Bijlage A4 Rapport van bevindingen Suwinet Inkijk Bijzondere bijstand en Sociale recherche

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 Duiven.
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. Dit door middel van het kennis nemen van documentatie, het kennis nemen van de resultaten van de uitgevoerde interne controles van de gemeente Duiven 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 uit de Verantwoordingsrichtlijn.
5 Concept rapportage. Opstellen van de voorliggende bijlage en het assurancerapport. Verificatie van de aansluiting van de bijlagen op de bewering van het bestuur.
6 Toepassen "hoor en wederhoor" met de gemeente Duiven.
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 Bijzondere Bijstand in het kader van de Participatiewet	Uitgevoerd door de gemeente Duiven	Onderzoek is uitgevoerd conform Richtlijn 3000A Attest opdrachten. Er wordt voor de uitvoering van deze taak uitsluitend gebruik gemaakt van Suwinet-Inkijk.
Suwi-taak: uitvoering Sociale Recherche in het kader van de Participatiewet	Uitgevoerd door de gemeente Duiven	Onderzoek is uitgevoerd conform Richtlijn 3000A Attest opdrachten. Er wordt voor de uitvoering van deze taak uitsluitend gebruik gemaakt van Suwinet-Inkijk.

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 de gemeente Duiven (papieren stroom, aanvraagprocessen, etc.) ondersteund door eigen applicaties is 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 2022. 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 informatiebeveiliging <u>Betrokken partij(en):</u> Gemeente/ samenwerkingspartij/ 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>	Inspectie van het beleid en vaststellen dat het beleid is vastgesteld door de leiding van de organisatie. Kennisnemen van de door de gemeente Duiven uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen en -indien noodzakelijk- aanvullende interviews met de sleutel-functionarissen.		Er is een organisatiebreed informatiebeveiligingsbeleid en daarnaast een speciaal voor Suwinet ontwikkeld beveiligingsbeleid/-plan aangeleverd. <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). Aanbeveling voor de gemeente Duiven: • 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.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	Het risico bestaat dat de bescherming van de aansluiting op Suwinet, in tegenstelling tot bescherming van haar eigen ICT omgeving, onvoldoende aandacht krijgt. Maatregel 5.1.1.1 Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat ten minste de volgende punten: a) De strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid. b) De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden. c) De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers. d) De gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn. e) De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd. f) De bevordering van het beveiligingsbewustzijn.			

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	Toelichting: De organisatie moet beschikken over een Suwinet informatiebeveiligings-beleid (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.			
5.1.2 Beoordeling van het informatie-beveiligingsbeleid Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD	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. Maatregel 5.1.2.1 Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli	Inspectie van het beveiligingsbeleid en vaststellen dat het beleid actueel is en conform de (bestaande) bestuurs- en P&C-cycli is bijgesteld. Kennisnemen van de door de gemeente Duiven uitgevoerde controlewerkzaam-heden, gerichte deelwaarnemingen en -indien noodzakelijk- aanvullende interviews met de sleutel-functionarissen.		Het informatiebeveiligingsbeleid is in de huidige bestuursperiode geactualiseerd. Het informatiebeveiligingsbeleid wordt aantoonbaar minimaal één keer per bestuursperiode of bij grote wijzigingen binnen de organisatie opnieuw beoordeeld en indien nodig aangepast. 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. Over de voortgang in het bereiken van de beveiligingsdoelstellingen wordt periodiek, minimaal jaarlijks, intern gerapporteerd via de ENSIA verantwoordingssystematiek. De voortgang wordt aantoonbaar jaarlijks besproken tussen bestuur en management. Over de voortgang in het bereiken van de beveiligingsdoelstellingen wordt periodiek, minimaal jaarlijks, intern gerapporteerd via de ENSIA verantwoordingssystematiek.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	en externe ontwikkelingen beoordeeld en zo nodig bijgesteld. Toelichting: Het Suwinet informatiebeveiligingsbeleid (eventueel als onderdeel van het algehele informatiebeveiligingsbeleid) dient actueel te zijn en periodiek[1] te worden beoordeeld en zo nodig te worden bijgesteld bij grote wijzigingen of aan de hand van externe ontwikkelingen.			
6.1.1 Rollen en verantwoordelijk-heden bij informatie-beveiliging Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD	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. Maatregel 6.1.1.1 De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van	Inspectie van het beleid. Vaststellen dat taken, bevoegdheden en verantwoordelijkheden (CTFS) ten aanzien van de IB functie t.a.v. Suwinet formeel zijn vastgesteld. Vaststelling dat deze functies en onderliggende rol(-len) ook als zodanig zijn ingericht en beschreven. Vaststelling dat een incidentenproces t.a.v. Suwinet is ingericht. Vaststelling dat incidenten worden geanalyseerd en		De beveiligingsrollen van het lijnmanagement, de proces verantwoordelijke(n) en de systeem- en/of gegevenseigenaar zijn belegd. De governance voor informatiebeveiliging is vastgesteld door het bestuur. We hebben geconstateerd dat omtrent Suwinet het volgende is geregeld: • De Inspectie SZW is de verticale toezichthouder voor Suwinet; • BKWI is als beheerder van Suwinet verantwoordelijk voor de landelijke operationele beschikbaarheid van Suwinet; • Het dagelijks bestuur is bestuurlijk verantwoordelijk; • De proceseigenaar is verantwoordelijk voor het rechtmatig gebruik van Suwinet; qua beschikbaarheid, integriteit en vertrouwelijkheid is de proceseigenaar ambtelijk verantwoordelijk; • De gebruikersbeheerders van Suwinet zijn verantwoordelijk voor het autorisatieproces en de juistheid en actualiteit van de automatisatiematrix. De gebruikersbeheerder kan met de autorisatiematrix in de hand de gebruikersadministratie bijwerken; • De security officer Suwinet is verantwoordelijk voor de controles op logging en het juist gebruik van Suwinet; • De gemandateerde is verantwoordelijk voor het tijdig periodiek binnenhalen van de rapportages over het systeemgebruik;

