantwoordelijke functionarissen. **Note: dit normaspect is gerelateerd aan norm 18.1.4 waarin is opgenomen dat het beleid ten aanzien van het verwerken van persoonsgegevens dient te worden gecommuniceerd aan alle personen die betrokken zijn bij deze verwerking.*

[20] Het verantwoordelijke management dient jaarlijks de behoefte t.a.v. bewustwordingsactiviteiten voor het komende jaar vast te stellen.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
9. Toegangsbeveiliging			
9.2.1 Registratie en afmelden van gebruikers	Criterium BIO: Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. Doelstelling: Gebruikers en beheerders de juiste toegangsrechten geven (niet meer en niet minder) dan welke nodig zijn voor de hen opgedragen (wettelijke)taken. *Risico:* *Het risico bestaat dat medewerkers onrechtmatig toegang hebben tot Suwinet of tot de via Suwinet beschikbaar gestelde gegevens.* *Voor Suwinet geldt een verhoogd risico omdat het Suwinet account van een gemeente ook toegang tot Suwinet kan krijgen vanuit het domein van een ander op Suwinet aangesloten gemeente.*	9.2.1.1 Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties. 9.2.1.2 Het gebruiken van groepsaccounts is niet toegestaan, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD ** Let op: Voor Suwinet en DKD Inlezen is de "inleesapplicatie" met de eventuele bijbehorende database in scope.* Toelichting: Beheersmaatregelen 9.2.1, 9.2.2, 9.2.5 en 9.2.6 hangen nauw met elkaar samen: 9.2.1 richt zich op de registratie en het afmelden van gebruiker 9.2.2 richt zich op het proces van het toekennen van rechten aan gebruikers 9.2.5 richt zich op het periodiek beoordelen van toegangsrechten van gebruikers 9.2.6 richt zich op het proces van intrekken of wijzigen van toegangsrechten De procedure voor het beheren van gebruikersidentificaties (denk aan HR procedure in-/ uit dienst en functiewijziging) is gericht op de gebruikers en, indien van toepassing, de beheerders met toegang tot Suwinet gegevens en behoort te omvatten: a) het gebruik van unieke gebruikersidentificaties zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			hun acties; op gebruikersniveau is het gebruik van groepsaccounts niet toegestaan. Het gebruik van groepsidentificaties voor beheertaken dient alleen te worden toegelaten als deze om bedrijfs- of operationele redenen noodzakelijk zijn. Hiervoor geldt dat dit op het juiste niveau behoort te worden goedgekeurd en gedocumenteerd en dat adequate login wordt toegepast zodat te allen tijde herleidbaar is wie met dit account wanneer en tot welke gegevens toegang heeft gehad; b) Het onmiddellijk ongeldig maken of verwijderen van de gebruikersidentificatie van gebruikers die de gemeente hebben verlaten (zie ook 9.2.6);Daarnaast dient de gemeente een actief beleid te hebben gericht op het herbenoemen van / disablen van admin-accounts bij installatie van software. Diepgang: Opzet en bestaan van de beheersingsmaatregelen. Test aanpak: Inspecteer het autorisatiebeheerproces en stel vast dat dit proces in lijn is met bovenstaande aandachtspunten. Neem als uitgangspunt het HR proces waar joiners, movers en leavers primair bekend zijn en in de workflow zitten. Betrek hierbij (de beschrijving van de eventuele) interface tussen de personeelsinformatiesystemen en de IAM-tooling. Betrek hierbij ook de specifieke methodiek voor inloggen (bijv. single sign-on) gehanteerd bij de gemeente.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			Betrek hierbij ook de wachtwoordinstellingen van de Suwinet-applicaties. Doe een deelwaarneming om de opzet en het bestaan van de beheersingsmaatregelen te kunnen vaststellen en stel vast da I Zie verder ook 9.2.2, 92.5 en 9.2.6. Interview de verantwoordelijke functionarissen.
9.2.2 Gebruikers toegang verlenen	Criterium BIO: Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. Doelstelling Bewerkstelligen dat de geclaimde identiteit van de gebruiker kan worden bewezen en dat daardoor alleen bevoegde gebruikers toegang krijgen tot Suwinet diensten. *Risico:* *Onbevoegde gebruikers kunnen toegang krijgen tot Suwinet diensten.*	9.2.2.1 Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris. 9.2.2.2 Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven[21]. 9.2.2.3 Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD ** Let op: Voor Suwinet en DKD Inlezen is de "inleesapplicatie" met de eventuele bijbehorende database in scope.* Toelichting: Beheersmaatregelen 9.2.1, 9.2.2, 9.2.5 en 9.2.6 hangen nauw met elkaar samen: 9.2.1 richt zich op de registratie en het afmelden van gebruiker 9.2.2 richt zich op het proces van het toekennen van rechten aan gebruikers

[21] Voor Suwinet inkijk geldt dat deze risicoafweging door BKWI is uitgevoerd en dat op basis hiervan de typerollen zijn bepaald.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			9.2.5 richt zich op het periodiek beoordelen van toegangsrechten van gebruikers 9.2.6 richt zich op het proces van intrekken of wijzigen van toegangsrechten De procedure voor het toewijzen of intrekken van toegangsrechten aan gebruikersidentificaties is gericht op de gebruikers en, indien van toepassing, de beheerders met toegang tot Suwinet gegevens en behoort te omvatten: a) autorisatie verkrijgen van de eigenaar van het informatiesysteem of de informatiedienst voor het gebruik van het informatiesysteem of de informatiedienst. Afzonderlijke goedkeuring voor toegangsrechten door het dagelijks bestuur/ de directie is mogelijk ook relevant; b) verifiëren dat het verleende toegangsniveau in overeenstemming is met de beleidsregels voor toegang en consistent is met andere eisen zoals een scheiding van taken (zie ook 6.1.2); c) waarborgen dat toegangsrechten niet worden geactiveerd (bijv. door dienstverleners) voordat de autorisatieprocedures zijn afgerond; d) bijhouden van een centraal overzicht van toegangsrechten die aan een gebruikersidentificatie zijn toegekend om toegang te verkrijgen tot informatiesystemen en -diensten; e) aanpassen van toegangsrechten van gebruikers van wie de rollen of functies zijn gewijzigd en toegangsrechten van gebruikers die de gemeente hebben verlaten onmiddellijk verwijderen of blokkeren;

