ACCORIS ®



Wigo4it

Assurancerapport NOREA Richtlijn 3000D
TPM Suwinet DKD-inlezen

Third Party Mededeling

Ten behoeve van gemeenten Amsterdam, Den Haag, Rotterdam en Utrecht

ICT-beveiligingsassessment Suwinet

Datum rapport: 30 november 2023
Rapportnummer: AAS2023-1736
Dit rapport heeft 36 pagina's

ACCORIS®
AUDIT SERVICES

Inhoudsopgave

1.	Assurancerapport van de onafhankelijke auditor	4
1.1	Inleiding	4
1.2	Opdracht	4
1.3	Verantwoordelijkheid van de opdrachtgever	5
1.4	Verantwoordelijkheid van de auditor	5
1.5	Beperkingen	5
1.6	Uitgevoerde werkzaamheden	6
1.7	Conclusie	6
1.8	Beoogde gebruikers en doel	9
2.	Criteria	10
3.	Object van onderzoek	11
3.1	Transport	11
3.2	Opslag	13
4.	Verantwoordelijkheid gemeenten Amsterdam, Den Haag, Rotterdam en Utrecht	14
Bijlage A - Beschrijving van de testresultaten van de auditor		21
Bijlage B - Details van het object van onderzoek		33
Bijlage C - Schematisch overzicht van het object van onderzoek		36

ACCORIS®
AUDIT SERVICES

Colofon

Rapport	**ICT-beveiligingsassessment Suwinet DKD-inlezen**
Aard van het rapport	**NOREA richtlijn 3000D**
Organisatie	**Wigo4it**
Ten behoeve van	**Wigo4it en gemeenten Amsterdam, Den Haag, Rotterdam en Utrecht**
Datum	**30 november 2023**
Rapportnummer	**AAS2023-1736**
Versie	**1**
Status	**Definitief**
Auditor	5.1, 2, e 5.1, 2, e
Telefoon	5.1, 2, e
E-mail	5.1, 2, e @accoris.nl
Auditorganisatie	**Accoris Audit Services B.V.**
Vestigingsadres	5.1, 2, e
	5.1, 2, e Zoetermeer
	Nederland
Telefoon	5.1, 2, e
E-mail	5.1, 2, e @accoris.nl
Website	**www.accoris.nl**

ACCORIS®
AUDIT SERVICES

1. Assurancerapport van de onafhankelijke auditor

1.1 Inleiding

Voor het gebruik van Suwinet zijn gemeenten ervoor verantwoordelijk dat wordt voldaan aan de 'Verantwoordingsrichtlijn GeVS 2022' versie 1.0. In het kader van ENSIA dienen gemeenten jaarlijks een ICT-beveiligingsassessment uit te voeren om de naleving van deze norm aan te tonen.

Gemeenten kunnen voor de uitvoering van wettelijke taken gebruik maken van de diensten van serviceorganisaties. Deze organisaties moeten inzicht geven in de ICT-beveiliging van de door die organisaties gebruikte Suwinet-aansluiting, zodat gemeenten in staat zijn om de ENSIA-vragenlijst te beantwoorden en de Collegeverklaring op te stellen. Gemeenten kunnen met serviceorganisaties overeenkomen dat het ICT-beveiligingsassessment van de serviceorganisatie dient te worden voorzien van een Third Party Mededeling van een gekwalificeerde IT-auditor (RE).

Wigo4it is de serviceorganisatie voor de gemeenten Den Haag, Rotterdam, Amsterdam en Utrecht (G4-gemeenten). In dit rapport hebben wij de resultaten van ons onderzoek naar Suwinet DKD-inlezen van Wigo4it opgenomen, zodat Wigo4it dit rapport kan verstrekken aan deze gemeenten.

1.2 Opdracht

Ingevolge de opdracht van Wigo4it hebben wij op 30 november 2023 ons onderzoek afgerond naar de interne beheersingsmaatregelen van Wigo4it met betrekking tot het beheer van de objecten binnen de DKD-inlees-keten.

Wij hebben ons onderzoek uitgevoerd conform de NOREA richtlijn 3000D (Direct audit), inzake opzet en bestaan van de interne beheersingsmaatregelen. Voor de gehanteerde normen verwijzen wij naar de 'Handreiking ENSIA voor IT-auditors (RE's)' versie 4.0 dd. 15 oktober 2021 van NOREA.

