

Bijlage A3 Rapport van bevindingen Suwinet Inkijk carve-out P-wet

Bij het door BKBO bv uitgevoerde IT assessment geven we als IT auditor assurance op basis van een attest opdracht. Dat wil zeggen dat we nagaan of de bewering van het dagelijks bestuur over de beveiliging van Suwinet getrouw is.

In het kader van deze assurance opdracht hebben wij de volgende werkzaamheden uitgevoerd:

- 1 Uitvoeren risicoanalyse. Op basis van de eigen risicoanalyse, zoals die voor elke audit wordt uitgevoerd, hebben we vastgesteld wat de diepgang van onze werkzaamheden zal zijn gegeven de veronderstelde kwaliteit van oplevering van de gegevensverzameling.
- 2 Kennisnemen van de uitgevoerde controlewerkzaamheden (zelfevaluatie) door de gemeente Westervoort.
- 3 Vervolgens hebben we als IT-auditor aanvullende werkzaamheden verricht, zoals:
 - het inventariseren van de opzet en het vaststellen van het bestaan en/of de werking van de relevante maatregelen m.b.t. de webapplicatie Suwinet Inkijk. Dit door middel van het kennis nemen van documentatie en de resultaten van de uitgevoerde interne controles van de gemeente Westervoort en eigen waarnemingen.
 - het houden van interviews met de verantwoordelijke functionarissen Alexander Zagkotsis (Interim CISO), Dunja Hogenkamp (SO Suwi), Jos Thijssen (voormalig CISO/FG), Ronald Vollenberg (CISO Zevenaar), vooral gericht op het onderkennen van risico's en het onderzoek in hoeverre deze risico's worden afgedekt door maatregelen.
- 4 Oordeelsvorming per individuele norm.
- 5 Concept rapportage. Opstellen van de voorliggende bijlage en het assurancerapport.
- 6 Toepassen "hoor en wederhoor" met de gemeente Westervoort.
- 7 Verwerking resultaten van de "hoor en wederhoor" in de definitieve assurance rapportage en bijlagen
- 8 Ingeval van een ENSIA rapportage, wordt de rapportage op een speciale wijze gewaarmerkt.

Over de beveiliging van de volgende taak wordt gerapporteerd in deze bijlage:

Taak	Organisatie	Opmerkingen over het uitgevoerde onderzoek
Suwi-taak: uitvoering van de Participatiewet/IOAW/IOAZ	Uitbesteed aan RSD De Liemers	Onderzoek is uitgevoerd conform Richtlijn 3000A Attest opdrachten gesteund op de TPM van RSD De Liemers.
Suwi taak: uitvoering Wet Gemeentelijke Schuldhulpverlening door schuldhulpverleners (uitsluitend schuldhulpverlening voor zelfstandig ondernemers)	Uitbesteed aan RSD De Liemers	Onderzoek is uitgevoerd conform Richtlijn 3000A Attest opdrachten gesteund op de TPM van RSD De Liemers.

Buiten scope van het onderzoek

Het verwerken van gegevens door het Inlichtingenbureau valt buiten de scope van ons onderzoek. De verwerking binnen de organisatie van noch RSD De Liemers noch de gemeente Westervoort (papieren stroom, aanvraagprocessen, etc.) ondersteund door eigen applicaties is eveneens niet betrokken in de ENSIA-verantwoording en controle door de IT-auditor.

Hieronder treft u een beschrijving van de uitgevoerde werkzaamheden aan. Ons onderzoek was beperkt tot de normen die onderdeel zijn van de Verantwoordingsrichtlijn 2023. Uitdrukkelijk merken wij op dat we geen onderzoek hebben uitgevoerd naar de werking van de interne beheersingsmaatregelen.

Om de leesbaarheid van dit rapport te vergroten zijn de oordelen in deze tabel weergegeven als "voldoet" (met de kleur groen) of "voldoet niet" (met de kleur rood). Hierbij moet "voldoet" worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven norm effectief zijn opgezet en geïmplementeerd op 20 maart 2024". "Voldoet niet" moet worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven norm niet in alle materiële opzichten effectief zijn opgezet en/of geïmplementeerd op 20 maart 2024". De kleur grijs staat voor 'geen oordeel', dit houdt in dat de norm niet van toepassing is.