[1] *Hiervoor geldt dat de periodiciteit aansluit bij de (bestaande) bestuurs- en P&C-cycli. Voor gemeenten geldt dat dit de raadsperiode (4 jaar) is.*

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	informatiebeveiliging binnen haar organisatie. Maatregel 6.1.1.3 De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd. Maatregel 6.1.1.4 Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel. <u>Toelichting:</u> 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.	gerapporteerd aan het verantwoordelijk management en dat waar nodig aanvullende maatregelen worden getroffen. Kennisnemen van de door de gemeente Duiven uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen en -indien noodzakelijk- aanvullende interviews met de sleutel-functionarissen.		• De medewerkers zijn verantwoordelijk voor het juiste gebruik door henzelf van Suwinet. De rol van CISO is zowel beschreven als geformaliseerd en concreet aan een daartoe deskundige medewerker van de organisatie toegewezen. Er wordt een register van (beveiligings)incidenten bijgehouden. Met betrekking tot Suwinet hebben zich geen incidenten voorgedaan. Er is minimaal één beveiligingsincident aangeleverd, op grond waarvan we kunnen vaststellen dat beveiligingsincidenten adequaat worden gevolgd, geanalyseerd en opgelost. • De gebruikersbeheerders van Suwinet zijn verantwoordelijk voor het autorisatieproces en de juistheid en actualiteit van de automatisatiematrix. De gebruikersbeheerder kan met de autorisatiematrix in de hand de gebruikersadministratie bijwerken; • De security officer Suwinet is verantwoordelijk voor de controles op logging en het juist gebruik van Suwinet; • De gemandateerde is verantwoordelijk voor het tijdig periodiek binnenhalen van de rapportages over het systeemgebruik; • De medewerkers zijn verantwoordelijk voor het juiste gebruik door henzelf van Suwinet.
6.1.2 Scheiding van taken <u>Betrokken partij(en):</u> Gemeente/ samenwerkingspartij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen	<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[2] van de organisatie te verminderen. <u>Doelstelling:</u> Ervoor zorgen dat de juiste taken en verantwoordelijkheden binnen de	Inspectie van taakbeschrijvingen, autorisatiematrix en autorisatiebeheer-proces. Kennisnemen van de door de gemeente Duiven uitgevoerde controlewerkzaam-heden, gerichte deelwaarnemingen		De taken en verantwoordelijkheden voor het gebruik en het beheer van Suwinet zijn naar rato van de organisatiegrootte o.i. voldoende gescheiden. Er is een actuele autorisatie toekenningsmatrix of RACI model of een schematisch overzicht van de functies/rollen en bijbehorende autorisaties (matrix) van Suwinet aangeleverd. Hierdoor is bekend wie welke functie heeft en dus welke pagina's en/of functionaliteiten geraadpleegd mogen worden.