Ons onderzoek heeft zich gericht op de opzet en het bestaan van de interne beheersings-maatregelen bij Wigo4it ten behoeve van de informatiebeveiliging van de Suwinet-keten van Wigo4it. Deze keten betreft de infrastructuur (netwerken en servers) en applicaties die de DKD-inlees-functionaliteit realiseren en ter beschikking stellen aan de G4. Een nadere beschrijving van deze keten hebben wij in hoofdstuk 3 Object van onderzoek opgenomen.

In het kader van ENSIA bestaat het geselecteerde normenkader Suwinet uit 14 BIO controls, waarvan de onderliggende 'BIO-Overheidsmaatregelen' door de IT-auditor dienen te worden onderzocht. Deze 14 BIO controls zijn van toepassing voor DKD-inlezen. Conform de Handreiking ENSIA voor IT-auditors (RE's) zijn ook de 'General IT-Controls' (GITC) in scope van het onderzoek. De GITC zijn met name van toepassing op Wigo4it. De van toepassing zijnde GITC zijn in het Suwinet-normenkader echter niet c.q. niet in voldoende mate gespecificeerd. In overleg met Wigo4it zijn hiervoor 2 relevante normen uit de Baseline Informatiebeveiliging Overheid (BIO) geselecteerd. Het betreft de BIO controls met betrekking tot changemanagement als onderdeel van de GITC, welke wij onder vermelding van de BIO-norm afzonderlijk hebben opgenomen.

De G4 zijn eindverantwoordelijk voor alle 14 geselecteerde BIO-controls en dienen een toereikende PDCA-cyclus rond de uitbesteding van wettelijke taken aan serviceorganisatie Wigo4it te hebben ingericht.

1.3 Verantwoordelijkheid van de opdrachtgever

Wigo4it is als opdrachtgever verantwoordelijk voor de beschrijving van het object van onderzoek, het onderkennen van de beveiligingsrisico's van de Suwinet-omgeving, het opzetten en implementeren van beveiligingsmaatregelen om te voldoen aan de 16 BIO controls die zijn geselecteerd uit het normenkader uit de 'Verantwoordingsrichtlijn GeVS 2022' versie 1.0 en de van toepassing zijnde General IT Controls volgens de 'Handreiking ENSIA voor IT-auditors (RE's)' versie 4.0 dd. 15 oktober 2021 van NOREA en het uitvoeren van een eigen ICT-beveiligingsassessment om de kwaliteit van de genomen maatregelen vast te stellen.

1.4 Verantwoordelijkheid van de auditor

Onze verantwoordelijkheid is, op basis van de door ons uitgevoerde werkzaamheden, per voor de audit geselecteerde beveiligingsrichtlijn inzake Suwinet, een oordeel te geven over de opzet en het bestaan van de interne beheersingsmaatregelen ten behoeve van de directie van Wigo4it en de G4-gemeenten.

Wij hebben onze opdracht uitgevoerd overeenkomstig het Nederlands recht en rekening houdende met Richtlijn 3000 (herzien) 'Assurance-opdrachten door IT-Auditors' (Richtlijn 3000D, directe-opdrachten). Dit vereist dat wij voldoen aan de voor ons geldende ethische voorschriften en onze werkzaamheden zodanig plannen en uitvoeren dat een redelijke mate van zekerheid wordt verkregen over de vraag of de interne beheersingsmaatregelen, in alle van materieel belang zijnde aspecten, op afdoende wijze zijn opgezet en bestaan per 30 november 2023.

Onze assurance-opdracht om te rapporteren over opzet en bestaan van interne beheersings-maatregelen bij Wigo4it omvatte het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie over de opzet en het bestaan van deze interne beheersingsmaatregelen.

Wij hebben werkzaamheden uitgevoerd afhankelijk van onze oordeelsvorming, met inbegrip van het inschatten van de risico's dat de interne beheersingsmaatregelen niet op afdoende wijze zijn opgezet of niet bestaan. Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om daarop een onderbouwing voor onze oordelen te bieden.

1.5 Beperkingen

Wij zijn afhankelijk van de medewerkers van Wigo4it ten aanzien van de juistheid en volledigheid van de verstrekte informatie. Echter, wij hebben de nodige werkzaamheden uitgevoerd om de juistheid en volledigheid van de door ons ontvangen informatie vast te stellen.

