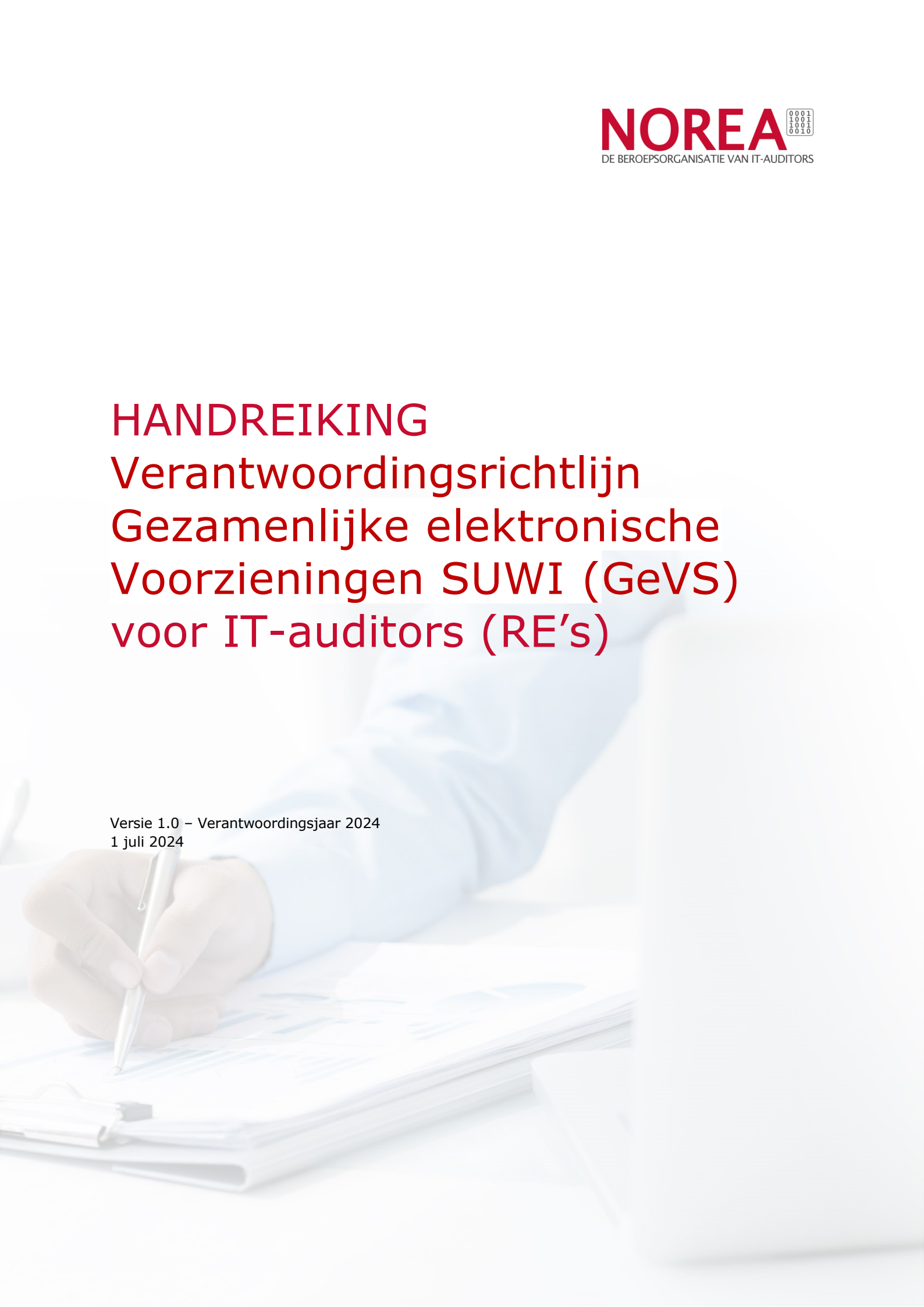
NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

HANDREIKING Verantwoordingsrichtlijn Gezamenlijke elektronische Voorzieningen SUWI (GeVS) voor IT-auditors (RE's)



Versie 1.0 – Verantwoordingsjaar 2024
1 juli 2024

1 Over deze handreiking Verantwoordingsrichtlijn Gezamenlijke elektronische Voorzieningen SUWI (GeVS) voor IT-auditors (RE's)

1.1 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 afgeven van assurance(-rapporten) bij verantwoordingen van partijen (anders dan gemeenten[1]) die gebruik maken van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS)[2].

In het kader van het afstemmen van verwachtingen wordt deze handreiking ook ter beschikking gesteld aan de bij Bureau Keteninformatisering Werk en Inkomen (BKWI) bekende GeVS partijen.

Voor vragen en opmerkingen kunt u zich wenden tot:

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

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

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

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

[1] Voor gemeenten geldt de verantwoording via de ENSIA-systematiek. Zie hiervoor de specifieke ENSIA-guidance van VNG (stelselbeheerder) en NOREA (Handreiking ENSIA voor IT-auditors (RE's).
[2] https://bkwi.nl/standaarden/ketenafspraken-ict-beheer

Versiebeheer

Versie	Datum	Toelichting
Versie 0.7	21 mei 2024	t.b.v. Domeingroep Privacy en Beveiliging SUWI / Vaktechnische Commissie NOREA
Versie 1.0	1 juli 2024	Vastgesteld NOREA

1.2 Aanleiding

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

Daartoe zijn nadere afspraken gemaakt over de informatiebeveiliging, over het te hanteren normenkader en de verantwoording over de naleving daarvan. Deze afspraken zijn vastgelegd in de Verantwoordingsrichtlijn Informatiebeveiliging GeVS (laatste versie 2022). Jaarlijks moeten afnemers van Suwinet-services zich verantwoorden over de informatiebeveiliging conform deze verantwoordingsrichtlijn. De Verantwoordingsrichtlijn GeVS 2022[1] beschrijft de scope en procedure van verantwoording voor alle partijen die gebruik maken van de GeVS.

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. In dit kader zijn nadere afspraken gemaakt over de toepassing van de Verantwoordingsrichtlijn GeVS 2022[2].

Gemeenten verantwoorden zich over het gebruik van Suwinet-services door middel van de Collegeverklaring ENSIA en bijbehorende bijlagen (meer in het bijzonder de bijlage Suwinet).

In ENSIA-verband is door NOREA reeds een Handreiking opgesteld voor de door IT-auditors (RE's) uit te voeren werkzaamheden in het kader van de Verantwoordingslijn GeVS. Zie voor nadere toelichtingen o.a. www.ensia.nl en www.norea.nl (Werkgroep ENSIA).

Ten behoeve van de niet-ENSIA partijen bestaat eveneens de behoefte om op overeenkomstige wijze invulling te geven aan de door IT-auditors (RE's) uit te voeren werkzaamheden, waarvoor deze handreiking is opgesteld.

1.3 Achtergrond en doelstelling

De Suwi-partijen bepalen gezamenlijk voor de GeVS het niveau van informatiebeveiliging. E.e.a. wordt neergelegd in de Verantwoordingsrichtlijn GeVS.

Vanaf 1 januari 2020 geldt de Baseline Informatiebeveiliging Overheid (BIO). De BIO vervangt onder meer de BIG en de BIR en voorziet in een uniform en uitgebreid normenkader informatiebeveiliging voor de gehele overheidssector. Organisaties die de BIO (moeten) implementeren werken daarmee aan het verzekeren van een adequaat niveau van informatiebeveiliging. Het Ketenoverleg heeft besloten dat vanaf 2020 dit niveau gebaseerd wordt op het normenkader van de BIO en verantwoording op basis daarvan moet plaatsvinden. Iedere partij verantwoordt zich in het eigen jaarverslag en levert voor 1 mei van het kalenderjaar volgend op het verantwoordingsjaar een Transparantierapportage op aan BKWI.

BKWI maakt aan de hand van alle Transparantierapportages van betrokken partijen een Totaalrapportage op ten behoeve en onder verantwoordelijkheid van het Ministerie SZW. Aan de hand van de inhoud van de Totaalrapportage kan het Ministerie SZW beoordelen worden of de informatiebeveiliging binnen de GeVS adequaat is en of alle afnemers voldoen aan het afgesproken beveiligingsniveau, dat is neergelegd in de specifiek van toepassing zijnde normen uit de BIO. Deze Handreiking is gebaseerd op de Verantwoordingsrichtlijn GeVS 2022.

[1] https://bkwi.nl/standaarden/privacy-beveiliging/verantwoordingsrichtlijn-gevs-2022-v10

[2] Beperking verantwoordingsverplichting tot verantwoording over opzet en bestaan maatregelen per 31-12 van het verslagjaar.

Doelstelling van deze Handreiking is om de auditors van de hierboven genoemde partijen een kader te geven voor de van hen gevraagde werkzaamheden ten behoeve van het afgeven van een assurance-rapport bij de Verantwoording GeVS.

De beheerders van GeVS (BKWI en Inlichtingenbureau (IB)) verantwoorden zich voor 15 maart van het kalenderjaar volgend op het verantwoordingsjaar op het normenkader van de BIO. De onderhavige Handreiking kan ook bij de controlewerkzaamheden met betrekking tot de verantwoording van de beheerders worden toegepast.

2 Handreiking

Doelstelling van deze Handreiking is om de auditors van de hierboven genoemde partijen een kader te geven voor de van hen gevraagde werkzaamheden ten behoeve van het afgeven van een assurance-rapport bij de Verantwoording GeVS. Dit kader geldt voor controlejaar 2024. 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 om aanvullende vereisten op de geldende standaarden af te leiden.

Bij verschillen van inzicht tussen partijen rond de interpretatie van de GeVS is het primair aan de betrokken partijen waaronder direct betrokken auditor(s) om in overleg tot een oplossing te komen. (Vertegenwoordigers van) NOREA kunnen daarbij eventueel als gesprekspartner deelnemen, altijd vanuit het perspectief van GeVS (dus gericht op het geven van assurance). Voor substantiële meningsverschillen heeft de NOREA een consultatieprocedure vastgesteld. Zie paragraaf 2.16 Consultatie).