De uitspraak “voldoet” of “voldoet niet” beperkt zich tot de eigen oordeelsvorming van de auditor.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
5.1.1 Beleidsregels voor informatie-beveiliging (Ref 2019: Suwinet: B.01) <u>Betrokken partij(en):</u> Gemeente/ samenwerkings-partij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD	<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 aantoonbaar aan de vereiste beveiligingsvoorwaarden voldoet. <u>Risico:</u> Het risico bestaat dat de bescherming van de aansluiting op Suwinet, in tegenstelling tot bescherming van haar eigen ICT omgeving, onvoldoende aandacht krijgt.	Inspectie van het beleid en vaststellen dat het beleid is vastgesteld door de leiding van de organisatie. Kennisnemen van de aangeleverde assurance rapportage, uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen.		Er is een informatiebeveiligingsplan/-beleid aangeleverd. Daarnaast is er een speciaal voor Suwinet ontwikkeld informatiebeveiligingsbeleid/-plan Suwinet aangeleverd. We hebben vastgesteld dat uw informatiebeveiligingsbeleid is gebaseerd op de BIO. <u>Formele vaststelling</u> Het informatiebeveiligingsbeleid is vastgesteld door de directie daartoe gemandateerd door het bestuur. <u>Publicatie</u> Het informatiebeveiligingsbeleid is gepubliceerd en kenbaar gemaakt aan alle medewerkers (eigen personeel en inhuur). Aanbevelingen voor de gemeente Westervoort: • Er is sprake van een complexe samenwerkingsstructuur. Houd de beleidstukken van de samenwerkingspartners tegen het licht en harmoniseer en actualiseer deze waar mogelijk en nodig. • Wijzig het bestaande informatiebeveiligingsbeleid zodanig dat het is gebaseerd op de Baseline Informatiebeveiliging Overheid. Laat het gewijzigde informatiebeveiligingsbeleid daarna opnieuw formeel vaststellen door het bestuur • Pas het informatiebeveiligingsbeleid elke bestuursperiode aan en neem de aanbevelingen daarin mee. • Het Suwi assurancerapport van de serviceorganisatie/partij waaraan u Suwinet taken heeft uitbesteed bevat informatie die voor u als gebruikersorganisatie van belang is. Neem daarom kennis van dit rapport en besteed daarbij speciaal aandacht aan het hoofdstuk 'Verantwoordelijkheden gebruikersorganisatie'. Hierin staat per norm beschreven welke maatregelen u zelf dient te nemen om aan de betreffende norm te kunnen voldoen.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
5.1.2 Beoordeling van het informatie-beveiligingsbeleid (Ref 2019: Suwinet: C.01) <u>Betrokken partij(en):</u> Gemeente/ samenwerkings-partij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inlijk Suwinet Inlezen Suwinet DKD	<u>Criterium BIO:</u> Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is. <u>Doelstelling:</u> Bewerkstellingen dat de getroffen beveiligingsmaatregelen continue voldoen aan het juiste beveiligingsniveau. <u>Risico:</u> De getroffen beveiligingsmaatregelen kunnen ontoereikend zijn in relatie tot aangescherpte wetgeving, verandering van risicoklasse van gegevens en de toegepaste technologieën.	Kennisnemen van de aangeleverde assurance rapportage, uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen.		<u>De gemeente Westervoort</u> Het bestuur en het management dienen actief het informatiebeveiligingsbeleid en -plan binnen de eigen organisatie uit te dragen. Om zo te borgen dat haar medewerkers bekend zijn met de inhoud en betekenis van het informatiebeveiligingsbeleid en -plan. Een informatiebeveiligingsbeleid en -plan zonder opvolging en naleving zijn zinloos. Geconstateerd is dat de gemeente Westervoort taken waarvoor Suwinet wordt gebruikt, heeft uitbesteed aan RSD De Liemers. Zie hiervoor norm 6.1.1. <u>RSD De Liemers</u> Op basis van het assurancerapport van de door RSD De Liemers ingeschakelde IT auditor, kunnen we vaststellen dat de vereiste interne beheersmaatregelen daadwerkelijk zijn geïmplementeerd door RSD De Liemers.
6.1.1 Rollen en verantwoordelijkheden bij informatie-beveiliging (Ref 2019: Suwinet: B.04) <u>Betrokken partij(en):</u> Gemeente/ samenwerkings-	<u>Criterium BIO:</u> Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. <u>Doelstelling:</u> 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. <u>Risico:</u>	Kennisnemen van de aangeleverde assurance rapportage, uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen.		<u>RSD De Liemers</u> Alle verantwoordelijkheden voor informatiebeveiliging behoren bij RSD De Liemers duidelijk te zijn gedefinieerd (in de vorm van een bijvoorbeeld een RACI-matrix) ¹ De gedocumenteerde rollen zijn door het bestuur 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. <u>Uitbesteding aan RSD De Liemers</u>

