NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

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

Versie 1.0 – Verantwoordingsjaar 2026
30 september 2026

1 Over deze handreiking ENSIA 3
1.1 Aanleiding 5
1.2 Achtergrond 5
1.3 Toepassingsgebied Suwinet 6
1.4 Toepassing NOREA-Richtlijn 3000 (Herzien) 'Assurance-opdrachten door IT-auditors' 7

2 Handreiking 8
2.1 Verantwoordingsproces 8
2.2 Uitvoeren werkzaamheden door de IT-auditor 9
2.3 Formele aspecten van de assurance-opdracht 10
2.4 Ethische voorschriften en beroepsregels 10
2.5 'Pre-audit' 11
2.6 Opdrachtaanvaarding en continuering 11
2.7 Kwaliteitsbeheersing 11
2.8 Risico-inschatting 12
2.9 Het verkrijgen van assurance-informatie 12
2.10 Uitbesteding door partijen 13
2.11 Schriftelijke bevestiging (letter of representation) 14
2.12 Het vormen van het oordeel 14
2.13 Het opstellen van het assurance-rapport 14
2.14 Normgerichte oordeelsvorming in kader van de Suwinet audit 15
2.15 Overige rapportages 15
2.16 Documentatie 15
2.17 Consultatie 15

3. Tot slot 16

Bijlagen 17
Bijlage 1: Normenkader GeVS 2026 18
Bijlage 1.1 Normenkader GeVS 2026 18
Bijlage 1.2 Controle op werking 20
Bijlage 1.3 Non-occurance 20
Bijlage 1.4 Optionele controle werking maatregelen 2027 20
Bijlage 1.5 General IT Controls bij het gebruik van Suwinet Inlezen of DKD inlezen 21
Bijlage 2: Testaanpak bij de te onderzoeken normen relevant voor Suwinet (inclusief controle op werking) 22
Bijlage 3: Tabel steekproefomvang / deelwaarnemingen 60
Bijlage 4: Overwegingen ENSIA IT-Audit in samenwerkingsverbanden Suwinet 62
Bijlage 5: Format assurance-rapport 63
Bijlage 5.1 Toelichting format assurance-rapport 63
Bijlage 5.2 Assurance-rapport op niveau gemeente 64
Bijlage 5.3 Assurance-rapport op niveau serviceorganisatie 78
Bijlage 6: Waarmerken stukken en digitaal ondertekenen 85
Bijlage 7: Begrippenkader 86
Bijlage 8: Afkortingenlijst 88

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 geven van assurance over het gebruik van de Gezamenlijke elektronische Voorzieningen SUWINET (GeVS)[1] – hierna Suwinet - betrekking hebbende werkzaamheden van gemeenten en hun samenwerkingspartners. Het betreft hier niet alleen het gebruik van de voorziening zelf, maar ook de beveiliging van de gegevensverwerkingen en gegevensuitwisselingen die daarmee plaatsvinden. Het gebruik van GeVS is beperkt tot de toegestane wettelijke taken[2].

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, www.bkwi.nl en/of www.ensia.nl

Deze handreiking zal op basis van het ENSIA-proces (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] Producten

[2] Zie voor actuele overzicht gemeenten: VNG Realisatie

Versiebeheer

Versie	Datum	Toelichting
Versie 0.1	30 juli 2026	Ten behoeve sub-groep Suwinet van de NOREA-werkgroep ENSIA / BKWI
Versie 0.2	17 augustus 2026	T.b.v. afstemming: - Werkgroep ENSIA - VNG - SZW / BKWI
Versie 0.3	24 augustus 2026	T.b.v. afstemming: - Werkgroep ENSIA - Vaktechnische Commissie NOREA - VNG - SZW / BKWI
Versie 0.4	1 september 2026	T.b.v. afstemming: - Werkgroep ENSIA - Vaktechnische Commissie NOREA - VNG - SZW / BKWI
Versie 0.5	16 september 2026	T.b.v. veststellen: - door Bestuur NOREA - door MAV (Governance Ministerie SZW)
Versie 1.0	***30 september***	***Na besluitvorming:*** ***- Bestuur NOREA*** ***- Managementoverleg Afspraken en Voorzieningen (MAV)*** ***Ter publicatie***

1.1 Aanleiding

De Verantwoordingsrichtlijn GeVS 2026[1] beschrijft de scope en procedure van verantwoording voor alle partijen die gebruik maken van de GeVS. De Verantwoordingsrichtlijn GeVS 2026 geldt ook indien gemeenten e.e.a. ook vastleggen in de ENSIA-tooling.

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 de -verantwoording over Suwinet zich tot opzet en bestaan van de maatregelen per 31-12-2026 en voor een beperkt aantal maatregelen over opzet, bestaan en werking oververantwoordingsjaar 2026 (1 januari -31 december 2026). In aanvulling op de Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2026 (en 2027) dienen daarbij de bevindingen met betrekking tot opzet en bestaan enerzijds en werking (voor zover van toepassing) anderzijds separaat gerapporteerd te worden. Zie voor aanvullende informatie ook website BKWI.

In deze Handreiking wordt nader ingegaan op de door IT-auditors (RE's) in het kader van het 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 gemeentesecretaris, als ambtelijk verantwoordelijke, een belangrijke rol in de governance van ENSIA. Zo wijst de gemeentesecretaris de ENSIA-coördinator van de gemeente formeel aan.

---

[1] https://bkwi.nl/standaarden/privacy-beveiliging/verantwoordingsrichtlijn-gevs-2026

[2] Voor de goede orde: Documentnaam BKWI luidt "Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2026" en de titeltekst luidt "Verantwoordingsrichtlijn GeVS 2025". Beide worden in dit document naast elkaar gebruikt.

[3] Opgemerkt wordt dat de HANDREIKING Verantwoordingsrichtlijn Gezamenlijke elektronische Voorzieningen SUWI (GeVS) voor IT-auditors (RE's) expliciet 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).

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 wordt aangesloten op de BIO[1]. Daarnaast blijft de noodzaak om domein specifieke toezichtinformatie te blijven leveren. De verantwoording in ENSIA betreft in 2026:

- Basisregistratie Personen (BRP)
- Wet- en regelgeving Reisdocumenten (PUN en PNIK)
- Digitale persoonsidentificatie (DigiD)[2]
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Ondergrond (BRO)
- de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)[3]
- BIO versie 1.04zv (zie ook voetnoot 1)

De onderdelen DigiD en Suwinet zijn elk onderworpen aan een IT-audit. De 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)).

Vanaf verantwoordingsjaar 2026 moeten zowel DigiD als Suwinet via de 3000D-methodiek worden verantwoord (bij voorkeur zowel intern richting het College als extern) richting de eerder vermelde toezichthouders. Voor de verantwoording rond Suwinet is het normenkader uit de Verantwoordingsrichtlijn GeVS 2026 leidend.

1.3 Toepassingsgebied Suwinet

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 Inkijk' (Wgs). Zie voor nadere toelichtingen hierop ook bijlage 1. 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 (eveneens via de 3000D-methodiek).

Het Ketenoverleg heeft hiervoor als meest recente document de *Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2026* uitgebracht. Hierin is het vereiste, adequate niveau van informatiebeveiliging gebaseerd op het BIO 1.04 normenkader zodat verantwoording op basis daarvan moet plaatsvinden[4].

---

[1] Hierbij dient rekening gehouden te worden met de werkafspraken die in september 2025 gemaakt zijn rond de invoering van BIO 2 versie 1.3 bij en door gemeenten. Deze zal eerst volledig van toepassing zijn over het verslagjaar 2027.

[2] PM in ENSIA tooling op basis normering verantwoordingsjaar 2025

[3] PM Idem

[4] BIO 2 versie 1.3 is op 23 september 2025 vastgesteld door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO). In dat kader is vastgelegd dat gemeenten tot het moment van inwerkingtreden BIO 1.04 mogen blijven hanteren. Op 5 maart 2026 is BIO 2 versie 1.3 gepubliceerd in de Staatscourant en daarmee van kracht voor alle overheden. Op 15 augustus 2026 is de Cyberbeveiligingswet van kracht geworden waar het hanteren van BIO 2 versie 1.3 eveneens in is verankerd. Conform in 2025 gemaakte afspraken ten behoeve van de verantwoording over het jaar 2026 mogen (dé facto: moeten) gemeenten zich in lijn met de GeVS 2026 verantwoorden op basis van BIO 1.04.

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 2026) gaat uit van het verantwoorden door de verantwoordingsplichtige partij (gemeente en / of samenwerkingspartijen van gemeenten) op basis van het door een IT-auditor (RE) afgegeven oordeel. In dat kader zijn de bepalingen van NOREA-Richtlijn 3000 onderdeel 3000D 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. De opdrachtgevende partij dient daarbij de ontvangen verantwoordings- en assurance-informatie te betrekken bij de uitvoering van de werkzaamheden in de eigen organisatie en de verantwoording (met bijbehorende assurance-informatie van de IT-auditor) die daarover moet worden afgelegd.

Het is de bedoeling dat alle samenwerkingspartijen en gemeenten zich over het verantwoordingsjaar 2026 volgens de 3000D methode gaan verantwoorden over de vereisten van de vigerende Verantwoordingsrichtlijn Informatiebeveiliging GeVS.

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 door Suwi-partijen alsmede hun samenwerkingspartners getroffen maatregelen gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensverwerking op basis van de beschikbare normen. Dit kader geldt voor het verantwoordingsjaar 2026.

(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 2026 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, meer in het bijzonder SUWI-regelgeving (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

<u>Verantwoordelijkheden gemeenten / samenwerkingspartijen</u>
In het kader van het 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 Suwigegevens 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 Het verdient aanbeveling dat de betrokken partijen (gemeente – samenwerkingspartij(-en) / samenwerkingspartijen onderling) hierover schriftelijk nadere afspraken maken.

<u>Verantwoordingsproces gemeenten in detail</u>
Het verantwoordingsproces voor Suwinet begint met het uitwerken van een zelfevaluatie informatiebeveiliging 2026(optioneel) en het verzamelen/vastleggen van documentatie rond opzet, bestaan en, waar geïndiceerd, werking van de maatregelen. De ENSIA-vragenlijst informatiebeveiliging 2025 kan daarbij als leidraad voor de aspecten opzet en bestaan van de maatregelen gehanteerd worden. Het geheel is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO) aangevuld met domeinspecifieke aspecten. Voor de evaluatie van de werking van de maatregelen, voor daartoe voor 2026 geselecteerde normen, is door de VNG aanvullende ondersteunende documentatie ontwikkeld. Zie hiervoor: https://ensia.nl.

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

Het is wenselijk dat de auditor hierover tijdig met de gemeente gedetailleerde afspraken maakt welke passend zijn voor de specifieke situatie bij de gemeente[1].

[1] Lees waar nodig voor gemeente dienstverlenende partij / samenwerkingspartner / GR / etc.