In het kader van de ENSIA-vragenlijst zijn 16 BIO controls inzake DKD-inlezen geselecteerd en conform de 'Handreiking ENSIA voor IT-auditors (RE's)' versie 4.0 dd. 15 oktober 2021 van NOREA) de GITC, waarover wij rapporteren. Vanwege deze selectie van BIO controls zijn wij niet in staat om een samenvattende conclusie te verschaffen omtrent de informatiebeveiliging van de Suwinet-omgeving van Wigo4it als geheel. Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de werking van de interne beheersingsmaatregelen; wij brengen derhalve daarover geen oordeel tot uitdrukking.

Wij kunnen geen verantwoordelijkheid aanvaarden voor wijzigingen in de door ons gehanteerde feiten en omstandigheden na de datum waarop wij de desbetreffende werkzaamheden hebben afgerond, tenzij wij tijdig van de wijzigingen in de door ons gehanteerde feiten en omstandigheden op de hoogte zijn gebracht.

1.6 Uitgevoerde werkzaamheden

Wij hebben de opzet van de interne beheersingsmaatregelen van Wigo4it geïnventariseerd en getoetst door het houden van interviews en het bestuderen van de documentatie. Het bestaan hebben wij getoetst door het doen van eigen waarnemingen en door van een aantal beheersingsmaatregelen vast te stellen of ze worden nageleefd conform de opzet.

De interviews en eigen waarnemingen inzake onze audit van DKD-inlezen hebben plaatsgevonden tussen 24 november 2023 en 30 november 2023. Wij hebben tot en met 30 november 2023 nadere documentatie en toelichting ontvangen.

1.7 Conclusie

Onze conclusie is gevormd op basis van onze werkzaamheden zoals die is uiteengezet in dit rapport inzake Wigo4it. Per beveiligingsrichtlijn hebben wij in de volgende tabel een overzicht weergegeven van onze conclusie over de opzet en het bestaan van de interne beheersingsmaatregelen van Wigo4it per 30 november 2023. Bij het vormen van onze conclusie hebben wij gebruik gemaakt van de criteria die in hoofdstuk 2 staan beschreven.

Met **VOLDOET** is in de navolgende tabel aangegeven dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn volgens de criteria genoemd in hoofdstuk 2 in alle materiële opzichten en met een redelijke mate van zekerheid effectief zijn.

Daar waar de richtlijnen specifiek niet op Wigo4it van toepassing zijn is dit, indien van toepassing, met een ***)** aangegeven.

ACCORIS®
AUDIT SERVICES

BIO-control	Beschrijving van de beveiligingsrichtlijn	Oordeel
5.1.1	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	**VOLDOET**
5.1.2	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	**VOLDOET**
6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	**VOLDOET**
6.1.2	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	**VOLDOET**
7.2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	**VOLDOET**
9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	**VOLDOET**
9.2.2	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	**VOLDOET**
9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	**VOLDOET**
9.2.6	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast	**VOLDOET**
10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van crypto grafische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	**VOLDOET**
12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	**VOLDOET**
12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	**VOLDOET**

BIO-control	Beschrijving van de beveiligingsrichtlijn	Oordeel
12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	**VOLDOET**
18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving	**VOLDOET**
ITGC **(i.c. 12.1.2, 14.2.2)**	**12.1.2** Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst. **14.2.2** Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	**VOLDOET**

1.8 Beoogde gebruikers en doel

Dit rapport hebben wij verstrekt aan Wigo4it, zodat Wigo4it dit rapport kan aanbieden aan de gemeenten Amsterdam, Den Haag, Rotterdam en Utrecht.

Voor zover het Wigo4it is toegestaan om het rapport aan voornoemde partijen beschikbaar te stellen zal het rapport origineel, volledig en ongewijzigd beschikbaar worden gesteld. Dit rapport is uitsluitend bestemd voor Wigo4it en de gemeenten Amsterdam, Den Haag, Rotterdam en Utrecht aangezien anderen, die niet op de hoogte zijn van de precieze scope, aard en doel van de werkzaamheden, de resultaten onjuist kunnen interpreteren.

Het is niet toegestaan om deze rapportage, of onderdelen of samenvattingen daarvan, zowel mondeling als schriftelijk, aan derden (niet zijnde de hiervoor genoemde partijen) te verstrekken zonder onze uitdrukkelijke voorafgaande schriftelijke toestemming. Aan het verstrekken van onze toestemming kunnen wij nadere voorwaarden verbinden.

Zoetermeer, 30 november 2023

Accoris Audit Services B.V.