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			f) met eigenaren van de informatiesystemen of -diensten periodiek de toegangsrechten beoordelen (zie ook 9.2.5). Diepgang: Opzet en bestaan van de beheersingsmaatregelen. Test aanpak: Stel vast dat is vastgelegd welke personen bevoegdheden hebben voor het verlenen van toegangsrechten (bijvoorbeeld in een mandaatregister en/ of functieprofielen). Doe een deelwaarneming om de opzet en het bestaan van de beheersingsmaatregelen te kunnen vaststellen. Interview de verantwoordelijke functionarissen.
9.2.5 Beoordeling van toegangsrechten van gebruikers	Criterium BIO: Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. Doelstelling: Het vaststellen of: de autorisaties en veranderingen hierin juist en tijdig zijn aangebracht, de juiste functiescheiding zijn toegepast en voldaan wordt aan de principes van doelbinding en proportionaliteit, oneigenlijk autorisatie-toekenningen hebben plaatsgevonden. *Risico:*	9.2.5.1 Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld. (Overruled door 9.2.5.3) 9.2.5.2 De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident. 9.2.5.3 Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD ** Let op: Voor Suwinet en DKD Inlezen is de "inleesapplicatie" met de eventuele bijbehorende database in scope.* Toelichting:

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
	Bij het ontbreken van controle op de toegangsrechten worden afwijkingen in het autorisatieproces niet gesignaleerd worden. Bij het ontbreken controles op het gebruik van autorisaties wordt misbruik niet gesignaleerd.		Beheersmaatregelen 9.2.1, 9.2.2, 9.2.5 en 9.2.6 hangen nauw met elkaar samen: 9.2.1 richt zich op de registratie en het afmelden van gebruiker 9.2.2 richt zich op het proces van het toekennen van rechten aan gebruikers 9.2.5 richt zich op het periodiek beoordelen van toegangsrechten van gebruikers 9.2.6 richt zich op het proces van intrekken of wijzigen van toegangsrechten Het (lijn)management behoort de toegangsrechten van gebruikers en, indien van toepassing, beheerders met toegang tot Suwinet gegevens regelmatig te beoordelen in een formeel proces. Bij het beoordelen van toegangsrechten van gebruikers behoren de volgende aspecten in overweging te worden genomen: a) toegangsrechten van gebruikers behoren regelmatig en na wijzigingen, zoals promotie, degradatie of beëindiging van het dienstverband, te worden beoordeeld; b) toegangsrechten van gebruikers behoren te worden beoordeeld en opnieuw te worden toegekend bij functieverandering binnen dezelfde gemeente; c) autorisaties voor speciale toegangsrechten behoren vaker te worden beoordeeld; d) toewijzingen van speciale toegangsrechten behoren regelmatig te worden gecontroleerd om te waarborgen dat speciale toegangsrechten niet onbevoegd zijn verkregen;

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			e) van wijzigingen in speciale accounts behoren voor periodieke beoordeling logbestanden te worden bijgehouden. <u>Diepgang:</u> Opzet en bestaan van de beheersingsmaatregelen. <u>Testaanpak:</u> Stel vast hoe het eigenaarschap van Suwinet gegevens is geregeld. Stel vast dat de periodieke review minimaal eenmaal per halfjaar plaatsvindt. Stel vast dat de periodieke review in lijn is met bovenstaande aandachtspunten. Stel met behulp van tenminste één deelwaarneming vast dat de opvolging van bevindingen uit de periodieke review worden gedocumenteerd en behandeld als beveiligingsincident*. Interview de verantwoordelijke functionarissen. ** Note: indien er geen beveiligingsincidenten m.b.t. autorisatie van Suwinet hebben plaatsgevonden in het verantwoordingsjaar dan is norm alleen qua opzet te beoordelen. Geef dat aan "voldoet in opzet"*

9.2.6 Toegangsrechten intrekken of aanpassen	<u>Criterium BIO:</u> De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast. <u>Doelstelling:</u> Het tijdig beëindigen of wijzigen van de toegangsrechten. <u>*Risico:*</u> *Als toegangsrechten niet bijtijds worden beëindigd of gewijzigd, bestaat het risico op onbevoegde kennisname van Suwinet gegevens.*	(Geen onderliggende specifieke overheidsmaatregel)	<u>Betrokken partij(en):</u> Gemeente / samenwerkingspartij <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD ** Let op: Voor Suwinet en DKD Inlezen is de "inleesapplicatie" met de eventuele bijbehorende database in scope.* <u>Toelichting:</u> Beheersmaatregelen 9.2.1, 9.2.2, 9.2.5 en 9.2.6 hangen nauw met elkaar samen: 9.2.1 richt zich op de registratie en het afmelden van gebruiker 9.2.2 richt zich op het proces van het toekennen van rechten aan gebruikers 9.2.5 richt zich op het beoordelen van toegangsrechten van gebruikers 9.2.6 richt zich op het proces van intrekken of wijzigen van toegangsrechten Bij beëindiging van het dienstverband behoren de toegangsrechten van een persoon voor informatie en bedrijfsmiddelen die samenhangen met informatieverwerkende faciliteiten en diensten t.a.v. Suwinet gegevens te worden ingetrokken of opgeschort. Hierdoor kan worden vastgesteld of het noodzakelijk is om toegangsrechten in te trekken. Wijzigingen in het dienstverband behoren te worden weerspiegeld in het intrekken van alle toegangsrechten die niet voor het nieuwe dienstverband zijn goedgekeurd. De toegangsrechten