2.1 Verantwoordingsproces

<u>Verantwoordelijkheden aangesloten partijen</u>
In het kader van de verantwoordingsrichtlijn GeVS gelden de navolgende specifieke verantwoordelijkheden voor de aangesloten partijen:

- Elke verantwoordingsplichtige partij is verantwoordelijk voor het opstellen van een transparantierapportage over het verslagjaar (1-1 t/m 31-12). De Transparantierapportage bestaat uit[1]:
    - Een In Control Verklaring (ICV) van de bestuurder;
    - Een bijlage met een overzicht van de normen waaraan niet voldaan wordt[2].
    - Een getrouwheidsverklaring van een Register EDP-auditor (hierna IT-auditor) (in de vorm van een assurance-rapport)
- De transparantierapportage en het assurance-rapport worden voor 1 mei van het kalenderjaar volgend op het verantwoordingsjaar aangeboden aan BKWI.

De 'In control verklaring van de bestuurder' en de bijlage met het overzicht van de normen waaraan niet voldaan wordt (hierna bijlage, gezamenlijk ook aangeduid als Verantwoording GeVS) vormen daarmee het object van controle voor de IT-auditor. Dit is de 'assertion based' benadering kenmerkend voor GeVS. De IT-auditor zal zich daarbij mede richten op de inhoud van de genoemde stukken en de door de aangesloten partij verzamelde ondersteunende informatie ten behoeve van de assurance-werkzaamheden gericht op de Verantwoording GeVS. 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.

[1] Zie ook: https://bkwi.nl/standaarden/privacy-beveiliging/verantwoordingsrichtlijn-gevs-2022-v10 bladzijde 3

[2] De 'In Control Verklaring (ICV) van de bestuurder' en de bijlage met een overzicht van de normen waaraan niet voldaan wordt vormen gezamenlijk de Verantwoording GeVS.

Verantwoordelijkheden IT-auditor
De IT-auditor dient ervoor te zorgen dat de betreffende documenten door hem gewaarmerkt zijn. Dit betreft de Verantwoording GeVS (zie Bijlage 1). Zie ook bijlage 6 voor het elektronisch ondertekenen van het assurance-rapport en het elektronisch 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 Verantwoording GeVS (o.a. (voor-) bespreking met ambtelijk verantwoordelijken, portefeuillehouder(s) en behandeling in bestuur aangesloten partij).

De IT-auditor dient erop toe te zien dat de aangesloten partij de door hem getekende c.q. gewaarmerkte documenten op de juiste wijze aanlevert aan BKWI in het kader van het verantwoordingsproces.

2.2 Uitvoeren werkzaamheden door de IT-auditor

Voor de IT-auditor verandert ten aanzien van zijn verantwoordelijkheid voor het goed voorbereiden, inrichten en uitvoeren van zijn audit niets.

Hoewel de Verantwoording GeVS het object van controle vormen, is de door de aangesloten partij gedocumenteerde ondersteunende assurance-informatie voor de IT-auditor het basismateriaal waar elke IT-auditor vanuit dient te gaan en wat als assurance-informatie geldt 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 documentatie / basismateriaal. Hierbij dient hij ook kennis te nemen van de relevante onderdelen van de verantwoordingsprocessen bij aangesloten partijen (denk aan het bepaalde in artikel 5.22 en 6.4 van de Regeling Suwi of andere wet- en regelgeving) 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[1].

De opdracht bestaat met name uit het uitvoeren van procescontroles. De procescontroles geven de IT-auditor de mogelijkheid ook -en met name tussentijds- te beoordelen of de opgeleverde resultaten voldoen aan daaraan te stellen eisen. Daarbij valt te denken aan de 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 aangesloten partij tijdig in de gelegenheid wordt gesteld verbeteringen door te voeren. De IT-auditor is daarbij niet inhoudelijk betrokken ter voorkoming van zelftoetsing.

2.3 Formele aspecten van de assurance-opdracht

Een GeVS-audit betreft een assurance-opdracht gericht op het geven van een oordeel met een redelijke mate van zekerheid, conform Richtlijn 3000 A (Attestopdracht). Het bestuur van de aangesloten partij komt met een 'In control verklaring' en bijlage waarover de IT-auditor met redelijke mate van zekerheid een oordeel geeft. Beoogde gebruikers van deze rapportage en het assurance-rapport (oordeel) van de IT-auditor zijn BKWI en het Ministerie van SZW die toezien op de informatiebeveiliging in het kader van GeVS. De uitvoering van de GeVS-audit dient in opdracht van het bestuur van de aangesloten partij plaats te vinden.

Doel van de GeVS-audit is het verkrijgen van voldoende geschikte assurance-informatie om een oordeel met redelijke mate van zekerheid te verschaffen of de Verantwoording GeVS van de aangesloten partij, in alle van materieel belang zijnde aspecten, juist is. Hierbij zijn de eisen vanuit de Suwi-regelgeving inclusief de Verantwoordingsrichtlijn GeVS (versie 2022) leidend.

[1] Richtlijn 3000 – par. 50: Bij het opzetten en uitvoeren van werkzaamheden dient de IT-auditor de relevantie en betrouwbaarheid van de informatie die gebruikt zal worden als assurance-informatie in overweging te nemen.

De criteria voor een GeVS IT-audit betreffen de normen Suwinet (Verantwoordingsrichtlijn GeVS 2022 – nader uitgewerkt in Bijlage 2). De criteria worden ook in de Verantwoording GeVS kenbaar gemaakt en zijn daarmee toegankelijk voor de gebruikers.

Het gaat om opzet en bestaan van de maatregelen per 31 december van het verslagjaar en de werking over de periode 1 januari tot en met 31 december van het verslagjaar. Eventuele veranderingen / verbetermaatregelen in de periode tussen 31 december 2021 en de datum van afgeven van het assurance-rapport dient het bestuur van de aangesloten partij in principe in de Verantwoording GeVS toe te lichten[1]. De verbetermaatregelen / het verbeterplan betrekt de auditor in zijn onderzoek.

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 van de aangesloten partij is dit een risico ten aanzien van het fundamentele beginsel objectiviteit (inclusief onafhankelijkheid). Idem voor actieve betrokkenheid bij de uitvoering van bij werkzaamheden die leiden tot het opstellen van de Verantwoording GeVS door het bestuur van de aangesloten partij.

2.5 Pre-audit GeVS

De Verantwoordingsrichtlijn GeVS is minimaal beschikbaar voor de aangesloten partijen in de loop van het jaar voorafgaand aan het verslagjaar. De IT-audit vindt (veelal pas) plaats nadat de Verantwoording GeVS is opgesteld door de aangesloten partij. De aangesloten partij heeft echter vaak de behoefte om tussentijds een terugkoppeling te ontvangen van de IT-auditor over de status van GeVS binnen de organisatie. Het advies is om een zogenaamde pre-audit af te spreken en uit te voeren waarbij de IT-auditor de normen tussentijds toetst, het proces van oplevering beoordeelt en de uitkomsten rapporteert aan het bestuur van de aangesloten partij. De aangesloten partij wordt op deze wijze in de gelegenheid gesteld de nodige verbeteringen door te voeren alvorens de Verantwoording GeVS definitief wordt opgesteld.

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

2.6 Opdrachtaanvaarding en continuering

Vereisten vanuit de Richtlijn Opdrachtaanvaarding van NOREA zijn onverkort van toepassing. Het object van onderzoek betreft in brede zin informatiebeveiligingsaspecten. Competentie en capaciteit van de IT-auditor op dit terrein is dan ook een randvoorwaarde. Ervaring met het uitvoering van GeVS-audits alsmede kennis van het domein van de aangesloten partij 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 Verantwoording GeVS en het assurance-rapport (o.a. als gevolg van de Wet open overheid) dient voor GeVS-audits expliciet een opdrachtgerichte kwaliteitsbeoordeling (OKB) overwogen te worden. Hierbij is een eenduidig gedocumenteerde risico-inschatting van de audit-organisatie leidend. De auditor dient de overwegingen ter zake in het dossier vast te leggen.

Een opdrachtgerichte kwaliteitsbeoordeling omvat in het algemeen een bespreking met de voor de opdracht verantwoordelijke beroepsbeoefenaar, een onderzoek van de verantwoording en bijbehorende documentatie dat object van het onderzoek is en van het assurance-rapport en in het bijzonder de juistheid daarvan. Het omvat ook het onderzoeken van geselecteerde dossierstukken die betrekking hebben op de belangrijke standpunten die het opdrachtteam heeft ingenomen en de

[1] Teneinde de uniformiteit en eenduidigheid van de Verantwoording GeVS te waarborgen kan e.e.a. ook in het verbeterplan van de aansluithouder (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.

eindoordelen en adviezen die zijn gevormd. De OKB moet zijn afgerond voordat het rapport wordt afgegeven. Zie verder ook NOREA Handreiking opdrachtgerichte kwaliteitsbeoordeling[1].

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 GeVS-opdracht is gezien het feit dat het onderdelen van en / of verbonden aan de Rijksoverheid 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 het te controleren objecten (GeVS aansluiting);
- Interne Controle Risico: betreft een inschatting van de kwaliteit van de beheeromgeving van de aangesloten bij de totstandkoming van de 'In control verklaring' en de bijlage;
- Detectierisico: is de resultante en stelt eisen aan de kwaliteit van de eigen auditorganisatie en de aard en omvang van de auditwerkzaamheden 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 rond het gebruik van Suwinet op Midden tot Hoog worden ingeschat zal het DR Midden tot Laag moeten zijn. De auditor dient de uit te voeren auditwerkzaamheden in de vorm van gegevensgerichte werkzaamheden hiervoor vast te stellen.

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

2.9 Het verkrijgen van assurance-informatie

De Verantwoording GeVS komt tot stand onder verantwoordelijkheid van en binnen beheeromgeving van de aangesloten partij. De hier bedoelde processen kunnen 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 de aangesloten partij is verzameld[2]. 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 het verantwoordingsproces van de aangesloten partij 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, bestaan en werking voldaan wordt aan de desbetreffende norm.

