NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

HANDREIKING ENSIA voor IT-auditors (RE's)

Eénduidige Normatiek Single Information Audit voor gemeenten

Versie 4.0 – Update Verantwoordingsjaar 2021
15 oktober 2021

1 Over deze handreiking ENSIA

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

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

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

Voor vragen en opmerkingen kunt u zich wenden tot:

NOREA
Postbus 7984,
1008 AD Amsterdam
telefoon: 020-3010380
e-mail: norea@norea.nl

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

Deze ENSIA handreiking zal op basis van het ENSIA-proces 2021 (zelfevaluatie en verantwoording door gemeenten en uitgevoerde audit(s)) door de ENSIA-Werkgroep van NOREA worden geëvalueerd en zo nodig verbeterd. Het is de bedoeling om de handreiking op basis van ervaring en evaluatie jaarlijks als NOREA-handreiking (conform artikel 15 Reglement Beroepsbeoefening) vast te stellen.

Deze versie vervangt de voorgaande versie(s) en is in zijn geheel van toepassing op de uitvoering van de werkzaamheden over het verslagjaar 2021.

Versiebeheer

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

Versie 3.1	28 september 2021	Ter beoordeling Werkgroep ENSIA en VC
Versie 4.0	15 oktober 2021	Definitief: Update t.b.v. audit 2021

1.1 Aanleiding

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

1.2 Achtergrond

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

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

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

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

Voor alle verantwoordingen geldt dat waar mogelijk is, wordt aangesloten op de BIO. Daarnaast blijft de noodzaak om domein specifieke toezichtinformatie te blijven leveren. De verantwoording in ENSIA betreft in 2021:

- Basisregistratie Personen (BRP)
- Wet- en regelgeving Reisdocumenten (PUN en PNIK)
- Digitale persoonsidentificatie (DigiD)
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Ondergrond (BRO)
- de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)
- Informatiebeveiliging, systeembeheer en architectuur van de WOZ

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

De reikwijdte van de Collegeverklaring over 2021 en daarmee de assurance-opdracht van de IT-auditor is ten opzichte van 2020 niet gewijzigd.

1.3 Toepassingsgebied ENSIA

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

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

website van Logius: https://logius.nl/diensten/digid/ict-beveiligingsassessments-digid/hoe-werkt-het .

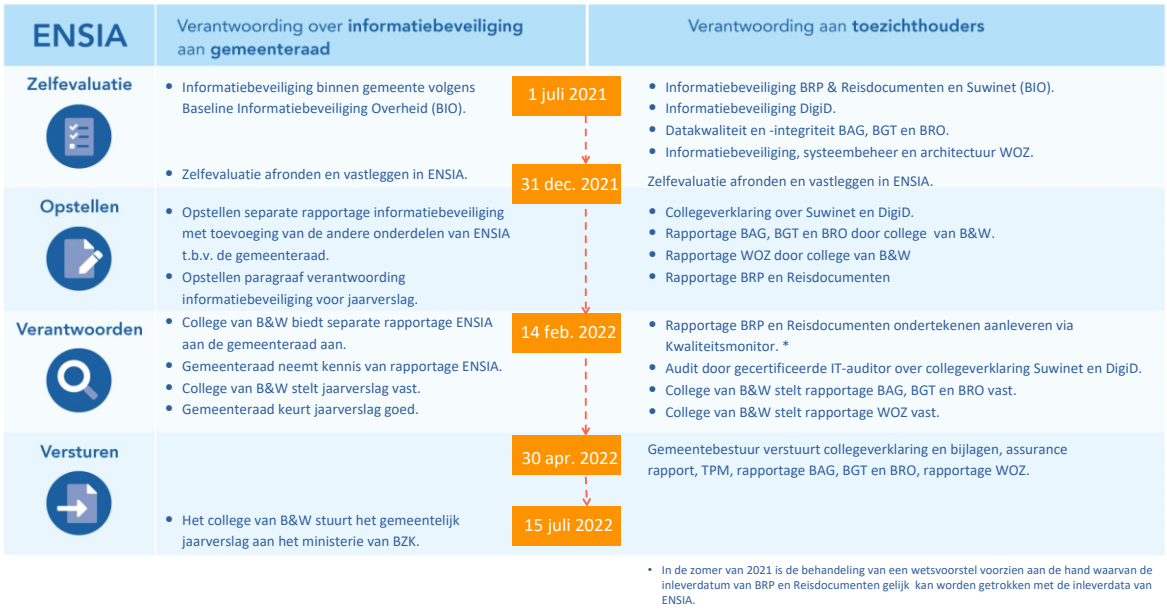
Met Suwinet wordt alleen gerefereerd aan de gemeente als afnemer. Als afnemer kent Suwinet 'Suwi inkijk', 'Suwi inlezen' en 'Digitaal Klantdossier (DKD) inlezen'. In verband met de overgang van BIG naar BIO heeft het Ketenoverleg de *Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2020 versie 1.0* uitgebracht. Hierin is het vereiste, adequate niveau van informatiebeveiliging gebaseerd op het BIO normenkader zodat verantwoording op basis daarvan moet plaatsvinden. Voor het verantwoordingjaar 2021 zijn hierin geen wijzigingen doorgevoerd.

1.4 Werkwijze ENSIA

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

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

Hierbij doorloopt de gemeenten voor 2021 in hoofdlijnen het weergegeven proces:



1.5 Toelichting zelfevaluatie en tool gemeenten

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

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

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

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

Bij de beoordeling van deze zelfevaluaties wordt gebruik gemaakt van de door de gemeente uitgevoerde en gedocumenteerde werkzaamheden over de opzet en het bestaan van de beheersmaatregelen.

2 Handreiking

Doel van deze handreiking is de IT-auditor een uniform toetsingskader te bieden voor het uitvoeren van een ENSIA-audit op basis van de beschikbare normen. Dit kader geldt voor controlejaar 2021. 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 NCSC-richtlijnen af te leiden.

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

2.1 Verantwoordingsproces

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

- De gemeente is verantwoordelijk voor het uitvoeren van de zelfevaluatie per assessmentplichtige DigiD-aansluiting waarvan de gemeente de houder is. Voor DigiD-aansluitingen die op naam staan van samenwerkingsverbanden waaraan de gemeente deelneemt, dienen de samenwerkingsverbanden zelfstandig de voorgeschreven DigiD-assessments per aansluiting te laten uitvoeren.
- Praktijk is dat de werkzaamheden in het domein werk en inkomen belegd kunnen zijn bij diverse samenwerkingsverbanden. Ongeacht de organisatie van de samenwerkingsverbanden blijft het gemeentebestuur verantwoordelijk voor het gebruik van Suwinet. De gemeente dient e.e.a. te betrekken in de zelfevaluatie. Zie bijlage 7 voor een nadere toelichting.
- Bij eventuele bevindingen in het kader van de zelfevaluatie dient de gemeente een verbeterplan op te stellen. Dit verbeterplan dient concrete verbetermaatregelen te omvatten voor alle hiervoor bedoelde bevindingen.

Verantwoordingsproces in detail
Het verantwoordingsproces begint met het invullen van de zelfevaluatie vragenlijst informatiebeveiliging 2021. De vragenlijst informatiebeveiliging is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO) aangevuld met domeinspecifieke aspecten.

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

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

De gemeente heeft tot en met **31 december 2021** de tijd om de vragenlijsten van de zelfevaluatie in te vullen en in te leveren. Inleveren kan pas als alle vragen beantwoord zijn.

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

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

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

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

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

De gemeente levert vóór 1 mei 2022[1] het assurance-rapport, de gewaarmerkte Collegeverklaring ENSIA met bijbehorende bijlagen bij de Collegeverklaring ENSIA en de ontvangen assurance-rapporten (TPM's) op aan de toezichthouder. Deze documenten kunnen tot deze datum met behulp van het ENSIA-tool ter beschikking gesteld worden.

Verantwoordelijkheden IT-auditor
De IT-auditor dient er voor te zorgen dat de betreffende documenten door hem gewaarmerkt zijn, zoals aangegeven in de formats voor collegeverklaring en assurance-rapport (zie ook bijlage 8 over het waarmerken van stukken).

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

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

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

2.2 Wat verandert er voor de IT-auditor

Voor de IT-auditor verandert ten aanzien van zijn verantwoordelijkheid voor het goed voorbereiden en inrichten van zijn controle in principe niets. Met dien verstande dat elk audit project om een specifieke

[1] Voor het verantwoordingsjaar 2021 wordt vooralsnog uitgegaan van het gebruikelijke verantwoordingstraject. Indien naar aanleiding van maatregelen ter bestrijding van Covid-19 (of andere grootschalige gebeurtenissen) hiervoor andere afspraken gemaakt worden dan zal dit evenals de afgelopen jaren tijdig door de betrokken partijen (toezichthouders, VNG-realisatie en NOREA) kenbaar gemaakt worden.

voorbereiding vraagt waarbij rekening wordt gehouden met het onderscheid tussen 'direct reporting opdrachten' en 'attest-opdrachten'.
Bij de methode van 'direct reporting' (zoals bij de DigiD assessments gebruikelijk) is de IT-auditor zelf in 'the lead' en is voorbereiding in de vorm van het zelfstandig opvragen van stukken belangrijk.

Bij ENSIA is de oplevering thans in de vorm van een attest-opdracht op basis van de collegeverklaring en bijlagen ('attestation based audit'/ 'assertion based audit').

Hoewel de Collegeverklaring ENSIA het object van controle vormt, zijn de ingevulde vragenlijsten (de zelfevaluaties) in de ENSIA-tool en de door de gemeente gedocumenteerde ondersteunende assurance-informatie voor de IT-auditor het basismateriaal waar elke IT auditor vanuit kan gaan en evidence vormt tijdens het veldwerk. Op basis van de eigen risicoanalyse, zoals die voor elke audit project wordt uitgevoerd, stelt de IT auditor zelfstandig o.b.v. risicoanalyse vast wat de diepgang van zijn werkzaamheden zullen zijn gegeven de veronderstelde kwaliteit van oplevering van de gegevensverzameling. Hierbij dient hij ook kennis te nemen van de andere onderdelen van het ENSIA-proces en de eventueel in samenhang daarmee uitgebrachte rapportages om eventuele aanvullende aandachtspunten voor zijn werkzaamheden te kunnen vaststellen. Hij zal nog eigen waarnemingen moeten uitvoeren om het aangeleverde materiaal te valideren

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

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

2.3 Formele aspecten van de assurance-opdracht

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

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

De criteria voor een ENSIA IT-audit betreffen de normen inzake DigiD (Norm ICT-beveiligings-assessments DigiD versie 2.0[1] en Suwinet (Verantwoordingsrichtlijn GeVS 2020). De criteria worden ook in de collegeverklaring kenbaar gemaakt en zijn daarmee toegankelijk voor de gebruikers.

Het gaat om opzet en bestaan (*) van de maatregelen per 31 december 2021. Eventuele veranderingen/ verbetermaatregelen in de periode tussen 31 december 2021 en de datum van

[1] Update van de testaanpak DigiD-assessment 2.0 d.d. 26 mei 2020 inclusief de DigiD FAQ zoals gepubliceerd op de NOREA site.

afgeven van het assurance-rapport dient het College in principe in de collegeverklaring toe te lichten[1]. De verbetermaatregelen / het verbeterplan betrekt de auditor in zijn onderzoek.

(*) De IT-auditor geeft geen oordeel over de werking van de maatregelen gedurende een periode.

De NOREA beroepsorganisatie hanteert overigens het standpunt dat uitsluitend een herhaalde beoordeling van opzet en bestaan op den duur een schijnzekerheid impliceert als niet ook de werking in de beoordeling wordt betrokken. Het invoeringstraject daarvan vraagt echter de nodige voorbereidingstijd. Vooralsnog blijft de ENSIA-audit over 2021 beperkt tot op opzet en bestaan van de beheersmaatregelen.

2.4 Ethische voorschriften en beroepsregels

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

2.5 Pre-audit ENSIA

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

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

2.6 Opdrachtaanvaarding en continuering

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

2.7 Kwaliteitsbeheersing

Het Reglement Kwaliteitsbeheersing NOREA (RKBN) is van toepassing, dit komt ook tot uitdrukking in het assurance-rapport. Gegeven de aard van de opdracht, het maatschappelijke belang en mogelijk brede verspreidingskring van de collegeverklaring en het assurance-rapport (o.a. als gevolg van de Wet openbaarheid van bestuur) is voor ENSIA-audits een opdrachtgerichte kwaliteitsbeoordeling (OKB) van toepassing. Hiervan kan in uitzonderingsgevallen worden afgeweken, afhankelijk van de risico-inschatting van de audit-organisatie. De auditor dient de overwegingen ter zake in het dossier vast te leggen.

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

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 ENSIA-opdracht is gezien het feit dat het de decentrale overheid betreft en het feit dat de opdracht als complex wordt aangemerkt, te bestempelen als een opdracht met een gemiddeld tot hoog risico op afwijkingen van materieel belang.

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

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

Ten behoeve van het afgeven van het assurance-rapport dient het ACR laag te zijn. Omdat zowel ICR en IHR in de beginperiode op Midden tot Hoog worden ingeschat zal het DR Midden tot Laag moeten zijn. Dit betekent voor 2021 relatief nog veel uit te voeren controlewerkzaamheden in de vorm van gegevensgerichte maatregelen. Naar verwachting zal dit de komende jaren minder worden.

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

2.9 Het verkrijgen van assurance-informatie

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

Een professioneel kritische houding wordt van de IT-auditor verwacht bij het gebruik van deze informatie. Om zelfstandig tot een oordeel te komen zal de IT-auditor niet alleen de 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. De regels uit de Richtlijn Documentatie (NOREA 230) zijn hier onverkort van toepassing.

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

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

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

2.10 Uitbesteding door gemeenten

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

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

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

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

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

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

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

Zie voor een nadere toelichting bijlage 8 "Overwegingen Audit in samenwerkingsverbanden Suwinet". Het gaat hierbij om overwegingen die betrokken kunnen worden bij het uitvoeren van de werkzaamheden in de samenwerkingsverbanden. Deze mogen echter geen afbreuk doen aan de fundamentele eisen die aan het uitvoeren van de werkzaamheden door de IT-auditor zijn gesteld.

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

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

De (ENSIA-) auditor van de gemeente dient hiervoor de vaktechnische verantwoordelijkheid te kunnen nemen. Hij dient dit – waar mogelijk in overleg met de auditor van de externe partij – te betrekken in de risicoanalyse, uitwerking van de controle-aanpak, bespreking van bevindingen, etc. en uitvoering van een dossierreview. De inspanning zal beperkter kunnen zijn indien de auditor van de externe partij werkzaamheden conform de ENSIA-normering en deze handreiking uitvoert en in de rapportage een bijlage opneemt van de uitgevoerde werkzaamheden naar analogie van wat bij een

3402-rapportage type 2 / rapportage conform SOC 2 (beide gericht op opzet bestaan en werking) vereist is[1].