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

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
Suwinet DKD	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. Maatregel 6.1.2.1 Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen. <u>Toelichting:</u> Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd (in de vorm van bijvoorbeeld een RACI-matrix[3]) De gedocumenteerde rollen zijn door het dagelijks bestuur/ de directie (dit kan per gemeente verschillen) onderkend, goedgekeurd en van toepassing verklaard. Taken en	en -indien noodzakelijk- aanvullende interviews met de sleutel-functionarissen.		

[3] *RACI staat voor Responsible, Accountable, Consulted en Informed. Idealiter onderdeel van een ingerichte AO/IB.*

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	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.			
7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD	Criterium BIO: Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie. Doelstelling: Het bewustmaken van gebruikers van Suwinet gegevens. Risico: Indien gebruikers van Suwinet gegevens zich niet of onvoldoende bewust zijn van de (hoge) vertrouwelijkheid, bestaat het risico dat deze gegevens onvoldoende worden beschermd. Maatregel 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.	Kennisnemen van de door de gemeente Duiven uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen en -indien noodzakelijk- aanvullende interviews met de sleutel-functionarissen.		We hebben vastgesteld dat het management er aantoonbaar voor zorg draagt, dat de medewerkers voldoende kennis en bewustzijn hebben op het gebied van informatiebeveiliging. Training I-bewustzijn We hebben vastgesteld dat alle medewerkers die gebruik maken van Suwinet een training I-bewustzijn hebben gevolgd binnen drie maanden na indiensttreding. Hiervan wordt een centrale registratie bijgehouden.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	Maatregel 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. 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.			
9.2.1 Registratie en afmelden van gebruikers Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD	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	Kennisnemen van de door de gemeente Duiven uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen en -indien noodzakelijk- aanvullende interviews met de sleutel-functionarissen.		Er is een actueel overzicht van *alle* personen die beheeraccounts of een gebruikersaccount voor Suwinet hebben, beschikbaar. Suwinet Inkijk Alle gebruikers en beheerders hebben aantoonbaar een unieke inlognaam (identificatie). BKWI regelt dit namelijk. Vastgesteld is dat alle gebruikers van Suwinet andere gebruikers ID's gebruiken dan voor de kantoorautomatiseringsomgeving het geval is. Er worden geschikte technieken gebruikt om de identiteit van de gebruiker/ beheerder vast te stellen door de gemeente Duiven.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	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. Maatregel 9.2.1.1 Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties. Maatregel 9.2.1.2 Het gebruiken van groepsaccounts is niet toegestaan, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar. <u>Toelichting:</u> Beheersmaatregelen 9.2.1, 9.2.2 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 • 9.2.6 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			

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	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).			

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
9.2.2 Gebruikers toegang verlenen Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD	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. Maatregel 9.2.2.1 Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris. Maatregel 9.2.2.2 Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven[4]. Maatregel 9.2.2.3 Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	Kennisnemen van de door de gemeente Duiven uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen en -indien noodzakelijk- aanvullende interviews met de sleutel-functionarissen		Suwinet Inkijk Voor Suwinet-Inkijk wordt door de gemeente Duiven een door BKWI opgelegd adequaat wachtwoordbeleid gehanteerd. Er is een vastgestelde autorisatieprocedure voor het administreren van gebruikers en het toekennen/ intrekken van toegangsrechten en de controle daarop m.b.t. Suwinet.

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

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	<u>Toelichting:</u> Beheersmaatregelen 9.2.1, 9.2.2, 9.2.5 en 9.2.6 hangen nauw met elkaar samen: • 9.2.1 richt zich op de registratie en het afmelden van gebruiker • 9.2.2 richt zich op het proces van het toekennen van rechten aan gebruikers • 9.2.5 richt zich op het periodiek beoordelen van toegangsrechten van gebruikers • 9.2.6 richt zich op het proces van intrekken of wijzigen van toegangsrechten De procedure voor het 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			