De gemeente levert vóór 1 mei 2027 het assurance-rapport met de bijbehorende aanbiedingsbrief van de gemeentesecretaris op aan de toezichthouder (BKWI). Deze documenten bij voorkeur voor deze datum met behulp van het ENSIA-tool ter beschikking gesteld worden aan BKWI. Indien geen gebruik wordt gemaakt van de voorkeursoptie dient de verantwoording aangeleverd te worden via ENSIA@bkwi.nl.

Verantwoording bij volledige uitbesteding
Indien een gemeente aantoonbaar alle werkzaamheden waarbij gebruik wordt gemaakt van Suwinet heeft uitbesteed aan een dienstverlener / samenwerkingpartner kan de gemeente, als verantwoordingsplichtige, volstaan met het toesturen van de verantwoording van de dienstverlener / samenwerkingspartner. Op die verantwoording zijn de uitgangspunten van deze Handreiking van toepassing.

Voor de volledigheid:
- Het is de verantwoordelijkheid van de gemeente om aan te tonen dat sprake is van volledige uitbesteding van de hiervoor bedoelde werkzaamheden;
- Uit het rapport van de dienstverlener / samenwerkingspartij dient te blijken dat deze (mede) dient om te voldoen aan de verantwoordingsplicht van de gemeente (zie ook bijlage 5.3);
- Het is wenselijk dat de auditor hierover en waar mogelijk tijdig met de betrokken partijen afspraken maakt welke passend zijn voor de specifieke situatie bij de opdrachtgever.

Verantwoordelijkheden IT-auditor
De IT-auditor dient ervoor te zorgen dat de betreffende documenten door hem gewaarmerkt zijn, zoals aangegeven in het format voor het assurance-rapport (PDF/A – format) Hiervoor zijn de voorwaarden voor het elektronisch ondertekenen van de stukken onverkort van toepassing – zie ook Bijlage 6.

De IT-auditor dient bij de uitvoering van de werkzaamheden rekening te houden met de doorlooptijd van de formele behandeling van de verantwoording (zoals brief gemeentesecretaris, assurance-rapport van de IT-auditor en bijbehorende interne documenten) (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 (rechtstreeks aan BKWI en/of 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 (in de vorm van assurance-rapporten) alsmede de doorlooptijd van de formele behandeling ervan door de bestuursorganen van deze partijen.

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 niets ten aanzien van zijn verantwoordelijkheid voor het goed voorbereiden en inrichten van zijn controle.

Nieuw voor het verantwoordingsjaar 2026 is dat de gemeenten zich moeten verantwoorden op basis van de 3000D-systematiek waarbij het door de IT-auditor opgeleverde assurance-rapport de basis vormt voor de verantwoording door de gemeente

De organisatie (gemeente) is verantwoordelijk voor het inrichten van een samenhangend en op risicoanalyse gebaseerd stelsel van interne beheersingsmaatregelen alsmede het beschikbaar hebben van voldoende gedocumenteerde informatie op basis waarvan de opzet, het bestaan en, waar van toepassing, de werking ervan worden onderbouwd. De ingevulde vragenlijsten (de (optionele)

zelfevaluaties - eventueel in de ENSIA-tool (gemeenten), ISMS of andere documentatievormen) en de door de betrokken organisaties (gemeenten en samenwerkingspartners) gedocumenteerde ondersteunende assurance-informatie vormen voor de IT-auditor het basismateriaal en vormen mede onderdeel van de assurance-informatie voor 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. Eventuele aanpassingen dienen door de IT-auditor is zijn werkzaamheden betrokken te worden.

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 Suwinet-audit betreft een assurance-opdracht gericht op het geven van een oordeel met een redelijke mate van zekerheid, conform NOREA Richtlijn 3000D (Directe opdrachten). Daarbij meet of evalueert de IT-auditor het onderzoeksobject ten opzichte van de tussen partijen overeengekomen criteria (met andere woorden de in de Verantwoordingsrichtlijn GeVS 2026 opgenomen criteria). Beoogde gebruikers van 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 het beheer van Suwinet, in alle van materieel belang zijnde aspecten, voldoet aan de gestelde criteria. 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. Deze zijn ontleend aan de Verantwoordingsrichtlijn GeVS 2026. De criteria worden ook in het assurance-rapport kenbaar gemaakt en zijn daarmee toegankelijk voor de gebruikers.

Het gaat om opzet en bestaan van de maatregelen per 31 december 2026 en, waar voorgeschreven, opzet, bestaan en werking over de periode 1 januari tot en met 31 december 2026.

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 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 (optionele) self-assessment, documenteren van activiteiten die door of namens het college moet(-en) worden uitgevoerd.

2.5 'Pre-audit'

Het is de verantwoordelijkheid van de gemeente om het beheer van het gebruik van Suwinet in te richten en uit te voeren in overeenstemming met de geldende wet- en regelgeving waaronder de in de GeVS opgenomen criteria. De gemeente is verantwoordelijk voor het documenteren ervan[1]. 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.

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 uitvoeren 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 het assurance-rapport (o.a. als gevolg van de Wet open overheid) dient voor de op Suwinet gerichte audits expliciet een opdrachtgerichte kwaliteitsbeoordeling (OKB – zie RKBN deel 3) 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;
    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 en in het bijzonder Suwinet;
    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[2].

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

[1] Zie hiervoor ook de VNG-Handreiking Toets op werking Suwinet-normen 2026.

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

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 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

Het is de verantwoordelijkheid van de gemeente om het beheer van het gebruik van Suwinet in te richten en uit te voeren in overeenstemming met de geldende wet- en regelgeving waaronder de in de GeVS opgenomen criteria. De gemeente is verantwoordelijk voor het documenteren ervan[1].. Dit kan door de IT-auditor worden gebruikt als startpunt voor zijn audit. In beginsel is hierin de beoordeling vastgelegd met betrekking tot de individuele normen / vragen op basis van relevante assurance-informatie die door het college is verzameld[2]. 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.

---

[1] Zie hiervoor ook de VNG-Handreiking Toets op werking Suwinet-normen 2026.

[2] 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. Daar waar geen zelfevaluatie wordt gehanteerd dienen opzet, bestaan en, waar relevant, werking door de organisatie op een andere wijze aangetoond te worden.

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 verantwoordelijk voor het gebruik van Suwinet gegevens en dienen daarover verantwoording af te leggen in een Suwinet-verantwoording. Deze verantwoordelijkheid is nader verankerd in zowel de Cyberbeveiligingswet (Cbw) als BIO 2 versie 1.3.

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 voetnoot [1]), hetzij via de carve-out benadering waarbij de laatste benadering de voorkeur heeft.

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 4 "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.

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[2].

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.

---

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

2 Het gaat hierbij om de eisen die aan de inhoud van de betreffende bijlage worden gesteld en **<u>niet</u>** om de beoordeling van opzet, bestaan en werking.

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 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 directe 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).

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 3000D leidend.

In bijlage 5 is het format voor het assurance-rapport opgenomen. Dit format is ook van toepassing bij het afgeven van assurance bij verantwoordingen van samenwerkingspartijen van gemeenten. In het format voor het assurance-rapport is meer expliciet opgenomen op welk gebruik van Suwinet gegevens het oordeel betrekking heeft.

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 indien de dienstverlening een deel van de werkzaamheden omvat. Indien het gaat om integrale dienstverlening is de bijlage 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 Normgerichte oordeelsvorming in kader van de Suwinet audit

De Suwinet-audit wordt conform de vereisten Assurance-opdracht uitgevoerd overeenkomstig NOREA Richtlijn 3000D (Directe-opdrachten). Deze richtlijn biedt een passend kader voor assurance-opdrachten gericht op de beoordeling van beheersmaatregelen op het gebied van informatiebeveiliging binnen het Suwinet-domein. Op verzoek van de opdrachtgever (Ministerie SZW/BKWI) rapporteren wij onze bevindingen per afzonderlijke norm uit het toetsingskader. Per norm wordt een oordeel verstrekt over de opzet en het bestaan van de betreffende beheersmaatregel en, voor een selectie van maatregelen, over de werking daarvan gedurende de onderzoeksperiode.

Wij zullen geen algeheel oordeel verstrekken over het volledige toetsingskader. Het gehanteerde normenkader bestaat namelijk niet uit een integraal en samenhangend beheersingsframework, maar uit een selectie van relevante BIO-normen die specifiek voor Suwinet van toepassing zijn. Een overkoepelend oordeel zou daardoor een beperkte betekenis hebben en geen aanvullende waarde bieden voor de gebruiker van het rapport. Om die reden beperken wij ons tot een oordeel per afzonderlijke norm (in lijn met DigiD-systematiek), zodat op een gerichte en transparante wijze inzicht wordt verkregen in de mate waarin aan de geselecteerde normen wordt voldaan.

2.15 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.

2.16 Documentatie

De IT-auditor dient tijdig opdrachtdocumentatie op te stellen die een vastlegging van de basis voor het assurance-rapport verschaft. Richtlijn Documentatie (230) alsmede daarop gerichte bepalingen uit Richtlijn 3000 zijn onverkort van toepassing (inclusief 60 dagen termijn). Het dossier van de IT-auditor is zelfstandig leesbaar. Een integrale verwijzing naar de ENSIA zelfevaluatietool is niet toegestaan.

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 is niet toegestaan aangezien deze geïnterpreteerd kunnen worden als een (goedkeurend) oordeel met betrekking tot het betreffende deelonderwerp / vraag.

2.17 Consultatie

Indien een auditor[1] in het kader van de uitvoering van op Suwinet 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 gerichte opdrachten betrokken auditors / alle leden NOREA (verantwoordelijkheid NOREA) en / of stelselhouder / stelselbeheerder / toezichthouder en gemeenten en hun dienstverleners (verantwoordelijkheid ENSIA-gremia).

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

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

3. Tot slot

De op Suwinet 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 gerichte audit geen specifiek onderzoek op uit.

Bijlagen

Bijlage 1: Normenkader GeVS 2026

Bijlage 1.1 Normenkader GeVS 2026

Bijgaande tabel is ontleend aan de Verantwoordingsrichtlijn GeVS 2026 en geeft in hoofdlijnen het actuele normenkader weer. Dit normenkader verwijst naar de geselecteerde BIO-normen (basis BIO 1.04).

De Verantwoordingsrichtlijn GeVS 2027 is op 16 juni 2026 vastgesteld[18]. Voor het verantwoordingsjaar *2027* zijn geen inhoudelijke wijzigingen doorgevoerd. Wel heeft een omzetting plaatsgevonden van BIO 1.04 naar BIO 2 versie 1.3. Daarnaast zijn de afspraken tussen Ministerie van Sociale Zaken en Werkgelegenheid / BKWI / VNG (in kader ENSIA) en NOREA rond het toetsen van General IT Controls bij het gebruik van Suwinet Inlezen of DKD Inlezen (zie hierna onder toelichting) verwerkt. De verwijzing naar de normen uit BIO 2 versie 1.3 is in de navolgende opgenomen als (**X.XX)**. Zie voor nadere uitwerking ook GeVS 2027 en actuele informatie BIO 2 versie 1.3[19] voor nadere details.