¹ RACI staat voor Responsible, Accountable, Consulted en Informed.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
partij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD	Het risico bestaat dat door gebrek aan coördinatie van activiteiten niet op beveiligingsincidenten wordt geacteerd en dat door wijzigingen nieuwe kwetsbaarheden ontstaan.			Geconstateerd is dat de gemeente Westervoort taken waarvoor Suwinet wordt gebruikt, heeft uitbesteed aan RSD De Liemers. De uitbesteding door de gemeente Westervoort aan RSD De Liemers is geregeld naar publiekrecht. De uitbesteding, die in deze bijlage wordt verantwoord, betreft: - De uitvoering van de Participatiewet (werk en inkomen) - De uitvoering Wet Gemeentelijke Schuldhulpverlening door schuldhulpverleners (beperkt). Opdrachtgever heeft in een overeenkomst naar privaatrecht dan wel in een regeling naar publiek recht vastgelegd dat de gestelde interne beheersmaatregelen voor Suwinet qua opzet onverkort van toepassing zijn. <u>Assurance over beheersingsmaatregelen Suwinet</u> Op basis van het assurancerapport van de door RSD De Liemers ingeschakelde IT auditor, kunnen we vaststellen dat de vereiste interne beheersmaatregelen daadwerkelijk zijn geïmplementeerd door RSD De Liemers. Aanbevelingen voor de gemeente Westervoort: - We hebben geconstateerd dat uw organisatie een Gemeenschappelijke Regeling is aangegaan met RSD De Liemers. Deze GR dient door uw organisatie op https://www.overheid.nl/ onder de zoekleutel https://zoek.overheid.nl/lokale wet en regelgeving te worden gepubliceerd. Ga na of u de tekst van de GR zelf heeft gepubliceerd via de daartoe geëigende kanalen. - Vertaal uw informatiebeveiligingsbeleid naar te nemen maatregelen voor de door u opgerichte samenwerkingsverbanden of die waarin uw gemeente een deelname heeft.
6.1.2 Scheiding van taken (Ref 2019: Suwinet: B.05)	<u>Criterium BIO:</u> Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of	Kennisnemen van de aangeleverde assurance rapportage, uitgevoerde controlewerkzaamhe		Geconstateerd is dat de gemeente Westervoort taken waarvoor Suwinet wordt gebruikt, heeft uitbesteed aan RSD De Liemers. <u>Assurance over beheersingsmaatregelen Suwinet</u>

