Bijlage 4 Testaanpak bij de te onderzoeken normen relevant voor Suwinet

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
5. Informatiebeveiligingsbeleid			
Norm/Control geldt voor		**Norm van toepassing op**	
Suwinet Inkijk / Suwinet Inlezen / DKD Inlezen / WGS Inkijk / WGS Inlezen		Eigen organisatie	Dienstenleverancier
x / x / x / x / x		x	n.v.t.
5.1.1 Beleidsregels voor informatiebeveiliging	<u>Criterium BIO:</u> Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. <u>Doelstelling:</u> 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 *(en DKD, WGS)* aantoonbaar aan de vereiste beveiligingsvoorwaarden voldoet. *<u>Risico:</u>* *Het risico bestaat dat de bescherming van de aansluiting op Suwinet (en DKD, WGS), in tegenstelling tot bescherming van haar eigen ICT omgeving, onvoldoende aandacht krijgt.*	5.1.1.1 Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat ten minste de volgende punten: a) De strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid. b) De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden. c) De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers. d) De gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn.	<u>Betrokken partij(en):</u> Gemeente/ samenwerkingspartij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen DKD Inlezen WGS Inkijk WGS Inlezen <u>Toelichting:</u> De gemeente moet beschikken over een <u>Suwinet informatiebeveiligingsbeleid</u> (eventueel als onderdeel van het algehele informatiebeveiligingsbeleid). Het aansluitbeleid betreft het beleid aangaande de bescherming van de eigen informatiehuishouding <u>in relatie tot de eigen delen van Suwinet en de via Suwinet beschikbaar gestelde gegevens</u>. <u>Test aanpak:</u> Inspectie van het informatiebeveiligingsbeleid. Deze dient inzicht te geven in de in 5.1.1.1 genoemde

		e) De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd. f) De bevordering van het beveiligingsbewustzijn.	type maatregelen <u>voor de beveiliging van de eigen</u> <u>delen van Suwinet</u> *-en DKD, WGS-* (bijv. organisatorische-, technische- en beheersingsmaatregelen). Stel vast dat het beleid is vastgesteld* door de leiding van de organisatie (het dagelijks bestuur). Interview de verantwoordelijke functionarissen. **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*

Ref BIO 2021, BIO 1.04		**Verantwoordingsrichtlijn GeVS 2020**			**Onderliggende Specifieke overheidsmaatregelen BIO**	**Handreiking voor de IT auditor**
Norm/Control geldt voor					**Norm van toepassing op**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	WGS Inkijk	WGS Inlezen	Eigen organisatie	Dienstenleverancier
x	X	X	x	x	x	n.v.t.
5.1.2 Beoordeling van het informatie-beveiligingsbeleid		<u>Criterium BIO:</u> Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is. <u>Doelstelling:</u> Bewerkstellingen dat de getroffen beveiligingsmaatregelen continue voldoen aan het juiste beveiligingsniveau.			5.1.2.1 Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.	<u>Betrokken partij(en):</u> Gemeente/ samenwerkingspartij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen DKD Inlezen WGS Inkijk WGS Inlezen <u>Toelichting:</u>

	Risico: *De getroffen beveiligingsmaatregelen zijn ontoereikend in relatie tot aangescherpte wetgeving, verandering van risicoklasse van gegevens en de toegepaste technologieën.*		Het Suwinet informatiebeveiligingsbeleid (eventueel als onderdeel van het algehele informatiebeveiligingsbeleid) dient actueel te zijn en periodiek* te worden beoordeeld en zo nodig te worden bijgesteld bij grote wijzigingen of aan de hand van externe ontwikkelingen. **Note: Hiervoor geldt dat de periodiciteit aansluit bij de (bestaande) bestuurs- en P&C-cycli. Voor gemeenten geldt doorgaans dat dit de raadsperiode (4 jaar) is.* Test aanpak: Inspectie van het informatiebeveiligingsbeleid. Stel vast dat het beleid actueel is en conform de (bestaande) bestuurs- en P&C-cycli is bijgesteld. Interview de verantwoordelijke functionarissen.