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

Onderdeel van de assurance-informatie is het verkrijgen van een schriftelijke bevestiging van de verantwoordelijke partij met een zo recent als mogelijke datum, voorafgaand aan de datum van het assurance-rapport. Zie ook paragraaf 2.11.

---

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

[2] Uitgangspunt is dat de zelfevaluatie (lees 'In control verklaring' en bijlage zijn gebaseerd op / onderbouwd worden door relevante documentatie. Deze dient door de aansluithouder op een systematische wijze vastgelegd en gedocumenteerd te worden.

2.10 Uitbesteding door aangesloten partijen

Bij uitbesteding van werkzaamheden door aangesloten partijen zijn de volgende situaties voorzien:

- Volledige uitbesteding van de betreffende werkprocessen
- Gedeeltelijke uitbesteding van de betreffende werkprocessen en / of ondersteunende (IT-) processen.

Aangesloten partijen 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 organisatie en dienen daarover verantwoording af te leggen overeenkomstig de Verantwoordingsrichtlijn GeVS.

Dit betekent dat de IT-auditor zich met betrekking tot GeVS 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.

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 GeVS-audit.

Werkzaamheden auditor
Bij uitbesteding door de aangesloten partij 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 Richtlijn / ISAE 3402) verzorgt dat betrekking heeft op de in het kader van GeVS gestelde normen. In dit geval wordt de carve-out benadering gevolgd.

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

De (GeVS-) auditor van de aangesloten partij dient hiervoor de vaktechnische verantwoordelijkheid te kunnen nemen. De auditor 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 GeVS-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].

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 GeVS onvoldoende.

Verbeterplannen
Het ministerie van SZW en BKWI hebben ten behoeve van het toezicht op de naleving van de regels omtrent het gebruik van Suwinet een 'toezichtsarrangement' uitgewerkt. Door aansluithouders geformuleerde verbeterplannen maken hier een belangrijk onderdeel van uit.

Hoewel de IT-auditor geen oordeel geeft over de toereikendheid (en uitvoering) van het verbeterplan van de aangesloten organisatie naar aanleiding van eventuele bevindingen / tekortkomingen, is het wenselijk dat hij verifieert of de door of bij de aangesloten partij gesignaleerde bevindingen geadresseerd zijn, realistisch zijn en opgenomen in het verbeterplan. Eventuele bevindingen /

[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.

tekortkomingen dienen onder de aandacht van de opdrachtgever gebracht te worden zodat deze, onder verantwoordelijkheid van het bestuur, betrokken worden in de uitwerking van het verbeterplan en, waar nodig, de Verantwoording GeVS.

2.11 Schriftelijke bevestiging (letter of representation)

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

Deze omvat:
- Een herbevestiging van de Verantwoording GeVS;
- 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 Verantwoording GeVS alsmede de assurance die daarbij wordt afgegeven.

2.12 Het vormen van het oordeel

Bij het vormen van het oordeel zijn het stramien voor assurance-opdrachten en Richtlijn 3000 leidend.

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

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

In die gevallen waarin naar de mening van de IT-auditor de Verantwoording GeVS een getrouw beeld geeft van de informatiebeveiliging (rond GeVS) bij de aangesloten partij 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 Verantwoording GeVS, brengt de IT-auditor in het assurance-rapport dit tot uitdrukking in een paragraaf ter benadrukking van aangelegenheden. Zie hiervoor Richtlijn 3000 paragraaf 77b.

2.13 Wegingskader

Bij door oordeelsvorming door de IT-auditor in het kader van de uitgevoerde assurance-werkzaamheden gelden de volgende uitgangspunten:

a. Er wordt een assurance-rapport afgegeven met een oordeel over de Verantwoording GeVS als geheel.

b. Er wordt een oordeel afgegeven met een redelijke mate van zekerheid dat de Verantwoording GeVS als geheel geen onjuistheden van materieel belang bevat. Indien dit begrip ten behoeve van het statistische technieken moet worden gekwantificeerd, dient een betrouwbaarheid van 95% te worden gehanteerd. Zie Bijlage 4 voor een nadere uitwerking van dit uitgangspunt.

c. De oordeelsvorming vindt stapsgewijs plaats. Hierbij worden de volgende uitgangspunten gehanteerd:
    a. De IT-auditor bepaalt een oordeel per norm die in de werkzaamheden zijn betrokken. Zie hiervoor Bijlage 2 (relevante normen) en Bijlage 3 (handreiking werkzaamheden).

b. Voor alle individuele normen waarbij een kwantitatief oordeel mogelijk is geldt de volgende materialiteit voor fouten en onzekerheden gezamenlijk[1]:

	Goedkeurend oordeel	Oordeel met beperking	Oordeelonthouding / afkeurend oordeel
Onzekerheden in de audit & fouten in verantwoording	<= 2%	> 2% - <= 4%	> 4%

c. Een niet goedkeurend oordeel op elk van de navolgende normen leidt tot een niet goedkeurend oordeel (afkeurend oordeel) over het geheel van de verantwoording (zie hiervoor ook Bijlage 2 totaaloverzicht normen):

6. Organiseren van informatiebeveiliging	6.1.1	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
9. Toegangsbeveiliging	9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
9. Toegangsbeveiliging	9.2.2	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
9. Toegangsbeveiliging	9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
9. Toegangsbeveiliging	9.2.6	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
12. Beveiliging bedrijfsvoering	12.1.2	Wijzigingsbeheer: Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.
12. Beveiliging bedrijfsvoering	12.1.4	Logbestanden van gebeurtenissen die gebruikers-activiteiten, uitzonderingen en Informatiebeveiligings-gebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

[1] Materialiteit ziet op de vereiste nauwkeurigheid die de IT-auditor in zijn werk dient te hanteren; Hieruit volgt wat het effect is van de door de IT-auditor geconstateerde afwijkingen (fouten of onzekerheden) op zijn oordeel. Gepresenteerde grenzen ontleend aan materialiteitsbepaling geldig bij de Rijksoverheid en direct daaraan gelieerde organisaties (basis voor werkzaamheden Auditdienst Rijk / Algemene Rekenkamer).

12. Beveiliging bedrijfsvoering	12.4.1	Logbestanden van gebeurtenissen die gebruikers-activiteiten, uitzonderingen en informatiebeveiligings-gebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
12. Beveiliging bedrijfsvoering	12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
18. Naleving	18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

d. Het oordeel over de Ín control verklaring en de bijlage als geheel is onderwerp van professionele ooordeelsvorming van de IT-auditor. Hierbij mag het oordeel geen positievere strekking hebben dan het oordeel op de hiervoor onder c. benoemde normen individueel.

   Hierbij dient, bij eventuele noodzaak tot aanpassing afwijking van het goedkeurende oordeel, het navolgende schema als leidraad dienen:

Aard van de aangelegenheid die tot aanpassing leidt	**De oordeelsvorming van de IT-auditor over de (diepgaande) invloed van de gevolgen van het ontbreken van geschikte informatie of de mogelijke gevolgen voor de verantwoording**	
	Van materieel belang maar zonder diepgaande invloed	**Van materieel belang en met diepgaande invloed**
Verantwoording bevat een afwijking van materieel belang	Oordeel met beperking	Afkeurend oordeel
Geen mogelijkheid om voldoende en geschikte controle-informatie te verkrijgen	Oordeel met beperking	Oordeelonthouding

2.14 Het opstellen van het assurance-rapport

Voor de GeVS-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.

In Bijlage 5 zijn de formats assurance-rapporten opgenomen. Hieraan zijn, ook voorbeeldteksten toegevoegd voor een oordeel met beperking / een afkeurend oordeel en de oordeelonthouding.

Bij het door de IT-auditor ondertekende assurance-rapport wordt ook de door de IT-auditor gewaarmerkte Verantwoording GeVS gevoegd. Deze set wordt door de aangesloten partij gebruikt in het kader van het afleggen van verantwoording aan BKWI (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 beheersingsmaatregelen en de resultaten daarvan.

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

2.15 Overige rapportages

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

2.16 Consultatie

Indien een auditor[1] in het kader van de uitvoering van GeVS-opdrachten wil afwijken van Handreikingen / formats voorgeschreven door stelselhouder(s) / stelselbeheerder(s) / toezichthouder(s) of van de onderhavige Handreiking dient de auditor dit tijdig af te stemmen met NOREA.

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

De uitkomsten van de beoordeling worden meegedeeld aan de auditor en zijn bindend voor alle betrokken partijen bij de verdere uitvoering van zijn werkzaamheden.

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

2.17 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 dossiers van de aangesloten partij (opdrachtgever) is niet toegestaan.

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

3 Tot slot

De GeVS-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 GeVS-audit geen specifiek onderzoek op uit.

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

4 Bijlagen

Bijlage 1: Format Verantwoording GeVS ('In control verklaring' en bijlage)

Verantwoording inzake de beheersing gegevensuitwisseling SUWI 20*XX* Ingevolge artikel 6.4 Regeling SUWI

Het bestuur van <naam organisatie> geeft met deze verklaring inclusief de bijlage aan in hoeverre <naam organisatie> aan het normenkader GeVS (bijlage 1 van de Verantwoordingsrichtlijn GeVS 20**XX**)[1] voor <afnemers/beheerders> voldoet.

Reikwijdte verklaring
Deze verklaring betreft de verwerkingen van SUWI-gegevens en het gebruik van ondersteunende ICT-voorzieningen door <naam organisatie>, waarover assurance wordt gevraagd van een Register EDP-auditor. De verklaring omvat het gedurende het verantwoordingsjaar <jaartal> in opzet, bestaan en werking voldoen van de beheersingsmaatregelen aan het normenkader GeVS. De normen zijn geschikt voor het doel van deze verklaring. Deze verklaring is opgesteld ten behoeve van de totaalrapportage die door het ketenoverleg aan de minister van SZW wordt aangeboden.

Verklaring bestuurder
<Indien volledig wordt voldaan de normen: De bestuurder verklaart dat bij <naam organisatie> in voor <jaartal> de beoogde en ingerichte beheersingsmaatregelen voldoen aan het normenkader GeVS.> <Bij uitzonderingen: De bestuurder verklaart dat niet aan alle geselecteerde normen in het normenkader GeVS wordt voldaan. De op de uitzonderingen gerichte beheersmaatregelen zijn in een verbeterplan opgenomen, zijn belegd en worden gemonitord>.