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	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).			
9.2.5 Beoordeling van toegangsrechten van gebruikers <u>Betrokken partij(en):</u> Gemeente/ samenwerkingspartij/ 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.	Vaststelling van het eigenaarschap van de Suwinet gegevens is geregeld. Kennisnemen van de door de gemeente Duiven uitgevoerde controlewerkzaam-heden, gerichte deelwaarnemingen en -indien noodzakelijk- aanvullende interviews met de		We hebben vastgesteld dat het eigenaarschap van Suwinet (de Suwinet gegevens) adequaat is geregeld. <u>Rapportages van BKWI</u> BKWI verstrekt de gemeente Duiven generieke gebruiksrapportages over het gebruik van Suwinet. Deze geanonimiseerde rapportages zijn bedoeld om te ondersteunen bij het beoordelen van het gebruik van Suwinet. Generieke gebruiksrapportages worden elke maand automatisch klaargezet binnen Suwinet-Inkijk. Deze geven een globaal beeld van het gebruik en bevatten geen persoonsinformatie. Wanneer afwijkingen worden geconstateerd in de generiek rapportage is het zaak hiervoor een specifieke rapportage aan te vragen ter ondersteuning van het interne controleproces. Deze rapportages bevatten gegevens over de handelingen van geautoriseerde gebruikers, onder andere persoonsgegevens van zowel gebruikers (gebruikersnamen) als geraadpleegde personen (burgerservicenummers). De toegangsrechten van gebruikers m.b.t. Suwinet-Inkijk worden aantoonbaar minimaal

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	Risico: Bij het ontbreken van controle op de toegangsrechten worden afwijkingen in het autorisatieproces niet gesignaleerd. Bij het ontbreken van controles op het gebruik van autorisaties wordt misbruik niet gesignaleerd. Maatregel 9.2.5.1 Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld. (overruled door 9.2.5.3) Maatregel 9.2.5.2 De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident. Maatregel 9.2.5.3 Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld. 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	sleutel-functionarissen.		één keer per half jaar beoordeeld aan de hand van de specifieke rapportages van BKWI in een formeel proces. Er is onderzocht of de juiste functiescheiding is toegepast en voldaan wordt aan de principes van doelbinding en proportionaliteit. Daarover is aantoonbaar gerapporteerd aan het management. Er zijn verslagen van de beoordeling van de toegangsrechten m.b.t. Suwinet-Inkijk overlegd.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	wijzigen van toegangsrechten Het (lijn)management behoort de toegangsrechten van gebruikers en, indien van toepassing, beheerders met toegang tot Suwinet gegevens regelmatig (= minimaal 1x per half jaar) te beoordelen in een formeel proces. Bij het beoordelen van toegangsrechten van gebruikers behoren de volgende aspecten in overweging te worden genomen: a) toegangsrechten van gebruikers behoren regelmatig en na wijzigingen, zoals promotie, degradatie of beëindiging van het dienstverband, te worden beoordeeld; b) toegangsrechten van gebruikers behoren te worden beoordeeld en opnieuw te worden toegekend bij functieverandering binnen dezelfde organisatie; c) autorisaties voor speciale toegangsrechten behoren vaker te worden beoordeeld; d) toewijzingen van speciale toegangsrechten behoren regelmatig te worden gecontroleerd om te waarborgen dat speciale toegangsrechten niet onbevoegd zijn verkregen; e) van wijzigingen in speciale accounts behoren voor periodieke beoordeling logbestanden te worden bijgehouden.			

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
9.2.6 Toegangsrechten intrekken of aanpassen <u>Betrokken partij(en):</u> Gemeente/ samenwerkingspartij <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 bijtijds worden beëindigd of gewijzigd, bestaat het risico op onbevoegde kennisname van Suwinet gegevens. <u>Toelichting:</u> Beheersmaatregelen 9.2.1, 9.2.2, 9.2.5 en 9.2.6 hangen nauw met elkaar samen: 9.2.1 richt zich op de registratie en het afmelden van gebruiker 9.2.2 richt zich op het proces van het toekennen van rechten aan gebruikers 9.2.5 richt zich op het beoordelen van toegangsrechten van gebruikers 9.2.6 richt zich op het proces van intrekken of wijzigen van toegangsrechten Bij beëindiging van het dienstverband behoren de toegangsrechten van een persoon voor informatie en bedrijfsmiddelen die samenhangen met informatie verwerkende	Vaststelling dat het intrekken of wijzigen van toegangsrechten in lijn is met de aandachtspunten. Kennisnemen van de door de gemeente Duiven uitgevoerde controlewerkzaamheden, gerichte deelwaarnemingen en -indien noodzakelijk- aanvullende interviews met de sleutel-functionarissen.		<u>Suwinet-Inkijk</u> Op basis van uw rapportages stellen we vast dat de toegangsrechten voor Suwinet-Inkijk tijdig zijn gewijzigd bij functiewijziging en ingetrokken wanneer de medewerker hetzij overgeplaatst is naar buiten het Suwi domein, hetzij de organisatie heeft verlaten.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	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, informatie verwerkende faciliteiten of abonnementen[5] . 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.			
10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	<u>Criterium BIO:</u> Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische	Er zijn voor deze control geen werkzaamheden uitgevoerd.		<u>Toelichting</u> De gemeente Duiven maakt voor de in deze bijlage verantwoorde taak alleen gebruik van Suwinet Inkijk.