Hoofdstuk	Nummer	Normen
5. Informatiebeveiligings beleid	5.1.1 **(5.01)**	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 **(5.01)**	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 **(5.02)**	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.
6. Organiseren van informatiebeveiliging	6.1.2 **(5.03)**	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 **(6.03)**	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 **(5.16)**	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.

[18] Referentie naar website BKWI opnemen (nog niet gepubliceerd 17-06-20026)

[19] Zie: Home NL - bio-overheid

9. Toegangsbeveiliging	9.2.2 **(5.18)**	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 **(5.18)**	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
9. Toegangsbeveiliging	9.2.6 **(5.18)**	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 **(8.24)**	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
12. Beveiliging bedrijfsvoering	12.1.1 **(5.37)**	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.
12. Beveiliging Bedrijfsvoering	**12.1.2 (8.32)**	**Wijzigingsbeheer: Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst. Alleen van toepassing bij het gebruik van Suwinet inlezen of DKD inlezen.**
12. Beveiliging Bedrijfsvoering	**12.1.4 (8.31)**	**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. Alleen van toepassing bij het gebruik van Suwinet Inlezen of DKD Inlezen.**
12. Beveiliging bedrijfsvoering	12.4.1 **(8.15)**	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 **(8.15)**	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
18. Naleving	18.1.4 **(5.34)**	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

Bijlage 1.2 Controle op werking

Gemeenten dienen zich vanaf 2026 te verantwoorden over opzet, bestaan *en werking voor een deel van de normen*. Hierbij dienen gemeenten zich te houden aan onderstaand schema. Waar de verantwoording over werking 'optioneel' is, mag de gemeente op werking laten toetsen, maar is het niet verplicht. Het eerstvolgende jaar nadat toetsing op werking voor een norm optioneel was, zal de toetsing op werking voor die norm verplicht worden.

Norm	Opzet	Bestaan	Werking over 2026	Werking over 2027
5.1.1	V	V	O	V
5.1.2	V	V	O	V
6.1.1	V	V	O	V
6.1.2	V	V	V	V
7.2.2	V	V	V	V
9.2.1	V	V	V	V
9.2.2	V	V	V	V
9.2.5	V	V	V	V
9.2.6	V	V	V	V
10.1.1	V	V	O	V
12.1.1	V	V	O	V
12.1.2	V	V	O	V
12.1.4	V	V	O	V
12.4.1.	V	V	V	V
12.4.2	V	V	O	V
18.1.4	V	V	O	V

V: Verplicht voor gemeenten, O: Optioneel voor gemeenten

Als controleperiode om een goed oordeel te kunnen vellen over de effectiviteit van de beheersingsmaatregelen wordt de periode 1-1-2026 t/m 31-12-2026 (kalenderjaar) gehanteerd.

In aanvulling op de aanwijzingen uit de BIO geldt dat bij de (interne) toets op werking van maatregelen minimaal de frequentie van minimaal 1x per kwartaal gehanteerd dient te worden. Voor de externe toets wordt verwezen naar bijlage 3.

Bijlage 1.3 Non-occurance

Bij een aantal normen kan zich de situatie voordoen dat wel voldaan is aan de opzet van de interne beheersingsmaatregel, maar het bestaan niet vastgesteld kan worden omdat de relevante gebeurtenis zich niet heeft voorgedaan in de onderzochte periode. In dat geval vermeldt de auditor 'Voldoet in opzet' voor de betreffende beheersingsmaatregel in de tabel oordelen en licht de auditor dit nader toe in de beschrijving van de uitgevoerde werkzaamheden.

In de situatie dat er geen occurences (non-occurance) zijn binnen de controleperiode (ofwel een lege populatie), maar de maatregelen in opzet geen afwijkingen hebben laten zien, zal de auditor de norm op bestaan / werking niet beoordelen ('geen oordeel'). De auditor vermeldt dit voor de betreffende beheersingsmaatregel in de tabel oordelen (onderdeel werking) en licht de auditor dit nader toe in de beschrijving van de uitgevoerde werkzaamheden. Zie verder ook bijlage 3.

Bijlage 1.4 Optionele controle werking maatregelen 2027

De optionele controle op de werking voor het verantwoordingsjaar 2026 voor normen waarvoor dit voor het verantwoordingsjaar 2027 verplicht gesteld is, vindt plaats door middel van een proefaudit door de IT-auditor.

Als controleperiode om een goed oordeel te kunnen vellen over de effectiviteit van de beheersingsmaatregelen wordt minimaal een periode van 3 maanden gehanteerd. De resultaten van

de proefaudit worden voor alle duidelijkheid niet opgenomen in het assurance-rapport dat mede bestemd is voor de toezichthouder en worden derhalve NIET gerapporteerd aan de toezichthouder.

Het proefaudit dient als separate opdracht overeengekomen te worden tussen opdrachtgever en auditor.

Voor de uit te voeren werkzaamheden voor de hier bedoelde normen op basis van BIO versie 1.04 kan de auditor zich oriënteren op de Handreiking Verantwoordingsrichtlijn GeVS voor RE's 2025[20]. Aan een integrale uitwerking op basis van BIO 2 versie 1.3. wordt in samenwerking met alle stakeholders (waaronder SZW/BKWI/ VNG) gewerkt.

Bijlage 1.5 General IT Controls bij het gebruik van Suwinet Inlezen of DKD inlezen

Om een uitspraak te kunnen doen omtrent de betrouwbaarheid en bruikbaarheid van logbestanden dient aan een aantal randvoorwaarden (General IT Controls) te zijn voldaan.

In het kader van Suwinet-inkijk worden de gebruikersactiviteiten en uitzonderingen vastgelegd door BKWI aan de kant van de centrale voorziening. De logging is dus ingeregeld aan de zijde van de beheerder (BKWI). Bij de afnemer dient een proces te zijn geïmplementeerd voor het beoordelen van de BKWI logging/ afnemersrapportages.

Voor Suwinet inlezen / DKD inlezen (gemeenten) moet de organisatie zelf de logging genereren, beschermen en analyseren. In dit kader is het noodzakelijk om de daarop betrekking hebbende procedures voor changemanagement te toetsen.

Voor zowel Suwinet Inkijk als Suwinet Inlezen geldt dat de randvoorwaarden ten aanzien van logische toegangsbeveiliging reeds opgenomen in het GeVS-normenkader. Aanvullingen ten aanzien van logische toegangsbeveiliging zijn niet benodigd.

Aangezien Suwinet Inlezen en DKD Inlezen van toepassing kunnen zijn op diverse applicaties, die elk voor zich anders ingericht kunnen zijn, is geen éénduidig normenkader beschikbaar te stellen anders dan de in deze handreiking opgenomen geïndiceerde controlewerkzaamheden.

De IT-auditor dient zelf op basis van een *beknopte* omgevings- en risicoanalyse te bepalen welke General IT Controls van belang kunnen zijn om de betrouwbaarheid en bruikbaarheid van logbestanden te waarborgen.

In overleg tussen het Ministerie van Sociale Zaken en Werkgelegenheid / BKWI / VNG (in kader ENSIA) en NOREA zijn de beknopte omgevings- en risicoanalyse en de op basis daarvan te verrichten controlewerkzaamheden vertaald naar de BIO-normen 12.1.2 en 12.1.4. Dit is in deze Handreiking in alle van toepassing zijnde onderdelen expliciet gemaakt (o.a. door de tekst extra te benadrukken). *Het hier weergegeven normenkader GeVS 2026 geldt alleen wanneer sprake is van het gebruik van de inleesapplicatie*. *E.e.a. is in de volgende bijlage nader gedetailleerd uitgewerkt.*

[20] **https://www.norea.nl/uploads/bfile/0e5eb13c-b93f-427d-9209-cee5c4315f9b**

Bijlage 2: Testaanpak bij de te onderzoeken normen relevant voor Suwinet (inclusief controle op werking)

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	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 organisatie (gemeente) van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden. c) De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers.	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). Stel vast dat het beleid is gepubliceerd en gecommuniceerd aan medewerkers en relevante partijen zoals bijvoorbeeld subserviceorganisaties. Interview de verantwoordelijke functionarissen.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
		d) De gemeenschappelijke betrouwbaarheidseisen en normen die op de gemeente van toepassing zijn. e) De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd. f) De bevordering van het beveiligingsbewustzijn.	
5.1.2 Beoordeling van het informatie-beveiligingsbeleid	<u>Criterium BIO:</u> 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. <u>Doelstelling:</u> Bewerkstellingen dat de getroffen beveiligingsmaatregelen continue voldoen aan het juiste beveiligingsniveau. <u>*Risico:*</u> *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.	<u>Betrokken partij(en):</u> Gemeente / samenwerkingspartij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD <u>Toelichting:</u> 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.* <u>Diepgang:</u> Opzet en bestaan <u>Test aanpak:</u>

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			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 College van B&W van de gemeente 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. 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.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			**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	<u>Criterium BIO:</u> 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. <u>Doelstelling:</u> 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. <u>*Risico:*</u> *Onduidelijke taken en verantwoordelijkheden en het ontbreken van juiste functiescheiding kunnen leiden tot:* *- misbruik van bevoegdheden,* *- te ruim toegekende bevoegdheden,*	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.	<u>Betrokken partij(en):</u> Gemeente / samenwerkingspartij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD <u>Toelichting:</u> Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd (in de vorm van bijvoorbeeld een RACI-matrix[*]). **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;*

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
	- over het hoofd zien van en/of tot implementatie van tegenstrijdige beveiligingsmaatregelen.		• *Controleren van rechtmatig gebruik 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, bestaan en werking <u>Test aanpak:</u> 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. ***<u>Aanvullende test aanpak voor de controle op werking:</u>*** <u>Scope:</u>