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

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

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

2.11 Schriftelijke bevestiging (letter of representation)

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

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

2.12 Het vormen van het oordeel

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

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

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

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

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

2.13 Het opstellen van het assurance-rapport

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

Voor de goede orde zij vermeld dat voor het jaar 2021 geen aanpassingen zijn doorgevoerd in de gekozen bewoordingen. In bijlage 8 zijn de formats assurance-rapporten opgenomen. Hieraan zijn, in verlengde van het Addendum II ten behoeve van de werkzaamheden over 2019, ook voorbeeldteksten toegevoegd voor een oordeel met beperking/ oordeelonthouding. Daarnaast is in de formats assurance-rapporten meer expliciet opgenomen op welk gebruik van Suwinet gegevens en welke DigiD aansluitingen het oordeel betrekking heeft.

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

Nadere toelichting:
Bij assurance-rapporten bij serviceorganisaties is het vereist dat bij het toetsen van de werking ook een bijlage wordt toegevoegd met een beschrijving van de uitgevoerde toetsingen van de interne beheersmaatregelen en de resultaten daarvan. De ENSIA-audit betreft een type 1 audit (opzet en bestaan). Daarnaast is het doel en de doelgroep anders dan bij een ISAE3402-rapport.

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

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

2.14 Overige rapportages

Het is wenselijk dat de IT-auditor (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 gemeente.

2.15 Documentatie

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

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

3 Tot slot

De ENSIA-audit maakt onderdeel uit van een breder overheidsinitiatief om de veiligheid van digitale dienstverlening te vergroten, maar is zeker niet het enige middel. Blijvende managementaandacht voor de risico's van digitale dienstverlening en het treffen van de juiste 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 ENSIA-audit geen specifiek onderzoek op uit.

4 Bijlagen

Bijlage 1 Overzicht van de verschillen tussen de te onderzoeken normen DigiD 2019 / 2020 – ontwikkelingen 2021

Noot voor de auditor
De auditor dient zich ervan te vergewissen dat hij voorafgaande aan de uitvoering van het DigiD deel van de ENSIA audit, de laatste versie van de DigiD FAQ heeft geraadpleegd. Zie hiervoor de publicaties van de NOREA werkgroep DigiD assessments op https://www.norea.nl/werkgroep-digid-assessments
Let op! Daarnaast is het in uitzonderingssituaties vanaf het verantwoordingsjaar 2021 mogelijk dat DigiD aansluitingen richting Logius kunnen worden verantwoord via de constructie van de Leverancier Meervoudige Aansluitingen (= LMA). Hiervoor is een zwaardere en uitgebreidere speciale testaanpak ontwikkeld, welke eveneens is gepubliceerd op de eerder vermelde webpagina's van de NOREA site. Deze testaanpak geldt voor de LMA zelf en vervangt de in bijlage 2 van deze Handreiking vermelde testaanpak. De individuele DigiD aansluithouder die via een goedgekeurde LMA is aangesloten op het DigiD netwerk, hoeft zich NIET langer zelfstandig richting Logius te verantwoorden.

Context en toelichting

In 2019 heeft NOREA een aanvullende handreiking voor non-occurrence en aanbevelingen voor technische maatregelen gepubliceerd met betrekking tot de uitvoering van het ICT-beveiligingsassessment DigiD. Deze zijn onverkort van toepassing voor het verantwoordingsjaar 2021.Gelet op de uitkomsten van de DigiD-assessments over het verantwoordingsjaar 2020 vergt het navolgende punt aandacht van de betrokken IT-auditors.

- **U/PW.03:** de minimale configuratie en het gebruik van HSTS, X-Content-Type-Options, Content-Security-Policy (aangescherpt), en Referrer-Policy is verplicht.

Zie hiervoor ook de FAQ DigiD van NOREA.

Bijlage 2 Testaanpak bij de te onderzoeken normen ICT-beveiligingsassessment DigiD

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld. Doelstelling: Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.	Governance	Betrokken rol(len): • Applicatie-, hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting. Scope: • De contracten en/of Service Level Agreements voor de levering hosting-, applicatie- of SAAS diensten. Nadere toelichting: De organisatie dient een, door beide partijen ondertekend, contract te hebben waarin tenminste de volgende zaken zijn opgenomen: • een beschrijving van de te leveren diensten die onder het contract vallen; • de van toepassing zijnde leveringsvoorwaarden; • informatiebeveiligingseisen met de relevante eisen vanuit het beveiligingsbeleid; • het melden van beveiligingsincidenten; • de behandeling van gevoelige gegevens; • wanneer en hoe de leverancier toegang tot de systemen / data van de gebruikersorganisatie mag hebben; • Service Level Reporting; • het jaarlijks uitvoeren van audits bij de leverancier(s); • beding dat deze voorwaarden back-to-back worden doorgegeven aan mogelijke subleveranciers. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspectie van het beveiligingsbeleid. • Inspectie van contracten met leveranciers, SLA's en andere gerelateerde documenten.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			Non-occurrence (voor het onderdeel Service Level Reporting): • T.a.v. Service Level Reporting, kan de situatie zich voordoen dat er nog geen rapportering heeft plaatsgevonden, terwijl dit contractueel wel is overeengekomen. In dit geval dient op basis van (deel)waarnemingen binnen een proces dat onderworpen is aan dezelfde control te worden vastgesteld dat Service Level Reporting plaatsvindt.
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken. Doelstelling: Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit.	Applicatie Infrastructuur Proces	Betrokken rol(len): • Applicatie-, hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting. Scope: • De DigiD webapplicatie, DigiD webservers en de firewalls, IDS/IPS, etc. Nadere toelichting: De focus ligt op de beheerprocessen. Dit betreft enerzijds toegang tot de DigiD-applicatie en anderzijds toegang tot de DigiD webservers en de firewalls, IDS/IPS, etc. die een koppeling hebben met de DigiD omgeving. Aandachtspunten hierbij zijn: • Toekennen, controleren en intrekken van autorisaties. • Eisen aan wachtwoordinstellingen. • Aantoonbare controle op joiners/movers/leavers. • Wijzigen van de standaard wachtwoorden van administrator accounts. • Beperken eventuele shared accounts. • Uitvoeren periodieke reviews. Specifieke aandacht gaat uit naar wachtwoorden die leveranciers hebben om toegang tot de systemen of data van de houder van de DigiD aansluiting te krijgen (wie hebben die wachtwoorden, hoe worden die opgeslagen en wie hebben toegang. Hoe vaak worden ze gewijzigd, et cetera). Test aanpak:

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor

			• Interview de verantwoordelijke functionarissen.
			• Inspecteer het beveiligingsbeleid, joiners/movers/leavers procedure, de autorisatieprocedure, afspraken met leveranciers met betrekking tot toegang tot systemen en data en andere gerelateerde documenten.
			• Stel voor elk van deze processen en systemen, het bestaan vast met een deelwaarneming van tenminste één.
			• de toegekende autorisaties en de resultaten en opvolging van de periodieke review.
			
			<u>Non-occurrence (deels):</u>
			• Alleen voor de processen 'Toekennen, controleren en intrekken van autorisaties' en 'Uitvoeren periodieke reviews' waarbij geldt dat:
			  ○ Controle op joiners / movers / leavers wel aantoonbaar dient te hebben plaatsgevonden.
			  ○ De periodieke review dient te zijn opgenomen in een planning.

U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. <u>Doelstelling:</u> Effectief en veilig realiseren van de dienstverlening.	Applicatie Proces	<u>Betrokken rol(len):</u> • Applicatie of SAAS leverancier. • Houder van de DigiD-aansluiting. <u>Scope</u>: • De DigiD webapplicatie. <u>Nadere toelichting</u>: Deze norm richt zich meer op de procesmatige aspecten van het functioneel en het applicatiebeheer. Aandachtspunten hierbij zijn: • Beschrijving van taken, verantwoordelijkheden en bevoegdheden van de verschillende beheerrollen. • Een incidentenprocedure is opgesteld. • Meldingen van het NCSC of IBD of Z-CERT of andere CERTS worden geanalyseerd en zo nodig opgevolgd. • Incidenten worden geregistreerd, geanalyseerd, opgevolgd en afgehandeld. • Er is een periodieke rapportage aan het management inzake beveiligingsincidenten.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer de functie/taakbeschrijvingen van beheerders. • Inspecteer het incidentproces, de uitgevoerde analyse, de managementrapportage en opvolging van beveiligingsincidenten. Non-occurrence (voor het onderdeel opvolging van beveiligingsincidenten): • Voor het proces 'incidentmanagement', waarbij geldt dat op basis van (deel)waarnemingen binnen een proces dat onderworpen is aan dezelfde control , vastgesteld moet worden dat een incidentenprocedure effectief is geïmplementeerd. • Voor het proces 'periodieke rapportage aan het management', waarbij geldt dat op basis van (deel)waarnemingen t.a.v. een plaatsgevonden incident binnen een proces dat onderworpen is aan dezelfde control, vastgesteld moet worden dat rapportages aan het management inzake beveiligingsincidenten structureel plaatsvinden.
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt. Doelstelling: Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.	Applicatie	Betrokken rol(len): • Applicatie- of SAAS leverancier. Scope: • De DigiD webapplicatie en webserver. Nadere toelichting: Ongecontroleerde (ongevalideerde) invoer van gebruikers is een belangrijke bedreiging voor een webapplicatie. Als invoer van gebruikers rechtstreeks wordt gebruikt in HTML-uitvoer, cookiewaarden, SQL-queries, etc., bestaat er een (grote) kans dat een kwaadwillende de webapplicatie compromitteert. Een gebrek aan invoervalidatie kan tot kwetsbaarheden zoals XSS, commando- en SQL-injectie leiden. • HTTP request voor alle invoermethodes zoals gespecificeerd in de ICT-