[Plaats, datum]

[Bestuurder]

Bijlage: Bijlage Verantwoording inzake de beheersing gegevensuitwisseling SUWI 20*XX* Ingevolge artikel 6.4 Regeling SUWI

[1] Actuele Verantwoordingsrichtlijn GeVS geldig voor 2024 is Verantwoordingsrichtlijn GeVS 2022

Bijlage Verantwoording inzake de beheersing gegevensuitwisseling SUWI 20*XX* Ingevolge artikel 6.4 Regeling SUWI

Deze bijlage is een afzonderlijk onderdeel van de Verantwoording inzake de beheersing gegevensuitwisseling SUWI 20*XX* Ingevolge artikel 6.4 Regeling SUWI van <naam organisatie>. Deze verklaring heeft betrekking op het in het verantwoordingsjaar <jaartal> in opzet, bestaan en werking voldoen van de beheersingsmaatregelen van het normenkader GeVS 20XX. Deze bijlage is opgesteld ten behoeve van de totaalrapportage die door het ketenoverleg aan de minister van SZW wordt aangeboden.

Onderwerp van de verklaring is het <gebruik / beheer> van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS).

Normnaleving

<indien geen afwijkingen van de normen:

Zoals in de bestuurdersverklaring vermeld, voldoen de interne beheersmaatregelen inzake de GeVS voor het verantwoordingsjaar <jaartal> in opzet, bestaan en werking aan alle normen.>

<bij afwijkingen van de normen:

Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de GeVS voor verantwoordingsjaar <jaartal> in opzet, bestaan en werking aan alle normen:

Control/maatregel nummer BIO	Applicatie
…	<Suwinet-Inkijk> of <Suwinet-Inlezen in combinatie met <naam inleesapplicatie>>

Bijlage 2: Normenkader GeVS 2022

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

Hoofdstuk	Nummer	Normen
5. Informatiebeveiligings-beleid	5.1.1.	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
5. Informatiebeveiligings-beleid	5.1.2	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
6. Organiseren van informatiebeveiliging	6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.
6. Organiseren van informatiebeveiliging	6.1.2	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
7. Veilig personeel	7.2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
9. Toegangsbeveiliging	9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
9. Toegangsbeveiliging	9.2.2	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
9. Toegangsbeveiliging	9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
9. Toegangsbeveiliging	9.2.6	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
10. Cryptografie	10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en Geïmplementeerd.
12. Beveiliging bedrijfsvoering	12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.
12. Beveiliging bedrijfsvoering	12.1.2	Wijzigingsbeheer: Veranderingen in de organisatie, bedrijfs-processen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.
12. Beveiliging bedrijfsvoering	12.1.4[1]	Scheiding van ontwikkel-, test- en productieomgevingen: Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.

[1] In overleg met Domeingroep / VNG / NOREA toegevoegd

12. Beveiliging bedrijfsvoering	12.4.1[1]	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
12. Beveiliging bedrijfsvoering	12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	14.2.2[2]	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework.
18. Naleving	18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

[1] Idem

[2] Idem

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

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
5. Informatiebeveiligingsbeleid			
5.1.1 Beleidsregels voor informatiebeveiliging	Criterium BIO: Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. Doelstelling: Richting geven aan en handhaven van beveiliging van de Suwinet aansluiting en de gegevens die worden getransporteerd en ervoor te zorgen dat aansluiting van de 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, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen 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.	Betrokken partij(en): Organisatie / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: De Organisatie 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. Diepgang: Opzet en bestaan Test aanpak: Inspectie van het informatiebeveiligingsbeleid. Deze dient inzicht te geven in de in 5.1.1.1 genoemde type maatregelen voor de beveiliging van de eigen delen van Suwinet (bijv. organisatorische-, technische- en beheersingsmaatregelen). Stel vast dat het beleid is vastgesteld* door de leiding van de organisatie (het dagelijks bestuur). Stel vast dat het beleid is gepubliceerd en gecommuniceerd aan medewerkers en relevante partijen.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
		f) De bevordering van het beveiligingsbewustzijn.	Interview de verantwoordelijke functionarissen. **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): Organisatie / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: Het Suwinet informatiebeveiligingsbeleid (eventueel als onderdeel van het algehele informatiebeveiligingsbeleid) dient actueel te zijn en periodiek* te worden beoordeeld en zo nodig te worden bijgesteld bij grote wijzigingen of aan de hand van externe ontwikkelingen. **Note: Hiervoor geldt dat de periodiciteit aansluit bij de (bestaande) bestuurs- en P&C-cycli. Voor overheidsorganisaties geldt doorgaans dat dit een periode (4 jaar) is.* **Note: Sluit hierbij aan op het voor de organisatie vastgestelde beleid ten aanzien van periodieke beoordeling van het (specifieke Suwi-) beveiligingsbeleid.*

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
			Diepgang: Opzet, bestaan en werking van beheersmaatregelen. Test aanpak: Inspectie van het informatiebeveiligingsbeleid. Stel minimaal jaarlijks vast dat het beleid aantoonbaar actueel is en conform de (bestaande) bestuurs- en P&C-cycli is bijgesteld. Beoordeel hierbij ook of er sprake is van significante (beleids-) wijzigingen die van invloed zijn op het (eventueel tussentijds) bijstellen van het informatiebeveiligingsbeleid. Interview de verantwoordelijke functionarissen.
6. Organiseren van informatiebeveiliging			
6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	Criterium BIO: Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. Doelstelling: Het voorkomen dat risico's optreden als gevolg van het ontbreken van coördinatie op het gebied van activiteiten aangaande de bescherming van de eigen delen van Suwinet. *Risico:* *Het risico bestaat dat door gebrek aan coördinatie van activiteiten niet op beveiligingsincidenten wordt geacteerd en dat door wijzigingen nieuwe kwetsbaarheden ontstaan.*	6.1.1.1 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	Betrokken partij(en): Organisatie / 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.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
		Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	Diepgang: Opzet, bestaan en werking van de beheersmaatregelen. Test aanpak: Inspecteer het informatiebeveiligingsbeleid en stel minimaal jaarlijks vast dat taken, bevoegdheden en verantwoordelijkheden (CTFS) ten aanzien van de IB-functie t.a.v. Suwinet formeel zijn vastgesteld en stel vast dat deze functie en onderliggende rol(-len) ook als zodanig zijn ingericht* en beschreven. **Note: Idealiter zijn bovenstaande documenten onderdeel van een ingerichte AO/IB. Het gaat onder meer om de Suwi gebruikersbeheerder(s), de security officer(s) Suwi en Suwi gemandateerden.* Zie ook 12.4.1. Incidentmanagementproces (als onderdeel van informatiebeveiligingsbeleid) Interview de verantwoordelijke functionarissen.
6.1.2 Scheiding van taken	Criterium BIO: Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. Doelstelling: Ervoor zorgen dat de juiste taken en verantwoordelijkheden binnen de onderkende rollen juist worden uitgevoerd met inachtneming van de juiste	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): Organisatie / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd (in de vorm van bijvoorbeeld een RACI-matrix*).

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
	functiescheiding voor zover de organisatiegrootte dit toelaat. *<u>Risico:</u>* *Onduidelijke taken en verantwoordelijkheden en het ontbreken van juiste functiescheiding kunnen leiden tot:* *- misbruik van bevoegdheden,* *- te ruim toegekende bevoegdheden,* *- over het hoofd zien van en/of tot implementatie van tegenstrijdige beveiligingsmaatregelen.*		**Note: RACI staat voor Responsible, Accountable, Consulted en Informed. Idealiter onderdeel van een ingerichte AO/IB.* **Note: De taken, verantwoordelijkheden en bevoegdheden van de betrokken Suwinet functionarissen zijn beschreven in (een) autorisatiematrix(ces), daarbij is rekening gehouden met conflicterende rollen zoals:* • *t.a.v. invoerende en controlerende taken;* • *Beheer Suwinet versus Security officer Suwinet;* • *Beheerder(s) Suwinet/ Security officer Suwinet versus medewerkers met Suwinet inkijk en SUWI-inlezen rechten;* • *Autoriseren van toewijzing van toegang tot Suwinet gerelateerde gegevens;* • *Controleren van rechtmgebruik van Suwinet gerelateerde gegevens;* • *Controleren van de actualiteit van de gebruikersadministratie;* • *Melding van incidenten gerelateerd aan Suwinetgegevens;* De gedocumenteerde rollen zijn door het dagelijks bestuur/ de directie (dit kan per organisatie 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 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
			Diepgang: Opzet, bestaan en werking van de beersingsmaatregelen. Test aanpak: Inspecteer de relevante functie/taakbeschrijvingen van met name de sleutelfunctionarissen, de autorisatiematrix en het autorisatiebeheerproces, en stel vast dat deze voldoen aan bovenstaande aandachtspunten. Stel vast dat functionarissen benoemd zijn en actief invulling geven aan hun rol. Inspecteer of in de organisatie gedurende de gehele verslagperiode verbijzonderde interne controle heeft plaatsgevonden op blijvende handhaving van de vastgestelde inrichting van de AO/IB. Selecteer conform de tabel steekproefomvang het juiste aantal registraties van (personele en/of functionele) mutaties in de vastgestelde AO/IB en stel vast dat deze voldoen aan de vastgestelde criteria. 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.	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	Betrokken partij(en): Organisatie / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
	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.*	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.	Toelichting: a) 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. b) De organisatie moet in dit kader waarborgen scheppen die ervoor zorgen dat gebruikers hun gebruikersidentificaties niet delen met andere gebruikers. Bij voorkeur is dit opgenomen in de gedragsregels. Diepgang: Opzet, bestaan en werking van maatregelen rond bewustzijn, opleiding en training ten aanzien van informatiebeveiliging. 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[18]) aandacht wordt besteed aan bewustwording van informatiebeveiliging waarbij expliciet aandacht wordt besteed aan Suwi gerelateerde onderwerpen. Stel vast dat deze bewustwordingswerkzaamheden daadwerkelijke ten uitvoer zijn gebracht.