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			Suwinet-Inkijk. DKD/Suwinet-inlezen en, waar van toepassing, Wgs Inkijk en RooO. <u>Specifieke controles voor wat betreft werking</u> Denk aan het volgende: Stel aan de hand van een bewijsstuk vast, dat een aantoonbare interne controle op het naleven van de beheersingsmaatregelen op blijvende handhaving van de vastgestelde inrichting van de Administratieve Organisatie/Informatiebeveiliging minimaal 1x per kwartaal daadwerkelijk heeft plaatsgevonden gedurende de controleperiode. Stel vast dat het autoriseren tot zoekpagina's, bronpagina's en overzichtspagina's conform de inrichting van de AO is gebeurd tijdens de controleperiode. Bepaal het aantal verschillende rollen aan het begin en het einde van de controleperiode. Het gaat hier om de door BKWI aangemaakte standaard rollen. • Selecteer conform de tabel steekproefomvang het juiste aantal mutaties in de gebruikte Suwi rollen en stel vast dat er geen conflicterende taken en verantwoordelijkheden zijn, die niet zijn gescheiden. De autorisatiebeheerder van de organisatie zal - in overleg met de security officer en het management – hier uitvoering aan geven. Het is belangrijk om kritisch te zijn in het toekennen van rollen: het moet genoeg zijn voor de taakuitvoering, maar mag niet meer dan nodig zijn (en let in bredere zin op de toekenning van rollen op basis van het 'need-to-know' principe). Realiseer ook dat de combinatie van sommige pagina's extra risicovol is door de stapeling van gegevens. Dat geldt vooral voor autorisaties met andere zoeksleutels dan het BSN. BKWI geeft aan dat vooral gelet dient te worden op de volgende risicovolle Suwinet pagina's:

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			• Overzichtspagina 'Handhaving' voor de uitvoering van taken rondom handhaving en benadelingsonderzoek (sociale recherche). Dit is een risicovolle autorisatie vanwege de stapeling van gegevens. Advies: zeer beperkt toekennen. Als er gekozen wordt voor autorisatie van deze pagina is het niet de bedoeling dit in combinatie te doen met autorisaties voor Rechtmatigheid+ of Re-integratie. Deze pagina toont medebewoners tussen 21 en 40 jaar die mogelijk vallen onder de Kostendelersnorm. Er worden BRP gegevens gecombineerd met opleidingsgegevens van DUO. • Overzichtspagina 'Terugvordering en Verhaal' voor de uitvoering van taken rondom terugvordering en verhaal. Dit is een risicovolle autorisatie vanwege de stapeling van gegevens. Advies: zeer beperkt toekennen. Als er gekozen wordt voor autorisatie van deze pagina is het niet de bedoeling dit in combinatie te doen met autorisaties voor Rechtmatigheid+ of Re-integratie. • Bronpagina 'Vorderingen 58lid1', voor uitvoering van taken rondom het terugvorderen van benadeling, het vaststellen van recidive en eventuele boete. Ook dit is een risicovolle autorisatie vanwege de zeer privacygevoelige gegevens. Advies: zeer beperkt toekennen aan bijvoorbeeld alleen recidive beoordelaars. Overige medewerkers kunnen gebruik maken van de algemene informatie over alle bestaande GSD vorderingen via de pagina's Rechtmatigheid+ en Bijstandsregelingen. • Zoekpagina 'Zoek in BRP' voor de uitvoering van taken rondom rechtmatigheid, handhaving en benadelingsonderzoek. Door geboortedatum, postcode en

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			huisnummer in te voeren, kunt u een persoon traceren in de BRP. Dit is een risicovolle autorisatie vanwege het gebruik van een zoeksleutel anders dan BSN. Advies: zeer beperkt toekennen. • Zoekpagina 'Zoek+ in BRP' voor de uitvoering van taken rondom rechtmatigheid, handhaving en benadelingsonderzoek. Deze zoekpagina bevat meer zoeksleutels dan Zoek in BRP zoals geboortedatum, postcode, huisnummer, achternaam en geslacht. Doordat er gebruik kan worden gemaakt van meerdere zoeksleutels kan het zijn dat het zoekresultaat uitgebreider is dan op de pagina 'Zoek in BRP'. Dit is een risicovolle autorisatie vanwege het gebruik van een zoeksleutel anders dan BSN. Advies: zeer beperkt toekennen. • Zoekpagina 'Zoek in Kadaster' ten behoeve van taken rondom handhaving en benadelingsonderzoek. Zoeken via kadastrale aanduidingen of via locatie (adres). Zoeken is mogelijk met meerdere zoeksleutels, bijvoorbeeld Perceelnummer of Sectie. Dit is een risicovolle autorisatie vanwege het gebruik van een zoeksleutel anders dan BSN. Advies: zeer beperkt toekennen. • Zoekpagina 'Zoek in PIVA' ten behoeve van taken rondom handhaving en benadelingsonderzoek. Persoonsinformatievoorziening Nederlandse Antillen en Aruba (PIVA). Om personen te vinden via Zoek in PIVA moet er gezocht worden op Geboortedatum en Achternaam. Autorisatie voor deze zoekpagina moet per organisatie (GSD) individueel aangevraagd worden bij de RvIG. Dit is een risicovolle autorisatie vanwege het gebruik van een

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			zoeksleutel anders dan BSN. Advies: zeer beperkt toekennen. • Zoekpagina 'Zoek in RDW' ten behoeve van taken rondom handhaving en benadelingsonderzoek. Via de zoeksleutels BSN, kenteken, naam, adresgegevens en KvK-nummer kan de gebruiker voertuigen uit heden en verleden opzoeken. De getoonde gegevens komen overeen met de pagina RDW. Dit is een risicovolle autorisatie vanwege het gebruik van een zoeksleutel anders dan BSN. Advies: zeer beperkt toekennen. • Zoekpagina 'Zoek in RDW+' ten behoeve van taken rondom handhaving en benadelingsonderzoek. Via de zoeksleutels BSN, kenteken, naam, adresgegevens en KvK-nummer kan de gebruiker voertuigen uit heden en verleden opzoeken. Extra gegevens die middels deze autorisatie worden getoond zijn de verzekeringsgegevens van het voertuig. De getoonde gegevens komen overeen met de pagina RDW+. Dit is een risicovolle autorisatie vanwege het gebruik van een zoeksleutel anders dan BSN. Advies: zeer beperkt toekennen. • Tenslotte mogen de rollen van gebruikersbeheerder (voor het beheer van Suwinet) niet worden gecombineerd met een uitvoerende rol dan wel de rol van gemandateerde dan wel security officer.
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	7.2.2.1 Alle medewerkers hebben de verantwoordelijkheid	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie Scope:

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
	behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de gemeente, voor zover relevant voor hun functie. <u>Doelstelling:</u> Het bewustmaken van gebruikers van Suwinet gegevens <u>*Risico:*</u> *Indien gebruikers van Suwinet gegevens zich niet of onvoldoende bewust zijn van de (hoge) vertrouwelijkheid, bestaat het risico dat deze gegevens onvoldoende worden beschermd.*	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. 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.	Suwinet Inkijk Suwinet Inlezen Suwinet DKD <u>Toelichting:</u> 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 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 en werking 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 (minimaal 1 keer per kwartaal[21]) aandacht wordt besteed aan bewustwording van informatiebeveiliging waarbij expliciet aandacht wordt besteed aan Suwinet gerelateerde onderwerpen. Stel vast dat deze bewustwordingswerkzaamheden daadwerkelijk 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*

[21] 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 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			persoonsgegevens dient te worden gecommuniceerd aan alle personen die betrokken zijn bij deze verwerking. ***<u>Aanvullende test aanpak voor de controle op werking:</u>*** <u>Scope:</u> Suwinet-Inkijk. DKD/Suwinet-inlezen en, waar van toepassing, Wgs Inkijk en RooO. <u>Specifieke controles voor wat betreft werking</u> Denk aan het volgende: • Stel aan de hand van een overzicht uit Suwi het juiste aantal nieuwe gebruikers vast, die tijdens de controleperiode toegang hebben gekregen tot Suwinet gegevens. In dit overzicht staan alle nieuwe Suwi gebruikersaccounts vermeld. • Selecteer conform de tabel steekproefomvang het juiste aantal van deze medewerkers uit deze groep en stel vast dat deze geselecteerde medewerkers binnen drie maanden na indiensttreding een training (I-)bewustzijn succesvol hebben gevolgd. • Stel vast of de organisatie hier gedurende de controleperiode zelf aantoonbaar interne controle op heeft uitgevoerd.
9. Toegangsbeveiliging			
9.2.1 Registratie en afmelden van gebruikers	<u>Criterium BIO:</u> Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. <u>Doelstelling:</u> Gebruikers en beheerders de juiste toegangsrechten geven (niet meer en	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	<u>Betrokken partij(en):</u> Gemeente / samenwerkingspartij / IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
	niet minder) dan welke nodig zijn voor de hen opgedragen (wettelijke)taken. *<u>Risico:</u>* *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.*	gemotiveerd en vastgelegd door de proceseigenaar.	** Let op: Voor Suwinet en DKD Inlezen is de "inleesapplicatie" met de eventuele bijbehorende database in scope.* *Note: indien de gemeente / samenwerkingspartij de RooO regeling uitvoert verdient deze norm speciale aandacht omdat er gebruikers kunnen worden geautoriseerd voor de speciale RooO subpagina's van Suwi-Inkijk.* <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 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 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 <u>en</u> dat adequate login wordt toegepast zodat te allen tijde herleidbaar is wie met dit account wanneer en tot welke gegevens toegang heeft gehad;

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			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 en werking 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. 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 dat deze daadwerkelijk zijn ingericht. Zie verder ook 9.2.2, 9.2.5 en 9.2.6. Interview de verantwoordelijke functionarissen. ***Aanvullende test aanpak voor de controle op werking:*** Scope:

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			Suwinet-Inkijk. DKD/Suwinet-inlezen en, waar van toepassing, Wgs Inkijk en RooO. ***<u>Specifieke controles voor wat betreft werking:</u>*** Denk aan het volgende: • Vraag een overzicht van de toegekende, ingetrokken of gewijzigde gebruikersaccounts tijdens de controleperiode op. • Bepaal hoeveel wijzigingen in de zin van toegekende, ingetrokken of gewijzigde gebruikersaccounts voor Suwinet tijdens de controleperiode hebben plaatsgevonden. Selecteer conform de tabel steekproefomvang het juiste aantal mutaties en stel vervolgens vast: • dat de vastgestelde procedure rond toekennen / wijzigen / beëindigen van rechten in alle onderzochte gevallen correct is toegepast; • dat uitsluitend gebruik is gemaakt van individuele accounts die dus tot één persoon herleidbaar zijn (dus geen groepsaccounts – tenzij voldaan is aan de daaraan gestelde randvoorwaarden).
9.2.2 Gebruikers toegang verlenen	<u>Criterium BIO:</u> 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.	9.2.2.1 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	<u>Betrokken partij(en):</u> Gemeente / samenwerkingspartij / IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
	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.*	wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven[22]. 9.2.2.3 Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	** Let op: Voor Suwinet en DKD Inlezen is de "inleesapplicatie" met de eventuele bijbehorende database in scope.* *Note: indien de gemeente / samenwerkingspartij de RooO regeling uitvoert verdient deze norm speciale aandacht omdat er gebruikers kunnen worden geautoriseerd voor de speciale RooO subpagina's van Suwi-Inkijk.* 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 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);