Ref BIO 2021, BIO 1.04		**Verantwoordingsrichtlijn GeVS 2020**			**Onderliggende Specifieke overheidsmaatregelen BIO**	**Handreiking voor de IT auditor**
6. Organiseren van informatiebeveiliging						
Norm/Control geldt voor					**Norm van toepassing op**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	WGS Inkijk	WGS Inlezen	Eigen organisatie	Dienstenleverancier
x	X	x	x	x	x	n.v.t.
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 *(en DKD, WGS)*.			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 niet 6.1.1.3 De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd. 6.1.1.4 Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen DKD Inlezen WGS Inkijk WGS Inlezen Toelichting:

	<u>Risico:</u> *Het risico bestaat dat door gebrek aan coördinatie van activiteiten niet op beveiligingsincidenten wordt geacteerd en dat door wijzigingen nieuwe kwetsbaarheden ontstaan.*		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. <u>Test aanpak:</u> Inspecteer het informatiebeveiligingsbeleid en stel vast dat taken, bevoegdheden en verantwoordelijkheden (CTFS) ten aanzien van de IB functie t.a.v. Suwinet *(en DKD, WGS)* formeel zijn vastgesteld en stel vast dat deze functie en onderliggende rol(-len) ook als zodanig zijn ingericht* en beschreven. **Note: Idealiter zijn bovenstaande documenten onderdeel van een ingerichte AO/IB.* Stel vast dat een incidentmanagementproces (beveiligingsincidenten) ten aanzien van Suwinet *(en DKD, WGS)* is ingericht en stel het bestaan vast met een deelwaarneming van ten minste één. Stel vast dat beveiligingsincidenten worden geanalyseerd, gerapporteerd aan het verantwoordelijke management en waar nodig aanvullende maatregelen worden getroffen. Interview de verantwoordelijke functionarissen.

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

			Test aanpak: Inspecteer de relevante functie/taakbeschrijvingen van met name de sleutelfunctionarissen, de autorisatiematrix en het autorisatiebeheerproces, en stel vast dat deze voldoen aan bovenstaande aandachtspunten. Interview de verantwoordelijke functionarissen.

Ref BIO 2021, BIO 1.04		**Verantwoordingsrichtlijn GeVS 2020**			**Onderliggende Specifieke overheidsmaatregelen BIO**	**Handreiking voor de IT auditor**
7. Veilig personeel						
Norm/Control geldt voor					**Norm van toepassing op**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	WGS Inkijk	WGS Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	x	x	n.v.t.
7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging		Criterium BIO: Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie. Doelstelling: Het bewustmaken van gebruikers van Suwinet *(en DKD, WGS)* gegevens *Risico:* *Indien gebruikers van Suwinet (en DKD, WGS) gegevens zich niet of onvoldoende bewust zijn van de (hoge) vertrouwelijkheid, bestaat het risico dat*			7.2.2.1 Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen. 7.2.2.2 Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd. 7.2.2.3 niet	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen DKD Inlezen WGS Inkijk WGS Inlezen Toelichting: De organisatie moet beschikken over een procedure die zorg draagt voor het adequaat houden van het bewustzijn onder de medewerkers ten aanzien van informatiebeveiliging/ het werken met (privacy) gevoelige data. Dit kan worden bereikt door bewustwordingssessies, trainingen, social engineering, etc.

	deze gegevens onvoldoende worden beschermd.		<u>Test aanpak:</u> Stel vast op basis van inspectie dat in een procedure/ informatiebeveiligingsplan is vastgelegd dat periodiek (bij voorkeur meerdere malen per jaar, doch minimaal jaarlijks[1]) 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. Stel vast dat gebruikers die toegang hebben tot Suwinet *(en DKD, WGS)* gegevens binnen drie maanden na indiensttreding een training (I-)bewustzijn succesvol hebben gevolgd*. Interview de verantwoordelijke functionarissen. **Note: Dit normaspect is gerelateerd aan norm 18.1.4 waarin is opgenomen dat het beleid ten aanzien van het verwerken van persoonsgegevens dient te worden gecommuniceerd aan alle personen die betrokken zijn bij deze verwerking.*