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

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
			Selecteer conform de tabel steekproefomvang het juiste aantal (nieuwe) gebruikers vast die toegang hebben tot Siwinet gegegeven en stel dat deze medewerkers 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	<u>Criterium BIO:</u> Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. <u>Doelstelling:</u> Gebruikers en beheerders de juiste toegangsrechten geven (niet meer en niet minder) dan welke nodig zijn voor de hen opgedragen (wettelijke)taken. *<u>Risico:</u>* *Het risico bestaat dat medewerkers onrechtmatig toegang hebben tot Suwinet of tot de via Suwinet beschikbaar gestelde gegevens.* *Voor Suwinet geldt een verhoogd risico omdat het Suwinet account van een organisatie ook toegang tot Suwinet kan*	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.	<u>Betrokken partij(en):</u> Organisatie / samenwerkingspartij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD * Let op: Voor Suwinet Inlezen is de database in scope. <u>Toelichting:</u> Beheersmaatregelen 9.2.1, 9.2.2, 9.2.5 en 9.2.6 hangen nauw met elkaar samen: 9.2.1 richt zich op de registratie en het afmelden van gebruiker 9.2.2 richt zich op het proces van het toekennen van rechten aan gebruikers

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
	krijgen vanuit het domein van een ander op Suwinet aangesloten organisatie.		9.2.5 richt zich op het periodiek beoordelen van toegangsrechten van gebruikers 9.2.6 richt zich op het proces van intrekken of wijzigen van toegangsrechten De procedure voor het beheren van gebruikersidentificaties (denk aan HR procedure in-/ uit dienst en functiewijziging) is gericht op de gebruikers en, indien van toepassing, de beheerders met toegang tot Suwinet gegevens en behoort te omvatten: a) het gebruik van unieke gebruikersidentificaties zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor hun acties; op gebruikersniveau is het gebruik van groepsaccounts niet toegestaan. Het gebruik van groepsidentificaties voor beheertaken dient alleen te worden toegelaten als deze om bedrijfs- of operationele redenen noodzakelijk zijn. Hiervoor geldt dat dit op het juiste niveau behoort te worden goedgekeurd en gedocumenteerd en dat adequate login wordt toegepast zodat te allen tijde herleidbaar is wie met dit account wanneer en tot welke gegevens toegang heeft gehad; b) Het onmiddellijk ongeldig maken of verwijderen van de gebruikersidentificatie van gebruikers die de organisatie hebben verlaten (zie ook 9.2.6);

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
			c) Daarnaast dient de organisatie een actief beleid te hebben gericht op het herbenoemen van / disabelen van admin-accounts bij installatie van software. Diepgang: Opzet, bestaan en werking van de beheersingsmaatregelen. Test aanpak: Inspecteer het autorisatiebeheerproces en stel vast dat dit proces in lijn is met bovenstaande aandachtspunten. Neem als uitgangspunt het HR proces waar joiners, movers en leavers primair bekend zijn en in de workflow zitten. Betrek hierbij (de beschrijving van de eventuele) interface tussen de personeelsinformatiesystemen en de IAM-tooling en de werking ervan. Betrek hierbij ook de specifieke methodiek voor inloggen (bijv. single sign-on) gehanteerd bij de organisatie. Betrek hierbij ook de wachtwoordinstellingen van de Suwinet-applicaties. Inspecteer of in de organisatie gedurende de gehele verslagperiode verbijzonderde interne controle heeft plaatsgevonden op het naleven van de beheersmaatregelen rond het autorisatieproces. Bepaal hoeveel wijzigingen hebben plaatsgevonden gedurende de verslagperiode en selecteer conform de tabel steekproefomvang het juiste aantal mutaties en stel daarvan vast:

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
			- dat de vastgestelde procedure rond het toekennen / wijzigen / beëindigen van rechten is toegepast; - dat gebruik gemaakt wordt van accounts die tot één persoon herleidbaar zijn (geen groepsaccounts); - dat periodieke controles zijn uitgevoerd en correctieve acties zijn doorgevoerd. Zie verder ook 9.2.2, 92.5 en 9.2.6. Interview de verantwoordelijke functionarissen.
9.2.2 Gebruikers toegang verlenen	Criterium BIO: Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. Doelstelling Bewerkstelligen dat de geclaimde identiteit van de gebruiker kan worden bewezen en dat daardoor alleen bevoegde gebruikers toegang krijgen tot Suwinet diensten. *Risico:* *Onbevoegde gebruikers kunnen toegang krijgen tot Suwinet diensten.*	9.2.2.1 Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris. 9.2.2.2 Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven[19]. 9.2.2.3 E Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	Betrokken partij(en): Organisatie / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD * Let op: Voor Suwinet Inlezen is de database in scope. Toelichting: Beheersmaatregelen 9.2.1, 9.2.2, 9.2.5 en 9.2.6 hangen nauw met elkaar samen: 9.2.1 richt zich op de registratie en het afmelden van gebruiker 9.2.2 richt zich op het proces van het toekennen van rechten aan gebruikers 9.2.5 richt zich op het periodiek beoordelen van toegangsrechten van gebruikers

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

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
			9.2.6 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 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
			Diepgang: Opzet, bestaan en werking van de beheersingsmaatregelen. Test aanpak: Stel vast dat is vastgelegd welke personen bevoegdheden hebben voor het verlenen van toegangsrechten (bijvoorbeeld in een mandaatregister en/ of functieprofielen). Inspecteer of in de organisatie gedurende de gehele verslagperiode verbijzonderde interne controle heeft plaatsgevonden op het naleven van de beheersmaatregelen rond het autorisatieproces. Bepaal hoeveel wijzigingen hebben plaatsgevonden gedurende de verslagperiode en selecteer conform de tabel steekproefomvang het juiste aantal mutaties en stel daarvan vast dat het toewijzen (of intrekken) van toegangsrechten en uitgevoerd in overeenstemming met de 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	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	Betrokken partij(en): Organisatie / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
	wordt aan de principes van doelbinding en proportionaliteit, oneigenlijk autorisatie-toekenningen hebben plaatsgevonden. *<u>Risico:</u>* *Bij het ontbreken van controle op de toegangsrechten worden afwijkingen in het autorisatieproces niet gesignaleerd worden.* *Bij het ontbreken controles op het gebruik van autorisaties wordt misbruik niet gesignaleerd.*	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	* Let op: Voor Suwinet Inlezen is de database in scope. <u>Toelichting:</u> Beheersmaatregelen 9.2.1, 9.2.2, 9.2.5 en 9.2.6 hangen nauw met elkaar samen: 9.2.1 richt zich op de registratie en het afmelden van gebruiker 9.2.2 richt zich op het proces van het toekennen van rechten aan gebruikers 9.2.5 richt zich op het periodiek beoordelen van toegangsrechten van gebruikers 9.2.6 richt zich op het proces van intrekken of wijzigen van toegangsrechten Het (lijn)management behoort de toegangsrechten van gebruikers en, indien van toepassing, beheerders met toegang tot Suwinet gegevens regelmatig te beoordelen in een formeel proces. Bij het beoordelen van toegangsrechten van gebruikers behoren de volgende aspecten in overweging te worden genomen: a) toegangsrechten van gebruikers behoren regelmatig en na wijzigingen, zoals promotie, degradatie of beëindiging van het dienstverband, te worden beoordeeld; b) toegangsrechten van gebruikers behoren te worden beoordeeld en opnieuw te worden toegekend bij functieverandering binnen dezelfde organisatie; c) autorisaties voor speciale toegangsrechten behoren vaker te worden beoordeeld; d) toewijzingen van speciale toegangsrechten behoren regelmatig te worden gecontroleerd om te

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2022	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT-auditor
			waarborgen dat speciale toegangsrechten niet onbevoegd zijn verkregen; e) van wijzigingen in speciale accounts behoren voor periodieke beoordeling logbestanden te worden bijgehouden. <u>Diepgang:</u> Opzet, bestaan en werking van de beheersingsmaatregelen. <u>Testaanpak:</u> Stel vast hoe het eigenaarschap van Suwinet gegevens is geregeld. Stel vast dat de periodieke review minimaal eenmaal per 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 review worden gedocumenteerd en behandeld als beveiligingsincident*. Interview de verantwoordelijke functionarissen. ** Indien er geen beveiligingsincidenten m.b.t. autorisatie van Suwinet hebben plaatsgevonden in het verantwoordingsjaar dan is norm alleen qua opzet te beoordelen.*

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): Organisatie / samenwerkingspartij Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD * Let op: Voor Suwinet Inlezen is de database in scope. Toelichting: Beheersmaatregelen 9.2.1, 9.2.2, 9.2.5 en 9.2.6 hangen nauw met elkaar samen: 9.2.1 richt zich op de registratie en het afmelden van gebruiker 9.2.2 richt zich op het proces van het toekennen van rechten aan gebruikers 9.2.5 richt zich op het beoordelen van toegangsrechten van gebruikers 9.2.6 richt zich op het proces van intrekken of wijzigen van toegangsrechten Bij beëindiging van het dienstverband behoren de toegangsrechten van een persoon voor informatie en bedrijfsmiddelen die samenhangen met informatieverwerkende faciliteiten en diensten t.a.v. Suwinet gegevens te worden ingetrokken of opgeschort. Hierdoor kan worden vastgesteld of het noodzakelijk is om toegangsrechten in te trekken. Wijzigingen in het dienstverband behoren te worden weerspiegeld in het intrekken van alle toegangsrechten die niet voor het nieuwe dienstverband zijn goedgekeurd. De toegangsrechten die behoren te worden ingetrokken of aangepast