[22] 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 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			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; f) met eigenaren van de informatiesystemen of -diensten periodiek de toegangsrechten beoordelen (zie ook 9.2.5). <u>Diepgang:</u> Opzet en bestaan en werking van de beheersingsmaatregelen. <u>Test aanpak:</u> 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. ***<u>Aanvullende test aanpak voor de controle op werking:</u>*** <u>Scope:</u> Suwinet-Inkijk. DKD/Suwinet-inlezen en, waar van toepassing, Wgs Inkijk en RooO. ***<u>Specifieke controles voor wat betreft werking</u>*** Denk aan het volgende:

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			• Stel vast dat is vastgelegd welke personen bevoegdheden hebben voor het verlenen van toegangsrechten, ergo stel vast dat de gebruikersbeheerder Suwinet hiertoe is gemandateerd dan wel dat de gebruikersbeheerder per casus hiertoe opdracht krijgt van de leidinggevende. • Bepaal hoeveel wijzigingen hebben plaatsgevonden in de autorisaties gedurende de controleperiode en selecteer conform de tabel steekproefomvang het juiste aantal mutaties en stel daarvan vast dat het toewijzen (of wijzigen dan intrekken) van toegangsrechten is uitgevoerd in overeenstemming met de bovenstaande aandachtspunten.
9.2.5 Beoordeling van toegangsrechten van gebruikers	Criterium BIO: Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. <u>Doelstelling:</u> 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. <u>*Risico:*</u> *Bij het ontbreken van controle op de toegangsrechten worden afwijkingen in het autorisatieproces niet gesignaleerd worden.*	9.2.5.1 Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld. <u>(Overruled door 9.2.5.3)</u> 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 kwartaal beoordeeld.	<u>Betrokken partij(en):</u> Gemeente / samenwerkingspartij/ IT-serviceorganisatie <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 periodiek beoordelen van toegangsrechten van gebruikers 9.2.6 richt zich op het proces van intrekken of wijzigen van toegangsrechten

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
	Bij het ontbreken controles op het gebruik van autorisaties wordt misbruik niet gesignaleerd.		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; e) van wijzigingen in speciale accounts behoren voor periodieke beoordeling logbestanden te worden bijgehouden. <u>Diepgang:</u> Opzet en bestaan en werking 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 kwartaal plaatsvindt. Stel vast dat de periodieke review in lijn is met bovenstaande aandachtspunten.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2026	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			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 dan aan "voldoet in opzet – geen incidenten gemeld".* *Note: indien de gemeente / samenwerkingspartij de RooO regeling uitvoert verdient deze norm speciale aandacht omdat er gebruikers kunnen worden geautoriseerd voor de speciale RooO subpagina's van Suwi-Inkijk.* ***Aanvullende test aanpak voor de controle op werking:*** Scope: Suwinet-Inkijk. DKD/Suwinet-inlezen en, waar van toepassing, Wgs Inkijk en RooO. Specifieke controles voor wat betreft werking Denk aan het volgende: • Stel op basis van tenminste één deelwaarneming per kwartaal vast dat de opvolging van bevindingen uit de periodieke review van de auditee zelf is gedocumenteerd en behandeld als beveiligingsincident. • Stel daarbij aan de hand van een bewijsstuk vast dat gedurende de controleperiode aantoonbaar interne controle heeft plaatsgevonden op de naleving van de beheersingsmaatregelen binnen deze norm.

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. <u>Diepgang:</u> Opzet en bestaan en werking van de beheersingsmaatregelen. <u>Test aanpak:</u> 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. ***<u>Aanvullende test aanpak voor de controle op werking:</u>*** <u>Scope:</u> Suwinet-Inkijk. DKD/Suwinet-inlezen en, waar van toepassing, Wgs Inkijk en RooO.

			<u>Specifieke controles voor wat betreft werking</u> Denk aan het volgende: • Inspecteer of in de organisatie gedurende de controleperiode een verbijzonderde interne controle heeft plaatsgevonden op het naleven van de beheersingsmaatregelen rond het toekennen /wijzigen of intrekken van toegangsrechten. • Bepaal hoeveel wijzigingen hebben plaatsgevonden gedurende de controleperiode en selecteer conform de tabel steekproefomvang het juiste aantal mutaties en stel vervolgens vast dat bij het doorvoeren van de wijzigingen de vastgestelde procedures zijn gevolgd. • Selecteer conform de tabel steekproefomvang het juiste aantal medewerkers en stel vast dat de geselecteerde gebruikers nog werkzaam zijn binnen het Suwi domein.
10. Cryptografie			
10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	<u>Criterium BIO:</u> Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd. <u>Doelstelling:</u> Het voorkomen van ongeautoriseerde toegang tot netwerkdiensten.	10.1.1.1 In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: a) Wanneer cryptografie ingezet wordt. b) Wie verantwoordelijk is voor de implementatie.	<u>Betrokken partij(en):</u> Gemeente / samenwerkingspartij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inlezen Suwinet DKD

	<u>Risico:</u> *Ondanks het besloten karakter van Suwinet bestaat het risico dat de toegang tot gegevens niet adequaat is beschermd.*	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 database in scope.* <u>Toelichting:</u> Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie. <u>Diepgang:</u> Opzet en bestaan van de beheersingsmaatregelen. <u>Test aanpak:</u> 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[23]*

[23] 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 (op basis informatie BKWI (https://bkwi.nl/producten/suwinet-autorisatie/overzicht-autorisaties-op-suwinet-inkijk-voor-gsd-v20240715) 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.
Vanaf 2022 na overleg tussen vertegenwoordigers van het Ministerie van SZW, BKWI (,VNG) en NOREA zijn 12.1.2 en 12.1.4 betrokken in auditwerkzaamheden betrokken in uitvoering controlewerkzaamheden. Met ingang van GeVS 2026 integraal onderdeel normenkader. **Zie ook toelichting in bijlage 2.**			
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 omvatten: - Beschrijving en goedkeuring voorgestelde wijziging; - Beschrijving / beoordeling en goedkeuring gerealiseerde wijziging;

			- Beschrijving / beoordeling en goedkeuring uitgevoerde testwerkzaamheden; - Beschrijving / goedkeuring van overdracht naar productie-omgeving inclusief 'fall-back" procedures; - Definitie goedkeuring na overdracht productie-omgeving. 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 ontwikkel-, test- en productieomgevingen	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-orgnisatie. <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 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 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-serviceorganisatie. <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
Vanaf 2022 na overleg tussen vertegenwoordigers van het Ministerie van SZW, BKWI (,VNG) en NOREA zijn 12.1.2 en 12.1.4 betrokken in auditwerkzaamheden betrokken in uitvoering controlewerkzaamheden. Met ingang van GeVS 2026 integraal onderdeel normenkader. **Zie ook toelichting in bijlage 2.**			
12.4.1 Gebeurtenissen registreren	<u>Criterium BIO:</u>	12.4.1.1 Een logregel bevat minimaal:	<u>Betrokken partij(en):</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.*	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 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	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 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* en / of kan *betrokken worden bij de hier bedoelde werkzaamheden.* Er behoren procedures te worden vastgesteld om het gebruik van Suwinet-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig (minimaal 4 maal per jaar gelijkmatig verdeeld) te worden beoordeeld en gerapporteerd.

		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.	<u>Diepgang:</u> Opzet en bestaan en werking 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 van minimaal 4 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 vier 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. *Note: Uitgangspunt is algemene aanpak organisatie en alleen waar nader gespecificeerd Suwinet-specifieke uitwerkingen.* Interview de verantwoordelijke functionarissen.

			Aanvullende test aanpak voor de controle op werking: Scope: Suwinet-Inkijk. DKD/Suwinet-inlezen en, waar van toepassing, Wgs Inkijk en RooO. Specifieke controles voor wat betreft werking Denk aan het volgende: • Stel vast dat de periodieke review van de logging 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 organisatie geformuleerde opvolgingsproces. • Selecteer minimaal 2 van de minimaal 4 van de door de organisatie uitgevoerde werkzaamheden in dit kader van het incidentmanagement proces. • Instrueer de organisatie om in volgorde schermprints te maken zodat een re-performance kan worden uitgevoerd op minimaal 4 van de door de organisatie uitgevoerde werkzaamheden in dit kader. Het is aan de organisatie om aan te tonen dat de relevante werkzaamheden (periodieke review / opvolging van incidenten) zijn uitgevoerd.
12.4.2 Beschermen van informatie in logbestanden	Criterium BIO: Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	12.4.2.1 Er is een overzicht van logbestanden die worden gegenereerd.	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie

	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.*	12.4.2.2 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.	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 **PM: formeel geen onderdeel normenkader. Werkzaamheden randvoorwaardelijk voor overige werkzaamheden.**			
14.2.2	N.v.t.	Procedures voor wijzigingsbeheer met betrekking tot systemen: Wijzigingen aan systemen binnen de	Betrokken partijen: Gemeente / samenwerkingspartij / IT-service serviceorganisatie

Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework.		levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	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 praktijk 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.	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	Betrokken partij(en): Gemeente / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD

	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.*	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.	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. *Note: Het dient opgenomen te zijn als een bronsysteem bij een bepaalde verwerking en niet als een verwerking zelf.* Stel vast dat (conform artikel 37 lid 1 AVG) 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. 58-62 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 3: Tabel steekproefomvang / deelwaarnemingen

Geen algemeen toepasbare methodiek

NOREA heeft op dit moment geen algemeen toepasbare methodiek voor het bepalen van de steekproefomvang bij de toetsing van werking. Onderstaande tabel is ter handreiking. Gebruik van andere methoden is toegestaan, mits daar een rationele argumentatie bij gegeven wordt ('comply or explain'). De in de tabel opgenomen omvang dient per assurance-onderzoek gehanteerd te worden.

Bij het toetsen van de werking steunt de IT-auditor op uitgevoerde (verbijzonderde) interne controles op de beheersingsmaatregelen gedurende de gehele controleperiode. De auditor toets de werking van de beheersingsmaatregelen gespreid over deze gehele controleperiode. De populatie van de te onderzoeken aspecten (c.q. de steekproef / deelwaarneming) omvat daarmee de occurences over de gehele controleperiode.

Factoren die van invloed zijn op het auditrisico, en daarmee op de omvang van de waarnemingen, zijn onder meer:

- Bevindingen uit het verleden
- Wijzigingen in de uitvoering van de interne controle-activiteiten (o.a. personele wijzigingen)
- Veranderingen in het ontwerp van de beheersmaatregel
- Zwakke controle omgeving (1e, 2e en / of 3e lijnscontrole).

Sampling o.b.v. frequentie van de beheersmaatregel		**Minimale omvang van de te verrichten deelwaarnemingen bij een lager auditrisico**	**Minimale omvang van de te verrichten deelwaarnemingen bij een hoger auditrisico**
Frequentie op jaarbasis	Aantal occurences in de controleperiode[24]		
Jaarlijks	of 1 occurrence	1	1
Eens per kwartaal	of 2 – 4 occurrences	2	2
Eens per maand	Of 5 – 12 occurrences	2	3
Eens per week	Of 13 – 53 occurences	5	8
Dagelijks	Of 54 – 249 occurrences	15	25
Meer dan dagelijks (recurring)	>= 250 occurences	25	40

Context bij voorgaande tabel
Voor de periodiciteit jaarlijks, eens per kwartaal, eens per maand, eens per week en dagelijks wordt een niet-statistische steekproef (deelwaarneming) gehanteerd[25].