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

Ref BIO 2021, BIO 1.04		Verantwoordingsrichtlijn GeVS 2020			Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
9. Toegangsbeveiliging						
Norm/Control geldt voor					**Norm van toepassing op**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	WGS Inkijk	WGS Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	x	x	X
9.2.1 Registratie en afmelden van gebruikers		Criterium BIO: Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. Doelstelling: Gebruikers en beheerders de juiste toegangsrechten geven (niet meer en niet minder) dan welke nodig zijn voor de hen opgedragen (wettelijke)taken. *Risico:* *Het risico bestaat dat medewerkers onrechtmatig toegang hebben tot Suwinet of tot de via Suwinet beschikbaar gestelde gegevens.* *Voor Suwinet (en DKD, WGS) geldt een verhoogd risico omdat het Suwinet account van een organisatie ook toegang tot Suwinet kan krijgen vanuit het domein van een ander op Suwinet aangesloten organisatie.*			9.2.1.1 Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties. 9.2.1.2 Het gebruiken van groepsaccounts is niet toegestaan, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen DKD Inlezen WGS Inkijk WGS inlezen Toelichting: Beheersmaatregelen 9.2.1, 9.2.2, 9.2.5 en 9.2.6 hangen nauw met elkaar samen: 9.2.1 richt zich op de registratie en het afmelden van gebruiker 9.2.2 richt zich op het proces van het toekennen van rechten aan gebruikers 9.2.5 richt zich op het periodiek beoordelen van toegangsrechten van gebruikers 9.2.6 richt zich op het proces van intrekken of wijzigen van toegangsrechten De procedure voor het beheren van gebruikersidentificaties (denk aan HR procedure in-/ uit dienst en functiewijziging) is gericht op de gebruikers en, indien van toepassing, de beheerders met toegang tot Suwinet gegevens en behoort te omvatten:

			a) het gebruik van unieke gebruikersidentificaties zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor hun acties; op gebruikersniveau is het gebruik van groepsaccounts niet toegestaan. Het gebruik van groepsidentificaties voor beheertaken dient alleen te worden toegelaten als deze om bedrijfs- of operationele redenen noodzakelijk zijn. Hiervoor geldt dat dit op het juiste niveau behoort te worden goedgekeurd en gedocumenteerd en dat adequate login wordt toegepast zodat te allen tijde herleidbaar is wie met dit account wanneer en tot welke gegevens toegang heeft gehad; b) het default admin account dient bij installatie direct hernoemd te worden dan wel te worden disabled; c) het onmiddellijk ongeldig maken of verwijderen van de gebruikersidentificatie van gebruikers die de organisatie hebben verlaten (zie ook 9.2.6); d) het ervoor zorgen dat gebruikers hun gebruikersidentificaties niet delen met andere gebruikers. Bij voorkeur is dit opgenomen in de gedragsregels (zie ook 7.2.2). Test aanpak: Inspecteer het autorisatiebeheerproces en stel vast dat dit proces in lijn is met bovenstaande aandachtspunten. Neem als uitgangspunt het HR proces waar joiners, movers en leavers primair bekend zijn en in de workflow zitten. Stel vast dat gebruik gemaakt wordt van accounts die tot één persoon herleidbaar zijn (geen groepsaccounts).

						Stel vast dat periodieke controles zijn uitgevoerd en correctieve acties zijn doorgevoerd. Interview de verantwoordelijke functionarissen.
Ref BIO 2021, BIO 1.04		**Verantwoordingsrichtlijn GeVS 2020**			**Onderliggende Specifieke overheidsmaatregelen BIO**	**Handreiking voor de IT auditor**
Norm/Control geldt voor:					**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	WGS Inkijk	WGS Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	x	x	X
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 (en DKD, WGS) 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[2]. 9.2.2.3 Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen DKD Inlezen WGS Inkijk WGS Inlezen Toelichting: Beheersmaatregelen 9.2.1, 9.2.2, 9.2.5 en 9.2.6 hangen nauw met elkaar samen: 9.2.1 richt zich op de registratie en het afmelden van gebruiker 9.2.2 richt zich op het proces van het toekennen van rechten aan gebruikers 9.2.5 richt zich op het periodiek beoordelen van toegangsrechten van gebruikers 9.2.6 richt zich op het proces van intrekken of wijzigen van toegangsrechten De procedure voor het toewijzen of intrekken van toegangsrechten aan gebruikersidentificaties is gericht op de gebruikers en, indien van toepassing,

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

			de beheerders met toegang tot Suwinet *(en DKD, WGS)* 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). <u>Test aanpak:</u> Stel vast dat is vastgelegd welke personen bevoegdheden hebben voor het verlenen van toegangsrechten (bijvoorbeeld in een mandaatregister en/ of functieprofielen).