			omvatten ook de fysieke en logische toegangsrechten. Intrekking of aanpassing kan plaatsvinden door verwijdering, intrekking of vervanging van sleutels, identificatiekaarten, informatieverwerkende faciliteiten of abonnementen (*) Elk document dat toegangsrechten van medewerkers en contractanten identificeert, behoort de intrekking of aanpassing van toegangsrechten weer te geven. Indien een medewerker die uit dienst gaat of een externe gebruiker wachtwoorden kent van gebruikersidentificaties die actief blijven, dan behoren deze bij beëindiging of wijziging van dienstverband, contract of overeenkomst te worden gewijzigd. <u>Diepgang:</u> Opzet, bestaan en werking van de beheersingsmaatregelen. <u>Test aanpak:</u> Stel vast dat het beleid ter zake van het intrekken of wijzigen van toegangsrechten in lijn is met bovenstaande aandachtspunten. Inspecteer of in de organisatie gedurende de gehele verslagperiode verbijzonderde interne controle heeft plaatsgevonden op het naleven van de beheersingsmaatregelen rond het toekennen / intrekken van toegangsrechten. Bepaal hoeveel wijzigingen hebben plaatsgevonden gedurende de verslagperiode en selecteer conform de tabel steekproefomvang het juiste aantal mutaties en stel vast dat bij het doorvoeren van de wijzigingen de vastgestelde procedures zijn gevolgd. i Selecteer conform de tabel steekproefomvang het juiste aantal medewerkers en stel vast dat de

			geregisteerde gebruikers nog werkzaam zijn binnen het Suwi domein Interview de verantwoordelijke functionarissen.
10. Cryptografie			
10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	Criterium BIO: Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd. 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.*	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. 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.	Betrokken partij(en): Organisatie / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inlezen Suwinet DKD * Let op: Voor Suwinet Inlezen is de database in scope. Toelichting: Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie. Diepgang: Opzet, bestaan en werking van de beheersingsmaatregelen. Test aanpak: Inspecteer de classificatie van gegevens en daaraan gerelateerde risicoanalyse, de netwerkarchitectuur en het inrichtingsdocument waar de encryptie van gegevens in staat beschreven, en stel vast dat deze voldoen aan bovenstaande aandachtspunten. Beoordeel of de beveiliging van de verbindingen voldoet aan de laatste stand der techniek. Gebruik hierbij de gestelde eisen van het Forum

			Standaardisatie (Lijst open standaarden | Forum Standaardisatie) als uitgangspunt voor de beoordeling. Observeer de (wijze van toepassen van) encryptie van gegevens. Inspecteer of de daarbij toegepaste technieken / cryptografische configuratie voldoet aan de laatste stand der techniek[20]* Interview de verantwoordelijke functionarissen. * *Betrek hierbij informatie van NCSC over eisen toereikendheid*
12. Beveiliging bedrijfsvoering			
12.1.1 Gedocumenteerde bedieningsprocedures	Criterium BIO: Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben. Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen. *Risico:* *Als gebruikers en/ of beheerders niet kunnen beschikken over bedieningsprocedures (handleidingen) bestaat het risico dat (kritieke) informatieverwerkende faciliteiten niet correct en/ of veilig worden bediend.*	(geen onderliggende specifieke overheidsmaatregel)	Betrokken partij(en): Organisatie / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: Gebruikers en beheerders van Suwinet gegevens dienen te beschikken over bedieningsprocedures (handleidingen). Te denken valt hierbij aan: Handleiding voor gebruikers van Suwinet gegevens: a) verwerking en behandeling van informatie, zowel geautomatiseerd als handmatig; b) ondersteunings- en escalatiecontacten, waaronder externe ondersteuningscontacten in

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

			geval van onverwachte bedienings- of technische moeilijkheden; c) voorschriften voor de behandeling van speciale uitvoer en media, zoals het gebruik van speciale kantoorbenodigdheden of het beheer van vertrouwelijke uitvoer, waaronder procedures voor veilig verwijderen van uitvoer van mislukte taken; Handleiding voor beheerders van Suwinet gegevens: a) de installatie en configuratie van systemen; b) back-up; c) eisen ten aanzien van de planning, met inbegrip van onderlinge verbondenheid met andere systemen, tijdstip waarop de eerste taak begint en tijdstip van afronding van de laatste taak; d) voorschriften voor de afhandeling van fouten of andere uitzonderlijke omstandigheden die tijdens de uitvoering van de taak kunnen optreden, waaronder beperkingen ten aanzien van het gebruik van systeemhulpmiddelen; e) procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen; f) het beheren van audit- en systeemlog bestandinformatie; g) procedures voor het monitoren van activiteiten; h) Specifieke aandacht voor Suwinet inlezen. <u>Diepgang:</u> Opzet en bestaan van de beheersingsmaatregelen. <u>Test aanpak:</u> Inspecteer de gebruikers- en/of beheerderhandleidingen en stel vast dat deze

			aantoonbaar voldoen aan bovenstaande aandachtspunten. **Voor Suwinet-inlezen**: Er is een beschrijving van relevante ITIL-processen waarvan ook m.b.t. de Suwinet gerelateerde applicaties gebruik wordt gemaakt (changemanagement, release en deploy management, (security) incidentmanagement, configuratiemanagement, IT-service continuity management), zie ook 12.4.1 specifiek voor security incidentmanagement. Interview de verantwoordelijke functionarissen.
12.1.2 Wijzigingenbeheer	Wijzigingsbeheer: Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	(geen onderliggende specifieke overheidsmaatregel)	<u>Betrokken partijen:</u> organisatie / samenwerkingspartner / IT-service-organisatie. <u>Diepgang:</u> Opzet, bestaan en werking van de beheersingsaatregelen * Let op: Voor Suwinet Inlezen is de database in scope. <u>Testaanpak:</u> Inspecteer de documentatie rond het wijzigingenbeheer en stel vast dat deze minimaal de bovenstaande aandachtspunten omvatten. Inspecteer of in de organisatie gedurende de gehele verslagperiode verbijzonderde interne controle heeft plaatsgevonden op het naleven van de beheersingsmaatregelen rond het doorvoeren van wijzigingen.

			Bepaal hoeveel wijzigingen hebben plaatsgevonden gedurende de verslagperiode en selecteer conform de tabel steekproefomvang het juiste aantal mutaties en stel vast dat bij het doorvoeren van de wijzigingen de vastgestelde procedures zijn gevolgd. Stel voor Suwinet inlezen vast dat de specifieke procedures aantoonbaar hebben gewerkt. Bepaal hoeveel wijzigingen hebben plaatsgevonden gedurende de verslagperiode en selecteer conform de tabel steekproefomvang het juiste aantal mutaties en stel vast dat de specifieke procedures zijn gevolgd. Interview de verantwoordelijke functionarissen
12.1.4.1 Scheiding ontwikkel-, test- en productieomgevingen	Scheiding van ontwikkel-, test- en productieomgevingen: Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	(geen onderliggende specifieke overheidsmaatregel)	Betrokken partijen: organisatie / samenwerkingspartner / IT-service-organisatie. <u>Diepgang:</u> Opzet, bestaan en werking van de beheersingsmaatregelen * Let op: Voor Suwinet Inlezen is de database in scope. <u>Testaanpak:</u> Inspecteer de documentatie rond de scheiding van ontwikkel-, test- en productieomgevingen en stel vast dat deze minimaal de bovenstaande aandachtspunten omvatten. Inspecteer of in de organisatie gedurende de gehele verslagperiode verbijzonderde interne controle heeft plaatsgevonden op het naleven van de

			beheersingsmaatregelen de scheiding van ontwikkel-, test- en productieomgevingen. Bepaal hoeveel wijzigingen hebben plaatsgevonden gedurende de verslagperiode en selecteer conform de tabel steekproefomvang het juiste aantal mutaties en stal vast dat bij het doorvoeren van de wijzigingen de vastgestelde procedures zijn gevolgd (rond hanteren van (overdracht tussen) ontwikkel-, test- en productieomgevingen). Interview de verantwoordelijke functionarissen
12.1.4.2 Wijziging productieomgeving	Scheiding van ontwikkel-, test- en productieomgevingen: Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	(geen onderliggende specifieke overheidsmaatregel)	Betrokken partijen: organisatie / samenwerkingspartner / IT-service-organisatie. <u>Diepgang:</u> Opzet, bestaan en werking van de beheersingsmaatregelen * Let op: Voor Suwinet Inlezen is de database in scope. <u>Testaanpak:</u> Inspecteer de documentatie rond de scheiding van ontwikkel-, test- en productieomgevingen en stel vast dat deze minimaal de bovenstaande aandachtspunten omvatten. Inspecteer of in de organisatie gedurende de gehele verslagperiode verbijzonderde interne controle heeft plaatsgevonden op het naleven van de beheersingsmaatregelen de scheiding van ontwikkel-, test- en productieomgevingen.

			Bepaal hoeveel wijzigingen hebben plaatsgevonden gedurende de verslagperiode en selecteer conform de tabel steekproefomvang het juiste aantal mutaties en stal vast dat bij het doorvoeren van de wijzigingen de vastgestelde procedures zijn gevolgd (rond hanteren van (overdracht tussen) ontwikkel-, test- en productieomgevingen). Interview de verantwoordelijke functionarissen
12.4.1 Gebeurtenissen registreren	Criterium BIO: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. Doelstelling: 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. *Risico:* *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).	Betrokken partij(en): Organisatie / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: 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 organisatie 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 organisatie hiertoe in staat moet stellen door het aanleveren van voldoende fijnmazige (gedetailleerde) rapportages, zodat controle op de rechtmatigheid van het gebruik van Suwinet gegevens daarmee wordt gefaciliteerd. De fijnmazigheid van de door BKWI aangeleverde rapportages is eerder door de AP als voldoende

		Deze worden ingezet op basis van een risicoinschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd. 12.4.1.4 Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen. 12.4.1.5 De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	gekwalificeerd en kan derhalve voor andere beheerorganisaties als voorbeeld dienen. Er behoren procedures te worden vastgesteld om het gebruik van Suwinet-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig (minimaal 2 maal per jaar gelijkmatig verdeeld) te worden beoordeeld en gerapporteerd. <u>Diepgang:</u> Opzet, bestaan en werking van de beheersingsmaatregelen <u>Test aanpak</u>: Inspecteer de procedurebeschrijving met betrekking tot het monitoren van de logging en stel vast dat deze voldoet aan bovenstaande aandachtspunten. Inspectie van de vastlegging van de periodiek review van de logging, periodieke rapportage (minimaal 2 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 gebruik van Suwinet gegevens) aan het licht zouden zijn gekomen en dat inhoud is gegeven aan terzake door de organisatie geformuleerde opvolgingsproces. Zie ook uitwerking onder 6.1.1.