30 Nov 2023 15:27 +0100
Zoetermeer

5.1, 2, e

QUALIFIED SIGNATURE

5.1, 2, e

5.1, 2, e

5.1, 2, e

ACCORIS®
AUDIT SERVICES

2. Criteria

De criteria waarvan gebruik wordt gemaakt bij het uitvoeren van de opdracht houden in dat:

- De interne beheersingsmaatregelen die verband houden met de beveiligingsrichtlijnen op afdoende wijze zijn opgezet en geïmplementeerd per 30 november 2023;

- De risico's die het voldoen aan de beveiligingsrichtlijnen in gevaar brengen en daarmee de betrouwbaarheid van Suwinet aantasten, werden onderkend;

- De onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals opgezet en geïmplementeerd, een redelijke mate van zekerheid zouden moeten verschaffen om de risico's die het voldoen aan de beveiligingsrichtlijnen in gevaar brengen in voldoende mate beperken.

ACCORIS®
AUDIT SERVICES

3. Object van onderzoek

Wigo4it voert het technisch beheer uit van de keten bestaande uit infrastructuur (netwerken en servers) en applicaties, die de DKD-inlees-functionaliteit realiseren en ter beschikking stellen aan de G4.

Het object van onderzoek omvat dit technisch beheer en heeft zich gericht op de opzet en het bestaan van de interne beheersingsmaatregelen bij Wigo4it ten behoeve van de informatiebeveiliging van de Suwinet-keten van Wigo4it.

In het kader van uitbesteding hebben de G4 en Wigo4it een overeenkomst afgesloten; derhalve treedt Wigo4it op als serviceorganisatie. Tussen de G4 en Wigo4it zijn afspraken inzake informatiebeveiliging gemaakt. In dit kader dient Wigo4it zicht jaarlijks te verantwoorden over de informatiebeveiliging inzake DKD-inlees.

Voor het definiëren van het technisch beheer is onderscheid gemaakt tussen het beheer van het transporteren en het opslaan van Suwi-data. Voor nadere toelichting op het object van onderzoek verwijzen wij naar de beschrijving in bijlage B waarvan een schematisch overzicht van de dataflow is opgenomen in bijlage C.

3.1 Transport

Koppelingen met IB

Wigo4it heeft een koppelvlak ("SUWI-koppelvlak 1.0") ontwikkeld, dat gefaciliteerd wordt door de ESB (Electronic Service Bus). Deze verzorgt de koppeling tussen de interne systemen

(GALO en Socrates) en het koppelvlak ("DKD-inlees Koppelvlak") van het Inlichtingenbureau (IB). Daarnaast hebben de applicatie RMW en Digidos een directe koppeling met het IB, die niet gefaciliteerd wordt door de Bizztalk server. Wigo4it beheert de applicatie RMW technisch en functioneel voor de gemeenten Den Haag, Utrecht en Rotterdam. De gemeente Amsterdam heeft de applicatie RMW in eigen beheer. Met betrekking tot de applicatie Digidos, die uitsluitend gebruikt wordt door gemeente Den Haag, beheert Wigo4it de infrastructuur en server in de vorm van een PAAS-dienst conform SLA-beheervariant level 3. De professionals van de gemeente Den Haag kunnen ook via Digidos documenten uit Socrates opvragen.

Interne koppelingen

De ESB heeft ontsluit enerzijds het DKD-inlees koppelvlak voor:

- Bevragingen vanuit GALO;
- GALO en Socrates ("Socrates adapter");
- tussen Socrates en het DMS van Rotterdam waarin SUWI-gegevens worden meegeleverd in de berichten.

Data-export van Wigo4it naar G4 (extern)

Vanuit Socrates wordt Suwi-data aan de G4 verstrekt over de volgende koppelvlakken:

- ESB waaronder DMS Koppelvlak 1.0 (Rotterdam);
- MOVEit (Amsterdam en Utrecht);
- Data-extractie (over de XRM-file server) naar datawarehouse van alle G4-gemeenten, data-extracties worden gegenereerd en op de XRM-server geplaatst op basis van een geautomatiseerde job.
- Citrix Sharefile: Generieke functionaliteit voor uitwisseling van bestanden. Voor SUWI in gebruik voor:
  - het maandelijks verstrekken van de SUWI-rapportages aan de G4;
  - ondersteuning van de TOZO check, waarbij aan de hand van de door de gemeente verstrekte gegevens drie bronnen worden geraadpleegd (UWV, DUO en KvK) a.d.h.v. BSN's en bij KvK op basis van KvK-nummers. De KvK check en gegevens vormen het overgrote deel van de aanlevering voor deze regeling voor zelfstandige ondernemers en vallen buiten de DKD-keten. De SUWINET-controle behelst het controleren of de aanvrager recht heeft op studiefinanciering (DUO) of op een andere manier inkomen of een financiële regeling ontvangt (SUWICHECK). Door Wigo4it wordt via Sharefile het resultaat van de afweging (binair J/N) en de reden van eventuele uitval teruggegeven. Resultaat en reden van uitval kan bestaan uit 2 onderdelen, de Suwi-check en de KvK-check. Bij beide controles op de bron, wordt het moment (timestamp) van controleren vastgelegd. Er worden voor TOZO(1) geen SUWI-gegevens via Sharefile verzonden, maar slechts het resultaat van de check. Voor TOZO2 en TOZO3 is de informatie uitgebreid met de partner en inkomstentoets, waardoor wel (afgeleide) SUWI-gegevens over inkomen (LB) per maand van de lopende regeling worden aangeleverd aan de gemeente.

In Citrix Sharefile worden de uitgewisselde bestanden na twee weken weer automatisch geschoond. Wigo4it heeft een EU-aansluiting, waardoor de gegevensuitwisseling alleen binnen deze zone kan plaatsvinden.

3.2 Opslag

Binnen Wigo4it zijn de volgende applicaties en databases te onderkennen, waarbij Suwi-data gedurende een langere periode wordt opgeslagen:

- Socrates;
- RMW;
- Digidos Den Haag, echter, het beheer door Wigo4it is beperkt tot Server OS en infrastructuur;
- De data (berichten) van de GALO-verwerkingen wordt tijdelijk opgeslagen in de GALO-database;
- Citrix Sharefile.

4. Verantwoordelijkheid gemeenten Amsterdam, Den Haag, Rotterdam en Utrecht

Wigo4it is als serviceorganisatie van gemeenten Amsterdam, Den Haag, Rotterdam en Utrecht, de G4, (mede) verantwoordelijk voor de beschrijving van het object van onderzoek, het onderkennen van de beveiligingsrisico's, het opzetten en implementeren van beveiligingsmaatregelen om te voldoen aan de ENSIA-vragenlijst inzake Suwinet en het uitvoeren van een eigen ICT-beveiligingsassessment om de kwaliteit van de genomen maatregelen vast te stellen.

Het ICT-beveiligingsassessment inzake Suwinet omvat 16 BIO controls, aangevuld met ITGC (i.c. Change Management), waarover Wigo4it de gemeenten dient te informeren. Vanwege de rol van Wigo4it als serviceorganisatie worden de General IT Controls (GITC) zoals benoemd in de Handreiking ENSIA voor IT-auditors (RE's)' versie 4.0 dd. 15 oktober 2021 van NOREA in het ICT-beveiligingsassessment meegenomen.

De gemeenten zijn eindverantwoordelijk voor alle 16 BIO controls inclusief de GITC en dienen een toereikende PDCA-cyclus rond de uitbesteding van wettelijke taken aan serviceorganisatie Wigo4it te hebben ingericht.

De G4-gemeenten ontvangen Suwi-data van Wigo4it via de Citrix Sharefile en andere componenten die in bijlage C in het schematisch overzicht zijn opgenomen (witte en gele vlakken). Wigo4it heeft geen inzicht in de handmatige of geautomatiseerde koppelingen naar overige systemen binnen de G4. De G4-gemeenten dienen derhalve zelf hun eigen onderzoeksobject met betrekking tot het G1-deel van de Suwinet-keten te definiëren en vast te stellen, en op die scope de verantwoording te richten.

In de onderstaande tabel is aangegeven voor welke beveiligingsrichtlijnen een gebruikersorganisatie (mede) verantwoordelijkheid heeft en interne beheersingsmaatregelen heeft geïmplementeerd om te voldoen aan de beveiligingsrichtlijnen van Suwinet.

BIO-control	Beschrijving van de beveiligingsrichtlijn	Verantwoordelijkheid G4-gemeenten
5	**Beveiligingsbeleid**	
5.1	**Aansturing door de directie van de informatiebeveiliging**	
5.1.1	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	- De gemeente heeft een goedgekeurd Suwinet informatiebeveiligingsbeleid waarin de type maatregelen zijn gedefinieerd.