Algemeen uitgangspunt voor de oordeelsvorming bij geconstateerde afwijkingen: er wordt vanuit gegaan dat in de 1e, 2e (en eventueel 3e) lijnscontrole eventuele fouten reeds gedetecteerd en

[24] Alleen van toepassing bij afwijkende controleperiode. Ook opgenomen om vergelijkbaarheid met / aansluiting op andere NOREA Handreikingen te waarborgen

[25] Zie voor een uitleg van een statistische en niet-statistische steekproef Controle Standaard 530 (het gebruiken van steekproeven bij een controle) van de NBA

gecorrigeerd zijn. Er mag dus door de auditor geen fout gevonden worden. Eén fout leidt binnen de binaire oordeelsmethodiek (voldoet / voldoet niet) tot 'voldoet niet' op onderzochte element.

In aanvulling op de algemene uitgangspunten is in het kader van de werkzaamheden rond Suwinet als leidraad voor zowel de door de organisatie uit te voeren interne controlewerkzaamheden (4 gespreid over het jaar) en de door de auditor daarop uit te voeren werkzaamheden met een minimum aantal van 2 (over het jaar gespreide) waarnemingen vastgesteld.

Bijlage 4: Overwegingen ENSIA IT-Audit in samenwerkingsverbanden Suwinet

De uitgangspunten
De Verantwoordingsrichtlijn GeVS 2026 is volledig gebaseerd op de BIO. De gemeente geeft in de verantwoording aan in hoeverre wordt voldaan aan dit normenkader. Suwinet-regelgeving vraagt van het gemeentebestuur een verantwoording op basis vaneen door een IT-auditor (RE) afgegeven assurance-rapport (3000D). 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.

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 gemeentelijke verantwoording.

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 relevante processen en documentatie ervan heeft vormgegeven en kan steunen op de gemeentelijke organisatie.
- Zich een beeld vormt van de wijze waarop de informatie vanuit samenwerkingsverbanden in de gemeentelijke documentatie (en zelfevaluatie) is verwerkt.
- De aansluiting tussen het geheel van de beschikbare informatie 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: Format assurance-rapport

Bijlage 5.1 Toelichting format assurance-rapport

Bij het uitwerken van het format voor het assurance-rapport is rekening gehouden met:
a. De vereisten uit Richtlijn 3000: Richtlijn Assurance-opdrachten (3000, Attest- en Directe Opdrachten);
b. De vereisten opgenomen in de Verantwoordingsrichtlijn GeVS 2026 en bijbehorende documenten;
c. De wens van alle gebruikers van het assurance-rapport tot het behouden van alle informatie zoals voorheen opgenomen in de Collegeverklaring en bijbehorend bijlage Suwi, en, in lijn daarmee,
d. Een vergelijkbare aanpak en uitwerking voor de stelsels waarover gemeenten zich in het kader van ENSIA moeten verantwoorden inclusief / op basis van een assurance-rapport van een IT-auditor (RE).

Aandachtspunt:
In lijn met de uitgangspunten op basis van de geldende Suwi-regelgeving en van het Ministerie van SZW in het kader van het daarop uit te voeren toezicht dient de aansluithouder zich te verantwoorden over het geheel van de toepassingen. Derhalve wordt er één oordeel per norm gegeven. Daarbij geldt dat een niet goedkeurend oordeel bij één toepassing leidt tot een niet goedkeurend oordeel voor de norm als geheel.

Zie verder ook toelichting in paragraaf 2.14 van deze Handreiking

Hierna zijn de volgende formats opgenomen:
a. Assurance-rapport op niveau gemeente;
b. Assurance-rapport op niveau dienstverlener[26];

[26] Onder dienstverlener wordt ook bedoeld samenwerkingspartij zoals elders in deze Handreiking vermeld.

Bijlage 5.2 Assurance-rapport op niveau gemeente

Assurance-rapport van de onafhankelijke IT-auditor

Aan : <College van BenW van de gemeente> / <management dienstverlener>, Ministerie van Sociale Zaken en Werkgelegenheid en Bureau Keteninformatisering Werk en Inkomen
Datum : Rapportdatum
Van : Auditor
Kenmerk

Onze oordelen

Wij hebben een onderzoek met redelijke mate van zekerheid uitgevoerd naar de beveiligingsmaatregelen van alle gegevensuitwisselingen via de GeVS conform de Verantoordingsrichtlijn GeVS 2026 door <de gemeente> / <(sub)serviceorganisatie>.

Per norm hebben wij hieronder vermeld of wordt voldaan aan de norm. Om de leesbaarheid van dit rapport te vergroten zijn de oordelen in deze tabel weergegeven als 'voldoet' of 'voldoet niet'. Hierbij moet 'voldoet' ingeval het oordeel is beperkt tot opzet en bestaan worden geïnterpreteerd als 'Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven norm effectief zijn opgezet en geïmplementeerd op (oordeelsdatum)'. 'Voldoet niet' moet in geval het oordeel is beperkt tot opzet en bestaan worden geïnterpreteerd als 'Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven norm niet in alle materiële opzichten effectief zijn opgezet en/of geïmplementeerd op (oordeelsdatum)'.

De normen waarbij ook de effectieve werking wordt vastgesteld moet 'voldoet' worden geïnterpreteerd als 'Wij zijn van oordeel dat de getoetste interne beheersingsmaatregelen die verband houden met de op die regel aangegeven norm effectief werkten tijdens de controleperiode van [begindatum] tot [einddatum]'. 'Voldoet niet' moet vervolgens worden geïnterpreteerd als 'Wij zijn van oordeel dat de getoetste interne beheersingsmaatregelen die verband houden met de op die regel aangegeven norm niet in alle materiële opzichten effectief werkten tijdens de controleperiode van [begindatum] tot [einddatum]'.

De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel zijn de criteria die zijn beschreven in de sectie 'van toepassing zijnde criteria'.

Onze oordelen zijn gevormd op basis van de aangelegenheden die in dit assurance-rapport zijn uiteengezet.

Nummer	Normen	Oordeel opzet en bestaan	Oordeel werking[27]
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.	Voldoet / Voldoet niet	N.v.t.

[27] N.v.t. voor deze norm is toets op werking over controleperiode niet verplicht gesteld.

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.	Voldoet / Voldoet niet	N.v.t.
6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Voldoet / Voldoet niet	N.v.t.
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.	Voldoet / Voldoet niet / Voldoet in opzet	Voldoet / Voldoet niet
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.	Voldoet / Voldoet niet / Voldoet in opzet	Voldoet / Voldoet niet
9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Voldoet / Voldoet niet / Voldoet in opzet	Voldoet / Voldoet niet
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.	Voldoet / Voldoet niet / Voldoet in opzet	Voldoet / Voldoet niet
9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	Voldoet / Voldoet niet / Voldoet in opzet	Voldoet / Voldoet niet
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.	Voldoet / Voldoet niet / Voldoet in opzet	Voldoet / Voldoet niet
10.1.1[28]	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	Voldoet / Voldoet niet	N.v.t.
12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	Voldoet / Voldoet niet	N.v.t.

[28] N.v.t. bij opdrachtgevers die alleen Suwi-Inkijk gebruiken

12.1.2	Wijzigingsbeheer: Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging ehoren te worden beheerst. Alleen van toepassing bij het gebruik van Suwinet Inlezen of DKD Inlezen.	Voldoet / Voldoet niet	N.v.t.
12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen: Bedrijfsvoering-, Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen. Alleen van toepassing bij het gebruik van Suwinet Inlezen of DKD Inlezen	Voldoet / Voldoet niet	N.v.t.
12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Voldoet / Voldoet niet / Voldoet in opzet	Voldoet / Voldoet niet
12.4.2[29]	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Voldoet / Voldoet niet	N.v.t.
18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Voldoet / Voldoet niet	N.v.t.

De basis voor onze oordelen

Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht, de NOREA Richtlijn 3000D 'Assurance-opdrachten door IT-auditors '(Directe-opdrachten)'en de nadere regels zoals opgenomen in de Handreiking Suwinet (in kader ENSIA voor IT-auditors (RE's) 2026 versie 1.0 van NOREA. 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 <de gemeente> / <(sub)serviceorganisatie> en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor onze oordelen <behalve die normen waarvoor wij geen oordeel konden geven>.

Van toepassing zijnde criteria

Voor deze opdracht hanteren wij de Verantwoordingsrichtlijn GeVS (Gemeenschappelijke elektronische Voorziening Suwi) 2026 die door het Ministerie van Sociale Zaken en Werkgelegenheid (SZW) is vastgesteld. Meer in het bijzonder gaat het daarbij om het in de bijlage 1 van in de Verantwoordingsrichtlijn GeVS 2026 opgenomen normenkader.

De criteria waarvan gebruik wordt gemaakt bij het uitvoeren van de assurance-opdracht houden in dat:

- De risico's die het voldoen aan de normen in gevaar brengen en daarmee de betrouwbaarheid van het gebruik van Suwi aantasten, werden onderkend;

[29] N.v.t. bij opdrachtgevers die alleen Suwi-Inkijk gebruiken

- De onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het voldoen aan de normen niet zouden verhinderen;
- De interne beheersingsmaatregelen die verband houden met de normen op afdoende wijze zijn opgezet en daadwerkelijk zijn geïmplementeerd;
- De interne beheersingsmaatregelen die verband houden met een selectie van specifieke normen gedurende de controleperiode effectief hebben gewerkt.

Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek

Object van onderzoek

Het object van onderzoek waren de beveiligingsmaatregelen van alle gegevensuitwisselingen via de GeVS conform de Verantoordingsrichtlijn GeVS 2026 door <de gemeente> / <(sub)serviceorganisatie(s)>.

Aanvullende assurance waarop wordt 'gesteund' is ontleend aan: [type rapport, rapportdatum, kenmerk, auditorganisatie, eventueel naam IT auditor, onderzoeksperiode + eventuele bridgeletter(s) zodat de periodes aansluiten, van <dienstverlener>].
In Bijlage B geven wij u een meer gedetailleerde beschrijving van het object van onderzoek.

Beoogde gebruikers en doel

Ons assurance-rapport inclusief bijlagen is uitsluitend bestemd voor <de gemeente> / <(sub)serviceorganisatie>, gemeente(n)>, het Ministerie van Sociale Zaken en Werkgelegenheid en het Bureau Keteninformatiesering Werk en Inkomen. Het Ministerie van Sociale Zaken en Werkgelegenheid en het Bureau Keteninformatisering Werk en Inkomen kunnen hiermee toezicht houden op het gebruik van Suwi door de gemeenten voor het vertrouwen in en de integriteit van elektronische (overheids)dienstverlening.