			die behoren te worden ingetrokken of aangepast omvatten ook de fysieke en logische toegangsrechten. Intrekking of aanpassing kan plaatsvinden door verwijdering, intrekking of vervanging van sleutels, identificatiekaarten, informatieverwerkende faciliteiten of abonnementen . (*) *Note: elk document dat toegangsrechten van medewerkers en contractanten identificeert, behoort de intrekking of aanpassing van toegangsrechten weer te geven.* Indien een medewerker die uit dienst gaat of een externe gebruiker wachtwoorden kent van gebruikersidentificaties die actief blijven, dan behoren deze bij beëindiging of wijziging van dienstverband, contract of overeenkomst te worden gewijzigd. Diepgang: Opzet en bestaan van de beheersingsmaatregelen. Test aanpak: Stel vast dat het beleid ter zake van het intrekken of wijzigen van toegangsrechten in lijn is met bovenstaande aandachtspunten. Doe een deelwaarneming om de opzet en het bestaan van de beheersingsmaatregel te kunnen vaststellen. Interview de verantwoordelijke functionarissen.
10. Cryptografie			
10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	Criterium BIO: Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	10.1.1.1 In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: a) Wanneer cryptografie ingezet wordt.	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inlezen Suwinet DKD

	Doelstelling: Het voorkomen van ongeautoriseerde toegang tot netwerkdiensten. *Risico:* *Ondanks het besloten karakter van Suwinet bestaat het risico dat de toegang tot gegevens niet adequaat is beschermd.*	b) Wie verantwoordelijk is voor de implementatie. c) Wie verantwoordelijk is voor het sleutelbeheer. d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. e) De wijze waarop het beschermingsniveau vastgesteld wordt. f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld. 10.1.1.2 Cryptografische toepassingen voldoen aan passende standaarden.	** Let op: Voor Suwinet en DKD Inlezen is de "inleesapplicatie" met de eventuele bijbehorende dabase in scope.* Toelichting: Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie. Diepgang: Opzet en bestaan van de beheersingsmaatregelen. Test aanpak: Inspecteer de classificatie van gegevens en daaraan gerelateerde risicoanalyse, de netwerkarchitectuur en het inrichtingsdocument waar de encryptie van gegevens in staat beschreven, en stel vast dat deze voldoen aan bovenstaande aandachtspunten. Beoordeel of de beveiliging van de verbindingen voldoet aan de laatste stand der techniek. Gebruik hierbij de gestelde eisen van het Forum Standaardisatie (Lijst open standaarden | Forum Standaardisatie) als uitgangspunt voor de beoordeling. Observeer de (wijze van toepassen van) encryptie van gegevens. Inspecteer of de daarbij toegepaste technieken / cryptografische configuratie voldoet aan de laatste stand der techniek[22]*

[22] Voor de beoordeling van de cryptografische configuratie wordt verwezen naar de testaanpak zoals beschreven in het DigiD assessment.

			Interview de verantwoordelijke functionarissen. * Note: b*etrek hierbij informatie van NCSC over de eisen voor toereikendheid van cryptografische maatregelen.*
12. Beveiliging bedrijfsvoering			
12.1.1 Gedocumenteerde bedieningsprocedures	Criterium BIO: Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben. Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen. *Risico:* *Als gebruikers en/ of beheerders niet kunnen beschikken over bedieningsprocedures (handleidingen) bestaat het risico dat (kritieke) informatieverwerkende faciliteiten niet correct en/ of veilig worden bediend.*	(geen onderliggende specifieke overheidsmaatregel)	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: Gebruikers en beheerders van Suwinet gegevens dienen te beschikken over bedieningsprocedures (handleidingen)*. Te denken valt hierbij aan: Handleiding voor gebruikers van Suwinet gegevens: a) verwerking en behandeling van informatie, zowel geautomatiseerd als handmatig; b) ondersteunings- en escalatiecontacten, waaronder externe ondersteuningscontacten in geval van onverwachte bedienings- of technische moeilijkheden; c) voorschriften voor de behandeling van speciale uitvoer en media, zoals het gebruik van speciale kantoorbenodigdheden of het beheer van vertrouwelijke uitvoer, waaronder procedures voor veilig verwijderen van uitvoer van mislukte taken; Handleiding voor beheerders van Suwinet gegevens: a) de installatie en configuratie van systemen;

			b) back-up; c) eisen ten aanzien van de planning, met inbegrip van onderlinge verbondenheid met andere systemen, tijdstip waarop de eerste taak begint en tijdstip van afronding van de laatste taak; d) voorschriften voor de afhandeling van fouten of andere uitzonderlijke omstandigheden die tijdens de uitvoering van de taak kunnen optreden, waaronder beperkingen ten aanzien van het gebruik van systeemhulpmiddelen; e) procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen; f) het beheren van audit- en systeemlog bestandinformatie; g) procedures voor het monitoren van activiteiten; h) Specifieke aandacht voor DKD en/of Suwinet inlezen. *Note: *de website van BKWI bevat beheerhandleidingen en ander ondersteuningsmateriaal voor Suwinet-Inkijk.* <u>Diepgang:</u> Opzet en bestaan van de beheersingsmaatregelen. <u>Test aanpak:</u> Inspecteer de gebruikers- en/of beheerderhandleidingen en stel vast dat deze aantoonbaar voldoen aan bovenstaande aandachtspunten. **Voor DKD en/of Suwinet-inlezen**: Er is een beschrijving van relevante ITIL-processen waarvan