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
<u>Betrokken partij(en):</u> Gemeente/ samenwerkings- partij/ IT- serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD	misbruik van de bedrijfsmiddelen ² van de organisatie te verminderen. <u>Doelstelling:</u> Ervor 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.	den, gerichte deelwaarnemingen.		Op basis van het assurancerapport van de door RSD De Liemers ingeschakelde IT auditor, kunnen we vaststellen dat de vereiste interne beheersmaatregelen daadwerkelijk zijn geïmplementeerd door RSD De Liemers.
7.2.2 Bewustzijn, opleiding en training ten aanzien van informatie-beveiliging (Ref 2019: Suwinet: AP) <u>Betrokken partij(en):</u>	<u>Criterium BIO:</u> 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. <u>Doelstelling:</u>	Kennisnemen van de aangeleverde assurance rapportage, uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen.		Geconstateerd is dat de gemeente Westervoort taken waarvoor Suwinet wordt gebruikt, heeft uitbesteed aan RSD De Liemers. <u>Assurance over beheersingsmaatregelen Suwinet</u> Op basis van het assurancerapport van de door RSD De Liemers ingeschakelde IT auditor, kunnen we vaststellen dat de vereiste interne beheersmaatregelen daadwerkelijk zijn geïmplementeerd door RSD De Liemers.