						Inspecteer de procedure voor het toewijzen of intrekken van toegangsrechten en stel vast dat dit proces in lijn is met bovenstaande aandachtspunten. Interview de verantwoordelijke functionarissen.
Ref BIO 2021, BIO 1.04	**Verantwoordingsrichtlijn GeVS 2020**				**Onderliggende Specifieke overheidsmaatregelen BIO**	**Handreiking voor de IT auditor**
Norm/Control geldt voor:					**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	WGS Inkijk	WGS Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	x	x	X
9.2.5 Beoordeling van toegangsrechten van gebruikers	Criterium BIO: Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. <u>Doelstelling:</u> Het vaststellen of: de autorisaties en veranderingen hierin juist en tijdig zijn aangebracht, de juiste functiescheiding zijn toegepast en voldaan wordt aan de principes van doelbinding en proportionaliteit, oneigenlijk autorisatie-toekenningen hebben plaatsgevonden. <u>*Risico:*</u> *Bij het ontbreken van controle op de toegangsrechten worden afwijkingen in het autorisatieproces niet gesignaleerd worden. Bij het ontbreken controles op het gebruik van autorisaties wordt misbruik niet gesignaleerd.*				9.2.5.1 niet 9.2.5.2 niet 9.2.5.3 Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	<u>Betrokken partij(en):</u> Gemeente/ samenwerkingspartij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen DKD Inlezen WGS Inkijk WGS Inlezen <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, aantoonbaar te worden beoordeeld; b) toegangsrechten van gebruikers behoren aantoonbaar te worden beoordeeld en opnieuw te worden toegekend bij functieverandering binnen dezelfde organisatie; c) autorisaties voor speciale toegangsrechten behoren vaker te worden beoordeeld; d) toewijzingen van speciale toegangsrechten behoren regelmatig te worden gecontroleerd om te waarborgen dat speciale toegangsrechten niet onbevoegd zijn verkregen; e) van wijzigingen in speciale accounts behoren voor periodieke beoordeling logbestanden te worden bijgehouden. <u>Testaanpak:</u> Stel vast hoe het eigenaarschap van Suwinet *(en DKD, WGS)* 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 en bevraag de verantwoordelijke functionarissen.

Ref BIO 2021, BIO 1.04		Verantwoordingsrichtlijn GeVS 2020			Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
Norm/Control geldt voor:					**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	WGS Inkijk	WGS Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	x	x	X
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 (en DKD, WGS) gegevens.*			(Geen onderliggende specifieke overheidsmaatregel)	Betrokken partij(en): Gemeente/ samenwerkingspartij Scope: Suwinet Inkijk Suwinet Inlezen DKD Inlezen WGS Inkijk WGS Inlezen 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>Test aanpak:</u> Stel vast dat het intrekken of wijzigen van toegangsrechten in lijn is met bovenstaande aandachtspunten. Laat bijvoorbeeld een uitdraai maken van de huidige lijst van geautoriseerde gebruikers, controleer of deze gebruikers nog werkzaam zijn binnen het SUWI domein. Neem een willekeurige deelwaarneming van 5 % van de gebruikers. Interview de verantwoordelijke functionarissen.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020				Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
10. Cryptografie						
Norm/Control geldt voor:					**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	WGS Inkijk	WGS Inlezen	Eigen organisatie	Dienstenleverancier
n.v.t.	x	X	n.v.t.	x	x	n.v.t.
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 (en DKD, WGS inlezen) 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): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inlezen DKD Inlezen WGS Inlezen Toelichting: Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie. Test aanpak: Inspecteer de classificatie van gegevens en daaraan gerelateerde risicoanalyse, de netwerkarchitectuur en het inrichtingsdocument waar de encryptie van gegevens in staat beschreven, en stel vast dat deze voldoen aan bovenstaande aandachtspunten. Stel vast bij welke provider de gemeente de beveiligde verbinding heeft afgenomen. NB: Een gemeente kan alleen via een beveiligde verbinding aansluiten op Suwinet. Observeer de (wijze van encryptie) encryptie van gegevens. Inspecteer of de toegepaste

			cryptografische configuratie voldoet aan de laatste stand der techniek[3]. Interview de verantwoordelijke functionarissen.

Ref BIO 2021, BIO 1.04		Verantwoordingsrichtlijn GeVS 2020			Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
12. Beveiliging bedrijfsvoering						
Norm/Control geldt voor:					**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	WGS Inkijk	WGS Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	X	x	x	X
12.1.1 Gedocumenteerde bedieningsprocedures		Criterium BIO: Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben. Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen. *Risico:* *Als gebruikers en/ of beheerders niet kunnen beschikken over bedieningsprocedures (handleidingen) bestaat het risico dat (kritieke) informatieverwerkende faciliteiten niet correct en/ of veilig worden bediend.*			(geen onderliggende specifieke overheidsmaatregel)	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet InlezenDKD Inlezen WGS Inkijk WGS Inlezen Toelichting: Gebruikers en beheerders van Suwinet *(en DKD, WGS)* gegevens dienen te beschikken over bedieningsprocedures (handleidingen). Te denken valt hierbij aan: Handleiding voor gebruikers van Suwinet *(en DKD, WGS)* gegevens: a) verwerking en behandeling van informatie, zowel geautomatiseerd als handmatig; b) ondersteunings- en escalatiecontacten, waaronder externe ondersteuningscontacten in