			ook m.b.t. de Suwinet gerelateerde applicaties gebruik wordt gemaakt (changemanagement, release en deploy management, (security) incidentmanagement, configuratiemanagement, IT-service continuity management), zie ook 12.4.1 specifiek voor security incidentmanagement. Interview de verantwoordelijke functionarissen.
12.1.2 Wijzigingenbeheer	Wijzigingsbeheer: Veranderingen in de gemeente, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	(geen onderliggende specifieke overheidsmaatregel)	<u>Betrokken partijen:</u> gemeente / samenwerkingspartner / IT-serviceorganisatie. <u>Scope:</u> Suwinet Inlezen Suwinet DKD <u>Diepgang:</u> Opzet en bestaan van de beheersingsmaatregelen ** Let op: Voor Suwinet en DKD Inlezen is de "inleesapplicatie" met de eventuele bijbehorende database in scope.* <u>Testaanpak:</u> Inspecteer de documentatie rond het wijzigingenbeheer en stel vast dat deze minimaal de bovenstaande aandachtspunten omvatten. Doe minimaal een deelwaarneming om te beoordelen of de beheersingsmaatregelen met betrekking tot het wijzigingsbeheer bestaan. Interview de verantwoordelijke functionarissen
12.1.4.1	Scheiding van ontwikkel-, test- en productieomgevingen: Ontwikkel-, test- en	(geen onderliggende specifieke overheidsmaatregel)	Betrokken partijen: gemeente / samenwerkingspartner / IT-service-gemeente.

Scheiding ontwikkel-, test- en productieomgevingen	productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.		<u>Scope:</u> Suwinet Inlezen Suwinet DKD <u>Diepgang:</u> Opzet en bestaan van de beheersingsmaatregelen. * Let op: Voor Suwinet en DKD Inlezen is de "inleesapplicatie" met de eventuele bijbehorende database in scope <u>Testaanpak:</u> Inspecteer de documentatie rond het scheiding van ontwikkel-, test- en productieomgevingen en stel vast dat deze minimaal de bovenstaande aandachtspunten omvatten. Doe tenminste een deelwaarneming om vast te stellen of het onderscheid tussen ontwikkel-, test- en productieomgevingen bestaat. Interview de verantwoordelijke functionarissen
12.1.4.2 Wijziging productieomgeving	Scheiding van ontwikkel-, test- en productieomgevingen: Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	(geen onderliggende specifieke overheidsmaatregel)	Betrokken partijen: gemeente / samenwerkingspartner / IT-service-organisatie. <u>Scope:</u> Suwinet Inlezen Suwinet DKD <u>Diepgang:</u> Opzet en bestaan van de beheersingsmaatregelen

			* Let op: Voor DKD Inlezen is de "inleesapplicatie" met de eventuele bijbehorende database in scope <u>Testaanpak:</u> Inspecteer de documentatie rond de scheiding van ontwikkel-, test- en productieomgevingen en stel vast dat deze minimaal de bovenstaande aandachtspunten omvatten. Doe tenminste een deelwaarneming om vast te stellen of het onderscheid tussen tenminste test- en productieomgeving bestaat ervan uitgaande dat de gemeente geen software ontwikkeld. Interview de verantwoordelijke functionarissen
12.4.1 Gebeurtenissen registreren	<u>Criterium BIO:</u> Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. <u>Doelstelling:</u> Bewerkstellingen dat tijdig correctieve maatregelen kunnen worden getroffen en informatie te kunnen verschaffen over activiteiten van gebruikers en beheerders van de Suwinet diensten en vaststellen of oneigenlijk gebruik of misbruik is gemaakt van autorisatie. <u>*Risico:*</u> *Afwijkingen niet worden gesignaleerd en derhalve niet kunnen worden aangepakt.*	12.4.1.1 Een logregel bevat minimaal: a) de gebeurtenis; b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; c) het gebruikte apparaat; d) het resultaat van de handeling; e) een datum en tijdstip van de gebeurtenis. 12.4.1.2 Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden. 12.4.1.3 De informatieverwerkende omgeving wordt gemonitord door	<u>Betrokken partij(en):</u> Gemeente / samenwerkingspartij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD <u>Toelichting:</u> Voor deze norm geldt dat de beheerder van de applicatie (BKWI voor Suwinet Inkijk/ de IT-serviceorganisatie voor Suwinet Inlezen en Suwinet DKD) verantwoordelijk is voor het maken en bewaren van logbestanden (zie ook 12.4.2), en dat het de verantwoordelijkheid van de gemeente is om deze logbestanden te gebruiken om regelmatig de rechtmatigheid van het gebruik van Suwinet gegevens door medewerkers te beoordelen. Het is evident dat de beheerorganisatie de gemeente hiertoe in staat moet stellen door het aanleveren van

		een SIEM en/ of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risicoinschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd. 12.4.1.4 Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen. 12.4.1.5 De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	voldoende fijnmazige (gedetailleerde) rapportages, zodat controle op de rechtmatigheid van het gebruik van Suwinet gegevens daarmee wordt gefaciliteerd. De fijnmazigheid van de door BKWI aangeleverde rapportages is eerder door de AP als voldoende gekwalificeerd en kan derhalve voor andere beheerorganisaties als voorbeeld dienen. Er behoren procedures te worden vastgesteld om het gebruik van Suwinet-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig (minimaal 2 maal per jaar gelijkmatig verdeeld) te worden beoordeeld en gerapporteerd. <u>Diepgang:</u> Opzet en bestaan van de beheersingsmaatregelen <u>Test aanpak</u>: Inspecteer de procedurebeschrijving met betrekking tot het monitoren van de logging en stel vast dat deze voldoet aan bovenstaande aandachtspunten. Inspectie van de vastlegging van de periodiek review van de logging, periodieke rapportage (minimaal 2 maal per jaar gelijkmatig verdeeld) aan het management en follow-up acties naar aanleiding van review en analyse van de logging (PDCA). *Note: denk ook aan het vaststellen van de volledigheid op basis van doorlopende nummering/ timestamp; en is de logging mogelijk beïnvloedbaar voor de belanghebbende(n).* Stel vast dat de periodieke review van de logging minimaal twee keer per jaar met zodanige diepgang heeft plaatsgevonden dat met een redelijke mate van zekerheid kan worden gesteld dat materiele afwijkingen (onrechtmatig gebruik van Suwinet