² Onder bedrijfsmiddelen worden in dit verband de Suwinet gegevens (mede) begrepen.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
Gemeente/ samenwerkings- partij/ IT- serviceorganisatie <u>Scope:</u> Suwinet Inrijck Suwinet Inlezen Suwinet DKD	Het bewustmaken van gebruikers van Suwinet gegevens. <u>Risico:</u> Indien gebruikers van Suwinet gegevens zich niet of onvoldoende bewust zijn van de (hoge) vertrouwelijkheid, bestaat het risico dat deze gegevens onvoldoende worden beschermd.			
9.2.1 Registratie en afmelden van gebruikers (Ref 2019: Suwinet: U.02, U.03) <u>Betrokken partij(en):</u> Gemeente/ samenwerkings- partij/ IT- serviceorganisatie <u>Scope:</u> Suwinet Inrijck Suwinet Inlezen Suwinet DKD	<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 krijgen vanuit het domein van een ander op Suwinet aangesloten organisatie.	Kennisnemen van de aangeleverde assurance rapportage, uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen.		Geconstateerd is dat de gemeente Westervoort taken waarvoor Suwinet wordt gebruikt, heeft uitbesteed aan RSD De Liemers. <u>Assurance over beheersingsmaatregelen Suwinet</u> Op basis van het assurancerapport van de door RSD De Liemers ingeschakelde IT auditor, kunnen we vaststellen dat de vereiste interne beheersmaatregelen daadwerkelijk zijn geïmplementeerd door RSD De Liemers.
9.2.2 Gebruikers toegang verlenen	<u>Criterium BIO:</u> Een formele gebruikerstoegangsverleningsprocedure	Kennisnemen van de aangeleverde assurance		Geconstateerd is dat de gemeente Westervoort de taken waarvoor Suwinet worden gebruikt, heeft uitbesteed aan RSD De Liemers.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
(Ref 2019: Suwinet: U.02) <u>Betrokken partij(en):</u> Gemeente/ samenwerkings- partij/ IT- serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD	behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. <u>Doelstelling</u> Bewerkstelligen dat de geclaimde identiteit van de gebruiker kan worden bewezen en dat daardoor alleen bevoegde gebruikers toegang krijgen tot Suwinet diensten. <u>Risico:</u> Onbevoegde gebruikers kunnen toegang krijgen tot Suwinet diensten.	rapportage, uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen.		<u>Assurance over beheersingsmaatregelen Suwinet</u> Op basis van het assurancerapport van de door RSD De Liemers ingeschakelde IT auditor, kunnen we vaststellen dat de vereiste interne beheersmaatregelen daadwerkelijk zijn geïmplementeerd door RSD De Liemers.
9.2.5 Beoordeling van toegangsrechten van gebruikers (Ref 2019: Suwinet: C.04) <u>Betrokken partij(en):</u> Gemeente/ samenwerkings- partij/ IT- serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD	<u>Criterium BIO:</u> 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 functiescheidingen zijn toegepast en voldaan wordt aan de principes van doelbinding en proportionaliteit, oneigenlijke autorisatie-toekenningen hebben plaatsgevonden. <u>Risico:</u> Bij het ontbreken van controle op de toegangsrechten worden afwijkingen in het autorisatieproces niet gesignaleerd.	Kennisnemen van de aangeleverde assurance rapportage, uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen.		Geconstateerd is dat de gemeente Westervoort taken waarvoor Suwinet wordt gebruikt, heeft uitbesteed aan RSD De Liemers. <u>Assurance over beheersingsmaatregelen Suwinet</u> Op basis van het assurancerapport van de door RSD De Liemers ingeschakelde IT auditor, kunnen we vaststellen dat de vereiste interne beheersmaatregelen daadwerkelijk zijn geïmplementeerd door RSD De Liemers.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
9.2.6 Toegangsrechten intrekken of aanpassen (Ref 2019: Suwinet: U.02) <u>Betrokken partij(en):</u> Gemeente/ samenwerkings- partij <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD	<u>Criterium BIO:</u> De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast. <u>Doelstelling:</u> Het tijdig beëindigen of wijzigen van de toegangsrechten. <u>Risico:</u> Als toegangsrechten niet tijds worden beëindigd of gewijzigd, bestaat het risico op onbevoegde kennisname van Suwinet gegevens.	Kennisnemen van de aangeleverde assurance rapportage, uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen.		Geconstateerd is dat de gemeente Westervoort taken waarvoor Suwinet wordt gebruikt, heeft uitbesteed aan RSD De Liemers. <u>Assurance over beheersingsmaatregelen Suwinet</u> Op basis van het assurancerapport van de door RSD De Liemers ingeschakelde IT auditor, kunnen we vaststellen dat de vereiste interne beheersmaatregelen daadwerkelijk zijn geïmplementeerd door RSD De Liemers.
10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen (Ref 2019: Suwinet: U.11) <u>Betrokken partij(en):</u> Gemeente/ samenwerkings- partij/ IT- serviceorganisatie	<u>Criterium BIO:</u> Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd. <u>Doelstelling:</u> Het voorkomen van ongeautoriseerde toegang tot netwerkdiensten. <u>Risico:</u> Ondanks het besloten karakter van Suwinet bestaat het risico dat de	Kennisnemen van de aangeleverde assurance rapportage, uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen.		<u>Toelichting</u> RSD De Liemers maakt voor de in deze bijlage verantwoorde taak alleen gebruik van Suwinet Inkijk.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
<u>Scope:</u> Suwinet Inlezen Suwinet DKD	toegang tot gegevens niet adequaat is beschermd.			