[3] 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 *(en DKD, WGS)* 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. <u>Test aanpak:</u> Inspecteer de gebruikers- en/of beheerderhandleidingen en stel vast dat deze voldoen aan bovenstaande aandachtspunten. Interview de verantwoordelijke functionarissen.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020				Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
Norm/Control geldt voor:					**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	WGS Inkijk	WGS Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	x	x	X
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). 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 niet 12.4.1.5 niet	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen DKD Inlezen WGS Inkijk WGS Inlezen Toelichting: Voor deze norm geldt dat de beheerder van de applicatie (BKWI voor Suwinet Inkijk/ de IT-serviceorganisatie voor Suwinet Inlezen, Suwinet DKD en WGS-Inlezen) verantwoordelijk is voor het maken en bewaren van logbestanden (zie ook 12.4.2), en dat het de verantwoordelijkheid van de gemeente is om deze logbestanden te gebruiken om regelmatig de rechtmatigheid van het gebruik van Suwinet gegevens door medewerkers te beoordelen. Het is evident dat de beheerorganisatie de gemeente hiertoe in staat moet stellen door het aanleveren van voldoende fijnmazige (gedetailleerde) rapportages, zodat controle op de rechtmatigheid van het gebruik van Suwinet gegevens daarmee wordt gefaciliteerd. De fijnmazigheid van de door BKWI aangeleverde rapportages is eerder door de AP als voldoende gekwalificeerd en kan derhalve voor andere beheerorganisaties als voorbeeld dienen.

			Er behoren procedures te worden vastgesteld om het gebruik van Suwinet-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig (minimaal 2 maal per jaar gelijkmatig verdeeld) te worden beoordeeld en gerapporteerd. <u>Test aanpak</u>: Inspecteer de procedurebeschrijving met betrekking tot het monitoren van de logging en stel vast dat deze voldoet aan bovenstaande aandachtspunten. Inspectie van de vastlegging van de periodiek review van de logging, periodieke rapportage (minimaal 2 maal per jaar gelijkmatig verdeeld) aan het management en follow-up acties naar aanleiding van review en analyse van de logging (PDCA). *Note: Denk ook aan het vaststellen van de volledigheid op basis van doorlopende nummering/ timestamp; en is de logging mogelijk beïnvloedbaar voor de belanghebbende(n).* Stel vast dat de periodieke review van de logging met zodanige diepgang heeft plaatsgevonden dat met een redelijke mate van zekerheid kan worden gesteld dat materiele afwijkingen (onrechtmatig gebruik van Suwinet gegevens) aan het licht zouden zijn gekomen. Informeer bij de verantwoordelijk functionaris welke maatregelen de gemeente / organisatie heeft getroffen, zodat preventief de informatieverwerkende omgeving wordt gemonitord en dat mogelijke aanvallen tijdig kunnen worden gedetecteerd. Hierbij valt te denken aan

			systemen, zoals Siem en/of SOC of andere detectiesystemen. De gemeente / organisatie dient op basis van risico-inschatting aanvullende maatregelen te hebben getroffen ten aanzien van het monitoren van de informatieverwerkende omgeving, zodat tijdig kan worden gehandeld bij een dreigende situatie Als de verantwoordelijke proceseigenaar in expliciete risicoafweging heeft vastgelegd dat geen aanvullende maatregelen benodigd zijn, dan wel het restrisico accepteert, dan dient deze afweging te zijn geaccordeerd door de directeur bedrijfsvoering of GS en mag deze maximaal 1 jaar oud zijn (jaarlijkse risicoafweging). Eveneens moet de auditor vaststellen dat deze afweging een deugdelijke grondslag kent. Interview en bevraag de verantwoordelijke functionarissen.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020				Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
Norm/Control geldt voor:					**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	WGS Inkijk	WGS Inlezen	Eigen organisatie	Dienstenleverancier
n.v.t.	x	x	n.v.t.	x	x	X
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. 12.4.2.3 niet	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inlezen DKD Inlezen WGS Inlezen Toelichting: Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole en te worden beschermd tegen vervalsing en onbevoegde toegang. Test aanpak: Inspecteer de procedurebeschrijving met betrekking tot de bescherming van logfaciliteiten en logbestanden en stel vast dat deze voldoet aan bovenstaande aandachtspunten ofwel is deze robuust beschermd tegen vervalsing en onbevoegde toegang. Inspectie van de locatie van de logbestanden. Interview de verantwoordelijke functionarissen.