			gegevens) aan het licht zouden zijn gekomen en dat inhoud is gegeven aan terzake door de gemeente geformuleerde opvolgingsproces. Zie ook uitwerking onder 6.1.1. Interview de verantwoordelijke functionarissen.
12.4.2 Beschermen van informatie in logbestanden	Criterium BIO: Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang. Doelstelling: Alle handelingen die betrekking hebben op gebruikers en beheerders moeten herleidbaar zijn naar individuele personen. *Risico:* *Zonder vastlegging en bewaking kan achteraf niet worden vastgesteld wie bepaalde handelingen heeft uitgevoerd.*	12.4.2.1 Er is een overzicht van logbestanden die worden gegenereerd. 12.4.2.2 Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd. 12.4.2.3 Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden. 12.4.2.4 Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform BIO hoofdstuk 16.	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inlezen Suwinet DKD Toelichting: Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole en te worden beschermd tegen vervalsing en onbevoegde toegang. Diepgang: Opzet en bestaan van de beheersingsprocedures Test aanpak: Inspecteer de procedurebeschrijving met betrekking tot de bescherming van logfaciliteiten en logbestanden en stel vast dat deze voldoet aan bovenstaande aandachtspunten ofwel is deze robuust beschermd tegen vervalsing en onbevoegde toegang. Inspectie van de locatie van de logbestanden.

			Betrek hierbij, waar nodig, de van derden ontvangen verantwoordingsinformatie en de bijbehorende assurance-rapportages. Interview de verantwoordelijke functionarissen.
14. Acquisitie, , ontwikkeling en onderhoud van informatiesystemen			
14.2.2 Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework.	N.v.t.	Procedures voor wijzigingsbeheer met betrekking tot systemen: Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	Betrokken partijen: Gemeente / samenwerkingspartij / IT-service serviceorganisatie Scope: Suwinet Inlezen Suwinet DKD * Let op: Voor Suwinet en DKD Inlezen is de "inleesapplicatie" met de eventuele bijbehorende database in scope . Toelichting: Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework. Diepgang: Opzet en bestaan van de beheersingsmaatregelen Testaanpak: Inspecteer de procedures met betrekking tot wijzigingsbeheer en stel vast dat deze voldoen aan de algemene uitgangspunten. Onderzoek aan de hand van een aantal relevante wijzigingsformulieren of de procedure ook in de Suwinetpraktijk daadwerkelijk wordt gevolgd en wijzigingen aantoonbaar beheerst worden doorgevoerd, Interview de verantwoordelijke functionarissen

18. Naleving			
18.1.4 Privacy en bescherming van persoonsgegevens	Criterium BIO: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende het verwerken van persoonsgegevens. *Risico:* *Als de verwerking van Suwinet (persoons)gegevens niet overeenkomstig toepasselijke wet- en regelgeving plaatsvindt, wordt hierdoor de AVG overtreden.*	18.1.4.1 In overeenstemming met de AVG heeft iedere gemeente een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren. 18.1.4.2 Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: Organisaties behoren een beleid te ontwikkelen en te implementeren voor de privacy en bescherming van persoonsgegevens. Dit beleid behoort te worden gecommuniceerd aan alle personen die betrokken zijn bij het verwerken van persoonsgegevens. Indien organisaties voor Suwinet gebruik maken van de diensten van een serviceorganisatie (bijvoorbeeld bij het gebruik van Suwinet Inlezen of Suwinet DKD) dient met deze serviceorganisatie een Verwerkersovereenkomst te zijn afgesloten. Diepgang: Opzet en bestaan van de beheersingsmaatregelen. Test aanpak: Stel vast dat de gemeente een privacy-beleid heeft ontwikkeld en geïmplementeerd. Stel vast dat de Suwinet applicatie(s) is/ zijn opgenomen in het Verwerkingsregister. Stel vast dat een FG is aangesteld, dat deze in voldoende mate onafhankelijk en objectief is, en dat

			deze voldoende mandaat heeft om zijn/haar functie uit te voeren. Stel vast dat de naleving van de privacyregels regelmatig gecontroleerd wordt (zie ook 12.4.1). Stel vast dat de gemeente de Suwinet gegevens alleen gebruikt voor de taken waarvoor een wettelijke basis (doelbinding) is* en die dus noodzakelijk zijn voor de uitvoering van wet- en regelgeving. Voor een aantal taken van de gemeente is het gebruik van Suwinet gegevens niet toegestaan**. **Note: Suwinetgegevens mogen worden gebruikt voor de volgende Suwinet-taken* *:* • *Vaststellen van de rechtmatigheid van de uitkering (art.17 lid 1 PW en art.53a lid 1 en 6 PW, art.14 IOAW/ IOAZ)* • *Vaststellen definitieve einddatum van de uitkering na opschorting (art.17 lid 1 PW en art.53a lid 1 en 6 PW, art.14 IOAW/IOAZ)* • *Re-integratie werkzaamheden, ook voor ex-gedetineerden mits het de doelgroep van de P-wet betreft (art. 7 lid 1 PW)* • *Bijzondere bijstand (art. 35, 36, 36b PW)* • *Taken rondom Bbz, Besluit bijstandsverlening zelfstandigen (art. 78f, 78g PW)* • *Terugvordering en Verhaal, bijv. het raadplegen van de ex-partner voor vaststelling onderhoudsplicht (art. 5862i P-wet, art. 25-33 IOAW/IOAZ)* • *Tijdelijke Overbruggingsregeling Zelfstandig Ondernemers (Tozo).*