BIO-control	Beschrijving van de beveiligingsrichtlijn	Verantwoordelijkheid G4-gemeenten
5.1.2	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	- De gemeente evalueert periodiek het Suwinet informatiebeveiligingsbeleid en stelt deze zo nodig bij.
6	**Organiseren van informatiebeveiliging**	
6.1	**Interne organisatie**	
6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	- Taken en verantwoordelijkheden i.h.k.v. Suwinet zijn vastgelegd met inachtneming van controle-technische functiescheiding (CTFS) en zijn opgenomen in diverse relevante functiebeschrijvingen. - De rol van de CISO is in een CISO-functieprofiel vastgelegd. - De gemeente heeft een procedure voor Suwinet-incidenten en volgt deze procedure aantoonbaar. - Beveiligingsincidenten worden geanalyseerd en gerapporteerd aan het verantwoordelijk management.
6.1.2	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	- Verantwoordelijkheden zijn gedefinieerd in bijv. een RASCI-matrix. - Op basis van de RASCI-matrix is per systeem in de Suwi-keten een autorisatiematrix opgesteld. - De RASCI-matrix en autorisatiematrix wordt aantoonbaar periodiek gereviewed.
7	**Veilig personeel**	
7.1	**Tijdens het dienstverband**	

BIO-control	Beschrijving van de beveiligingsrichtlijn	Verantwoordelijkheid G4-gemeenten
7.2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	- 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.. - Medewerkers die gebruik maken van Suwinet hebben binnen 3 maanden na indiensttreding een i-bewustzijn training succesvol gevolgd.
9	**Toegangsbeveiliging**	
9.2	**Beheer van toegangsrechten van gebruikers**	
9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	- Er is een procedure voor het registreren en afmelden van gebruikers. - Deze procedure wordt aantoonbaar nageleefd. - Toegang tot Suwinet wordt door een bevoegde functionaris goedgekeurd. - Er wordt geen gebruik gemaakt van groepsaccounts tenzij dit gemotiveerd wordt en vastgelegd wordt door de proceseigenaar. Let hierbij op de gevolgen met betrekking tot logging en de analyse hiervan.
9.2.2	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	- Uitsluitend een daartoe bevoegde functionaris verleent toegang tot Suwinet. - Alle mutaties m.b.t. gebruikersaccounts worden bijgehouden in een registratie. - Er wordt gebruik gemaakt van unieke gebruikers-ID's. - Er wordt gebruik gemaakt van een sterke authenticatiemethode, bij voorkeur 2 factor authenticatie. - Een sterk wachtwoord is vereist voor toegang tot Suwinet-systemen.

BIO-control	Beschrijving van de beveiligingsrichtlijn	Verantwoordelijkheid G4-gemeenten
9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	- Er wordt minimaal halfjaarlijks een review uitgevoerd op accounts, rollen en rechten. - Het management stelt vast dat geen oneigenlijke autorisatie-toekenningen hebben plaatsgevonden. - Eventuele bevindingen uit de review worden opgevolgd als beveiligingsincident en afgehandeld.
9.2.6	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast	- Er is een procedure voor het registreren en afmelden van gebruikers. - Accounts van medewerkers die uit dienst zijn, zijn tijdig ingetrokken.
10	**Cryptografie**	
10.1	**Cryptografische beheersmaatregelen**	
10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	- Stel vast dat er een cryptografiebeleid is opgesteld met minimaal de volgende onderwerpen: 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 (denk hierbij aan het gebruik van PKI-overheid-certificaten en het gebruik van Digikoppeling voor communicatie met basisregistraties) e) De wijze waarop het beschermingsniveau vastgesteld wordt. f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld. - Stel vast dat er een netwerkarchitectuur is opgesteld voor de Suwinet-keten. - Observeer de encryptie van gegevens tijdens transport en opslag.

BIO-control	Beschrijving van de beveiligingsrichtlijn	Verantwoordelijkheid G4-gemeenten
12	**Beveiliging bedrijfsvoering**	
12.1	**Bedieningsprocedures en verantwoordelijkheden**	

12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	- Voor de gebruikers van de Suwinet-applicaties zijn gebruikers-handleidingen beschikbaar.
		- Voor zover de gemeente zelf applicaties in de Suwi-keten beheert of host, dienen de volgende bedieningsprocedures beschikbaar te zijn en te zijn geïmplementeerd:
		  - Back-up;
		  - Installatie en configuratie van de systemen;
		  - Patchmanagement;
		  - Continuïteit
		  - Systeemherstel in geval van storingen;
		  - Logging;
		  - Monitoring van activiteiten.