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			Beveiligingsrichtlijnen van NCSC moeten worden gevalideerd (testen op type, lengte, formaat en karakters van invoer en speciale tekens (bv. <, >, ', ", & , /, --, etc.). Test aanpak: Om deze beveiligingsrichtlijn volledig te testen is een source code review nodig. Er is echter niet gekozen voor een verplichte code review als onderdeel van de DigiD assessment. Indien uit de test grote tekortkomingen naar voren komen wordt deze wel aanbevolen. • Observeer het gedrag van de HTTP headers en responses. Voer hierbij een representatieve deelwaarneming uit op de invoer- en uitvoermogelijkheden die de applicatie biedt.
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren. Doelstelling: Voorkom manipulatie van het systeem van andere gebruikers	Applicatie	Betrokken rol(len): • Applicatie- of SAAS leverancier. Scope: • De DigiD webapplicatie. Nadere toelichting: Als een webapplicatie onvoldoende controles uitvoert op de uitvoer die het terugstuurt naar de gebruiker, kan het gebeuren dat er zich onbedoelde of ongewenste inhoud in de uitvoer bevindt. Uitvoervalidatie voorkomt dat de webapplicatie ongewenste opdrachten geeft aan de client, bijvoorbeeld in het geval van XSS. • De webapplicatie codeert dynamische onderdelen in de uitvoer waarbij mogelijke gevaarlijke tekens (bv. <, >, ', ", & , /, --, etc.) worden genormaliseerd. Test aanpak: Om deze beveiligingsrichtlijn volledig te testen is een source code review nodig. Er is echter niet gekozen voor een verplichte code review als onderdeel van de DigiD assessment. Deze wordt wel aanbevolen.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			• Observeer het gedrag van de webapplicatie op voor wat betreft onveilige uitvoer. Voer hierbij een representatieve deelwaarneming uit op de uitvoervelden van de applicatie.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken. <u>Doelstelling:</u> Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie	Applicatie Infrastructuur Proces	<u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting. <u>Scope:</u> • De DigiD webapplicatie en webserver en bijbehorende infrastructuur. <u>Nadere toelichting</u> Deze norm raakt diverse aspecten van privacy bevorderende en cryptografische technieken. Dit betreft de classificatie van gegevens, de encryptie van gevoelige gegevens tijdens de opslag en de encryptie van gegevens tijdens transport. Aandachtspunten hierbij zijn: • De classificatie van gegevens door de houder van de DigiD aansluiting op basis van een risico analyse. • Mogelijke versleuteling of hashing van gevoelige gegevens. Het gaat hier in ieder geval om het BSN als bijzonder persoonsgegeven. Overigens geldt dit alleen voor gegevens die in dezelfde DMZ worden opgeslagen als waar de webapplicatie draait. Gegevens in de backoffice vallen buiten de scope van dit onderzoek. • De HTTPS configuratie en de TLS configuratie. De publicatie in 2019 door het NCSC van de vernieuwde ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)v2 is aanleiding om de richtlijnen voor TLS aan te scherpen. Concreet dienen minimaal de TLS instellingen die het NCSC als 'Goed' of 'Voldoende' heeft aangemerkt te worden gebruikt. • <u>Test aanpak</u>: • Interview de verantwoordelijke functionarissen. • Inspecteer de classificatie van gegevens en daaraan gerelateerde risico analyse, de netwerkarchitectuur en het inrichtingsdocument waar de encryptie van gegevens in staat beschreven. • Observeer de encryptie van gegevens. Inspecteer de HTTPS en TLS configuraties.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Applicatie	Betrokken rol(len): • Applicatie-, hosting- of SAAS leverancier.
	Doelstelling: Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.		Scope: • De webserver. Nadere toelichting: HTTP headers moeten de risico's beperken van inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie. Aandachtspunten hierbij zijn: • Behandel alleen HTTP-requests waarvan de gegevens een correct type, lengte, formaat, tekens en patronen hebben. • Behandel alleen HTTP-requests van initiators met een correcte authenticatie en autorisatie. • Sta alleen de voor de ondersteunde webapplicaties benodigde HTTP-requestmethoden (GET, POST, etc.) toe en blokkeer de overige niet noodzakelijke HTTP-requestmethoden. • Verstuur alleen HTTP-headers die voor het functioneren van HTTP van belang zijn. • Toon in HTTP-headers alleen de hoogst noodzakelijke informatie die voor het functioneren van belang is. • Bij het optreden van een fout wordt de informatie in een HTTP-response tot een minimum beperkt. Een eventuele foutmelding zegt wel dat er iets is fout gegaan, maar niet hoe het is fout gegaan. Test aanpak: • Observeer het gedrag van de HTTP headers en responses. Voer hierbij een representatieve deelwaarneming uit op de invoer- en uitvoermogelijkheden die de applicatie biedt.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/PW.03	De webserver is ingericht volgens een configuratie-baseline. <u>Doelstelling:</u> Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.	Applicatie Infrastructuur	<u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS leverancier. <u>Scope:</u> • De webserver. <u>Nadere toelichting:</u> Deze norm richt zich enerzijds op de aanwezigheid van een configuratie-baseline voor de webserver en op de feitelijke configuratie van de webserver. Aandachtspunten hierbij zijn: • <u>Directory listings</u> Te configureren waarde: Directory listings worden niet ondersteund. • <u>Cookie flags</u> Te configureren waarde: Cookie flags staan op 'HttpOnly' en 'Secure'. HTTP security headers bieden steeds meer en fijnmazigere controle over de toegang tot, en het delen van, informatie. Het correct gebruik van security headers levert een extra beveiligingslaag op: • <u>X-Frame-Options</u> De X-Frame-Options header voorkomt dat de pagina in een iFrame wordt geladen, waarmee gegevens kunnen worden gestolen, pagina's worden aangepast of gebruikers worden misleid. Te configureren waarden: deny of sameorigin • <u>Strict-Transport-Security (HSTS)</u> HTTP Strict Transport Security (HSTS) zorgt ervoor dat browsers alleen over TLS communiceren met de webapplicatie. Door het forceren van HTTPS beschermt deze header gebruikers tegen afluisteren en Man-in-the-Middle (MitM)-aanvallen. HSTS voorkomt het gebruik van gemengde HTTP en HTTPS inhoud, beschermt tegen fouten van webservers zoals het laden van JavaScript via een onveilige verbinding en voorkomt dat gebruikers waarschuwingen over ongeldige certificaten kunnen negeren.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			Minimaal te configureren waarde: max-age=31536000 • X-Content-Type-Options De X-Content-Type-Options header voorkomt dat de browser het MIME-type van een bestand bepaalt op basis van kenmerken (sniffing). Wanneer deze header is ingesteld op nosniff, vertrouwt de browser het MIME-type dat door de server wordt meegegeven en zal de browser de bron blokkeren als deze fout is. Dit voorkomt spoofing van resources zoals CSS stylesheets en Javascript-bestanden die over HTTP worden verstuurd. Te configureren waarde: nosniff • Content-Security-Policy De Content-Security-Policy (CSP) geeft de browser instructies over welke resources vanaf welke locatie mogen worden ingeladen en hoe deze mogen worden gebruikt. Een CSP kan fijnmazige instructies bevatten per soort resource, zoals afbeeldingen, stylesheets en scripts. Bij het gebruik van een CSP zijn standaard de uitvoering van inline scripts en de eval()-functie uitgeschakeld Te configureren waarden: default-src 'self'; frame-src 'self'; frame-ancestors 'self'; Sta geen onveilige configuratie toe door het gebruik van 'unsafe-inline' (tenzij gebruik wordt gemaakt van een nonce) en 'unsafe-eval'. Het is niet toegestaan bronnen beginnend met http:// te whitelisten. • Referrer-Policy De Referrer-Policy beperkt het ongevraagd delen van privacygevoelige informatie bij het doen van verzoeken aan, en bij het doorsturen van de gebruiker naar, een andere website. Gebruik de instelling 'same-origin', zodat de referrer-header alleen wordt meegestuurd bij verzoeken binnen het eigen domein. Dit voorkomt het lekken van privacygevoelige informatie bij omleiden naar externe domeinen. De striktere instelling 'no-referrer' kan ook worden gebruikt, zodat de referrer-header nooit wordt meegestuurd. Test aanpak: • Interview de verantwoordelijke functionarissen. • Observeer de mogelijk tot het maken van directory listings, de cookies flags.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			• Inspecteer de configuratie-baseline van de webserver m.b.t. X-Frame-Options, Strict-Transport-Security (HSTS), X-Content-Type-Options, Content-Security-Policy en Referrer-Policy.
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen. <u>Doelstelling:</u> Voorkomen van misbruik van beheervoorzieningen.	Infrastructuur Proces	<u>Betrokken rol(len):</u> • Hosting- of SAAS leverancier. <u>Scope:</u> • De webserver en andere servers in de DMZ. <u>Nadere toelichting</u>: Dit betreft het gebruik van veilige netwerkprotocollen. Indien beheerinterfaces via het internet te benaderen zijn moet dit door middel van twee factor authenticatie, zoals de combinatie van een wachtwoord en source IP filtering, in combinatie met een veilig (communicatie) protocol worden afgehandeld. Er mag geen gebruik worden gemaakt van backdoors om de systemen te benaderen (ook niet voor noodtoegang). Daarnaast wordt een beknopt operationeel beleid verwacht. Aandachtspunten voor deze norm zijn: • Het gebruik van veilige protocollen (conform industrie standaarden) voor het benaderen van beheermechanismen (beheerinterfaces). • Het gebruik van sterke authenticatie voor zowel technisch als functioneel beheerders. <u>Test aanpak</u>: • Interview de verantwoordelijke functionarissen. • Inspecteer het operationele beleid met betrekking tot het gebruik van beheervoorzieningen en de daarbij vereiste authenticatie.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			• Observeer de protocollen die kunnen worden gebruikt voor het benaderen van beheerinterfaces en de authenticatiemethoden die daarbij worden afgedwongen. • Inspecteer de configuratie ten aanzien van de wachtwoordvereisten van de webserver en voor een deelwaarneming van minimaal één van de andere servers in de DMZ.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar. <u>Doelstellingen:</u> Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	Infrastructuur Proces	<u>Betrokken rol(len):</u> • Hosting- of SAAS leverancier. <u>Scope:</u> • De webserver en andere ICT componenten binnen de DMZ. <u>Nadere toelichting</u>: Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar. Hierbij kan worden verwezen naar actuele hardening-richtlijnen van de leverancier(s)/SANS/NIST/CIS met een vermelding van "pas toe of leg uit". Hierbij spelen de geïdentificeerde risico's in de "pas toe of leg uit" afweging een bepalende rol. Het gaat echter niet alleen om de hardeningsrichtlijn zelf, maar ook om het concreet toepassen ervan. De hardening van de DigiD webomgeving dient stringent te zijn geregeld: alles wat open staat moet een reden hebben en alles wat open staat moet secure worden aangeboden. De hardening van interne systemen mag minder stringent. Wel moeten de beheer functies secure zijn en mogen er geen onveilige protocollen worden gebruikt, moeten standaard wachtwoorden zijn gewijzigd. Voorbeeld applicaties moeten zijn verwijderd als deze niet daadwerkelijk worden gebruikt. Aandachtspunten hierbij zijn: • Inrichting van ICT-componenten (aantoonbaar) volgens de instructies en procedures van de leverancier. • Bijhouden van een actueel overzicht bij van de noodzakelijke protocollen, services en accounts voor de op het platform geïnstalleerde applicaties. • Deactiveren of verwijderen van alle protocollen, services en accounts op het platform als die niet volgens het ontwerp noodzakelijk zijn. • Periodiek toetsen of de in productie zijnde ICT-componenten niet meer dan de vanuit het ontwerp noodzakelijke functies bieden (statusopname). Afwijkingen worden hersteld. <u>Test aanpak</u>: • Interview de verantwoordelijke functionarissen. • Inspecteer de architectuur en hardening standaarden. • Inspecteer de configuratiebestanden en de uitkomsten van de penetratietest.
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er	Infrastructuur	<u>Betrokken rol(len):</u> • Hosting- of SAAS leverancier.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
	een DMZ die tussen het interne netwerk en het internet gepositioneerd is. Doelstelling: Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.		Scope: • De DMZ van de DigiD webapplicatie. Nadere toelichting: DMZ en compartimentering d.m.v. (2 virtuele) firewalls. Deze eis zowel materieel (feitelijk bestaan en inrichting van DMZ) als formeel qua opzet (netwerkschema of tekening) beoordelen, eventueel op basis van een adequate beschrijving. Overigens zal de organisatie moeten aantonen dat zij voldoende inzicht heeft in de architectuur, zowel van de DMZ als van de systemen die zich daarin bevinden. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer het netwerkarchitectuur schema inclusief de toegestane verkeersstromen tussen netwerksegmenten. • Inspectie van configuratie files, firewall regels en de uitkomsten van de penetratietest.
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen. Doelstelling: Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	Infrastructuur	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • De DMZ van de DigiD webapplicatie. Nadere toelichting: Beveiligingsrichtlijnen NW.04, C.06 en C.07 hangen nauw met elkaar samen: - NW.04 richt zich op de implementatie en het gebruik van IDS/IPS - C.06 richt zich op het tijdig signaleren van aanvallen - C.07 richt zich op periodieke analyse van de logging. Inkomend en uitgaand verkeer moet worden gemonitord om mogelijke aanvallen tijdig te detecteren en hier acties op te kunnen ondernemen. Hiervoor zal de organisatie een Intrusion Detection Systeem (IDS) moeten implementeren. Aanbevolen wordt om tevens gebruik te maken van een Intrusion Prevention Systeem

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			(IPS) dat automatisch preventieve maatregelen neemt tegen bedreigingen of een gecombineerde IDS/IPS. Het IDS of IPS dient geplaatst te worden **na** decryptie van het oorspronkelijk versleuteld netwerkverkeer omdat anders de inhoud van de berichten niet afdoende kan worden beoordeeld door het systeem. Aandachtpunten hierbij zijn: • Het gebruik van een IDS of IPS waarmee netwerkverkeer naar / van de DMZ van de DigiD webapplicatie wordt gemonitord. • Een inrichtingsdocument en een beheerprocedure waarin is vastgelegd waar en hoe de IDS / IPS ingezet. • Het gebruik van een adequate ruleset (b.v. Snort, Suricata, ETPro, etc.) die periodiek (= minimaal wekelijks) wordt geactualiseerd. <u>Test aanpak</u>: • Interview de verantwoordelijke functionarissen. • Inspecteer het netwerkarchitectuur schema, de inrichtingsdocumentatie en de beheerprocedure van de IDS/IPS. • Inspecteer de configuratiefiles van het IDS/IPS en de signature datum van de regelset.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd. Doelstelling: Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • Het netwerksegment met de webservers die een koppeling hebben met de DigiD omgeving van Logius inclusief de toegang vanuit internet. Nadere toelichting: Door middel van fysieke scheiding, veilige VPN verbindingen (zoals IPSec) of VLANs is het beheer- en productieverkeer van elkaar gescheiden. Deze beveiligingsrichtlijn is nauw verbonden met U/PW.05 omdat de voor het beheer uitsluitend veilige netwerkprotocollen mogen worden gebruikt. • Er is een inrichtingsdocument waaruit blijkt op welke wijze content beheer (web- en database-content), applicatiebeheer en technisch beheer worden uitgeoefend. • Het gebruik van fysieke scheiding, veilige VPN verbindingen (zoals IPSec) of VLANs het beheer- en productieverkeer van elkaar gescheiden. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer het netwerkarchitectuurschema inclusief de toegestane verkeersstromen tussen netwerksegmenten. • Inspecteer de configuratie files, firewall regels en de uitkomsten van de penetratietest.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar. Doelstelling Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting. Scope: • De webserver en andere ICT componenten binnen de DMZ. Nadere toelichting: Voor het configureren van netwerkcomponenten is een hardeningrichtlijn beschikbaar. Hierbij kan worden verwezen naar actuele hardening-richtlijnen van de leverancier(s)/SANS/NIST/CIS met een vermelding van "pas toe of leg uit". Hierbij spelen de geïdentificeerde risico's in de "pas toe of leg uit" afweging een bepalende rol. Het gaat echter niet alleen om de hardeningrichtlijn zelf, maar ook om het concreet toepassen ervan. De hardening van de DigiD omgeving dient stringent te zijn geregeld: alles wat open staat moet een reden hebben en alles wat open staat moet secure worden aangeboden. De hardening van interne systemen mag minder stringent. Wel moeten de beheer functies secure zijn en mogen er geen onveilige protocollen worden gebruikt, moeten standaard wachtwoorden zijn gewijzigd. Voorbeeld applicaties moeten zijn verwijderd als deze niet daadwerkelijk worden gebruikt. Door de vitale rol die het Domain Name System speelt in het bereikbaar houden van webapplicaties, verdient de beveiliging van DNS-services extra aandacht. Onder deze beveiligingsrichtlijn valt dan ook het verplicht gebruik van DNSSEC (DNS Security Extensions) voor de URL van het object van onderzoek. Met DNSSEC wordt de authenticiteit van DNS-antwoorden geverifieerd om misbruik te voorkomen. Aandachtspunten hierbij zijn: • Bijhouden van een actueel overzicht van de noodzakelijke netwerkprotocollen, -poorten en -services. • Uitschakel op de netwerkcomponenten alle netwerkprotocollen, -poorten en –services uit, behalve de noodzakelijke. • Aanpassen de (beveiligings)configuraties van netwerkprotocollen, -poorten en -services op de netwerkcomponenten aan conform richtlijnen. Test aanpak: • Interview de verantwoordelijke functionarissen.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			• Inspecteer de netwerkarchitectuur schema en hardening-richtlijnen. • Inspecteer de configuratiebestanden en de uitkomsten van de penetratietest.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICTcomponenten van de webapplicatie (scope). Doelstelling: Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de webapplicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting: Deze netwerk based scan dient zich ten minste gericht te hebben op de resultaten van de hardening en patching van de infrastructuur en het detecteren van mogelijke kwetsbaarheden op de infrastructuur. • Vulnerability assessments vinden intern plaats, minimaal een keer per jaar en vaker op basis van een risicoafweging zoals bijvoorbeeld bij wijziging van de configuratie van de DMZ. • De scope van het vulnerability assessment omvat tenminste de infrastructuur voor het netwerksegment met de DigiD webapplicatie. • Naar aanleiding van de resultaten van de vulnerability assessment is een actieplan opgesteld om de tekortkomingen op te heffen. • Er is voldoende voortgang geboekt in het opvolgen van bevindingen gezien de aard en complexiteit van de bevindingen. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer het netwerkarchitectuur schema en de opdracht tot het uitvoeren van vulnerability assessment. • Inspecteer het vulnerability assessment rapport, het actieplan naar aanleiding van de vulnerability assessment en het statusrapport met betrekking tot de bevindingen.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope). Doelstelling: Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).	Applicatie Infrastructuur Proces	Betrokken rol(len): • Applicatie-, hosting- of SAAS leverancier. Scope: • De DigiD webapplicatie, de webserver en andere servers in de DMZ van de DigiD webapplicatie. Nadere toelichting: De voorkeur heeft het op basis van een risicoafweging enkele keren per jaar een penetratietest te laten uitvoeren, zodat ingespeeld kan worden op nieuwe bedreigingen.
			• De penetratietest dient minimaal eenmaal per jaar te worden uitgevoerd en na significante wijzigingen, zoals vervanging applicatie, nieuwe versie, migratie webservers, database migratie, et cetera. • De scope van de penetratietest omvat tenminste de webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. • Naar aanleiding van de resultaten van de penetratietest is een actieplan opgesteld om de tekortkomingen op te heffen. • Er is voldoende voortgang geboekt in het opvolgen van bevindingen gezien de aard en complexiteit van de bevindingen. Testaanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer het netwerkarchitectuur schema en de opdracht tot het uitvoeren van de penetratie test. • Inspecteer het penetratietest rapport, het actieplan naar aanleiding van de penetratietest en het statusrapport met betrekking tot de bevindingen.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. Doelstelling: Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting Beveiligingsrichtlijnen NW.04, C.06 en C.07 hangen nauw met elkaar samen: - NW.04 richt zich op de implementatie en het gebruik van IDS/IPS - C.06 richt zich op het tijdig signaleren van aanvallen - C.07 richt zich op periodieke analyse van de logging. Hoewel deze richtlijn een brede reikwijdte heeft, is zij - in overleg met Logius – ingeperkt tot het detecteren van aanvallen met detectiesystemen in de webapplicatie-infrastructuur. Aandachtspunten zijn: • Het definiëren van alarm situaties en drempelwaarden. • Het configureren van de alarm situaties en drempelwaarden in het IDS/IPS en het genereren van de bijbehorende alerts. • De inbedding van alert afhandeling in het incidentenbeheerproces inclusief escalatieprocedure.
			Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspectie van de Use Cases en drempelwaarden. • Inspectie van alerts en de opvolging daarvan.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICTsystemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd. <u>Doelstelling:</u> Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.	Infrastructuur Proces	<u>Betrokken rol(len):</u> • Hosting- of SAAS leverancier. <u>Scope:</u> • De infrastructuur voor het netwerksegment met de DigiD webapplicatie. <u>Nadere toelichting</u> Beveiligingsrichtlijnen NW.04, C.06 en C.07 hangen nauw met elkaar samen: - NW.04 richt zich op de implementatie en het gebruik van IDS/IPS; - C.06 richt zich op het tijdig signaleren van aanvallen; - C.07 richt zich op periodieke analyse van de logging. De logging- en detectie-informatie en de conditie van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd. Aandachtpunten hierbij zijn: • Procedurebeschrijving met daarin beschreven op welke wijze en wanneer controles op logging moeten plaatsvinden en hoe taken op dit gebied belegd zijn. • Het uitvoeren van periodieke controles op: o wijzigingen aan de configuratie van webapplicaties; o optreden van verdachte gebeurtenissen en eventuele schendingen van de beveiligingseisen; o ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden; o toegangslogs; • Periodieke analyse op ongebruikelijke situaties (incidenten) die de werking van webapplicaties kunnen beïnvloeden. • Periodiek rapportage van de geanalyseerde en beoordeelde gelogde gegevens aan de systeemeigenaren en/of aan het management. • Opvolging van bevindingen naar aanleiding van de analyse. <u>Test aanpak</u>: • Interview de verantwoordelijke functionarissen. • Inspectie van de procedurebeschrijving met betrekking tot de logging.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			• Inspectie van de vastlegging van de periodiek review van de logging, periodieke rapportage aan het management en follow-up acties naar aanleiding van review en analyse van de logging.
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig,	Applicatie Infrastructuur Proces	<u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS leverancier. • Houder van DigiD aansluiting. <u>Scope:</u>