			• *Taken met betrekking tot de uitvoering van de Wet gemeentelijke schuldhulpverlening (Wgs).* ***Note: het gebruik van Suwinetgegevens is expliciet niet toegestaan voor:* • *De uitvoering van gemeentelijke regelingen zoals een korting of stadspas of andere ingrediënten van armoedebeleid. Gemeentelijke regelingen mogen alleen in Suwinet worden geraadpleegd als deze regeling is gebaseerd op de P-wet, IOAW of IOAZ (art. 8, 8a, 8b P-wet). Of dit zo is, is zichtbaar in de aanhef van de gemeentelijke regeling: gelet op artikel xx van de XXX-wet…* • *De interne controle op juistheid van de beslissingen van de medewerker. Het controleren van de juistheid van de beslissing van een medewerker valt niet onder de uitvoering van de P-wet, IOAW of IOAZ, maar onder interne controle. Daarvoor mag Suwinet niet worden geraadpleegd.* • *De controle op de naleving van Social Return. Sommige gemeenten nemen in contracten met dienstverleners passages op over het inzetten van werkzoekenden of bijstandsgerechtigden (Social Return). Het controleren of de leverancier/dienstverlener hieraan voldoet, valt niet onder de P-wet, IOAW of IOAZ.* • *Onderzoek naar de effectiviteit van de uitvoering van wet- en regelgeving.* • *De uitvoering van andere wetten zoals WMO, de Jeugdwet, de wet op de*

			lijkbezorging of de Wet Sociale Werkvoorziening. • *Voor de uitvoering van gemeentelijke incasso. Alleen voor de gemeentelijke belastingdeurwaarders geldt dat zij een overeenkomst hebben op grond van art. 5.23 van het Besluit Suwinet en conform het Aansluitprotocol (Bijlage III Regeling Suwinet).* Identificeer of er activiteiten zijn geweest welke nadere acties (denk aan datalekken) door betrokkenen noodzakelijk maken.

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. Suwinet-regelgeving vraagt van het gemeentebestuur een door een IT-auditor (RE) afgegeven assurance op de collegeverklaring. De Suwinet-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 SUWINET. 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 Suwinet 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 assurance-rapport. 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 SUWINET 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 Suwinet normen bij het samenwerkingsverband in de vorm van een Richtlijn 3000-opdracht. 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.

Bijlage 5: Formats assurance-rapporten

In deze bijlage zijn de formats voor de assurance-rapporten opgenomen behorend bij de Verantwoording gebruik van Suwinet <organisatienaam> zoals opgenomen in bijlage 1.2.
De formats voor de assurance-rapporten behorend bij Collegeverklaring ENSIA en bijlagen zijn opgenomen in de NOREA Handreiking ENSIA voor IT-auditors versie 5 d.d. 1 juli 2024.

5.1 Goedkeurend oordeel

ASSURANCE-RAPPORT

Inzake de Verantwoording gebruik van Suwinet <organisatienaam>

(Bestemd voor <organisatienaam>, gemeente <naam>,
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 Verantwoording gebruik van Suwinet <organisatienaam>

Ons oordeel
Ingevolge uw opdracht hebben wij de bijgevoegde Verantwoording gebruik van Suwinet <organisatienaam> onderzocht.

Naar ons oordeel is bijgevoegde Verantwoording gebruik van Suwinet <organisatienaam>, 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 SUWINET in kader van ENSIA voor IT-auditors (RE's) versie 1.0 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 <organisatienaam> 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 Verantwoording gebruik van Suwinet <organisatienaam>geeft het bestuur van <organisatienaam> aan in welke mate <organisatienaam> voldoet aan de informatiebeveiligingsnormen voor Suwinet. De Verantwoording gebruik van Suwinet <organisatienaam> is gebaseerd op 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 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 Suwinet gegevensverwerkingen:

Onderzochte gegevensverwerkingen Suwinet:
<TABEL OVERNEMEN UIT VERANTWOORDING GEBRUIK VAN SUWINET <ORGANISATIENAAM>>

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

<Alleen bij uitzonderingen: passage zonder paragraafkop over beperkingen bij het onderzoek. Zoals in de Verantwoording gebruik van Suwinet <organisatienaam> is aangegeven wordt nog niet aan alle normen inzake Suwinet voldaan>.

<indien van toepassing:
Benadrukking aangelegenheden
Wij hebben vastgesteld dat de op de uitzonderingen gerichte beheersmaatregelen 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 Verantwoording gebruik van Suwinet <organisatienaam>. De verantwoording is opgesteld voor de <organisatienaam>, <gemeente(n)> en voor het departementen en aangewezen uitvoeringsinstanties die toezien op de veiligheid van Suwinet. Doel van de collegeverklaring is om de <organisatienaam>, <gemeente(n)> en het departement dat toeziet op de veiligheid van Suwinet te informeren over het voldoen aan de geselecteerde normen Suwinet.

Ons assurance-rapport is derhalve uitsluitend bestemd voor de <organisatienaam>, <gemeente(n)> en het departement en aangewezen uitvoeringsinstanties die toezien op de veiligheid van 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 bestuur <organisatienaam>
Het bestuur van <organisatienaam> is verantwoordelijk voor het ontwerpen en implementeren van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensuitwisseling SUWI en voor de effectieve werking van dit stelsel.
Het bestuur van <organisatienaam> is verantwoordelijk voor het opstellen van de Verantwoording gebruik van Suwinet <organisatienaam>.

Het bestuur is ook verantwoordelijk voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de verantwoording 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 kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van de ethische voorschriften, professionele standaarden en andere wet- en regelgeving.

Onze assurance-opdracht bestond onder andere uit:
- het verkrijgen van kennis omtrent de verantwoording
- 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 verantwoording onjuistheden van materieel belang als gevolg van fraude en 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 verantwoording in overeenstemming is met de onderliggende beheersmaatregelen en uitgevoerde werkzaamheden; en
- het evalueren van de uitkomsten van onze werkzaamheden.