Ref BIO 2021, BIO 1.04	Verantwoordingsrichtlijn GeVS 2020	Onderliggende Specifieke overheidsmaatregelen BIO	Handreiking voor de IT auditor
18. Naleving			
Norm/Control geldt voor:		**Norm van toepassing op:**	
Suwinet Inkijk / Suwinet Inlezen / DKD Inlezen / WGS Inkijk / WGS Inlezen		Eigen organisatie	Dienstenleverancier
x / x / x / x / x		x	n.v.t.
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 (en DKD, WGS) niet overeenkomstig toepasselijke wet- en regelgeving plaatsvindt, wordt hierdoor de AVG overtreden.*	18.1.4.1 In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren. 18.1.4.2 Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen DKD Inlezen WGS Inkijk WGS Inlezen Toelichting: Organisaties behoren een beleid te ontwikkelen en te implementeren voor de privacy en bescherming van persoonsgegevens. Dit beleid behoort te worden gecommuniceerd aan alle personen die betrokken zijn bij het verwerken van persoonsgegevens. Indien gemeenten voor Suwinet gebruik maken van de diensten van een serviceorganisatie (bijvoorbeeld bij het gebruik van Suwinet Inlezen of Suwinet DKD) dient met deze serviceorganisatie een Verwerkersovereenkomst te zijn afgesloten. Test aanpak: Stel vast dat de organisatie een privacy-beleid heeft ontwikkeld en geïmplementeerd. Stel vast dat de Suwinet applicatie(s) is/ zijn opgenomen in het Verwerkingsregister. Stel vast dat een FG is aangesteld, dat deze in voldoende mate onafhankelijk en objectief is, en dat

			deze voldoende mandaat heeft om zijn/haar functie uit te voeren. Stel vast dat de naleving van de privacyregels regelmatig gecontroleerd wordt (zie ook 12.4.1). Stel vast dat de gemeente de Suwinet gegevens alleen gebruikt voor de taken waarvoor een wettelijke basis (doelbinding) is* en die dus noodzakelijk zijn voor de uitvoering van wet- en regelgeving. Voor een aantal gemeentelijke taken is het gebruik van Suwinet gegevens niet toegestaan**. Interview de verantwoordelijke functionarissen.

(*) BKWI publiceert desgevraagd periodiek een overzicht waarin de partijen zijn opgenomen die Suwinet gegevens gebruiken waarbij is vermeld voor welk doel welke bron wordt geraadpleegd. Dit overzicht is hier te vinden:
https://www.bkwi.nl/producten/suwinet-services/suwinet-inkijk/suwinet-wie-gebruikt-suwinet-voor-welk-doel-om-gegevens-van-welke-bron-te-raadplegen/

(**) Het gebruik van Suwinet of Suwi gerelateerde zaken is (o.a.) NIET toegestaan voor:
- De uitvoering van gemeentelijke regelingen zoals een korting of stadspas of andere ingrediënten van armoedebeleid. Gemeentelijke regelingen mogen alleen in Suwinet worden geraadpleegd als deze regeling is gebaseerd op de P-wet, IOAW of IOAZ (art. 8, 8a, 8b P-wet). Of dit zo is, is zichtbaar in de aanhef van de gemeentelijke regeling: gelet op artikel xx van de XXX-wet.
- De interne controle op juistheid van de beslissingen van de medewerker. Het controleren van de juistheid van de beslissing van een medewerker valt niet onder de uitvoering van de P-wet, IOAW of IOAZ, maar onder interne controle. Daarvoor mag Suwinet niet worden geraadpleegd.
- De controle op de naleving van Social Return. Sommige gemeenten nemen in contracten met dienstverleners passages op over het inzetten van werkzoekenden of bijstandsgerechtigden (Social Return). Het controleren of de leverancier/dienstverlener hieraan voldoet, valt niet onder de P-wet, IOAW of IOAZ.
- Onderzoek naar de effectiviteit van de uitvoering van wet- en regelgeving.
- De uitvoering van andere wetten zoals WMO, de Jeugdwet, de wet op de lijkbezorging, (bestaande) WSW.
- Voor de uitvoering van gemeentelijke incasso. Alleen voor de gemeentelijke belastingdeurwaarders geldt dat zij een overeenkomst hebben op grond van art. 5.23 van het Besluit Suwi en conform het Aansluitprotocol (Bijlage III Regeling Suwi). Daarmee hebben zij een eigen aansluiting op Suwinet.