			Voer daarbij een reperdormance uit op minimaal 1 van de door de organisatie uitgevoerde werkzaamheden 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): Organisatie / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inlezen Suwinet DKD Toelichting: Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole en te worden beschermd tegen vervalsing en onbevoegde toegang. Diepgang: Opzet, bestaan van de beheersingsprocedures Test aanpak: Inspecteer de procedurebeschrijving met betrekking tot de bescherming van logfaciliteiten en logbestanden en stel vast dat deze voldoet aan bovenstaande aandachtspunten ofwel is deze robuust beschermd tegen vervalsing en onbevoegde toegang. Inspectie van de locatie van de logbestanden.

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

18.1.4 Privacy en bescherming van persoonsgegevens	Criterium BIO: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende het verwerken van persoonsgegevens. *Risico:* *Als de verwerking van Suwinet (persoons)gegevens niet overeenkomstig toepasselijke wet- en regelgeving plaatsvindt, wordt hierdoor de AVG overtreden.*	18.1.4.1 In overeenstemming met de AVG heeft iedere 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): Organisatie / samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD Toelichting: Organisaties behoren een beleid te ontwikkelen en te implementeren voor de privacy en bescherming van persoonsgegevens. Dit beleid behoort te worden gecommuniceerd aan alle personen die betrokken zijn bij het verwerken van persoonsgegevens. Indien organisaties voor Suwinet gebruik maken van de diensten van een serviceorganisatie (bijvoorbeeld bij het gebruik van Suwinet Inlezen of Suwinet DKD) dient met deze serviceorganisatie een Verwerkersovereenkomst te zijn afgesloten. Diepgang: Opzet, bestaan en werking van de beheersingsmaatregelen. 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 organisatie de Suwinet gegevens alleen gebruikt voor de taken waarvoor een wettelijke basis (doelbinding) is* en die dus noodzakelijk zijn voor de uitvoering van wet- en regelgeving. Voor een aantal taken van de organisatie is het gebruik van Suwinet gegevens niet toegestaan**. Identificeer of er activiteiten zijn geweest welke nadere acties (denk aan datalekken) door betrokkenen noodzakelijk maken. Inspecteer of de organisatie gedurende de gehele verslagperiode verbijzonderde controle heeft uitgevoerd op deze activiteiten. Inspecteer, mede aan de hand van relevante aantal uit tabel steekproefomvang, de geselecteerde activiteiten op naleving van de daaromtrent gestelde (wettelijke / organisatorische) vereisten. Interview de verantwoordelijke functionarissen.

Bijlage 4: Tabel steekproefomvang / deelwaarnemingen

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

Bij het toetsen van de werking bij de aansluithouder of de serviceorganisaties steunt de auditor op uitgevoerde verbijzonderde interne controles op de beheersmaatregelen gedurende de gehele verslagperiode. De auditor toets de werking van de beheersmaatregelen gespreid over deze gehele verslagperiode. De populatie van de te onderzoeken aspecten (c.q. de steekproef / deelwaarneming) omvat daarmee de occurances over de gehele verslagperiode.

Factoren die van invloed zijn op het auditrisico, en daarmee op de omvang van de waarnemingen, zijn onder meer:
- Bevindingen uit het verleden
- Wijzigingen in de uitvoering van de interne controle-activiteiten (o.a. personele wijzigingen)
- Veranderingen in het ontwerp van de beheersmatregel
- Zwakke controle omgeving (1e, 2e en / of 3e lijnscontrole).

Sampling o.b.v. frequentie van de beheersmaatregel		**Minimale omvang van de te verrichten deelwaarnemingen bij een lager auditrisico**	**Minimale omvang van de te verrichten deelwaarnemingen bij een hoger auditrisico**
Frequentie op jaarbasis	Aantal occurances in de onderzoeksperiode[21]		
Jaarlijks	of 1 occurrence	1	1
Eens per kwartaal	of 2 – 4 occurrences	2	2
Eens per maand	of 5 – 12 occurrences	2	3
Eens per week	of 13 – 53 occurences	5	8
Dagelijks	of 53 – 249 occurrences	15	25
Meer dan dagelijks (recurring)	>= 250 occurences	25	40

Context bij voorgaande tabel
Voor de periodiciteit jaarlijks, eens per kwartaal, eens per maand, eens per week en dagelijks wordt een niet-statistische steekproef (deelwaarneming) gehanteerd[22].

Algemeen uitgangspunt voor de oordeelsvorming bij geconstateerde afwijkingen: Er wordt vanuit gegaan dat in de 1e, 2e (en eventueel 3e) lijns controle eventuele fouten reeds gedetecteerd en gecorrigeerd zijn. Er mag dus door de auditor geen fout gevonden worden. Eén fout leidt binnen de binaire oordeelsmethodiek (voldoet / voldoet niet) tot 'voldoet niet' op onderzochte element. Betrek in kader oordeelsvorming over de gehele verantwoording ook de uitgangspunten verwoord in paragraaf 2.13 Wegingskader.

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

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

Bijlage 5: Modellen assurance-rapporten

5.1 Assurance-rapport : Goedkeurend

ASSURANCE-RAPPORT

Inzake het gebruik van de
Gezamenlijke elektronische Voorzieningen SUWI *20XX (GeVS)*
ORGANISATIE AA
Ingevolge artikel 6.4 Regeling SUWI

(Bestemd voor *Bestuur organisatie AA,*
BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid)

Assurance-rapport van de onafhankelijke IT-auditor

Aan: *Bestuur van organisatie AA*

Verklaring over de beheersing gegevensuitwisseling SUWI 20*XX* Ingevolge artikel 6.4 Regeling SUWI

Ons oordeel
Ingevolge uw opdracht hebben wij de bijgevoegde Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS)20*XX* Ingevolge artikel 6.4 Regeling SUWI onderzocht.
Naar ons oordeel is de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS)20*XX* Ingevolge artikel 6.4 Regeling SUWI in alle van materieel belang zijnde aspecten, juist.

De basis voor ons oordeel
Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht en de NOREA Richtlijn 3000A "Assurance-opdrachten door IT-auditors (Attest-opdrachten)" en NOREA Handreiking SUWI 6.4 voor IT-auditors d.d. 1 juli 2024. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Verantwoordelijkheden van de IT-auditor'.

Wij zijn onafhankelijk van *organisatie AA* en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA.

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

Van toepassing zijnde criteria
Voor het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) heeft het Ministerie van Sociale Zaken en Werkgelegenheid (SZW) de normen (inclusief de bijbehorende subnormen) geselecteerd waaraan de interne beheersmaatregelen worden getoetst en waarover gerapporteerd moet worden in de Verantwoording inzake Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI. Deze normen zijn vermeld in de Verantwoordingsrichtlijn GeVS 2022.

Beoogde gebruikers en doel
Ons assurance-rapport is uitsluitend bestemd voor *Bestuur van organisatie AA*, BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid.

Het *Bestuur van organisatie AA* kan dit assurance-rapport behorende bij de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI gebruiken richting BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid om te voldoen aan artikel 6.4 van de Regeling SUWI. Ingevolgde dit artikel rapporteert *organisatie AA* voor 1 mei van elk jaar over de opzet, bestaan en werking van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensuitwisseling SUWI.

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

Beschrijving van de verantwoordelijkheden

Verantwoordelijkheden van het *Bestuur van organisatie AA*
Het *Bestuur van organisatie AA* is verantwoordelijk voor het ontwerpen en implementeren van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensuitwisseling SUWI en voor de effectieve werking van dit stelsel.

Het *Bestuur van organisatie AA* is verantwoordelijk voor het opstellen van de Verantwoording inzake het gebruik van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI.

Het *Bestuur van organisatie AA* is ook verantwoordelijk voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de Verantwoording inzake het gebruik van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS) 20*XX* mogelijk te maken zonder afwijkingen van materieel belang als gevolg van fraude of fouten.

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

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

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

Onze controle bestond onder andere uit:
- het verkrijgen van kennis omtrent de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI
- en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen;
- het op basis van deze kennis identificeren en inschatten van de risico's dat de Verantwoording inzake het gebruik van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI afwijkingen van materieel belang als gevolg van fraude of fouten bevat;
- het in reactie op deze risico's bepalen en uitvoeren van assurance-werkzaamheden en het verkrijgen van assurance-informatie die voldoende en geschikt is als basis voor ons oordeel;
- het evalueren of de Verantwoording inzake het gebruik van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI in overeenstemming is met de onderliggende beheersmaatregelen en uitgevoerde werkzaamheden; en
- het evalueren van de uitkomsten van onze werkzaamheden.

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

5.2 Assurance-rapport: Beperking

ASSURANCE-RAPPORT

Inzake het gebruik van de
Gezamenlijke elektronische Voorzieningen SUWI *20XX (GeVS)*
ORGANISATIE AA
Ingevolge artikel 6.4 Regeling SUWI

(Bestemd voor *Bestuur organisatie AA,*
BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid)

Assurance-rapport van de onafhankelijke IT-auditor

Aan: *Bestuur van organisatie AA*

Verklaring over de beheersing gegevensuitwisseling SUWI 20*XX* Ingevolge artikel 6.4 Regeling SUWI

Ons oordeel met beperking

Ingevolge uw opdracht hebben wij de bijgevoegde Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI onderzocht.
Naar ons oordeel is uitgezonderd de <gevolgen>[23] <de mogelijke effecten>[24] van de <aangelegenheid / aangelegenheden> beschreven in de paragraaf 'De basis voor ons oordeel met beperking' de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX*Ingevolge artikel 6.4 Regeling SUWI in alle van materieel belang zijnde aspecten, juist.

De basis voor ons oordeel met beperking

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

Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht en de NOREA Richtlijn 3000A "Assurance-opdrachten door IT-auditors (Attest-opdrachten)" en NOREA Handreiking SUWI 6.4 voor IT-auditors d.d. 1 juli 2024. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Verantwoordelijkheden van de IT-auditor'.