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

5.2 Oordeel met beperking

ASSURANCE-RAPPORT

Inzake de Verantwoording gebruik van Suwinet <organisatienaam>

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

Uniek identificatienummer IT-auditor

Assurance-rapport van de onafhankelijke IT-auditor

Aan: <opdrachtgever>

Assurance over Verantwoording gebruik van Suwinet <organisatienaam>

Ons oordeel met beperking
Ingevolge uw opdracht hebben wij de bijgevoegde Verantwoording gebruik van Suwinet <organisatienaam> onderzocht.

Naar ons oordeel is, uitgezonderd de <gevolgen>[23] <mogelijke effecten>[24] van de <aangelegenheid> <aangelegenheden> beschreven in de paragraaf 'De basis voor ons oordeel met beperking', bijgevoegde Verantwoording gebruik van Suwinet <organisatienaam>, 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 SUWINET in kader van ENSIA voor IT-auditors (RE's) versie 1.0 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 <organisatienaam> 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 Verantwoording gebruik van Suwinet <organisatienaam>geeft het bestuur van <organisatienaam> aan in welke mate <organisatienaam> voldoet aan de informatiebeveiligingsnormen voor Suwinet. Verantwoording gebruik van Suwinet <organisatienaam> is gebaseerd op 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 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 Suwinet gegevensverwerkingen:

Onderzochte gegevensverwerkingen Suwinet:
<TABEL OVERNEMEN UIT VERANTWOORDING GEBRUIK VAN SUWINET <ORGANISATIENAAM>>

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

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

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

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

<indien van toepassing:
Benadrukking aangelegenheden
Wij hebben vastgesteld dat de op de uitzonderingen gerichte beheersmaatregelen 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 Verantwoording gebruik van Suwinet <organisatienaam>. De Verantwoording gebruik van Suwinet <organisatienaam> is opgesteld voor <organisatienaam>, <gemeente(n)> en voor het departement en aangewezen uitvoeringsinstanties die toezien op de veiligheid van Suwinet. Doel van de Verantwoording gebruik van Suwinet <organisatie> is om het bestuur van <organisatienaam>, <de gemeente(n)> en het departement dat toeziet op de veiligheid van Suwinet te informeren over het voldoen aan de geselecteerde normen Suwinet.

Ons assurance-rapport is derhalve uitsluitend bestemd voor de <organisatienaam>, <gemeente(n)> en het departement en aangewezen uitvoeringsinstanties die toezien op de veiligheid van 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 bestuur <organisatienaam>
Het bestuur van <organisatienaam> is verantwoordelijk voor het ontwerpen en implementeren van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensuitwisseling SUWI en voor de effectieve werking van dit stelsel.
Het bestuur van <organisatienaam> is verantwoordelijk voor het opstellen van de Verantwoording gebruik van Suwinet <organisatienaam>.

Het bestuur is ook verantwoordelijk voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de verantwoording 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 kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van de ethische voorschriften, professionele standaarden en andere wet- en regelgeving.

Onze assurance-opdracht bestond onder andere uit:
- het verkrijgen van kennis omtrent de verantwoording
- 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 verantwoording onjuistheden van materieel belang als gevolg van fraude en 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 verantwoording in overeenstemming is met de onderliggende beheersmaatregelen en uitgevoerde werkzaamheden; en
- het evalueren van de uitkomsten van onze werkzaamheden.

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

5.3 Afkeurend oordeel

ASSURANCE-RAPPORT

Inzake de Verantwoording gebruik van Suwinet <organisatienaam>

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

Uniek identificatienummer IT-auditor

Assurance-rapport van de onafhankelijke IT-auditor

Aan: <opdrachtgever>

Assurance over Verantwoording gebruik van Suwinet <organisatienaam>

Ons afkeurend oordeel
Ingevolge uw opdracht hebben wij de bijgevoegde Verantwoording gebruik van Suwinet <organisatienaam> onderzocht.

Naar ons oordeel is, Verantwoording gebruik van Suwinet <organisatienaam>, 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 aangelenheid / 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 SUWINET in kader van ENSIA voor IT-auditors (RE's) versie 1.0 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 <organisatienaam> 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 Verantwoording gebruik van Suwinet <organisatienaam>geeft het bestuur van <organisatienaam> aan in welke mate <organisatienaam> voldoet aan de informatiebeveiligingsnormen voor Suwinet. Verantwoording gebruik van Suwinet <organisatienaam> is gebaseerd op 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 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 Suwinet gegevensverwerkingen:

Onderzochte gegevensverwerkingen Suwinet:
<TABEL OVERNEMEN UIT VERANTWOORDING GEBRUIK VAN SUWINET <ORGANISATIENAAM>>

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

<*indien van toepassing*:
Benadrukking aangelegenheden
Wij hebben vastgesteld dat de op de uitzonderingen gerichte beheersmaatregelen 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 Verantwoording gebruik van Suwinet <organisatienaam>. De Verantwoording gebruik van Suwinet <organisatienaam> is opgesteld voor <organisatienaam>, <gemeente(n)> en voor het departement en aangewezen uitvoeringsinstanties die toezien op de veiligheid van Suwinet. Doel van de Verantwoording gebruik van Suwinet <organisatie> is om het bestuur van <organisatienaam>, <de gemeente(n)> en het departement dat toeziet op de veiligheid van Suwinet te informeren over het voldoen aan de geselecteerde normen Suwinet.

Ons assurance-rapport is derhalve uitsluitend bestemd voor de <organisatienaam>, <gemeente(n)> en het departement en aangewezen uitvoeringsinstanties die toezien op de veiligheid van 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 bestuur <organisatienaam>
Het bestuur van <organisatienaam> is verantwoordelijk voor het ontwerpen en implementeren van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensuitwisseling SUWI en voor de effectieve werking van dit stelsel.
Het bestuur van <organisatienaam> is verantwoordelijk voor het opstellen van de Verantwoording gebruik van Suwinet <organisatienaam>.