12.1.1 Gedocumenteerde bedieningsprocedures (Ref 2019: Suwinet: nieuw) <u>Betrokken partij(en):</u> Gemeente/ samenwerkingspartij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD	<u>Criterium BIO:</u> Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben. <u>Doelstelling:</u> Correcte en veilige bediening van informatie verwerkende faciliteiten waarborgen. <u>Risico:</u> Als gebruikers en/ of beheerders niet kunnen beschikken over bedieningsprocedures (handleidingen) bestaat het risico dat (kritieke) informatie verwerkende faciliteiten niet correct en/ of veilig worden bediend.	Kennisnemen van de aangeleverde assurance rapportage, uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen.		Geconstateerd is dat de gemeente Westervoort taken waarvoor Suwinet wordt gebruikt, heeft uitbesteed aan RSD De Liemers. <u>Assurance over beheersingsmaatregelen Suwinet</u> Op basis van het assurancerapport van de door RSD De Liemers ingeschakelde IT auditor, kunnen we vaststellen dat de vereiste interne beheersmaatregelen daadwerkelijk zijn geïmplementeerd door RSD De Liemers. Aanbevelingen voor de gemeente Westervoort: - Het implementeren van wijzigingsbeheer is een zeer belangrijke beheersmaatregel. Gebruik formele procedures voor wijzigingsbeheer. Stel een wijzigingsadviescommissie in en stel een wijzigingsbeheerder aan. - Gebruik in verband met het vele thuiswerken alleen veilige video vergadertools, die bij voorkeur AES 256 bit TLS encryptie kent voor der verbinding van en naar de client, unieke vergader id's om vergaderingen af te schermen ondersteunt , ISAE 3000 of SOC-2 gecertificeerd is en ingeval het een cloudoplossing betreft compliant is aan AVG/GDPR of EU SchremsII, het datacenter heeft in de EU en de verwerking plaatsvindt in de EU.
12.4.1 Gebeurtenissen registreren (Ref 2019: Suwinet: C.06) <u>Betrokken partij(en):</u> Gemeente/ samenwerkingspartij/ IT-serviceorganisatie	<u>Criterium BIO:</u> Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. <u>Doelstelling:</u> Bewerkstellingen dat tijdig correctieve maatregelen kunnen worden getroffen om informatie te kunnen verschaffen over activiteiten van gebruikers en beheerders van de Suwinet diensten en	Kennisnemen van de aangeleverde assurance rapportage, uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen.		Geconstateerd is dat de gemeente Westervoort taken waarvoor Suwinet wordt gebruikt, heeft uitbesteed aan RSD De Liemers. <u>Assurance over beheersingsmaatregelen Suwinet</u> Op basis van het assurancerapport van de door RSD De Liemers ingeschakelde IT auditor, kunnen we vaststellen dat de vereiste interne beheersmaatregelen daadwerkelijk zijn geïmplementeerd door RSD De Liemers.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
<u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD	vaststellen of oneigenlijk gebruik of misbruik is gemaakt van autorisatie. <u>Risico:</u> Afwijkingen worden niet gesignaleerd en kunnen derhalve niet worden aangepakt.			
12.4.2 Beschermen van informatie in logbestanden (Ref 2019: Suwinet: C.05) <u>Betrokken partij(en):</u> Gemeente/ samenwerkings-partij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inlezen Suwinet DKD	<u>Criterium BIO:</u> Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang. <u>Doelstelling:</u> Alle handelingen die betrekking hebben op gebruikers en beheerders moeten herleidbaar zijn naar individuele personen. <u>Risico:</u> Zonder vastlegging en bewaking kan achteraf niet worden vastgesteld wie bepaalde handelingen heeft uitgevoerd.	Kennisnemen van de aangeleverde assurance rapportage, uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen.		<u>Toelichting</u> RSD De Liemers maakt voor de in deze bijlage verantwoorde taak alleen gebruik van Suwinet Inkijk.
18.1.4 Privacy en bescherming van persoonsgegevens (Ref 2019: Suwinet: nieuw) <u>Betrokken partij(en):</u> Gemeente/ samenwerkings-partij/ IT-serviceorganisatie	<u>Criterium BIO:</u> Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. <u>Doelstelling:</u> Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende het verwerken van persoonsgegevens.	Kennisnemen van de aangeleverde assurance rapportage, uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen.		<u>Verwerkingsverantwoordelijke</u> Geconstateerd is dat de gemeente Westervoort taken waarvoor Suwinet wordt gebruikt, heeft uitbesteed aan RSD De Liemers. De via Suwinet verzamelde gegevens worden overgedragen aan RSD De Liemers. Afhankelijk van het type overdracht is RSD De Liemers verwerkingsverantwoordelijke of verwerker vanaf het moment van overdracht. De gemeente Westervoort blijft er voor verantwoordelijk dat Suwi gegevens niet worden hergebruikt of doorgeleverd voor andere doeleinden dan waarvoor de gegevens oorspronkelijk verzameld zijn. Dit is bepaald in de geheimhoudingsplicht van artikel 74 van de wet Suwi. <u>Assurance over beheersingsmaatregelen Suwinet</u>

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
<u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD	<u>Risico:</u> Als de verwerking van Suwinet (persoons)gegevens niet overeenkomstig toepasselijke wet- en regelgeving plaatsvindt, wordt hierdoor de AVG overtreden.			Op basis van het assurancerapport van de door RSD De Liemers ingeschakelde IT auditor, kunnen we vaststellen dat de vereiste interne beheersmaatregelen niet allemaal daadwerkelijk zijn geïmplementeerd door RSD De Liemers. Dwingende aanbeveling voor de gemeente Westervoort: Draag RSD De Liemers op om de geconstateerde problemen met spoed op te lossen.