Wij zijn onafhankelijk van *organisatie AA* en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA.

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

Van toepassing zijnde criteria
Voor het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* heeft het Ministerie van Sociale Zaken en Werkgelegenheid (SZW) de normen (inclusief de bijbehorende subnormen) geselecteerd waaraan de interne beheersmaatregelen worden getoetst en waarover gerapporteerd moet worden in de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI. Deze normen zijn vermeld in de Verantwoordingsrichtlijn GeVS 2022.

Beoogde gebruikers en doel
Ons assurancer-apport is uitsluitend bestemd voor *Bestuur van organisatie AA*, BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid.

Het *Bestuur van organisatie AA* kan dit assurance-rapport behorende bij de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI gebruiken richting BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid om te voldoen aan artikel 6.4 van de Regeling SUWI. Ingevolgde dit artikel

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

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

rapporteert *organisatie AA* voor 1 mei van elk jaar over de opzet en werking van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensuitwisseling SUWI.

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

Beschrijving van de verantwoordelijkheden

Verantwoordelijkheden van het *Bestuur van organisatie AA*

Het *Bestuur van organisatie AA* is verantwoordelijk voor het ontwerpen en implementeren van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensuitwisseling SUWI en voor de effectieve werking van dit stelsel.

Het *Bestuur van organisatie AA* is verantwoordelijk voor het opstellen van de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI.

Het *Bestuur van organisatie AA* is ook verantwoordelijk voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* mogelijk te maken zonder afwijkingen van materieel belang als gevolg van fraude of fouten.

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

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

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

Onze controle bestond onder andere uit:
- het verkrijgen van kennis omtrent de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI
- en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen;
- het op basis van deze kennis identificeren en inschatten van de risico's dat de Verantwoording inzake het gebruik van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI afwijkingen van materieel belang als gevolg van fraude of fouten bevat;
- het in reactie op deze risico's bepalen en uitvoeren van assurance-werkzaamheden en het verkrijgen van assurance-informatie die voldoende en geschikt is als basis voor ons oordeel;
- het evalueren of de Verantwoording inzake het gebruik van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI in overeenstemming is met de onderliggende beheersmaatregelen en uitgevoerde werkzaamheden; en
- het evalueren van de uitkomsten van onze werkzaamheden.

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

5.3 Assurance-rapport: Afkeurend

ASSURANCE-RAPPORT

Inzake het gebruik van de Gezamenlijke elektronische Voorzieningen SUWI *20XX (GeVS)* *ORGANISATIE AA* Ingevolge artikel 6.4 Regeling SUWI

(Bestemd voor *Bestuur organisatie AA,*
BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid)

Assurancerapport van de onafhankelijke IT-auditor

Aan: *Bestuur van organisatie AA*

Verklaring over de beheersing gegevensuitwisseling SUWI 20*XX* Ingevolge artikel 6.4 Regeling SUWI

Afkeurend oordeel
Ingevolge uw opdracht hebben wij de bijgevoegde "Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI" onderzocht.
Naar ons oordeel is de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI vanwege het belang van de <aangelegenheid / aangelegenheden> beschreven in de paragraaf 'De basis voor ons afkeurend oordeel' niet in alle van materieel belang zijnde aspecten, niet juist.

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

Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht en de NOREA Richtlijn 3000A "Assurance-opdrachten door IT-auditors (Attest-opdrachten)" en NOREA Handreiking SUWI 6.4 voor IT-auditors d.d. 1 juli 2024. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Verantwoordelijkheden van de IT-auditor'.

Wij zijn onafhankelijk van *organisatie AA* en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA.

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

Van toepassing zijnde criteria
Voor het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* heeft het Ministerie van Sociale Zaken en Werkgelegenheid (SZW) de normen (inclusief de bijbehorende subnormen) geselecteerd waaraan de interne beheersmaatregelen worden getoetst en waarover gerapporteerd moet worden in de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI. Deze normen zijn vermeld in de Verantwoordingsrichtlijn GeVS 2022.

Beoogde gebruikers en doel
Ons assurancerapport is uitsluitend bestemd voor het *Bestuur van organisatie AA*, de BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid.

Het *Bestuur van organisatie AA* kan dit assurance-rapport behorende bij de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI gebruiken richting BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid om te voldoen aan artikel 6.4 van de Regeling SUWI. Ingevolgde dit artikel rapporteert *organisatie AA* voor 1 mei van elk jaar over de opzet, bestaan en werking van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensuitwisseling SUWI. Deze rapportage moet worden vergezeld van een oordeel van een tot de Nederlandse Orde van Register EDP-Auditors toegelaten persoon.

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

Beschrijving van de verantwoordelijkheden

Verantwoordelijkheden van het *Bestuur van organisatie AA*
Het *Bestuur van organisatie AA* is verantwoordelijk voor het ontwerpen en implementeren van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensuitwisseling SUWI en voor de effectieve werking van dit stelsel.

Het *Bestuur van organisatie AA* is verantwoordelijk voor het opstellen van de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI.

Het *Bestuur van organisatie AA* is ook verantwoordelijk voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de Verantwoording het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* mogelijk te maken zonder afwijkingen van materieel belang als gevolg van fraude of fouten.

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

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

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

Onze controle bestond onder andere uit:
- het verkrijgen van kennis omtrent de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI
- en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen;
- het op basis van deze kennis identificeren en inschatten van de risico's dat de Verantwoording inzake het gebruik van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI afwijkingen van materieel belang als gevolg van fraude of fouten bevat;
- het in reactie op deze risico's bepalen en uitvoeren van assurance-werkzaamheden en het verkrijgen van assurance-informatie die voldoende en geschikt is als basis voor ons oordeel;
- het evalueren of de Verantwoording inzake het gebruik van de Gezamenlijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI in overeenstemming is met de onderliggende beheersmaatregelen en uitgevoerde werkzaamheden; en
- het evalueren van de uitkomsten van onze werkzaamheden.

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

5.4 Assurance-rapport: Oordeelonthouding

ASSURANCE-RAPPORT

Inzake het gebruik van de Gezamenlijke elektronische Voorzieningen SUWI *20XX (GeVS)* *ORGANISATIE AA* Ingevolge artikel 6.4 Regeling SUWI

(Bestemd voor *Bestuur organisatie AA,*
BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid)

Assurancerapport van de onafhankelijke IT-auditor

Aan: *Bestuur van organisatie AA*

Verklaring over de beheersing gegevensuitwisseling SUWI 20*XX* Ingevolge artikel 6.4 Regeling SUWI

Onze oordeelonthouding
Wij hebben opdracht gekregen de bijgevoegde Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI te controleren.

Wij geven geen oordeel over de juistheid van de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI. Vanwege het belang van de <aangelegenheid> <aangelegenheden> beschreven in de paragraaf 'De basis voor onze oordeelonthouding' zijn wij niet in staat geweest om voldoende en geschikte assurance-informatie te verkrijgen om daarop ons oordeel te kunnen baseren bij de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI als geheel.

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

Van toepassing zijnde criteria
Voor het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* heeft het Ministerie van Sociale Zaken en Werkgelegenheid (SZW) de normen (inclusief de bijbehorende subnormen) geselecteerd waaraan de interne beheersmaatregelen worden getoetst en waarover gerapporteerd moet worden in de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI. Deze normen zijn vermeld in de Verantwoordingsrichtlijn GeVS 2022.

Beoogde gebruikers en doel
Ons assurance-rapport is uitsluitend bestemd voor *Bestuur van organisatie AA*, BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid.

Het *Bestuur van organisatie AA* kan dit assurance-rapport behorende bij de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI gebruiken richting BKWI en het Ministerie van Sociale Zaken en Werkgelegenheid om te voldoen aan artikel 6.4 van de Regeling SUWI. Ingevolgde dit artikel rapporteert *organisatie AA* voor 1 mei van elk jaar over de opzet en werking van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensuitwisseling SUWI. Deze rapportage moet worden vergezeld van een oordeel van een tot de Nederlandse Orde van Register EDP-Auditors toegelaten persoon.

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

Beschrijving van de verantwoordelijkheden

Verantwoordelijkheden van het *Bestuur van organisatie AA*
Het *Bestuur van organisatie AA* is verantwoordelijk voor het ontwerpen en implementeren van het stelsel van maatregelen en procedures, gericht op het waarborgen van een exclusieve, integere,

beschikbare en controleerbare gegevensuitwisseling SUWI en voor de effectieve werking van dit stelsel.

Het *Bestuur van organisatie AA* is verantwoordelijk voor het opstellen en getrouw weergeven van de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI.

Het *Bestuur van organisatie AA* is ook verantwoordelijk voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de Verantwoording het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* mogelijk te maken zonder afwijkingen van materieel belang als gevolg van fraude of fouten.

Verantwoordelijkheid van de IT-auditor

Onze verantwoordelijkheid is het geven van een oordeel over de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI op basis van onze controle, verricht in overeenstemming met Nederlands recht, waaronder de NOREA Richtlijn 3000A "Assurance-opdrachten door IT-auditors (Attest-opdrachten)". 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 controle-informatie te verkrijgen om daarop ons oordeel te kunnen baseren bij de Verantwoording inzake het gebruik van de Gemeenschappelijke elektronische Voorzieningen SUWI (GeVS) 20*XX* Ingevolge artikel 6.4 Regeling SUWI als geheel.

Wij zijn onafhankelijk van organisatie AA en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA.

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

Bij het uitvoeren van de werkzaamheden hebben wij de NOREA Handreiking SUWI 6.4 voor IT-auditors d.d. 1 juli 2024 toegepast.

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

Bijlage 6: Waarmerken stukken

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

DigiD

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

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

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

ENSIA / Suwi 6.4

Op basis van nader overleg tussen alle direct betrokken partijen is besloten deze beleidslijn onverkort te volgen voor ENSIA en Suwi 6.4.

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

Ter toelichting: Dit betekent dat het assurance-rapport, de 'in control verklaring' en de bijlage voorzien moeten zijn van een elektronische handtekening.

Aandachtspunt voor aansluithouders en IT-auditors

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