12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	- De gemeente analyseert de logging van de applicaties RMW en Socrates die door Wigo4it wordt aangeleverd - De gemeente creëert logbestanden van alle overige systemen waarin de Suwi-gegevens in de keten worden verwerkt en analyseert deze.

BIO-control	Beschrijving van de beveiligingsrichtlijn	Verantwoordelijkheid G4-gemeenten

12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	- Voor zover de gemeente zelf logbestanden creëert voor hun deel van de Suwi-keten, moeten deze:
		  - conform vastgestelde bewaarperiode te worden opgeslagen (o.b.v. risico-analyse);
		  - worden beschermd tegen vervalsing of onbevoegde toegang.
		- Aanpassingen op logbestanden of pogingen tot het verwijderen hiervan worden geregistreerd als beveiligingsincident.

18	**Naleving**	
18.1	**Naleving van wettelijke en contractuele eisen**	
18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving	- De gemeente heeft een privacy-beleid. - De Suwinet-applicaties van de Suwi-keten, voor zover dit de gemeente betreft, zijn opgenomen in het verwerkersregister. - Een FG is aangesteld die voldoende mandaat heeft om zijn/haar functie uit te voeren. De FG is in voldoende mate onafhankelijk en objectief. - De naleving van privacyregels wordt regelmatig gecontroleerd. Hierover wordt gerapporteerd aan het management. - De FG controleert dat de gemeente de opgevraagde Suwinet gegevens alleen gebruikt voor de taken waarvoor een wettelijke basis (doelbinding) is. Dit betreft die gegevens die dus noodzakelijk zijn voor de uitvoering van wet- en regelgeving. Voor een aantal gemeentelijke taken is het gebruik van Suwinet gegevens niet toegestaan.

BIO-control	Beschrijving van de beveiligingsrichtlijn	Verantwoordelijkheid G4-gemeenten
ITGC **(i.c. 12.1.2, 14.2.2)**	**12.1.2** Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst. **14.2.2** Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	- De gemeente heeft een wijzigingsproces en volgt deze na met betrekking tot wijzigingen in de Suwi-keten, voor zover het de gemeente betreft. - De gemeente voert acceptatietesten uit van de wijzigingen die door Wigo4it worden uitgevoerd voor zover het betrekking heeft op de applicaties RMW en Socrates. - De gemeente richt een OTAP-omgeving in voor systemen binnen het gemeente-deel van de Suwi-keten.

Bijlage A - Beschrijving van de testresultaten van de auditor

In het kader van onze opdracht hebben wij ter zake van Suwinet DKD-inlezen de volgende werkzaamheden uitgevoerd:

- Het verkrijgen van inzicht in de relevante kenmerken van de Werk en Inkomen gerelateerde werkzaamheden die door Wigo4it met behulp van Suwinet worden uitgevoerd;
- Het beoordelen van de scope, inclusief het beoordelen van de maatregelen die bij Wigo4it moeten worden onderzocht;
- Het houden van interviews met verantwoordelijke functionarissen, vooral gericht op het onderkennen van risico's en het onderzoek in hoeverre deze risico's worden afgedekt door maatregelen;
- Het inventariseren van de opzet en het beoordelen van het bestaan van de relevante maatregelen. Dit door middel van het kennis nemen van documentatie en het doen van eigen waarnemingen;
- Het analyseren van de uitkomsten van de werkzaamheden met als doel het geven van oordelen per geselecteerde beveiligingsrichtlijn van de ENSIA-vragenlijst;

Hierna hebben wij een korte beschrijving opgenomen van de door ons uitgevoerde werkzaamheden en onze oordelen, met zo nodig, adviezen over de interne beheersingsmaatregelen ter verbetering van de Suwinet-omgeving. Onze oordelen zijn verwoord als voldoet/voldoet (nog) niet (met reden) per beveiligingsrichtlijn.