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
	geautoriseerd en getest worden doorgevoerd. Doelstelling: Zeker stellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.		• De DigiD webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting: De focus ligt op het vaststellen dat het proces wijzigingsbeheer zodanig is opgezet en geïmplementeerd dat alle wijzigingen altijd eerst worden getest voordat deze in productie worden genomen en via wijzigingsbeheer worden doorgevoerd. In sommige gevallen kunnen formulieren worden gebouwd die beveiligingsrisico's introduceren en valt wijzigingenbeheer met betrekking tot formulieren wel in scope van de DigiD-assessment. Is dit niet het geval dan valt wijzigingenbeheer met betrekking tot formulieren niet in scope. Welke specifieke situatie zich voordoet hangt af van de applicatie (formulierengenerator) en de wijze waarop deze wordt gebruikt. Het is aan de auditor om te bepalen of er aanleiding is om wijzigingenbeheer ten aanzien van de formulieren in de DigiD-scope op te nemen. Ingeval van SAAS-toepassingen ligt de verantwoordelijkheid voor het testen van wijzigingen aan de applicatie doorgaans bij de leverancier en/of gebruikersgroep. Aandachtspunten hierbij zijn: • Wijzigingsbeheer procedure, waarbij zo nodig onderscheid wordt gemaakt tussen wijzigingen op de applicatie, de servers en de netwerkcomponenten. • Het inrichten van een OTAP omgeving zodat wijzigingen eerst in een testomgeving worden getest voordat zij in productie kunnen worden genomen (n.b. voor netwerk wijzigingen is een testomgeving vaak niet mogelijk). • Het hanteren van een testscript en de vastlegging van de testresultaten. • Een formele acceptatie voor het in productie nemen van de wijziging. • Het beperken van het aantal personen die wijzigingen in productie kunnen nemen. • Bij het uitbrengen van een nieuwe release van de applicatie of een grote upgrade van het onderliggende platform moet, bij voorkeur door middel van een penetratietest, worden onderzocht of er geen nieuwe kwetsbaarheden zijn geïntroduceerd. Test aanpak: • Interview de verantwoordelijke functionarissen.
			• Inspecteer de wijzigingsprocedure en de inrichting van de OTAP omgeving. • Inspecteer, voor elk type wijziging (applicatie, servers, netwerk), één wijziging en de daaraan gerelateerde documentatie.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			Non-occurrence (voor het onderdeel inspecteren van een doorgevoerde wijziging): Hierbij geldt dat op basis van (deel)waarnemingen binnen een proces dat onderworpen is aan dezelfde control vastgesteld moet worden dat de wijzigingsprocedure effectief is geïmplementeerd.
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen. Doelstelling: Zeker stellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	Applicatie Infrastructuur Proces	Betrokken rol(len): • Applicatie-,Hosting- of SAAS leverancier. Scope: • Hypervisor (VM Ware, etc.). • Operating system (Windows, etc.). • Databases. • Netwerk componenten. • Firewall. • Webapplicatie en daarvoor benodigde software componenten Nadere toelichting: De focus is op het patching proces. Dit proces kan gedifferentieerd zijn naar bijvoorbeeld het OS, DBMS en netwerk. Applicaties en systemen dienen periodiek gepatcht te worden. Een maandelijks patching cyclus is aanvaardbaar tenzij er security alerts zijn. Voor internet facing systemen dienen de laatste stabiele beveiligingspatches te zijn geïnstalleerd. Indien patching niet mogelijk is in verband met een legacy applicatie die niet meer zou functioneren na patching, zal dit risico aantoonbaar moeten zijn afgewogen. Aandachtpunten hierbij zijn: • Het beschrijven van patchmanagementbeleid waarin is aangegeven hoe de organisatie omgaat met updates: hoe snel implementeert de organisatie een kritieke patch en welke stadia moet de patch doorlopen. • Registratie van patches met vastlegging of de patches niet, wel of versneld worden doorgevoerd. • Het tijdig doorvoeren van patches. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspectie van het patchmanagementbeleid.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			• Inspectie van configuratie files en de uitkomsten van de penetratietest.

Bijlage 3 Procesmatige kwaliteitsaspecten bij DigiD penetratietesten

Van toepassing op beveiligingsrichtlijn C.04:
Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).

Doelstelling
Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).

Kwaliteitsaspecten
Randvoorwaarden
- Penetratietester staat onafhankelijk ten opzichte van het te onderzoeken object.
- Penetratietester heeft aantoonbare eerdere ervaringen van de penetratietester met DigiD penetratietesten.
- Overeengekomen opdracht met doel, vraagstelling, normen, scope, stappenplan, doorlooptijd en budget.
- Penetratietest vrijwaring ondertekend door opdrachtgever en evt. betrokken derden zoals hosting partij.
- Afspraak over beschikbaarheid van penetratietesters en beheerders bij de onderzochte organisatie.
- Afspraak tussen auditor en penetratietester over het gebruik van penetratietesttools.
- Gedocumenteerde afspraken over communicatie tussen penetratietesters en contactpersonen bij de opdrachtgevende organisatie.
- Instemming opdrachtgever met uit te voeren penetratietest.

Scope en normstelling
- Vastgesteld object (versienummer) van het onderzoek relevant voor DigiD.
- Vastgestelde Logius normen voor DigiD (subset uit de NCSC normen), minimaal OWASP top 10, eventueel aangevuld met SANS 25, WASC criteria, GHDB en leveranciers-specifieke normen en baselines.
- Voor DigiD audit is een black box/grey box benadering, waarbij zonder veel voorkennis ingelogd wordt als gebruiker, voldoende.
- Vaststellen met welke functionele scope de volledige technische oplossing wordt afgedekt (bijvoorbeeld een selectie van formulieren waarmee alle componenten worden geraakt), waarbij wordt aangetoond dat de technische oplossing adequaat wordt getest).
- Maatwerk formulieren die niet op basis van standaard configuratie functionaliteit zijn ontwikkeld altijd testen.
- Indien standaard formulieren worden gebruikt, waarbij alleen functionele aanpassingen doorgevoerd kunnen worden, kan volstaan worden met vaststellen van de betrouwbare werking van de formulierengenerator (o.b.v. het assurance-rapport (de TPM) van de service provider).

Verkenningsfase (vaststellen ingang criteria)
- Inventarisatie gebruikte (webfacing) infrastructuur, applicaties, componenten, e.d.
- Infrastructuurtest vindt altijd plaats op de productieomgeving.
- Applicatietest vindt plaats op test omgeving. Opdrachtgever toont aan dat de versie van de applicatie van acceptatieomgeving gelijk is aan die in de productie omgeving.
- Acceptatieomgevingen met representatieve testgegevens zijn beschikbaar.

- DigiD testaccounts zijn beschikbaar en gekoppeld aan testgegevens, evt. gekoppeld aan mobiele nummers penetratietesters.
- Penetratietester(s) zijn bekend met de werking van de applicatie.
- Contactpersonen bij de opdrachtgever zijn bekend met de werking van de applicatie.

Initiële kwetsbaarheden analyse
- Fingerprinting van het object: vaststellen gebruikte merken en versies.
- Inventariseren bekende kwetsbaarheden op basis van publicaties van leveranciers en openbare cyber security bronnen.
- Selectie van tests voor aantonen van de mogelijke kwetsbaarheden.

Geautomatiseerde tests (dynamisch testen)
- Keuze geschikte penetratietest tools en hun dekkingsgraad van het te testen object (niet ieder penetratietest tool ondersteunt alle technologieën, denk aan AJAX, Silverlight, Java en dergelijke).
- Inzicht in het deel van de norm dat door de tool(s) wordt afgedekt en welk deel afzonderlijk zal moeten worden getest.
- Doorlopende bewaking door de penetratietester tijdens de uitvoering om schade te voorkomen, bij voorkeur automatisch afbreken van geautomatiseerde testen bij foutmeldingen waaruit een kritiek probleem blijkt.

Handmatige tests
- Adequate expertise van de penetratietester(s), eventueel aanwezige certificeringen ter onderbouwing; aantoonbare kennis/ervaring met gebruikte technologieën.
- Technische details van gecontroleerde SSL/TLS-certificaten en versleutelde verbindingen.
- Details van gecontroleerde cookies en volledige dekking tijdens de testen.
- Alle bevindingen uit de geautomatiseerde testen zijn handmatig geverifieerd.
- Op basis van bevindingen uit de geautomatiseerde testen zijn handmatige vervolgtesten uitgevoerd.
- Kwetsbaarheden in functionele flows zijn handmatig onderzocht, bijvoorbeeld manipulatie van velden bij meerstaps-formulieren.

Optioneel: Code review (statisch testen) afhankelijk van de norm
- In principe kunnen alle normen getest worden op basis van het bepalen van het gedrag van de applicatie. Bij gerede twijfel over het gedrag alsnog een code review uitvoeren.
- Dekkingsgraad van de review bepalen (selecte of aselecte steekproef dan wel volledige populatie onderzoeken).
- Aantoonbare ervaring van de penetratietester(s) met de programmeertaal en omgeving, eventueel beschikbare certificeringen ter onderbouwing.
- Bij gebruik van tools voor statische testen: dekkingsgraad ten opzichte van de norm.

Risicoanalyse op bevindingen (vaststellen uitgang criteria)
- Risicoafweging van aangetroffen afwijkingen t.o.v. de norm tegen het daadwerkelijk kunnen exploiteren.
- Risico’s uitdrukken in kans X impact of erkende risicoclassificatie.
- Onderbouwen van de ernst van de aangetroffen afwijkingen.
- Geen uitspraken over risiconiveau vanuit business perspectief (beoordeling hiervan kan alleen door de opdrachtgever plaatsvinden).

Rapportage

- Conceptrapportage
  - Classificatie van de rapportage conform DigiD normen, beleid opdrachtgever en auditor en eventueel naar publieke standaarden.
  - Beschrijving object van het onderzoek: webfacing infrastructuur, servers, verbindingen.
  - Tijdstip van uitgevoerde testen.
  - Het IP-adres waarvandaan de test is uitgevoerd.
  - Indien van toepassing: overzicht van onderdelen die niet of onvoldoende getest konden worden.
  - Overzicht afwijkingen ten opzichte van de norm met bijbehorende mate van risico o.b.v. norm en na risicoanalyse.
  - Overzicht en details resultaten en afwijkingen per onderdeel uit de norm.
  - Proof of Concepts of details in rapportage waarmee de bevinding kan worden gereproduceerd.
  - Concrete aanbevelingen per bevinding.
- Afstemming met auditor (review).
  - Versleutelde, beveiligde uitwisseling met de auditor.
  - Controle op volledigheid en consistentie.
  - Controle of met de verkregen diepgang tijdens de testen de norm is afgedekt.
- Melden kritieke bevindingen aan opdrachtgever indien deze naar verwachting in een productieomgeving aanwezig zijn.
  - In overleg met de auditor melden.
  - Proof of Concept of stappen om te reproduceren.
  - Versleuteld, beveiligde uitwisseling details van de kwetsbaarheid.
- Afstemming met opdrachtgever.
  - Versleuteld, beveiligde uitwisseling met de auditor.
  - Afstemming over planning van oplossing en hertesten van bevindingen.
- Definitieve rapportage.
  - Versleutelde, beveiligde uitwisseling met de opdrachtgever.
  - Bevindingen waarvoor een hertest is uitgevoerd zijn als zodanig opgenomen in het rapport met de uitkomst van de hertest (t.b.v. traceerbaarheid).
- Archiveren rapportage.
  - Indien van toepassing: archivering in een afgeschermde omgeving met passende beveiligingsmaatregelen.

Periodiciteit

- Minimaal zal jaarlijkse, ten tijde van de DigiD audit, een penetratietest uitgevoerd moeten worden door een penetratietester die onafhankelijk is ten opzichte van het te onderzoeken object.
- Bij het uitbrengen van een nieuwe release van de applicatie of een grote upgrade van het onderliggende platform moet, bij voorkeur door middel van een penetratietest, worden onderzocht of er geen nieuwe kwetsbaarheden zijn geïntroduceerd. Deze penetratietest zou specifiek gefocust mogen zijn op wijzigingen in de applicatie of de infrastructuur en behoeft niet noodzakelijkerwijs door een penetratietester te worden uitgevoerd die onafhankelijk staat ten opzichte van het te onderzoeken object.

- Het is aan te bevelen om, op basis van en risicoafweging, frequenter penetratietesten uit te (laten) voeren, zodat ingespeeld kan worden op nieuwe bedreigingen.