[5] *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.*

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inlezen Suwinet DKD	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. Maatregel 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. Maatregel 10.1.1.2 Cryptografische toepassingen voldoen aan passende standaarden. Toelichting: Er behoort beleid te worden ontwikkeld en geïmplementeerd voor			

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.			
12.1.1 Gedocumenteerde bedienings-procedures Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD	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 informatie verwerkende faciliteiten waarborgen. Risico: 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. 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	Inspectie van de gebruikers- en/of beheerderhandleidingen en vaststelling dat deze voldoen aan genoemde aandachtspunten. Interview de verantwoordelijke functionarissen.		Suwinet-Inkijk De infrastructuur van Suwinet wordt beheerd door BKWI. Suwinet is aangesloten op DigiNetwerk. Organisaties die zijn aangesloten op Suwinet-Infrastructuur kunnen hierdoor ook diensten aanbieden en/of afnemen bij partijen die ook zijn aangesloten op DigiNetwerk, zoals gemeenten en ministeries. Zowel DigiNetwerk als Suwinet zijn besloten netwerken. De inrichting, back-up en restore en de bediening daarvan valt daarom buiten de scope van het onderhavig onderzoek en de afspraken daarover zijn terug te vinden in de Keten SLA. Via de downloadpagina van BKWI zijn gebruikershandleidingen te downloaden. Tevens zijn er een e-learning -speciaal voor Suwinet via de VNG Academy- en webinars over logging beschikbaar. Aanbeveling voor de gemeente Duiven: • Gebruik in verband met het vele thuiswerken alleen veilige video vergadertools, die bij voorkeur TLS 1.2 encryptie kent voor de 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 Schrems II het datacenter heeft in de EU en de verwerking plaatsvindt in de EU.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	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.			

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
12.4.1 Gebeurtenissen registreren <u>Betrokken partij(en):</u> Gemeente/ samenwerkingspartij/ IT-serviceorganisatie <u>Scope:</u> Suwinet Inkijk Suwinet Inlezen Suwinet DKD	<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 vaststellen of oneigenlijk gebruik of misbruik is gemaakt van autorisatie. <u>Risico:</u> Afwijkingen worden niet gesignaleerd en kunnen derhalve niet worden aangepakt. Maatregel 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. Maatregel 12.4.1.2 Een logregel bevat in geen geval gegevens die tot	Vaststellen dat de periodieke review van de logging met zodanige diepgang heeft plaatsgevonden dat met een redelijke mate van zekerheid kan worden gesteld dat materiële afwijkingen (onrechtmatig gebruik van Suwinet gegevens) aan het licht zouden zijn gekomen.		<u>Suwinet-Inkijk</u> BKWI heeft een wettelijke verplichting gegevens te loggen waarmee het gebruik van Suwinet-Inkijk per medewerker kan worden nagegaan. Het is echter geen verantwoordelijkheid van BKWI om deze gegevens te analyseren of het gebruik te controleren. Deze verantwoordelijkheid ligt uitsluitend bij de gemeente Duiven. <u>Analyseren van de logging van Suwinet-Inkijk</u> De logging van Suwinet-Inkijk kan slechts beperkt worden geanalyseerd. Alleen de specifieke rapportages van BKWI bieden hiertoe mogelijkheden. We hebben geconstateerd bij norm 9.2.5 dat minstens eenmaal per half jaar een specifieke rapportage is opgevraagd bij BKWI op basis waarvan de logging van Suwinet-Inkijk is geanalyseerd.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	het doorbreken van de beveiliging kunnen leiden. Maatregel 12.4.1.3 De informatie verwerkende 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 risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd. <u>Toelichting:</u> Voor deze norm geldt dat de beheerder van de applicatie (BKWI voor Suwinet Inkijk/ de IT-serviceorganisatie voor Suwinet Inlezen en Suwinet DKD) verantwoordelijk is voor het maken en bewaren van logbestanden (zie ook 12.4.2), en dat het de verantwoordelijkheid van de 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 gebruikende entiteit 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			