Bijlage A bevat de beschrijving van de uitgevoerde (test)werkzaamheden en onze oordelen <en aanbevelingen> ter verbetering van het gebruik van Suwi.

Bijlage B bevat de beschrijving van het object van onderzoek.

Verantwoordelijkheden van de <gemeente> / <(sub)serviceorganisatie>

Het bestuur van de <gemeente> / <(sub)serviceorganisatie> is verantwoordelijk voor het gebruik van Suwi, het onderkennen van beveiligingsrisico's met betrekking tot het gebruik van Suwi en het opzetten en implementeren van interne beheersingsmaatregelen om te voldoen aan de normen zoals opgenomen in de Verantwoordingsrichtlijn GeVS 2026.

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 de door ons af te geven oordelen over de opzet en implementatie van interne, en voor geselecteerde normen de werking van, beheersingsmaatregelen die verband houden met de normen in overeenstemming met de hiervoor vermelde criteria.

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

Ons onderzoek om te rapporteren over opzet, bestaan en, voor de van toepassing zijnde normen uit de Verantwoordingsrichtlijn GeVS 2026, de werking van interne beheersingsmaatregelen bestond onder andere uit:

- Het verkrijgen van inzicht in de relevante kenmerken van het gebruik van Suwi;
- Het vaststellen van de scope van het onderzoek, inclusief het vaststellen van de maatregelen die bij dienstverleners moeten worden onderzocht;
- Het houden van interviews met verantwoordelijke functionarissen, vooral gericht op het onderkennen van risico's en het onderzoek in hoeverre deze risico's worden afgedekt door maatregelen;
- Het evalueren van de opzet, het vaststellen van het bestaan en voor de van toepassing zijnde normen uit de Verantwoordingsrichtlijn GeVS 2026 de werking van de relevante maatregelen. Dit door middel van kennis nemen van documentatie, het kennis nemen van de resultaten van de uitgevoerde interne controles alsmede eigen waarnemingen;
- Het evalueren van de uitkomsten van onze werkzaamheden.

Plaats, rapportdatum
<EUTL Handtekening>
Auditor
<eventueel Auditorganisatie>

Bijlage A: Beschrijving van de testresultaten van de auditor

Nummer	Normen	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en eventuele aanbevelingen[30]
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.		**Opzet en bestaan** Voldoet / Voldoet niet **Werking** N.v.t.
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.		**Opzet en bestaan** Voldoet / Voldoet niet **Werking** N.v.t.
6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.		**Opzet en bestaan** Voldoet / Voldoet niet **Werking** N.v.t.
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.		**Opzet en bestaan** Voldoet / Voldoet niet / Voldoet in opzet **Werking**

[30] N.v.t. voor deze norm is toets op werking over controleperiode niet verplicht gesteld.

			Voldoet / Voldoet niet
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.		**Opzet en bestaan** Voldoet / Voldoet niet / Voldoet in opzet **Werking** Voldoet / Voldoet niet
9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.		**Opzet en bestaan** Voldoet / Voldoet niet / Voldoet in opzet **Werking** Voldoet / Voldoet niet
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.		**Opzet en bestaan** Voldoet / Voldoet niet / Voldoet in opzet **Werking** Voldoet / Voldoet niet
9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.		**Opzet en bestaan** Voldoet / Voldoet niet / Voldoet in opzet **Werking** Voldoet / Voldoet niet

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.		**Opzet en bestaan** Voldoet / Voldoet niet / Voldoet in opzet **Werking** Voldoet / Voldoet niet
10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.		**Opzet en bestaan** Voldoet / Voldoet niet **Werking** N.v.t.
12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.		**Opzet en bestaan** Voldoet / Voldoet niet **Werking** N.v.t.
12.1.2	Wijzigingsbeheer: Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging ehoren te worden beheerst. Alleen van toepassing bij het gebruik van Suwinet Inlezen of DKD Inlezen.		**Opzet en bestaan** Voldoet / Voldoet niet **Werking** N.v.t.
12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen: Bedrijfsvoering-, Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde		**Opzet en bestaan** Voldoet / Voldoet niet **Werking**

	toegang tot of veranderingen aan de productieomgeving te verlagen. Alleen van toepassing bij het gebruik van Suwinet Inlezen of DKD Inlezen		N.v.t.
12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.		**Opzet en bestaan** Voldoet / Voldoet niet / Voldoet in opzet **Werking** Voldoet / Voldoet niet
12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.		**Opzet en bestaan** Voldoet / Voldoet niet **Werking** N.v.t.
18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.		**Opzet en bestaan** Voldoet / Voldoet niet **Werking** N.v.t.

Bijlage B: Object van onderzoek

Het object van onderzoek zijn de beveiligingsmaatregelen van alle gegevensuitwisselingen via de GeVS conform de verantoordingsrichtlijn GeVS 2026 door <gemeente> / <(sub)serviceorganisatie>. Het object van onderzoek heeft betrekking op de Verantwoordingsrichtlijn GeVS 2026 die is gebaseerd op geselecteerde normen uit de Baseline Informatieveiligheid Overheid (BIO 1.04), meer in het bijzonder de in het kader van ENSIA geselecteerde normen.

Suwinet-gegevens worden ten behoeve van de dienstverlening door <gemeente> / <(sub)serviceorganisatie> 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> / <(sub)serviceorganisatie> 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 naar het al dan niet voldoen aan deze maatregelen is uitgevoerd door de IT-auditor van deze serviceorganisatie[s]. De normen die betrekking hebben op de taken die belegd zijn bij de serviceorganisatie(s) maken geen onderdeel uit van het onderzoek bij <gemeente> / <(sub)serviceorganisatie>, tenzij sprake is van een gedeelde norm.

Het onderzoek van het gebruik van Suwinet heeft plaatsgevonden op dat deel van het gebruik en het bijbehorende normenkader dat niet onder uitbesteding aan deze serviceorganisatie[s] valt. Het onderzoek van de overige normen wordt afgedekt door onderstaande assurance-rapportage[s] (AR) van de 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>[31]	[Niet van toepassing] [Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente][32]	 [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]
Adresonderzoek door Burgerzaken	[Niet van toepassing] [Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	 [Ja] [Nee] [Ja] [Nee]
Uitvoering Regeling opvang ontheemden Oekraïne (RooO)	[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 de paragraaf 'Onze oordelen' vermeld, voldoet <naam gemeente> aan alle interne beheersmaatregelen inzake Suwinet op 31 december 2026 in opzet en bestaan aan de geselecteerde normen en voor geselecteerde norman aan werking over de periode 1 januri – 31 december 2026.]

➢ Bij afwijkingen van de normen betreffende SUWI-taken de volgende tekst opnemen:
[Zoals in de praragraaf 'Onze oordelen' vermeld, voldoen met uitzondering van de volgende maatregelen de interne beheersmaatregelen voor de SUWI-taken van <naam gemeente> op 31 december 2026 in opzet en bestaan en voor geselecteerde norman aan werking over de periode 1 januri – 31 december 2026, aan de doelstellingen uit de verantwoordingsrichtlijn GeVS 2026:

[31] Naam RMC-gemeente invullen.

[32] Hier gemeenten vermelden waarvoor RMC-gemeente informatie verwerkt.

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 beheersmaatregelen 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]
[Binnen de gemeente] [Naam serviceorganisatie: naam serviceorganisatie] [Andere gemeente: naam andere gemeente]	Regeling opvang ontheemden Oekraïne	[Maatregel]	[Suwinet-Inkijk]

]

Bijlage 5.3 Assurance-rapport op niveau serviceorganisatie

Assurance-rapport over de serviceorganisatie van de onafhankelijke IT-auditor

Aan : directie/bestuur <naam serviceorganisatie>
Datum : Rapportdatum
Van : Auditor
Kenmerk

Onze oordelen

Wij hebben een onderzoek met redelijke mate van zekerheid uitgevoerd naar de beveiligings-maatregelen van alle gegevensuitwisselingen via de GeVS conform de verantwoordingsrichtlijn GeVS 2026 door <naam serviceorganisatie>.

Per norm hebben wij hieronder vermeld of wordt voldaan aan de norm. Om de leesbaarheid van dit rapport te vergroten zijn de oordelen in deze tabel weergegeven als 'voldoet' of 'voldoet niet'. Hierbij moet 'voldoet' ingeval het oordeel is beperkt tot opzet en bestaan worden geïnterpreteerd als 'Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven norm effectief zijn opgezet en geïmplementeerd op <oordeelsdatum>'. 'Voldoet niet' moet in geval het oordeel is beperkt tot opzet en bestaan worden geïnterpreteerd als 'Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven norm niet in alle materiële opzichten effectief zijn opgezet en/of geïmplementeerd op <oordeelsdatum>'.

De normen waarbij ook de effectieve werking wordt vastgesteld moet 'voldoet' worden geïnterpreteerd als 'Wij zijn van oordeel dat de getoetste interne beheersingsmaatregelen die verband houden met de op die regel aangegeven norm effectief werkten tijdens de controleperiode <van begindatum tot einddatum>'. 'Voldoet niet' moet vervolgens worden geïnterpreteerd als 'Wij zijn van oordeel dat de getoetste interne beheersingsmaatregelen die verband houden met de op die regel aangegeven norm niet in alle materiële opzichten effectief werkten tijdens de controleperiode <van begindatum tot einddatum>'.

De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel zijn de criteria die zijn beschreven in de sectie 'van toepassing zijnde criteria'.

Onze oordelen zijn gevormd op basis van de aangelegenheden die in dit assurance-rapport zijn uiteengezet.

Nummer	Normen	Oordeel opzet en bestaan	Oordeel werking[33]
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.	Voldoet / Voldoet niet	N.v.t.

[33] N.v.t. voor deze norm is een toets op werking over controleperiode niet verplicht gesteld.

Nummer	Normen	Oordeel opzet en bestaan	Oordeel werking33
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.	Voldoet / Voldoet niet	N.v.t.
6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Voldoet / Voldoet niet	N.v.t.
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.	Voldoet / Voldoet niet / Voldoet in opzet	Voldoet / Voldoet niet
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.	Voldoet / Voldoet niet / Voldoet in opzet	Voldoet / Voldoet niet
9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Voldoet / Voldoet niet / Voldoet in opzet	Voldoet / Voldoet niet
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.	Voldoet / Voldoet niet / Voldoet in opzet	Voldoet / Voldoet niet
9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	Voldoet / Voldoet niet / Voldoet in opzet	Voldoet / Voldoet niet
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.	Voldoet / Voldoet niet / Voldoet in opzet	Voldoet / Voldoet niet
10.1.1 (34)	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	Voldoet / Voldoet niet	N.v.t.
12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	Voldoet / Voldoet niet	N.v.t.