Bijlage 4 Testaanpak bij de te onderzoeken normen relevant voor Suwinet

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	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 organisatie 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 organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat ten minste de volgende punten: a) De strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid. b) De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden. c) De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers. d) De gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn. e) De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd. f) De bevordering van het beveiligingsbewustzijn.	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 aansluitbeleid 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. 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 de leiding van de organisatie (het dagelijks bestuur). Interview de verantwoordelijke functionarissen.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			**Note: zie bijvoorbeeld de handreiking informatiebeveiligingsbeleid van de IBD: https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/07/201907-Handreiking-Informatiebeveiligingsbeleid-BIO-v1.1.docx*
5.1.2 Beoordeling van het informatie-beveiligingsbeleid	Criterium BIO: Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is. Doelstelling: Bewerkstellingen dat de getroffen beveiligingsmaatregelen continue voldoen aan het juiste beveiligingsniveau. *Risico:* *De getroffen beveiligingsmaatregelen kunnen ontoereikend zijn in relatie tot aangescherpte wetgeving, verandering van risicoklasse van gegevens en de toegepaste technologieën.*	5.1.2.1 Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: Het Suwinet informatiebeveiligingsbeleid (eventueel als onderdeel van het algehele informatiebeveiligingsbeleid) dient actueel te zijn en periodiek* te worden beoordeeld en zo nodig te worden bijgesteld bij grote wijzigingen of aan de hand van externe ontwikkelingen. **Note: Hiervoor geldt dat de periodiciteit aansluit bij de (bestaande) bestuurs- en P&C-cycli. Voor gemeenten geldt doorgaans dat dit de raadsperiode (4 jaar) is.* Test aanpak: Inspectie van het informatiebeveiligingsbeleid. Stel vast dat het beleid actueel is en conform de (bestaande) bestuurs- en P&C-cycli is bijgesteld. Interview de verantwoordelijke functionarissen.
6. Organiseren van informatiebeveiliging			

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
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 De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie. 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 organisatie met relevante rollen en functies. Controle technische functiescheiding (CTFS) is hierbij van belang waar van toepassing waar het gaat om het onderscheiden van verantwoordelijkheid. Test aanpak: Inspecteer het informatiebeveiligingsbeleid en stel vast dat taken, bevoegdheden en verantwoordelijkheden (CTFS) ten aanzien van de IB functie t.a.v. Suwinet formeel zijn vastgesteld en stel vast dat deze functie en onderliggende rol(-len) ook als zodanig zijn ingericht* en beschreven. **Note: Idealiter zijn bovenstaande documenten onderdeel van een ingerichte AO/IB.* Stel vast dat een incidentmanagementproces (beveiligingsincidenten) ten aanzien van Suwinet is ingericht en stel het bestaan vast met een deelwaarneming van ten minste één. Stel vast dat beveiligingsincidenten worden geanalyseerd, gerapporteerd aan het verantwoordelijke

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			management en waar nodig aanvullende maatregelen worden getroffen. Interview de verantwoordelijke functionarissen.
6.1.2 Scheiding van taken	Criterium BIO: Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. Doelstelling: Ervoor zorgen dat de juiste taken en verantwoordelijkheden binnen de onderkende rollen juist worden uitgevoerd met inachtneming van de juiste functiescheiding voor zover de organisatiegrootte dit toelaat. *Risico:* *Onduidelijke taken en verantwoordelijkheden en het ontbreken van juiste functiescheiding kunnen leiden tot:* *- misbruik van bevoegdheden,* *- te ruim toegekende bevoegdheden,* *- over het hoofd zien van en/of tot implementatie van tegenstrijdige beveiligingsmaatregelen.*	6.1.2.1 Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen* waarnemen of voorkomen. * Onder bedrijfsmiddelen worden in dit verband de Suwinet gegevens (mede) begrepen.	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd (in de vorm van bijvoorbeeld een RACI-matrix*). **Note: RACI staat voor Responsible, Accountable, Consulted en Informed. Idealiter onderdeel van een ingerichte AO/IB.* De gedocumenteerde rollen zijn door het 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 organisatie te verminderen. Het gaat hierbij om de verantwoordelijkheden van lijnmanagement, security management, maar ook bijvoorbeeld informatiemanagement en control.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			Test aanpak: Inspecteer de relevante functie/taakbeschrijvingen van met name de sleutelfunctionarissen, de autorisatiematrix en het autorisatiebeheerproces, en stel vast dat deze voldoen aan bovenstaande aandachtspunten. Interview de verantwoordelijke functionarissen.
7. Veilig personeel			
7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Criterium BIO: 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. Doelstelling: Het bewustmaken van gebruikers van Suwinet gegevens *Risico:* *Indien gebruikers van Suwinet gegevens zich niet of onvoldoende bewust zijn van de (hoge) vertrouwelijkheid, bestaat het risico dat deze gegevens onvoldoende worden beschermd.*	7.2.2.1 Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen. 7.2.2.2 Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd. 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.	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: De organisatie 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. Test aanpak: Stel vast op basis van inspectie dat in een procedure/ informatiebeveiligingsplan is vastgelegd dat periodiek (bij voorkeur meerdere malen per jaar, doch minimaal jaarlijks[7]) aandacht wordt besteed aan bewustwording van informatiebeveiliging

[7] 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 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			waarbij expliciet aandacht wordt besteed aan Suwi gerelateerde onderwerpen. Stel vast dat deze bewustwordingswerkzaamheden daadwerkelijke ten uitvoer zijn gebracht. Stel vast dat gebruikers die toegang hebben tot Suwinet gegevens binnen drie maanden na indiensttreding een training (I-)bewustzijn succesvol hebben gevolgd*. Interview de verantwoordelijke functionarissen. **Note: Dit normaspect is gerelateerd aan norm 18.1.4 waarin is opgenomen dat het beleid ten aanzien van het verwerken van persoonsgegevens dient te worden gecommuniceerd aan alle personen die betrokken zijn bij deze verwerking.*
9. Toegangsbeveiliging			
9.2.1 Registratie en afmelden van gebruikers	Criterium BIO: Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. Doelstelling: Gebruikers en beheerders de juiste toegangsrechten geven (niet meer en niet minder) dan welke nodig zijn voor de hen opgedragen (wettelijke)taken. *Risico:* *Het risico bestaat dat medewerkers onrechtmatig toegang hebben tot Suwinet of tot de via Suwinet beschikbaar gestelde gegevens.* *Voor Suwinet geldt een verhoogd risico omdat het Suwinet account van een*	9.2.1.1 Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties. 9.2.1.2 Het gebruiken van groepsaccounts is niet toegestaan, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD 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

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
	organisatie ook toegang tot Suwinet kan krijgen vanuit het domein van een ander op Suwinet aangesloten organisatie.		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 en dat adequate login wordt toegepast zodat te allen tijde herleidbaar is wie met dit account wanneer en tot welke gegevens toegang heeft gehad; b) het default admin account dient bij installatie direct hernoemd te worden dan wel te worden disabled; c) het onmiddellijk ongeldig maken of verwijderen van de gebruikersidentificatie van gebruikers die de organisatie hebben verlaten (zie ook 9.2.6); d) het ervoor zorgen dat gebruikers hun gebruikersidentificaties niet delen met andere gebruikers. Bij voorkeur is dit opgenomen in de gedragsregels (zie ook 7.2.2).

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			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. Stel vast dat gebruik gemaakt wordt van accounts die tot één persoon herleidbaar zijn (geen groepsaccounts). Stel vast dat periodieke controles zijn uitgevoerd en correctieve acties zijn doorgevoerd. Interview de verantwoordelijke functionarissen.
9.2.2 Gebruikers toegang verlenen	Criterium BIO: Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. Doelstelling Bewerkstelligen dat de geclaimde identiteit van de gebruiker kan worden bewezen en dat daardoor alleen bevoegde gebruikers toegang krijgen tot Suwinet diensten. *Risico:* *Onbevoegde gebruikers kunnen toegang krijgen tot Suwinet diensten.*	9.2.2.1 Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris. 9.2.2.2 Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven[8]. 9.2.2.3 Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD 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

[8] 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 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			9.2.6 richt zich op het proces van intrekken of wijzigen van toegangsrechten De procedure voor het toewijzen of intrekken van toegangsrechten aan gebruikersidentificaties is gericht op de gebruikers en, indien van toepassing, de beheerders met toegang tot Suwinet gegevens en behoort te omvatten: a) autorisatie verkrijgen van de eigenaar van het informatiesysteem of de informatiedienst voor het gebruik van het informatiesysteem of de informatiedienst. Afzonderlijke goedkeuring voor toegangsrechten door het dagelijks bestuur/ de directie is mogelijk ook relevant; b) verifiëren dat het verleende toegangsniveau in overeenstemming is met de beleidsregels voor toegang en consistent is met andere eisen zoals een scheiding van taken (zie ook 6.1.2); c) waarborgen dat toegangsrechten niet worden geactiveerd (bijv. door dienstverleners) voordat de autorisatieprocedures zijn afgerond; d) bijhouden van een centraal overzicht van toegangsrechten die aan een gebruikersidentificatie zijn toegekend om toegang te verkrijgen tot informatiesystemen en -diensten; e) aanpassen van toegangsrechten van gebruikers van wie de rollen of functies zijn gewijzigd en toegangsrechten van gebruikers die de organisatie hebben verlaten onmiddellijk verwijderen of blokkeren; f) met eigenaren van de informatiesystemen of -diensten periodiek de toegangsrechten beoordelen (zie ook 9.2.5).

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			Test aanpak: Stel vast dat is vastgelegd welke personen bevoegdheden hebben voor het verlenen van toegangsrechten (bijvoorbeeld in een mandaatregister en/ of functieprofielen). Inspecteer de procedure voor het toewijzen of intrekken van toegangsrechten en stel vast dat dit proces in lijn is met bovenstaande aandachtspunten. Interview de verantwoordelijke functionarissen.
9.2.5 Beoordeling van toegangsrechten van gebruikers	Criterium BIO: Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. Doelstelling: Het vaststellen of: de autorisaties en veranderingen hierin juist en tijdig zijn aangebracht, de juiste functiescheiding zijn toegepast en voldaan wordt aan de principes van doelbinding en proportionaliteit, oneigenlijk autorisatie-toekenningen hebben plaatsgevonden. *Risico:* *Bij het ontbreken van controle op de toegangsrechten worden afwijkingen in het autorisatieproces niet gesignaleerd worden.* *Bij het ontbreken controles op het gebruik van autorisaties wordt misbruik niet gesignaleerd.*	9.2.5.1 Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld. (Overruled door 9.2.5.3) 9.2.5.2 De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident. 9.2.5.3 Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD 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 Het (lijn)management behoort de toegangsrechten van gebruikers en, indien van toepassing,

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			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 organisatie; 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>Testaanpak:</u> Stel vast hoe het eigenaarschap van Suwinet gegevens is geregeld. Stel vast dat de periodieke review minimaal eenmaal per halfjaar plaatsvindt. Stel vast dat de periodieke review in lijn is met bovenstaande aandachtspunten. Stel ten aanzien van tenminste één beoordeling vast dat de opvolging van bevindingen uit de periodieke

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			review worden gedocumenteerd en behandeld als beveiligingsincident. Interview de verantwoordelijke functionarissen.
9.2.6 Toegangsrechten intrekken of aanpassen	Criterium BIO: 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. Doelstelling: Het tijdig beëindigen of wijzigen van de toegangsrechten. *Risico:* *Als toegangsrechten niet bijtijds worden beëindigd of gewijzigd, bestaat het risico op onbevoegde kennisname van Suwinet gegevens.*	(Geen onderliggende specifieke overheidsmaatregel)	Betrokken partij(en): Gemeente/ samenwerkingspartij Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD 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 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

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			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 (*) 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>Test aanpak:</u> Stel vast dat het intrekken of wijzigen van toegangsrechten in lijn is met bovenstaande aandachtspunten. Laat bijvoorbeeld een uitdraai maken van de huidige lijst van geautoriseerde gebruikers, controleer of deze gebruikers nog werkzaam zijn binnen het SUWI domein. Neem een willekeurige deelwaarneming van 5 % van de gebruikers. Interview de verantwoordelijke functionarissen.
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	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>

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
	cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd. Doelstelling: Het voorkomen van ongeautoriseerde toegang tot netwerkdiensten. *Risico:* *Ondanks het besloten karakter van Suwinet bestaat het risico dat de toegang tot gegevens niet adequaat is beschermd.*	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.	Suwinet Inlezen Suwinet DKD Toelichting: Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie. Test aanpak: Inspecteer de classificatie van gegevens en daaraan gerelateerde risicoanalyse, de netwerkarchitectuur en het inrichtingsdocument waar de encryptie van gegevens in staat beschreven, en stel vast dat deze voldoen aan bovenstaande aandachtspunten. Stel vast bij welke provider de gemeente de beveiligde verbinding heeft afgenomen. NB: Een gemeente kan alleen via een beveiligde verbinding aansluiten op Suwinet. Observeer de (wijze van encryptie) encryptie van gegevens. Inspecteer of de toegepaste cryptografische configuratie voldoet aan de laatste stand der techniek[9]. Interview de verantwoordelijke functionarissen.
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:	(geen onderliggende specifieke overheidsmaatregel)	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen

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

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
	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.*		Suwinet DKD <u>Toelichting:</u> 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;

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			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. <u>Test aanpak:</u> Inspecteer de gebruikers- en/of beheerderhandleidingen en stel vast dat deze voldoen aan bovenstaande aandachtspunten. Interview de verantwoordelijke functionarissen.
12.4.1 Gebeurtenissen registreren	<u>Criterium BIO:</u> Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. <u>Doelstelling:</u> Bewerkstellingen dat tijdig correctieve maatregelen kunnen worden getroffen en informatie te kunnen verschaffen over activiteiten van gebruikers en beheerders van de Suwinet diensten en vaststellen of oneigenlijk gebruik of misbruik is gemaakt van autorisatie. <u>*Risico:*</u> *Afwijkingen niet worden gesignaleerd en derhalve niet kunnen worden aangepakt.*	12.4.1.1 Een logregel bevat minimaal: a) de gebeurtenis; b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; c) het gebruikte apparaat; d) het resultaat van de handeling; e) een datum en tijdstip van de gebeurtenis. 12.4.1.2 Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden. 12.4.1.3 De informatieverwerkende omgeving wordt gemonitord door 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	<u>Betrokken partij(en):</u> Gemeente/ samenwerkingspartij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD <u>Toelichting:</u> Voor deze norm geldt dat de beheerder van de applicatie (BKWI voor Suwinet Inkijk/ de IT-serviceorganisatie voor Suwinet Inlezen en Suwinet DKD) verantwoordelijk is voor het maken en bewaren van logbestanden (zie ook 12.4.2), en dat het de verantwoordelijkheid van de gemeente is om deze logbestanden te gebruiken om regelmatig de rechtmatigheid van het gebruik van Suwinet gegevens door medewerkers te beoordelen. Het is evident dat de beheerorganisatie de gemeente hiertoe in staat moet stellen door het aanleveren

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
		en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd. 12.4.1.4 Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen. 12.4.1.5 De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	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. Er behoren procedures te worden vastgesteld om het gebruik van Suwinet-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig (minimaal 2 maal per jaar gelijkmatig verdeeld) te worden beoordeeld en gerapporteerd. <u>Test aanpak</u>: Inspecteer de procedurebeschrijving met betrekking tot het monitoren van de logging en stel vast dat deze voldoet aan bovenstaande aandachtspunten. Inspectie van de vastlegging van de periodiek review van de logging, periodieke rapportage (minimaal 2 maal per jaar gelijkmatig verdeeld) aan het management en follow-up acties naar aanleiding van review en analyse van de logging (PDCA). *Note: Denk ook aan het vaststellen van de volledigheid op basis van doorlopende nummering/ timestamp; en is de logging mogelijk beïnvloedbaar voor de belanghebbende(n).* Stel vast dat de periodieke review van de logging met zodanige diepgang heeft plaatsgevonden dat met een redelijke mate van zekerheid kan worden gesteld dat materiele afwijkingen (onrechtmatig

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			gebruik van Suwinet gegevens) aan het licht zouden zijn gekomen. Interview de verantwoordelijke functionarissen.
12.4.2 Beschermen van informatie in logbestanden	Criterium BIO: Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang. Doelstelling: Alle handelingen die betrekking hebben op gebruikers en beheerders moeten herleidbaar zijn naar individuele personen. *Risico:* *Zonder vastlegging en bewaking kan achteraf niet worden vastgesteld wie bepaalde handelingen heeft uitgevoerd.*	12.4.2.1 Er is een overzicht van logbestanden die worden gegenereerd. 12.4.2.2 Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd. 12.4.2.3 Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden. 12.4.2.4 Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform BIO hoofdstuk 16.	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inlezen Suwinet DKD Toelichting: Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole en te worden beschermd tegen vervalsing en onbevoegde toegang. 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. Interview de verantwoordelijke functionarissen.
18. Naleving			

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
18.1.4 Privacy en bescherming van persoonsgegevens	Criterium BIO: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende het verwerken van persoonsgegevens. *Risico:* *Als de verwerking van Suwinet (persoons)gegevens niet overeenkomstig toepasselijke wet- en regelgeving plaatsvindt, wordt hierdoor de AVG overtreden.*	18.1.4.1 In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren. 18.1.4.2 Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: Organisaties behoren een beleid te ontwikkelen en te implementeren voor de privacy en bescherming van persoonsgegevens. Dit beleid behoort te worden gecommuniceerd aan alle personen die betrokken zijn bij het verwerken van persoonsgegevens. Indien gemeenten 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. Test aanpak: Stel vast dat de organisatie een privacy-beleid heeft ontwikkeld en geïmplementeerd. Stel vast dat de Suwinet applicatie(s) is/ zijn opgenomen in het Verwerkingsregister. Stel vast dat een FG is aangesteld, dat deze in voldoende mate onafhankelijk en objectief is, en dat deze voldoende mandaat heeft om zijn/haar functie uit te voeren. Stel vast dat de naleving van de privacyregels regelmatig gecontroleerd wordt (zie ook 12.4.1). Stel vast dat de gemeente de Suwinet gegevens alleen gebruikt voor de taken waarvoor een wettelijke basis (doelbinding) is* en die dus

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
			noodzakelijk zijn voor de uitvoering van wet- en regelgeving. Voor een aantal gemeentelijke taken is het gebruik van Suwinet gegevens niet toegestaan**. Interview de verantwoordelijke functionarissen.