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	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.			
12.4.2 Beschermen van informatie in logbestanden <u>Betrokken partij(en):</u> Gemeente/ samenwerkingspartij/ 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. Maatregel 12.4.2.1 Er is een overzicht van logbestanden die worden gegenereerd. Maatregel 12.4.2.2 Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging	Er zijn voor deze control geen werkzaamheden uitgevoerd.		<u>Toelichting</u> De gemeente Duiven maakt voor de in deze bijlage verantwoorde taak alleen gebruik van Suwinet Inkijk.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd. Maatregel 12.4.2.3 Er is een (onafhankelijke) interne audit procedure die minimaal halfjaarlijks toetst op het ongewijzigd bestaan van logbestanden. 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.			
18.1.4 Privacy en bescherming van persoonsgegevens Betrokken partij(en): Gemeente/ samenwerkingspartij/ IT-serviceorganisatie Scope: Suwinet Inkijk Suwinet Inlezen Suwinet DKD	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	Vaststelling dat de organisatie een privacy-beleid heeft ontwikkeld en geïmplementeerd. Vaststelling dat de Suwinet applicatie(s) is/ zijn opgenomen in het Verwerkingsregister. Vaststelling dat een FG is aangesteld, dat deze in voldoende mate onafhankelijk en objectief is, en dat deze voldoende mandaat heeft om		Het is essentieel om het gebruik van persoonsgegevens te monitoren, te loggen en regelmatig op doelbinding en rechtmatigheid te beoordelen. Het betreft systemen waarbinnen de vanuit Suwinet afkomstige gegevens verwerkt worden. We hebben vastgesteld dat de gemeente Duiven een op de AVG gebaseerd privacybeleid heeft geïmplementeerd. We hebben vastgesteld dat Suwinet is opgenomen in het Verwerkingsregister. We hebben vastgesteld dat bij de gemeente Duiven/1Stroom een FG formeel is aangesteld met voldoende mandaat en met voldoende onafhankelijkheid ten opzichte van het management van de organisatie. We hebben kunnen vaststellen dat periodiek wordt gecontroleerd of de privacyregels -voor Suwinet in het bijzonder- worden nageleefd.

Norm	Beschrijving maatregel	Uitgevoerde werkzaamheden	Oordeel	Vastgestelde feiten en aanbevelingen
	overeenkomstig toepasselijke wet- en regelgeving plaatsvindt, wordt hierdoor de AVG overtreden. Maatregel 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. Maatregel 18.1.4.2 Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheids-gebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging. <u>Toelichting:</u> 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.	zijn/haar functie uit te voeren. Vaststellen dat de naleving van de privacyregels regelmatig gecontroleerd wordt (zie ook 12.4.1). Vaststelling 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. Kennisnemen van de door de gemeente Duiven uitgevoerde controlewerkzaamhe den, gerichte deelwaarnemingen en -indien noodzakelijk- aanvullende interviews met de sleutel-functionarissen.		Vastgesteld is dat Suwinet wordt gebruikt voor de volgende Suwi-taken: • Taken rondom Bijzondere bijstand en Sociale recherche in het kader van de P-wet Ook hebben we vastgesteld dat Suwinet is gebruikt voor taken mbt het energiefonds en de Gelrepas. Het Suwi-gebruik voor het energiefonds vindt zijn grondslag in art. 35 lid 1 PW. Voor de Gelrepas is het gebruik van Suwinet niet toegestaan. Medewerkers zijn hier inmiddels op gewezen en dit is vastgelegd in de procesbeschrijving Hoofdproces Inkomensondersteuning en een nieuwe werkinstructie raadplegen Suwinet. De via Suwinet verzamelde gegevens worden overgedragen (de organisatie is verwerkingsverantwoordelijk vanaf het moment van overdracht), en deze gegevens mogen niet worden hergebruikt of doorgeleverd voor andere doelen dan waarvoor de gegevens oorspronkelijk verzameld zijn. Dit is bepaald in de geheimhoudingsplicht van artikel 74 van de wet Suwi.