Bijlage 5 Afbakening werkzaamheden Suwinet

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

- Suwinet Inkijk
- Suwinet Inlezen
- DKD-Inlezen
- WGS Inkijk
- WGS Inlezen[4]

BKWI heeft aangegeven dat zij van plan zijn om oktober (2022) aan alle gemeenten een overzicht te verstrekken van de door hun gebruikte Suwinet-services (ook gebruik door GSD's e.d.). In principe zal DKD Inlezen in het overzicht worden meegenomen, aangezien BKWI verantwoordelijk is voor de techniek en de administratie.

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

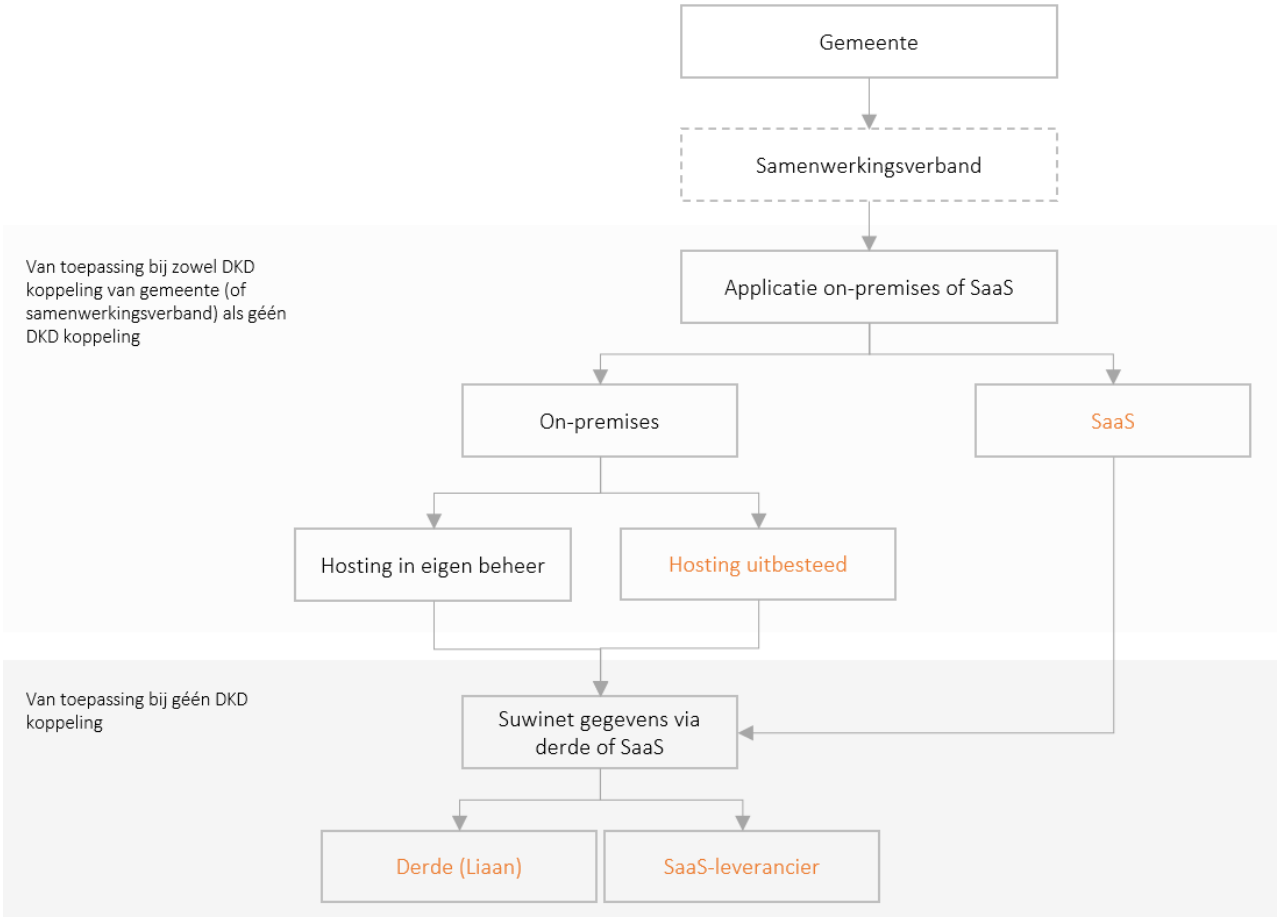
Met name de voorzieningen Suwinet Inlezen, Suwinet DKD-Inlezen en WGS-Inlezen zijn minder zichtbaar aanwezig bij de gemeenten omdat de Suwinet gegevens via een koppeling in de applicatie van de gemeente wordt geladen. Hierbij bestaat de mogelijkheid dat een derde partij ook een rol in het proces speelt,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