(*) BKWI publiceert desgevraagd periodiek een overzicht waarin de partijen zijn opgenomen die Suwinet gegevens gebruiken waarbij is vermeld voor welk doel welke bron wordt geraadpleegd. Dit overzicht is hier te vinden:
https://www.bkwi.nl/_Resources/Persistent/140bd66162ff272fcbb3441cff1a9b775d0ad02e/20191210%20Overzicht%20Suwinet%20gebruikers%20doel%20en%20bron.pdf

(**) Het gebruik van Suwinet is (o.a.) 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, (bestaande) WSW.
- 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 Suwi en conform het Aansluitprotocol (Bijlage III Regeling Suwi). Daarmee hebben zij een eigen aansluiting op Suwinet.

Bijlage 5 Afbakening werkzaamheden Suwinet

In het kader van de Wet Suwi kunnen gemeenten kunnen gebruik maken van drie soorten voorzieningen, te weten:

- Suwinet Inkijk
- Suwinet Inlezen
- Suwinet DKD-Inlezen

BKWI heeft aangegeven dat zij van plan zijn om begin september (2020) aan alle gemeenten een overzicht te verstrekken van de door hun gebruikte Suwinet-services (ook gebruik door GSD's e.d.). In principe zal DKD Inlezen in het overzicht worden meegenomen, aangezien BKWI verantwoordelijk is voor de techniek en de administratie.

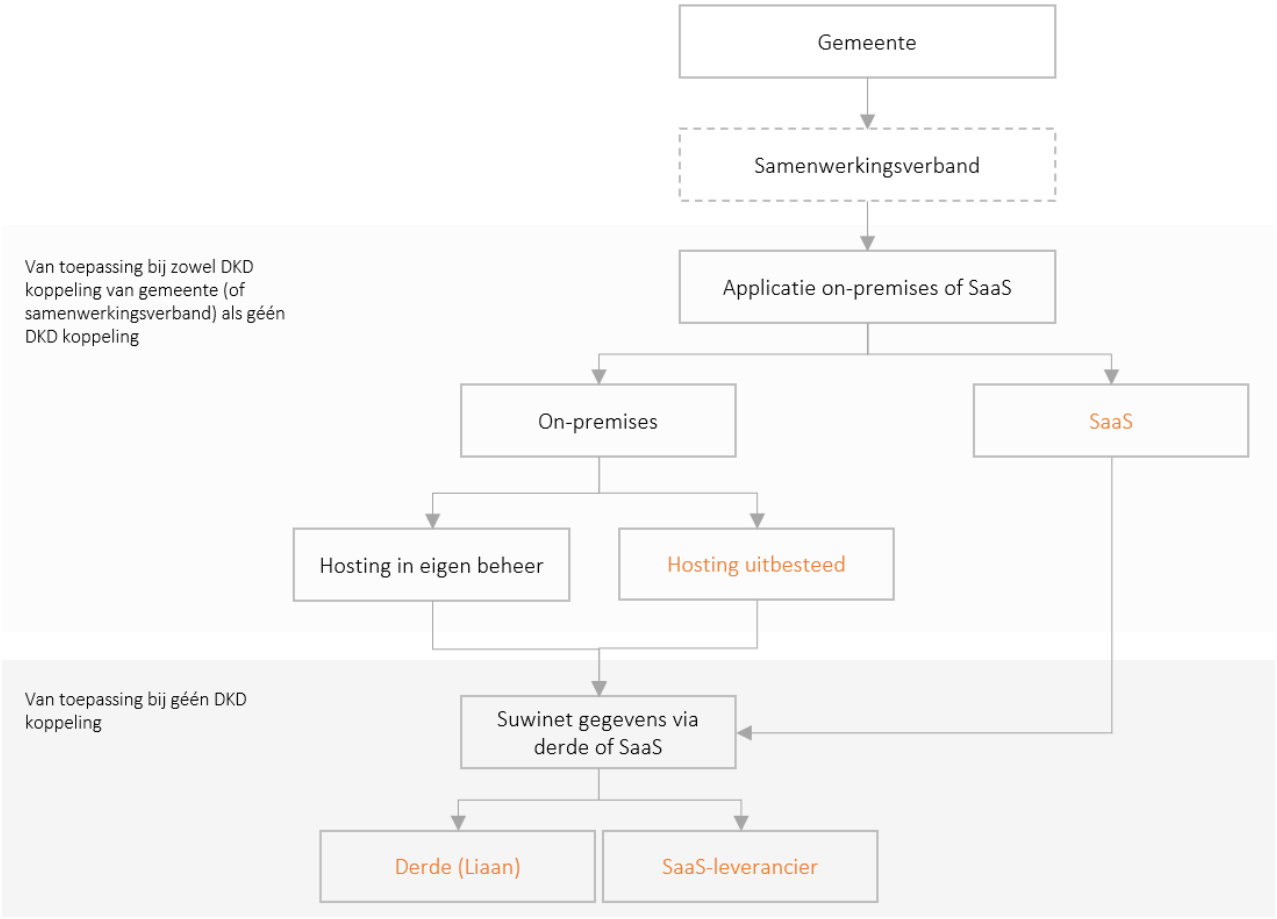
Het verdient aanbeveling dat de IT-auditor bij aanvang van de opdracht dit overzicht bij de gemeente opvraagt. In het geval de gemeente (nog) niet beschikt over het overzicht kan deze het overzicht bij BKWI opvragen via het email adres ensia@BKWI.nl.

Met name de voorzieningen Suwinet Inlezen en Suwinet DKD-Inlezen zijn minder zichtbaar aanwezig bij de gemeenten omdat de Suwinet gegevens via een koppeling in de applicatie van de gemeente wordt geladen. Hierbij bestaat de mogelijkheid dat een derde partij ook een rol in het proces speelt, doordat zij de data verrijken.

Zonder volledig te willen zijn, komen de onderstaande vier inrichtingen van DKD-Inlezen in de praktijk het meest voor:

1. Gemeente* heeft een DKD koppeling. De gemeente host de applicatie in eigen beheer. De applicatie kan ook worden gehost bij een derde partij.
2. Gemeente heeft een DKD koppeling. De gemeente maakt gebruik van een SAAS-oplossing
3. Gemeente heeft geen DKD koppeling. De gemeente maakt gebruik van een SAAS-oplossing, waarin DKD-gegevens zijn opgenomen. Deze gegevens zijn afkomstig van een tussenpartij, zoals bijvoorbeeld Liaan. Dit voorbeeld betreft bijvoorbeeld de Snelbalie van Centric.
4. Gemeente heeft geen DKD koppeling. De gemeente host de applicatie in eigen beheer. Deze gegevens zijn afkomstig van een tussenpartij, zoals bijvoorbeeld Liaan. De applicatie kan ook worden gehost bij een derde partij.

* Indien het een samenwerkingsverband betreft, blijft de situatie gelijk. Echter het aanspreekpunt voor de gemeente is altijd het samenwerkingsverband. Een samenwerkingsverband kent vele verschijningsvormen en kan onder andere ook een andere gemeente betreffen.



Afbeelding: Stroomdiagram DKD-inlezen

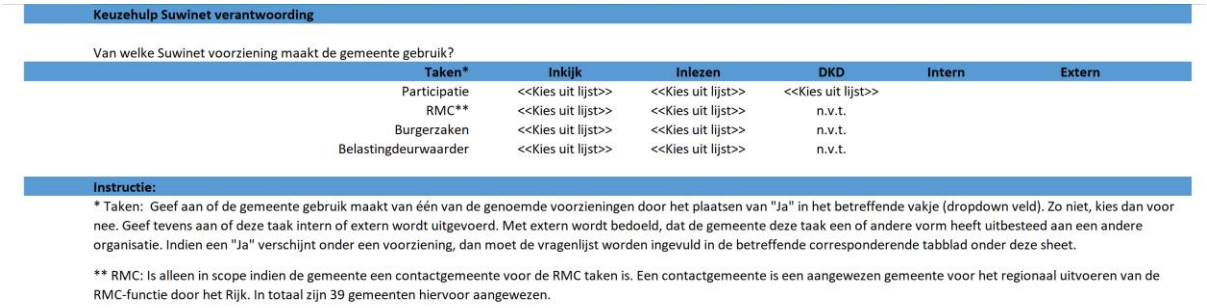
Vanuit het perspectief van de gemeente zijn er een beperkt aantal aanspreekpunten te onderkennen, te weten:

- Hostingpartij (datacenter / IT-serviceorganisatie).
- Leverancier software (SAAS-oplossing), indien leverancier ook de data beheert.
- Samenwerkingsverband (met daarachter een van bovenstaande mogelijkheden).
-

Alle partijen achter het eerste aanspreekpunt van de gemeente dienen te worden gevangen in een TPM of TPM's (assurance-rapport).

Uiteraard zijn er varianten op bovenstaande mogelijk, echter het is onmogelijk om alles te omvatten. In basis zou dit het vertrekpunten moeten zijn en zal de auditor het pad van de (Suwinet)gegevens moeten volgen. Vanaf het eerste aanspreekpunt, zal een TPM beschikbaar moeten zijn of kan de auditor zelf gaan toetsen.

Om behulpzaam te zijn bij het bepalen van de scoping van de werkzaamheden inzake ENSIA-Suwinet, is een keuzehulp beschikbaar gesteld op de website van het NOREA. Deze keuzehulp geeft inzicht in de voorziening waarvan de gemeente gebruik maakt (Inkijk, Inlezen of DKD) en voor welke taak de voorziening wordt ingezet (Participatie, RMC, Burgerzaken of Belastingdeurwaarder). Ten slotte wordt gevraagd welke taak intern of extern wordt uitgevoerd.



Keuzehulp Suwinet verantwoording

Van welke Suwinet voorziening maakt de gemeente gebruik?

Taken*	Inkijk	Inlezen	DKD	Intern	Extern
Participatie	<<Kies uit lijst>>	<<Kies uit lijst>>	<<Kies uit lijst>>		
RMC**	<<Kies uit lijst>>	<<Kies uit lijst>>	n.v.t.		
Burgerzaken	<<Kies uit lijst>>	<<Kies uit lijst>>	n.v.t.		
Belastingdeurwaarder	<<Kies uit lijst>>	<<Kies uit lijst>>	n.v.t.		

Instructie:

* Taken: Geef aan of de gemeente gebruik maakt van één van de genoemde voorzieningen door het plaatsen van "Ja" in het betreffende vakje (dropdown veld). Zo niet, kies dan voor nee. Geef tevens aan of deze taak intern of extern wordt uitgevoerd. Met extern wordt bedoeld, dat de gemeente deze taak een of andere vorm heeft uitbesteed aan een andere organisatie. Indien een "Ja" verschijnt onder een voorziening, dan moet de vragenlijst worden ingevuld in de betreffende corresponderende tabblad onder deze sheet.

** RMC: Is alleen in scope indien de gemeente een contactgemeente voor de RMC taken is. Een contactgemeente is een aangewezen gemeente voor het regionaal uitvoeren van de RMC-functie door het Rijk. In totaal zijn 39 gemeenten hiervoor aangewezen.

Afbeelding: Keuzehulp Suwinet

Reikwijdte verantwoording
Wij vragen in deze paragraaf de aandacht voor de reikwijdte en invulling van de verantwoording betreffende het gebruik van de Gemeenschappelijke Voorziening Suwinet (GeVS), het gebruik van de voorziening Suwinet-/DKD-Inlezen en betreffende het gebruik van Suwinet voor niet-SUWI-taken. Ook de Suwinet-Inkijk functionaliteit wordt in deze paragraaf nader toegelicht. Suwinet-Inkijk betreft de zuivere raadpleeg faciliteit. Suwinet-Inlezen betreft de gemeentelijke bedrijfsapplicatie waarin gegevens via Suwinet- of DKD-Inlezen kunnen worden ingelezen (= inleesapplicaties).

De Autoriteit Persoonsgegevens (AP) heeft indertijd onderzoek gedaan naar de aansluiting van niet-SUWI-partijen op Suwinet (november 2014). Bij dit onderzoek heeft de AP vastgesteld dat in een aantal overeenkomsten sprake is van toepassing van Suwinet-Inlezen. Op grond van het wettelijk kader SUWI heeft de AP geconcludeerd dat de beheerder BKWI net als bij Suwinet-Inkijk, overzicht en controle moet hebben over het feitelijk gegevensgebruik door afnemers. Deze toelichting onderstreept ook op deze criteria het belang van beveiliging.

General IT Controls bij het gebruik van Suwinet Inlezen of DKD inlezen
Om een uitspraak te kunnen doen inzake de betrouwbaarheid en bruikbaarheid van de logbestanden voor Suwinet Inlezen / DKD-Inlezen (het gaat hier met name norm om 12.4.1), dient aan een aantal randvoorwaarden (ITGC) te zijn voldaan. 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.
De IT-auditor dient zelf, op basis van een (beknopte) omgevings- en risicoanalyse, te bepalen welke ITGC controls van belang kunnen zijn om de betrouwbaarheid en bruikbaarheid van de logbestanden te waarborgen.
Ee.e.a is dus afhankelijk van de omgevings- en risicoanalyse, maar de domeinen waaraan naar verwachting aandacht aan geschonken dient te worden, zijn:

Logische toegangsbeveiliging t.a.v. beheerders die beschikken over bijzondere rechten (superuser en administrator rechten) op applicatie- en netwerk niveau en daarmee toegang hebben of kunnen krijgen tot Suwinet gegevens (denk aan database- en technisch applicatie- netwerk- en infrastructuurbeheerders).