Het bestuur is ook verantwoordelijk voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de verantwoording 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 kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van de ethische voorschriften, professionele standaarden en andere wet- en regelgeving.

Onze assurance-opdracht bestond onder andere uit:
- het verkrijgen van kennis omtrent de verantwoording
- 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 verantwoording onjuistheden van materieel belang als gevolg van fraude en 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 verantwoording in overeenstemming is met de onderliggende beheersmaatregelen en uitgevoerde werkzaamheden; en
- het evalueren van de uitkomsten van onze werkzaamheden.

.

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

... (naam IT Auditor RE)

5.4 Oordeelonthouding

ASSURANCE-RAPPORT

Inzake de Verantwoording gebruik van Suwinet <organisatie>

(Bestemd voor <organisatienaam>, gemeente <naam>,
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 Verantwoording gebruik van Suwinet <organisatienaam>

Onze oordeelonthouding
Wij hebben de opdracht gekregen om bijgevoegde Verantwoording gebruik van Suwinet <organisatienaam> te onderzoeken.

Wij geven geen oordeel over de juistheid van de, bijgevoegde Verantwoording gebruik van Suwinet <organisatienaam>. 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 Verantwoording gebruik van Suwinet <organisatienaam>.

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 Verantwoording gebruik van Suwinet <organisatienaam>geeft het bestuur van <organisatienaam> aan in welke mate <organisatienaam> voldoet aan de informatiebeveiligingsnormen voor Suwinet. Verantwoording gebruik van Suwinet <organisatienaam> is gebaseerd op 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 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 gegevensverwerkingen Suwinet:
<TABEL OVERNEMEN UIT VERANTWOORDING GEBRUIK VAN SUWINET <ORGANISATIENAAM>>

Wij hebben geen onderzoek uitgevoerd naar hierboven niet genoemde 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 beheersmaatregelen 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 Verantwoording gebruik van Suwinet <organisatienaam>. De Verantwoording gebruik van Suwinet <organisatienaam> is opgesteld voor <organisatienaam>, <gemeente(n)> en voor het departement en aangewezen

uitvoeringsinstanties die toezien op de veiligheid van Suwinet. Doel van de Verantwoording gebruik van Suwinet <organisatie> is om het bestuur van <organisatienaam>, en het departement dat toeziet op de veiligheid van Suwinet te informeren over het voldoen aan de geselecteerde normen Suwinet.

Ons assurance-rapport is derhalve uitsluitend bestemd voor de <organisatienaam>, <gemeente(n)> en het departement en aangewezen uitvoeringsinstanties die toezien op de veiligheid van 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 bestuur <organisatienaam>
Het bestuur van <organisatienaam> is verantwoordelijk voor het ontwerpen en implementeren van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensuitwisseling SUWI en voor de effectieve werking van dit stelsel.
Het bestuur van <organisatienaam> is verantwoordelijk voor het opstellen van de Verantwoording gebruik van Suwinet <organisatienaam>.

Het bestuur is ook verantwoordelijk voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de verantwoording 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, bijgevoegde Verantwoording gebruik van Suwinet <organisatienaam> op basis van onze audit, verricht in overeenstemming met Nederlands rechtNOREA Richtlijn 3000A "Assurance-opdrachten door IT-auditors (Attest-opdrachten)" en NOREA Handreiking SUWINET in kader van ENSIA voor IT-auditors (RE's) versie 1.0 d.d. 1 juli 202. 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 bijgevoegde Verantwoording gebruik van Suwinet <organisatienaam> als geheel.

Wij zijn onafhankelijk van <organisatienaam> 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)

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 Suwinetgegevens 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.
BIO	Baseline Informatiebeveiliging Overheid
Carve out methode	Bij de carve-out methode wordt in een assurance-rapport (zoals een DigiD assessment) een verwijzing opgenomen naar het assurance-rapport (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 beheersmaatregelen in een assurance rapport overgenomen en er wordt dus niet verwezen naar de van derden verkregen assurance-rapporten (TPM's) waar eventueel gebruik van is gemaakt. De auditor van het assurance-rapport is vaktechnisch volledig verantwoordelijk en voert indien nodig een dossierreview uit voor een assurance-rapport 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 Suwinet-gegevens van de gebruikersorganisatie (gemeenten) worden verwerkt. Met nadruk wordt opgemerkt dat de softwareleverancier van de applicatie waarin de Suwinet-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. Zie ook het begrip 'serviceorganisatie'.

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.
Serviceorganisatie	Een organisatie die Suwinet taken verricht voor een gemeente. Dit zijn veelal publiekrechtelijke lichamen krachtens de Wet gemeenschappelijke regelingen zoals een intergemeentelijke sociale dienst maar het kan ook een grotere gemeente in de regio zijn die bepaalde Suwinet taken uitvoert voor andere gemeenten. Het is ook mogelijk dat een publiekrechtelijke organisaties op basis van een privaatrechtelijke overeenkomst extra Suwinet-diensten verricht voor deelnemers aan de gemeenschappelijke regeling of zelfs niet deelnemende gemeenten. En bijzondere vorm van serviceorganisaties in dit verband zijn de IT-serviceorganisaties. Zie hiervoor dit begrip elders in deze begrippenlijst.
Third Party Mededeling (TPM)	Een TPM is een assurance-rapport 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 assurance-rapport 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 assurance-rapport (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.

Bijlage 7: Afkortingenlijst

BAG	:	Basisregistraties Adressen en Gebouwen
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
NCSC	:	Nationaal Cyber Security Centrum
PUN	:	Paspoort Uitvoeringsregeling Nederland
SOS	:	Security Officer Suwinet
Suwinet	:	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