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

1. Gemeente[5] heeft een DKD koppeling. De gemeente host de applicatie in eigen beheer. De applicatie kan ook worden gehost bij een derde partij.
2. Gemeente heeft een DKD koppeling. De gemeente maakt gebruik van een SAAS-oplossing
3. Gemeente heeft geen DKD koppeling. De gemeente maakt gebruik van een SAAS-oplossing, waarin DKD-gegevens zijn opgenomen. Deze gegevens zijn afkomstig van een tussenpartij, zoals bijvoorbeeld Liaan. Dit voorbeeld betreft bijvoorbeeld de Snelbalie van Centric.
4. Gemeente heeft geen DKD koppeling. De gemeente host de applicatie in eigen beheer. Deze gegevens zijn afkomstig van een tussenpartij, zoals bijvoorbeeld Liaan. De applicatie kan ook worden gehost bij een derde partij.

[4] WGS Inlezen is naar verwachting actief vanaf medio november 2022. Indien de gemeente WGS Inlezen in 2022 activeert, maakt deze wel onderdeel uit van de scoping voor ENSIA 2022.

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



Afbeelding: Stroomdiagram DKD-inlezen

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

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

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

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

Reikwijdte verantwoording

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

De Autoriteit Persoonsgegevens (AP) heeft indertijd onderzoek gedaan naar de aansluiting van niet-SUWI-partijen op Suwinet (november 2014). Bij dit onderzoek heeft de AP vastgesteld dat in

een aantal overeenkomsten sprake is van toepassing van Suwinet-Inlezen. Op grond van het wettelijk kader SUWI heeft de AP geconcludeerd dat de beheerder BKWI net als bij Suwinet-Inkijk, overzicht en controle moet hebben over het feitelijk gegevensgebruik door afnemers. Deze toelichting onderstreept ook op deze criteria het belang van beveiliging.

General IT Controls bij het gebruik van Suwinet Inlezen, DKD inlezen en GWS-Inlezen
Om een uitspraak te kunnen doen inzake de betrouwbaarheid en bruikbaarheid van de logbestanden voor Suwinet Inlezen / DKD-Inlezen / GWS-Inlezen (het gaat hier met name norm om 12.4.1), dient aan een aantal randvoorwaarden (ITGC) te zijn voldaan. Aangezien Suwinet Inlezen, DKD Inlezen en GWS-Inlezen van toepassing kunnen zijn op diverse applicaties die elk voor zich anders ingericht kunnen zijn, is geen éénduidig normenkader beschikbaar te stellen. De IT-auditor dient zelf, op basis van een (beknopte) omgevings- en risicoanalyse, te bepalen welke ITGC controls van belang kunnen zijn om de betrouwbaarheid en bruikbaarheid van de logbestanden te waarborgen. Tevens moet hij zijn afweging documenteren.
E.e.a is dus afhankelijk van de omgevings- en risicoanalyse, maar de domeinen waaraan naar verwachting aandacht aan geschonken dient te worden, zijn:

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

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

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

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

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

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

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

Schuldhulpverlening
De Wet Schuldhulpverlening is in de loop van 2021 van kracht geworden. Gemeenten kunnen ten behoeve van uitvoering van deze wet een aparte aansluiting Suwinet aanvragen (WGS Inkijk of WGS Inlezen). De uitrol vindt gefaseerd plaats in 2021 respectievelijk (november) 2022. Voor verantwoordingsjaar 2022 dient een actieve GWS Inkijk of GWS Inlezen mede te worden verantwoord conform de systematiek die SZW hanteert voor de ENSIA-toetsing. Hierbij zijn de maatregelen voor GWS Inkijk gelijk aan Suwinet Inkijk en WGS Inlezen gelijk aan DKD Inlezen.

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

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