Wijzigingsbeheer t.a.v. wijzigingslogs en releasemanagement zodat te allen tijde achterhaald kan worden wie, wanneer, welke wijziging heeft doorgevoerd.

Beoordeling logging
Om de controle op het gebruik van Suwinet gegevens te faciliteren, worden aan de loggegevens eisen gesteld. Het is belangrijk dat de logging voldoende fijnmazig is zodat controle op de rechtmatigheid van het gebruik van Suwinet gegevens daarmee wordt gefaciliteerd.

Een logregel aangaande een handeling bevat minimaal:
- De datum en het tijdstip van de handeling;
- Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID;
- Waar mogelijk de identiteit van het werkstation of de locatie;

- De handeling; Het object waarop de handeling werd uitgevoerd;
- Het resultaat van de handeling.

De IT-serviceorganisatie stuurt maandelijks de loggingsrapportage over de afgelopen maand aan de Afnemer (de gemeente).

De gemeente analyseert periodiek* en actief:
- de gelogde gebruikersgegevens ten aanzien van het gebruik van Suwinet diensten;
- het optreden van verdachte gebeurtenissen en mogelijke schendingen van de beveiligingseisen;
- eventuele ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden.

*Uitgangspunt is dat de controle op de logging rapportages frequent plaatsvindt. Conform het Suwinet normenkader dient de controle minimaal twee keer per jaar te worden uitgevoerd.

Schuldhulpverlening
De Wet Schuldhulpverlening is in de loop van 2021 van kracht geworden. Gemeenten kunnen ten behoeve van uitvoering van deze wet een aparte aansluiting Suwinet-Inkijk aanvragen. De uitrol vindt
gefaseerd plaats in 2021.

Conform systematiek die SZW hanteert is het volgende voor de ENSIA-toetsing vastgelegd:
a. voor aansluitingen die in 2021 operationeel zijn geworden, is opname in de ENSIA verantwoording optioneel. Indien deze wordt opgenomen in de ENSIA verantwoording, valt deze onder de assurance-opdracht;
b. vanaf 2022 dient Suwinet-Inkijk ongeacht moment van operationeel worden in de ENSIA-verantwoording te worden opgenomen.

RMC
Alle gemeenten in Nederland participeren in één van de 40 RMC-regio's (Regionale Meld- en Coördinatiefunctie). Elke RMC-regio heeft één contactgemeente. Deze gemeente coördineert de melding en registratie van voortijdige schoolverlaters door scholen. Voor ENSIA geldt, dat enkel de contactgemeente de verantwoording van het gebruik van Suwinet in het kader van ENSIA verantwoorden in de ENSIA-tool. Gemeenten die geen contactgemeente zijn, laten deze verantwoording achterwege. Uitzondering betreft de situatie dat de contactgemeente werkzaamheden verricht op het account van een niet-contactgemeente. De niet-contactgemeente dient zich te verantwoorden voor het gebruik van het betreffende Suwi-account.

Een overzicht van de Regionale Meld- en Coördinatiepunten is te vinden via deze link:
https://www.rijksoverheid.nl/onderwerpen/vsv/vraag-en-antwoord/contact-rmc-regios

Bijlage 6 Formats Collegeverklaringen en bijlagen

Gemeentelijk kenmerk collegeverklaring:	

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente <naam gemeente>

Doel en achtergrond verklaring

Met deze verklaring geven wij, het college van burgemeester en wethouders, aan in welke mate de gemeente <naam gemeente> voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet. Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA[10] en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen. De inhoud wordt getoetst door een onafhankelijke IT-auditor.
De verklaring is bestemd voor de stelselhouders van DigiD en Suwinet, te weten het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Sociale Zaken en Werkgelegenheid.

Reikwijdte en diepgang verklaring

De toetsing gaat over de opzet en het bestaan van de beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD en Suwinet op 31 december 2021.
De beheersingsmaatregelen inzake DigiD en Suwinet die zijn uitbesteed aan dienstverlener(s) worden niet getoetst door de auditor. Deze collegeverklaring en de verantwoording van de dienstverlener(s) dekken tezamen de normen inzake DigiD en Suwinet af. Het overzicht van normen [en eventuele afwijkingen] en waar deze belegd zijn, is opgenomen in de bijlagen:
bijlage 1 DigiD met kenmerk [kenmerk]
bijlage 2 Suwinet met kenmerk [kenmerk]

Verklaring college

[[Indien volledig wordt voldaan aan de normen: [Het college verklaart dat bij gemeente <naam gemeente> op 31 december 2021 de beheersingsmaatregelen (in opzet en bestaan) voldoen aan de geselecteerde normen inzake DigiD en Suwinet.]]

[[Bij uitzonderingen: [Het college verklaart dat voor [DigiD] [en] [Suwinet] niet aan alle normen wordt voldaan. Wij hebben [een] verbeterplan[nen] opgesteld om aan de normen te voldoen, de acties zijn belegd en worden gemonitord.]]

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

Samenvattend beeld

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

[Plaatsnaam], [datum]

College van B&W gemeente <naam gemeente>

[naam/namen en functie(‘s)]

Naam auditfirma:	
Naam auditor:	
Datum [ondertekening auditor]:	[Handtekening of paraaf auditor]

[Hieronder start de bijlage DigiD. De bijlage DigiD dient voorzien te worden van een gemeentelijk kenmerk. Vul onderstaande tabel in en schuif deze door naar de volgende pagina, zodat de bijlage begint met uw kenmerk.]

Gemeentelijk kenmerk bijlage 1 DigiD:	

Bijlage 1 DigiD (1)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting <naam aansluiting> en aansluitnummer <aansluitnummer>

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

- [voeg hier (een opsomming) van de geboden functionaliteit toe bijvoorbeeld 'Het genereren van aanvraagformulieren voor een uitkering bij de Snelbalie'].

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- [geef hier de naam van de applicatie op, bijvoorbeeld Snelbalie]

Deze applicatie betreft [[maak een keuze uit [geheel maatwerk] [een combinatie van maatwerk en standaard software] [een geheel standaardpakket]] en wordt onderhouden door [naam gemeente en/ of naam leverancier(s)].

Deze applicatie is extern benaderbaar via [de] [het] volgende internetadres(sen): [neem hier de extern benaderbare website(s) op].

DigiD aansluiting <Naam aansluiting> bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door [naam gemeente en/of naam leverancier[s]] in de vorm van [neem vorm op bijvoorbeeld, fysieke hosting, IAAS, PAAS, SAAS].

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

[[Alleen indien er een serviceorganisatie is, anders weglaten] <Naam gemeente> heeft een deel van de DigiD web-omgeving uitbesteed aan [naam leverancier[s]]. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie[s]. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie[s]. De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier[s] van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM['s] / assurancerapportage['s] van de gemeentelijke serviceorganisatie[s]:

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

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

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM['s] / assurancerapportage[s] van onze serviceorganisatie[s] het gehele normenkader afdekken. Het kan voorkomen dat een norm deels bij een leverancier en deels bij de gemeente getoetst is (zogenaamde gedeelde norm).]]

De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk [kenmerk van het assurancerapport van onze auditor].

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm [[opnemen indien van toepassing [inclusief de normen die getoetst zijn bij leverancier[s]]].

DigiD Norm		**Getoetst bij Gemeente**	**(Optioneel) Getoetst bij leverancier 1**	**(Optioneel) Getoetst bij leverancier 2**	**Totaal oordeel norm**
B.05	Contractmanagement	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/TV.01	Identificatie en authenticatie	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/WA.02	Webapplicatiebeheer proces	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/WA.03	Automatische data invoer controle	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/WA.04	Normaliseren uitvoer	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/WA.05	Cryptografie/ Privacy bevordering	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/PW.02	Garanderen webprotocollen	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/PW.03	Configureren webserver	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/PW.05	Toegang tot beheermechanismen	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/PW.07	Hardening van platformen	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/NW.03	DMZ	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/NW.04	Protectie- en detectiemechanismen	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs

DigiD Norm		Getoetst bij Gemeente	(Optioneel) Getoetst bij leverancier 1	(Optioneel) Getoetst bij leverancier 2	Totaal oordeel norm
U/NW.05	Scheiding beheer- en productieomgeving	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
U/NW.06	Hardening van netwerken	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.03	Vulnerability-assessments	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.04	Penetratietesten	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.06	Signaleringsfuncties	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.07	Monitoring functies	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.08	Wijzigingenbeheer	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs
C.09	Patchmanagement	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs	• Voldoet • Voldoet niet • Grijs

Hoeft volgens de gemeente en volgens hoofdstuk “verantwoordelijkheden gebruikersorganisatie” van de TPM van de serviceorganisatie niet bij de gemeente en/of bij leverancier getoetst te worden.

[Hieronder start de bijlage Suwinet. De bijlage Suwinet dient voorzien te worden van een gemeentelijk kenmerk. Vul deze tabel in en schuif deze door naar de volgende pagina.]

Gemeentelijk kenmerk bijlage 2 Suwinet:	

Bijlage 2 Gebruik van Suwinet

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2021 van de gemeente <naam gemeente>. Onderwerp van de verklaring is het gebruik van Suwinet. Deze verklaring heeft betrekking op de Verantwoordingsrichtlijn GeVS 2020 welke is gebaseerd op geselecteerde controls uit de Baseline Informatieveiligheid Overheid (BIO).

Suwinet-gegevens worden ten behoeve van de dienstverlening aan onze burgers [wel][niet] door serviceorganisaties verwerkt. Hierbij is de eventuele aanwezigheid van IT-serviceorganisaties in aanmerking genomen.

[[Alleen indien er een serviceorganisatie is, anders weglaten] Het college van B en W is als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van Suwinet en legt hierover verantwoording af. <Naam gemeente> heeft een deel van de [Suwinet taken] [en] [of] [niet-SUWI-taken] uitbesteed aan [naam serviceorganisatie(s)] [en] [of] [naam andere gemeente(n)]. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie[s] [en] [of] [[naam andere gemeente]]. In de navolgende tabellen is opgenomen of het onderzoeken over het al dan niet voldoen aan deze maatregelen is uitgevoerd door de IT-auditor van deze serviceorganisatie[s]. De controls die betrekking hebben op de taken die belegd zijn bij de serviceorganisatie(s) maken geen onderdeel uit van de zelfevaluatie van onze gemeente, tenzij sprake is van een gedeelde norm. De zelfevaluatie ENSIA voor Suwinet is toegepast op dat deel van het gebruik en normenkader dat niet onder uitbesteding aan onze serviceorganisatie[s] valt. De overige normen worden afgedekt door onderstaande Third Party Mededeling[en] (TPM['s]) / assurancerapportage['s] (AR) van onze serviceorganisatie[s] [en] [of] [[naam andere gemeente]].

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

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

Gebruik van Suwinet voor SUWI-taken

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

Taak	Organisatie	TPM/AR
Participatiewet (Pw)	[binnen de gemeente]	
	[en] [of]	
	[naam serviceorganisatie]: [[naam serviceorganisatie]]	[Ja] [Nee]
	[en] [of]	
	[andere gemeente]: [[naam andere gemeente]]	[Ja] [Nee]
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	[binnen de gemeente]	
	[en] [of]	
	[naam serviceorganisatie]: [[naam serviceorganisatie]]	[Ja] [Nee]
	[en] [of]	
	[andere gemeente]: [[naam andere gemeente]]	[Ja] [Nee]
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	[binnen de gemeente]	
	[en] [of]	
	[naam serviceorganisatie]: [[naam serviceorganisatie]]	[Ja] [Nee]
	[en] [of]	
	[andere gemeente]: [[naam andere gemeente]]	[Ja] [Nee]

Gebruik van Suwinet voor niet-SUWI-taken

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

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

Naleving BIO-maatregelen:

[[Indien geen afwijkingen van de maatregelen:

[Zoals in de Collegeverklaring vermeld, voldoet de gemeente <naam gemeente> aan alle interne beheersmaatregelen inzake Suwinet op 31 december 2021 in opzet en bestaan aan de geselecteerde controls.]]

[[Bij afwijkingen van de normen betreffende SUWI-taken:

[Met uitzondering van de volgende maatregelen voldoen de interne beheersingsmaatregelen voor de SUWI-taken op 31 december 2021 in opzet en bestaan aan de doelstellingen uit de verantwoordingsrichtlijn GeVS 2020:

Organisatie	SUWI-taak	BIO maatregel	Applicatie
[binnen de gemeente] [en] [of] [naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [andere gemeente]: [[naam andere gemeente]]	Participatiewet (Pw)		[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie] [DKD-Inlezen met [naam inleesapplicatie]
[binnen de gemeente] [en] [of] [naam serviceorganisatie]: [[naam serviceorganisatie]] [en] [of] [andere gemeente]: [[naam andere gemeente]]	Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)		[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie] [DKD-Inlezen met [naam inleesapplicatie]
[binnen de gemeente] [en] [of] [naam serviceorganisatie]: [[naam serviceorganisatie]]	Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)		[Suwinet-Inkijk] [Suwinet-Inlezen met [naam inleesapplicatie] [DKD-Inlezen met [naam inleesapplicatie]

[en] [of] [andere gemeente]: [[naam andere gemeente]]			

]]

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

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

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

[en] [of] [Andere gemeente]: [[naam andere gemeente]]			

]]

Bijlage 7 Formats assurance-rapporten

Assurance-rapport van de onafhankelijke IT-auditor
(Bij gebruik DigiD en Suwinet)

Uniek identificatienummer IT-auditor

Aan: <Opdrachtgever>

Ingevolge uw opdracht hebben wij de bijgevoegde collegeverklaring ENSIA 2021 inzake Informatiebeveiliging van DigiD en Suwinet (hierna: collegeverklaring), inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> onderzocht.

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

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

Onderzochte DigiD aansluitingen:

Aansluitnummer	Aansluitnaam

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

Ons oordeel
Wij hebben de bijgevoegde collegeverklaring ENSIA 2021 inzake informatiebeveiliging van DigiD en Suwinet (hierna: collegeverklaring), inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> onderzocht.

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

De collegeverklaring omvat het op 31 december 2021 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen voor DigiD en Suwinet. Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

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

<Alleen bij uitzonderingen >
Benadrukking aangelegenheden
Wij hebben vastgesteld dat de op de uitzonderingen gerichte beheersmaatregelen in verbeterplannen zijn opgenomen, zijn belegd en worden gemonitord. Ons onderzoek heeft zich niet gericht op de juistheid, volledigheid en uitvoering van de verbeterplannen. Deze aanvullende informatie is niet bedoeld om afbreuk te doen aan ons oordeel.

De basis voor ons oordeel
Wij hebben onze assurance-opdracht met betrekking tot de collegeverklaring verricht in overeenstemming met Richtlijn 3000-A (Herzien) 'Assuranceopdrachten door IT-auditors' van NOREA. Deze assurance-opdracht is gericht op het verkrijgen van een redelijke mate van

zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Onze verantwoordelijkheden voor de assurance-opdracht betreffende de collegeverklaring'.