[34] N.v.t. bij opdrachtgevers die alleen Suwi-Inkijk gebruiken

Nummer	Normen	Oordeel opzet en bestaan	Oordeel werking33
12.1.2	Wijzigingsbeheer: Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.35	Voldoet / Voldoet niet	N.v.t.
12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen: Bedrijfsvoering-, Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.36	Voldoet / Voldoet niet	N.v.t.
12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Voldoet / Voldoet niet / Voldoet in opzet	Voldoet / Voldoet niet
12.4.2 (37)	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Voldoet / Voldoet niet	N.v.t.
18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Voldoet / Voldoet niet	N.v.t.

De basis voor onze oordelen

Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht, de NOREA Richtlijn 3000D 'Assurance-opdrachten door IT-auditors '(Directe-opdrachten)'en de nadere regels zoals opgenomen in de Handreiking Suwinet (in kader ENSIA voor IT-auditors (RE's) 2026 versie 1.0 van NOREA. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Verantwoordelijkheden van de IT-auditor'.

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

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor onze oordelen <behalve die normen waarvoor wij geen oordeel konden geven>.

Van toepassing zijnde criteria

Voor deze opdracht hanteren wij de Verantwoordingsrichtlijn GeVS (Gemeenschappelijke elektronische Voorziening Suwi) 2026 die door het Ministerie van Sociale Zaken en Werkgelegenheid (SZW) is vastgesteld. Meer in het bijzonder gaat het daarbij om het in de bijlage 1 van in de Verantwoordingsrichtlijn GeVS 2026 opgenomen normenkader.

De criteria waarvan gebruik wordt gemaakt bij het uitvoeren van de assurance-opdracht houden in dat:

[35] Alleen mogelijk van toepassing bij het gebruik van Suwinet Inlezen of DKD Inlezen.

[36] Alleen mogelijk van toepassing bij het gebruik van Suwinet Inlezen of DKD Inlezen

[37] N.v.t. bij opdrachtgevers die alleen Suwi-Inkijk gebruiken

- De risico's die het voldoen aan de normen in gevaar brengen en daarmee de betrouwbaarheid van het gebruik van Suwi aantasten, werden onderkend;
- De onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het voldoen aan de normen niet zouden verhinderen;
- De interne beheersingsmaatregelen die verband houden met de normen op afdoende wijze zijn opgezet en daadwerkelijk zijn geïmplementeerd;
- De interne beheersingsmaatregelen die verband houden met een selectie van specifieke normen gedurende de controleperiode effectief hebben gewerkt.

Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek

Object van onderzoek

Het object van onderzoek waren de beveiligingsmaatregelen van alle gegevensuitwisselingen via de GeVS conform de Verantwoordingsrichtlijn GeVS 2026 die door de gebruikersorganisaties zijn uitbesteed tijdens de controleperiode <van begindatum tot einddatum aan <naam serviceorganisatie>.

→ Instructie voor de auditor alleen die rijen laten staan die van toepassing zijn

In onderstaande tabel zijn de Suwi voorzieningen vermeld die in scope zijn van ons onderzoek:

	Inkijk	Inlezen	Uitbestede taken
Participatiewet inclusief IOAW en IOAZ	√	√	Uitvoering P-wet inclusief Wet Inkomensvoorziening voor oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW) en Wet Inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)
BBZ-regeling	√		Uitvoering Bijstand voor Zelfstandigen
Bijzondere bijstand	√		Uitvoering bijzondere bijstand
Sociale recherche	√		Uitvoering sociale recherche
Adresonderzoek Burgerzaken	√		Uitvoering Adresonderzoek in verband met het bijhouden van de BRP (niet Suwi taak)
Regeling opvang ontheemden Oekraïne (RooO)	√		Uitvoering RooO (niet Suwi taak)
Schuldhulpverlening	√	√	Uitvoering Wet gemeentelijke schuldhulpverlening (Suwi taak)

→

Instructie voor de auditor alleen vermelden indien van toepassing

Aanvullende assurance waarop wordt 'gesteund' is ontleend aan: [type rapport, rapportdatum, kenmerk, auditorganisatie, eventueel naam IT auditor, onderzoeksperiode + eventuele bridgelettetter(s) zodat de periodes aansluiten, van <dienstverlener>].

In Bijlage B geven wij u een meer gedetailleerde beschrijving van het object van onderzoek.

Zelfstandig gebruik Suwi-voorzieningen door de gebruikersorganisaties

Indien de gebruikersorganisatie naast de uitbestede Suwi-taken ook zelfstandig gebruik maakt van Suwinet gegevens, zijn zij zelf verantwoordelijk voor het opzetten en implementeren van interne beheersingsmaatregelen ter waarborging van de vertrouwelijkheid van de Suwinet-gegevens.

Het eventuele zelfstandig gebruik van Suwinet gegevens door de gebruikersorganisaties is niet in deze assurance-rapportage betrokken en dient door de IT-auditor(s) van de gebruikersorganisatie te worden onderzocht.

Beoogde gebruikers en doel

Ons assurance-rapport inclusief bijlagen is uitsluitend bestemd voor de volgende gebruikersorganisaties:

Gebruikersorganisaties

Desgewenst heeft de gebruikersorganisatie onze toestemming om dit assurance-rapport te verstrekken aan het Ministerie van Sociale Zaken en Werkgelegenheid en het Bureau Keteninformatiesering Werk en Inkomen om toezicht te kunnen houden op het gebruik van Suwi door de gemeenten voor het vertrouwen in en de integriteit van elektronische (overheids)dienstverlening.

Bijlage A bevat de beschrijving van de uitgevoerde (test)werkzaamheden en onze oordelen en aanbevelingen ter verbetering van het gebruik van Suwi[38].

Bijlage B bevat de beschrijving van het object van onderzoek[39].

Bijlage C bevat de gedetailleerde informatie over de naleving van de BIO-maatregelen[40]

Verantwoordelijkheden van <naam serviceorganisatie>

Het bestuur van <naam serviceorganisatie> is verantwoordelijk voor het gebruik van Suwi, het onderkennen van beveiligingsrisico's met betrekking tot het gebruik van Suwi en het opzetten en implementeren van interne beheersingsmaatregelen om te voldoen aan de normen zoals opgenomen in de Verantwoordingsrichtlijn GeVS 2026.

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 de door ons af te geven oordelen over de opzet en implementatie van interne, en voor geselecteerde normen de werking van, beheersingsmaatregelen die verband houden met de normen in overeenstemming met de hiervoor vermelde criteria.

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 fouten en fraude ontdekken.
Wij passen het 'Reglement Kwaliteitsbeheersing NOREA (RKBN)' toe. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en

[38] Zie ook voorbeeld bijlage 5.2
[39] Zie ook voorbeeld bijlage 5.2
[40] Zie ook voorbeeld bijlage 5.2

procedures inzake de naleving van ethische voorschriften, professionele standaarden en andere relevante wet- en regelgeving.

Ons onderzoek om te rapporteren over opzet, bestaan en, voor de van toepassing zijnde normen uit de Verantwoordingsrichtlijn GeVS 2026, de werking van interne beheersingsmaatregelen bestond onder andere uit:

- Het verkrijgen van inzicht in de relevante kenmerken van het gebruik van Suwi;
- Het vaststellen van de scope van het onderzoek, inclusief het vaststellen van de maatregelen die bij dienstverleners moeten worden onderzocht;
- Het houden van interviews met verantwoordelijke functionarissen, vooral gericht op het onderkennen van risico's en het onderzoek in hoeverre deze risico's worden afgedekt door maatregelen;
- Het evalueren van de opzet, het vaststellen van het bestaan en voor de van toepassing zijnde normen uit de Verantwoordingsrichtlijn GeVS 2026 de werking van de relevante maatregelen. Dit door middel van kennis nemen van documentatie, het kennis nemen van de resultaten van de uitgevoerde interne controles alsmede eigen waarnemingen;
- Het evalueren van de uitkomsten van onze werkzaamheden.

Plaats, rapportdatum
<EUTL Handtekening>
Auditor
<eventueel Auditorganisatie>

Verantwoordelijkheden gebruikersorganisatie

De opzet en implementatie van interne beheersingsmaatregelen bij <naam serviceorganisatie> zijn uitsluitend gericht op de Suwi-taken die <naam serviceorganisatie> voor de gebruikersorganisaties uitvoert.

Indien de gebruikersorganisatie daarnaast zelfstandig Suwi-taken uitvoert dan wel door andere serviceorganisaties laat uitvoeren (hierbij kan gedacht worden aan taken in het kader van bijzondere bijstand en/of de uitvoering van de BBZ-regeling), dan wel Suwinet-gegevens voor andere doeleinden gebruikt (zoals het gebruik ten behoeve van adresonderzoek Burgerzaken) en daarvoor Suwinet-inkijk en/of Suwinet voorzieningen gebruikt, dient men op basis van zelfstandig uit te (laten) voeren onderzoek vast te stellen of de noodzakelijk geachte interne beheersingsmaatregelen door de gebruikersorganisatie of de andere serviceorganisaties zijn geïmplementeerd.

Dit rapport geeft inzicht in het interne controlesysteem dat ten grondslag ligt aan de dienstverlening van <naam serviceorganisatie>.
<Naam serviceorganisatie> merkt op dat onderstaande verantwoordelijkheden ook indien alle Suwi taken zijn uitbesteed, zijn belegd bij de gebruikersorganisatie. Derhalve dienen minimaal deze maatregelen door de auditor van de gemeente te worden getoetst en worden meegenomen in de algehele oordeelsvorming.

Nr	Normen	Gewenste interne beheersingmaatregelen van de gebruikersorganisatie
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.	De gebruikersorganisatie dient een informatiebeleid te hebben geformaliseerd, gepubliceerd en gecommuniceerd aan de medewerkers.
6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	De gebruikersorganisatie dient de verantwoordelijkheden inzake de uitbestede Suwi taken hetzij naar publiek recht hetzij naar privaatrecht contractueel te hebben overgedragen aan <naam serviceorganisatie>.
		Op basis van professional judgement aanvullen met overige beheersingsmaatregelen die door de gebruikersorganisatie moeten worden genomen

Bijlage 6: Waarmerken stukken en digitaal ondertekenen

Het assurance-rapport moet een kenmerk (nummer) hebben van de auditorganisatie (een nieuwe versie van het assurance-rapport vereist een nieuw kenmerk). Een assurance-rapport wordt uitgebracht op briefpapier van de auditorganisatie.

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

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

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

DigiD

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

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

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

Let op: 'Assurance rapporten die worden uitgegeven na 2023 moeten zijn voorzien van een elektronische handtekening met een EUTL-certificaat.

SUWI

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

Aandachtspunt voor aansluithouders en IT-auditors

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

Bijlage 7: 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 dienstverlener.
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 8: 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