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

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

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

Verantwoordelijkheden van het college van gemeente <naam gemeente>
Het college van burgemeester en wethouders van gemeente <naam gemeente> is verantwoordelijk voor het opstellen van de collegeverklaring. Voor het inschatten of de risico's van afwijkingen van materieel belang zijn in relatie tot DigiD en Suwinet, zijn naast de collegeverklaring en dit assurance rapport ook de interne beheersingsmaatregelen van de gebruikers van de collegeverklaring relevant. De criteria waarvan bij het maken van deze verklaring gebruik werd gemaakt hielden in dat:

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

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

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

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

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

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

Onze assurance-opdracht bestond onder andere uit:

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

Plaats en datum

... (naam IT-auditeenheid)

... (naam IT Auditor RE)

Assurance-rapport van de onafhankelijke IT-auditor
(Bij gebruik van uitsluitend Suwinet)

Uniek identificatienummer IT-auditor

Aan: <Opdrachtgever>

Ingevolge uw opdracht hebben wij de bijgevoegde collegeverklaring ENSIA 2021 inzake Informatiebeveiliging van Suwinet (hierna: collegeverklaring), inclusief de bijlagen 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> onderzocht.

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

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

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

Ons oordeel
Wij hebben de bijgevoegde collegeverklaring ENSIA 2021 inzake informatiebeveiliging van Suwinet (hierna: collegeverklaring), inclusief de bijlage 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> onderzocht.

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

De collegeverklaring omvat het op 31 december 2021 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen voor Suwinet1. Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

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

<Alleen bij uitzonderingen >
Benadrukking aangelegenheden
Wij hebben vastgesteld dat de op de uitzonderingen gerichte beheersmaatregelen in verbeterplannen zijn opgenomen, zijn belegd en worden gemonitord. Ons onderzoek heeft zich niet gericht op de juistheid, volledigheid en uitvoering van de verbeterplannen. Deze aanvullende informatie is niet bedoeld om afbreuk te doen aan ons oordeel.

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

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

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

Beperking in gebruik en verspreidingskring
Dit assurance-rapport is bestemd voor gebruikers van de collegeverklaring. De collegeverklaring is opgesteld voor de gemeenteraad en voor het ministerie van Sociale Zaken en Werkgelegenheid (SZW) die toezien op de veiligheid van Suwinet. Doel van de collegeverklaring is om de gemeenteraad en het ministerie van Sociale Zaken en Werkgelegenheid (SZW) die toezien op de veiligheid van Suwinet te informeren over het in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen voor Suwinet. Ons assurance-rapport is derhalve uitsluitend bestemd voor de gemeenteraad en het departement dat toeziet op de veiligheid van Suwinet en dient niet te worden verspreid aan of te worden gebruikt door anderen.

Verantwoordelijkheden van het college van gemeente <naam gemeente>
Het college van burgemeester en wethouders van gemeente <naam gemeente> is verantwoordelijk voor het opstellen van de collegeverklaring. Voor het inschatten of de risico's van afwijkingen van materieel belang zijn in relatie tot Suwinet, zijn naast de collegeverklaring en dit assurance rapport ook de interne beheersingsmaatregelen van de gebruikers van de collegeverklaring relevant. De criteria waarvan bij het maken van deze verklaring gebruik werd gemaakt hielden in dat:
- de risico's die het bereiken van de geselecteerde normen voor Suwinet in gevaar brengen, werden geïdentificeerd; en
- de onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de vermelde interne beheersingsdoelstellingen niet zouden verhinderen.

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

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

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

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

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

Onze assurance-opdracht bestond onder andere uit:
- het verkrijgen van kennis omtrent de collegeverklaring en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen;
- het op basis van deze kennis inschatten van de risico's dat de collegeverklaring onjuistheden van materieel belang bevat;

- het reageren op de ingeschatte risico's, waaronder het ontwikkelen van een algehele aanpak, en het bepalen van de aard, de tijdsfasering en de omvang van verdere procedures;
- het uitvoeren van verdere procedures die duidelijk zijn gekoppeld aan de gesignaleerde risico's, waarbij gebruik wordt gemaakt van een combinatie van inspectie, waarnemingen ter plaatse en inwinnen van inlichtingen; en
- het evalueren van de toereikendheid van de assurance-informatie zoals opgenomen in de collegeverklaring en bijbehorende bijlage(n).

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

Format assurance-rapport met beperking

Assurance-rapport van de onafhankelijke IT-auditor
(Bij gebruik DigiD en Suwinet)

Uniek identificatienummer IT-auditor

Aan: <Opdrachtgever>

Ingevolge uw opdracht hebben wij de bijgevoegde collegeverklaring ENSIA 2021 inzake Informatiebeveiliging van DigiD en Suwinet (hierna: collegeverklaring), inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> onderzocht.

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

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

Onderzochte DigiD aansluitingen:

Aansluitnummer	Aansluitnaam

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

Ons oordeel met beperking
Naar ons oordeel is bijgevoegde collegeverklaring, inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente>, uitgezonderd de aangelegenheid beschreven in de sectie 'de basis voor ons oordeel met beperking', in alle van materieel belang zijnde aspecten, juist.

De collegeverklaring omvat het op 31 december 2021 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen voor DigiD en Suwinet. Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

De basis voor ons oordeel met beperking
<Beschrijf hier de basis voor het oordeel met beperking>
Een actueel voorbeeld: Het coronavirus heeft ook invloed op (de werkprocessen bij) de gemeente xxx en organisaties waarmee de gemeente samenwerkt. In het kader van onze werkzaamheden zijn wij niet in de gelegenheid geweest om voldoende en geschikte assurance-informatie te verkrijgen ten aanzien van de volgende aangelegenheden:

- *<beschrijving ontbrekende controle-informatie>*
-

Deze zijn van materieel belang in het kader van de oordeelsvorming over de collegeverklaring maar hebben hier geen diepgaande invloed op ons oordeel.

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

Wij hebben onze assurance-opdracht met betrekking tot de collegeverklaring verricht in overeenstemming met Richtlijn 3000-A (Herzien) 'Assuranceopdrachten door IT-auditors' van

NOREA. Deze assurance-opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Onze verantwoordelijkheden voor de assurance-opdracht betreffende de collegeverklaring'.
Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

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

<Alleen bij uitzonderingen >
Benadrukking aangelegenheden
Wij hebben vastgesteld dat de op de uitzonderingen gerichte beheersmaatregelen in verbeterplannen zijn opgenomen, zijn belegd en worden gemonitord. Ons onderzoek heeft zich niet gericht op de juistheid, volledigheid en uitvoering van de verbeterplannen. Deze aanvullende informatie is niet bedoeld om afbreuk te doen aan ons oordeel.

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

Verantwoordelijkheden van het college van gemeente <naam gemeente>
Het college van burgemeester en wethouders van gemeente <naam gemeente> is verantwoordelijk voor het opstellen van de collegeverklaring. Voor het inschatten of de risico's van afwijkingen van materieel belang zijn in relatie tot DigiD en Suwinet, zijn naast de collegeverklaring en dit Assurance rapport ook de interne beheersingsmaatregelen van de gebruikers van de collegeverklaring relevant. De criteria waarvan bij het maken van deze verklaring gebruik werd gemaakt hielden in dat:
- de risico's die het bereiken van de geselecteerde normen voor DigiD en Suwinet in gevaar brengen, werden geïdentificeerd; en
- de onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de vermelde interne beheersingsdoelstellingen niet zouden verhinderen.

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

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

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

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

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

Onze assurance-opdracht bestond onder andere uit:

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

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

Format assurance-rapport oordeelonthouding

Assurance-rapport van de onafhankelijke IT-auditor
(Bij gebruik DigiD en Suwinet)

Uniek identificatienummer IT-auditor

Aan: <Opdrachtgever>

Ingevolge uw opdracht hebben wij de bijgevoegde collegeverklaring ENSIA 2021 inzake Informatiebeveiliging van DigiD en Suwinet (hierna: collegeverklaring), inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> onderzocht.

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

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

Onderzochte DigiD aansluitingen:

Aansluitnummer	Aansluitnaam

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

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

De collegeverklaring omvat het op 31 december 2021 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen voor DigiD en Suwinet. Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel.

De basis voor onze oordeelonthouding
<Beschrijf hier de basis voor de oordeelonthouding>
Een actueel voorbeeld: Het coronavirus heeft ook invloed op (de werkprocessen bij) de gemeente <naam gemeente> en organisaties waarmee de gemeente samenwerkt. In het kader van onze werkzaamheden zijn wij niet in de gelegenheid geweest om voldoende en geschikte controle informatie te verkrijgen ten aanzien van de volgende aangelegenheden:

- *<beschrijving ontbrekende Assurance-informatie>*
-

Deze zijn van materieel belang en van diepgaande invloed in het kader van de oordeelsvorming over de collegeverklaring.

Beperking in gebruik en verspreidingskring

Dit assurance-rapport is bestemd voor gebruikers van de collegeverklaring. De collegeverklaring is opgesteld voor de gemeenteraad en voor de departementen die toezien op de veiligheid van DigiD en Suwinet. Doel van de collegeverklaring is om de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet te informeren over het in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigiD en Suwinet. Ons assurance-rapport is derhalve uitsluitend bestemd voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet en dient niet te worden verspreid aan of te worden gebruikt door anderen.

Verantwoordelijkheden van het college van gemeente <naam gemeente>
Het college van burgemeester en wethouders van gemeente <naam gemeente> is verantwoordelijk voor het opstellen van de collegeverklaring. Voor het inschatten of de risico's van afwijkingen van materieel belang zijn in relatie tot DigiD en Suwinet, zijn naast de collegeverklaring en dit assurance-rapport ook de interne beheersingsmaatregelen van de gebruikers van de collegeverklaring relevant. De criteria waarvan bij het maken van deze verklaring gebruik werd gemaakt hielden in dat:

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

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

Onze verantwoordelijkheden voor de assurance-opdracht betreffende de collegeverklaring
Onze verantwoordelijkheid is het geven van een oordeel over de collegeverklaring, inclusief de bijlagen 1 DigiD en 2 Suwinet waarnaar in de collegeverklaring wordt verwezen, van gemeente <naam gemeente> op basis van onze controle, verricht in overeenstemming met Richtlijn 3000-A (Herzien) 'Assuranceopdrachten door IT-auditors' van NOREA, Reglement Gedragscode ('Code of Ethics'), het Reglement Kwaliteitsbewaking en bijbehorende regelgeving van NOREA. Vanwege het belang van de aangelegenheid (<aangelegenheden>) beschreven in de paragraaf 'De basis voor onze oordeelonthouding' zijn wij niet in staat geweest om voldoende en geschikte assurance-informatie te verkrijgen om daarop ons oordeel te kunnen baseren.

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

Bijlage 8 Overwegingen ENSIA IT-Audit in samenwerkingsverbanden Suwinet

De uitgangspunten
De Verantwoordingsrichtlijn GeVS 2020 is volledig gebaseerd op de BIO. De gemeente geeft in de collegeverklaring aan in hoeverre wordt voldaan aan dit normenkader. Suwi-regelgeving vraagt van het gemeentebestuur een door een IT-auditor (RE) afgegeven assurance op de collegeverklaring. De Suwi-regelgeving steunt sterk op het principe van de horizontale verantwoording.

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

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

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

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

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

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

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

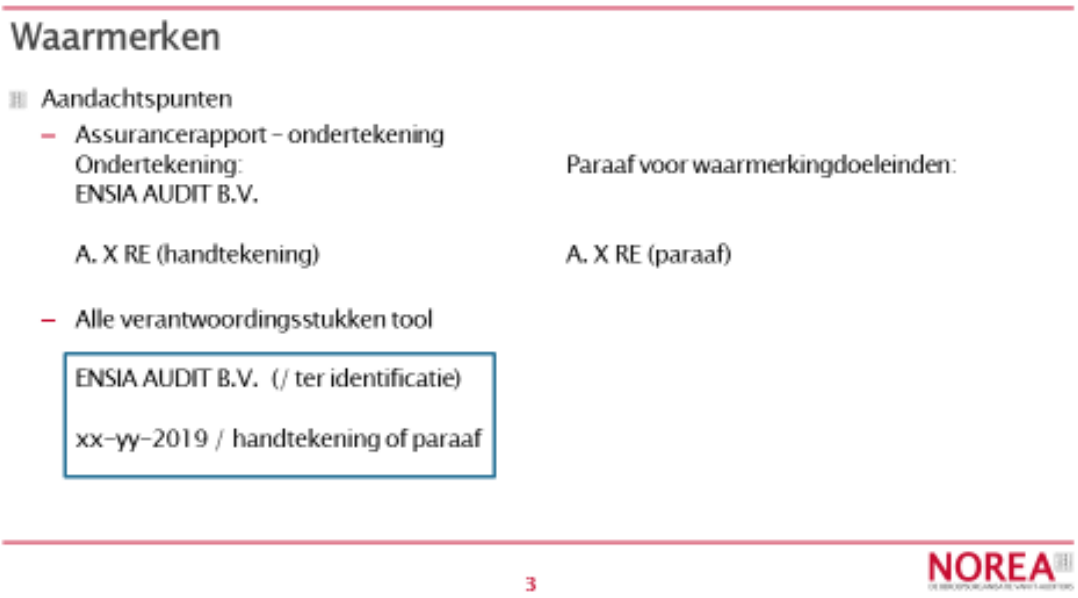
Bijlage 9 Waarmerken stukken

Het assurance-rapport moet een kenmerk (nummer) hebben van de auditorganisatie, de bijlage DigiD verwijst immers naar een kenmerk van het assurance-rapport (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.
- Het eenduidig identificeerbaar maken van de te waarmerken stukken. Dit geschiedt veelal door middel van het 'stempelen' van de betreffende stukken. Uit het waarmerk dient eenduidig te blijken dat de verantwoordelijke IT-auditor (en de organisatie) e.e.a. heeft uitgevoerd. Indien bij het waarmerken gebruik wordt gemaakt van ondertekening door middel van een paraaf dient deze eveneens toegevoegd te worden aan de ondertekening van het assurance-rapport.
- Bij gebruik van een gekwalificeerde handtekening moet het rapport worden opgeslagen in PDF/A-3 voor het embedden van de handtekening.

E.e.a. is in onderstaande illustratie nader uitgewerkt:



Bijlage 10 Begrippenkader

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

Penetratietest	Dit is een specifieke vorm van een vulnerability-assessment. Het is een proces waarbij met behulp van technische hulpmiddelen specifieke componenten of specifieke delen van de ICT-infrastructuur op zwakheden gecontroleerd worden. (NCSC) In de context van het DigiD assessment wordt met een penetratietest een technisch beveiligingsonderzoek bedoeld dat vanaf het internet wordt uitgevoerd door een (ervaren) penetratietester en waarbij scantools worden ingezet en aanvullende handmatige onderzoeks-werkzaamheden worden uitgevoerd.
SAAS leverancier	Een organisatie die een webapplicatie als online dienst aanbiedt waarbij de klanten de software niet hoeven aan te schaffen. De aanbieder draagt zorg voor onderhoud en doorontwikkeling van (de software van) de applicatie, hosting en applicatiebeheer.
Third Party Mededeling (TPM)	Een TPM is een 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 11 Afkortingenlijst

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