BIO-control	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en adviezen
5	**Beveiligingsbeleid**		
5.1	**Aansturing door de directie van de informatiebeveiliging**		
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 informatiebeveiligings-beleid wordt geëvalueerd. f. De bevordering van het beveiligingsbewustzijn.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie	Voldoet

BIO-control	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en adviezen
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.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, , eigen waarneming	Voldoet
6	**Organiseren van informatiebeveiliging**		
6.1	**Interne organisatie**		
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.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
6.1.1.2	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie	Voldoet
6.1.1.3	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie	Voldoet

BIO-control	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en adviezen
6.1.1.4	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
6.1.2.1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
7	**Veilig personeel**		
7.2	**Tijdens het dienstverband**		
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.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
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.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet

BIO-control	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en adviezen
7.2.2.3	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
9	**Toegangsbeveiliging**		
9.2	**Beheer van toegangsrechten van gebruikers**		
9.2.1.1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
9.2.1.2	Het gebruiken van groepsaccounts is niet toegestaan, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
9.2.2.1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet

BIO-control	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en adviezen
9.2.2.2	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
9.2.2.3	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
9.2.5.2	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
9.2.5.3	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
9.2.6	**Toegangsrechten intrekken of aanpassen** 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.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet

BIO-control	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en adviezen
9.4.3.3	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
10	**Cryptografie**		
10.1	**Cryptografische beheersmaatregelen**		
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.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
10.1.1.2	Cryptografische toepassingen voldoen aan passende standaarden.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet

BIO-control	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en adviezen
12	**Beveiliging bedrijfsvoering**		
12.1	**Bedieningsprocedures en verantwoordelijkheden**		
12.1.1	**Gedocumenteerde bedieningsprocedures** Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
12.4	**Verslaglegging en monitoren**		
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.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
12.4.1.2	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet

BIO-control	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en adviezen
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 risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
12.4.1.4	Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
12.4.1.5	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie	Voldoet
12.4.2.1	Er is een overzicht van logbestanden die worden gegenereerd.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet

BIO-control	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en adviezen
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.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
12.4.2.3	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
12.4.2.4	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
12.4.3	**Logbestanden van beheerders en operators** Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
14	**Acquisitie, ontwikkeling en onderhoud van informatiesystemen**		
14.2	**Beveiliging in ontwikkelings- en ondersteunende processen**		

BIO-control	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en adviezen
14.2.2.1	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
14.2.8.1	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
14.2.8.2	Van de resultaten van de testen wordt verslag gemaakt.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
16	**Beheer van informatiebeveiligingsincidenten**		
16.1	**Beheer van informatiebeveiligingsincidenten en -verbeteringen**		
16.1.2.1	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet

BIO-control	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en adviezen
16.1.2.2	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
16.1.2.4	Incidenten worden zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
18	**Naleving**		
18.1	**Naleving van wettelijke en contractuele eisen**		
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.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet
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.	**Opzet en bestaan** Houden van interviews, inspecteren van documentatie, eigen waarneming	Voldoet

Bijlage B - Details van het object van onderzoek

Integratieapplicatie en integratieplatform (ESB en Broker service)
De ESB en Broker service (verder te noemen ESB) verzorgen de communicatie tussen het DKD-inlees koppelvlak van het IB en de applicaties van Wigo4it, tussen de applicaties van Wigo4it onderling en tussen de applicaties van Wigo4it en de applicaties van de gemeenten. De ESB levert de volgende integratie onderdelen die bijdragen in de SUWI gegevensstromen:

- Het SUWI koppelvlak voor de ontkoppeling van de Wigo4it applicaties met het DKD-inlees koppelvlak.
- De Socrates adapter voor het ontsluiten van web services waarmee documenten met SUWI gegevens in Socrates worden opgeslagen.
- Het DMS koppelvlak voor het opslaan van documenten met SUWI gegevens in het DMS van Rotterdam.
- De managed file transfer koppelingen (MoveIT) met de gemeenten Utrecht en Amsterdam voor het overzetten van database kopieën van Socrates.

GALO
GALO is onderdeel van de ESB en bevat functionaliteit ter ondersteuning van de besluitvorming ter zake van bijstandsaanvragen door de professional van de G4 gemeenten. GALO is een geautomatiseerd proces en kent geen gebruikers. Bij ontvangst van een door de burger met behulp van de applicatie TripleForms ingevulde bijstandsaanvraag bevraagt GALO via de ESB verschillende bronnen uit de SUWI-keten op basis van een BSN. GALO stelt op basis van de SUWI-gegevens met behulp van (geautomatiseerde) beslisregels een (voorstel) besluit op ten behoeve van de professional en Socrates. Dit besluitvoorstel bevat de hoogte van de uitkering tezamen de daarop betrekking hebbende SUWI-gegevens. GALO houdt de bijstandsaanvragen en (voorstel) besluiten met bijbehorende SUWI-gegevens gedurende 28 dagen vast in de ESB-GALO-database. De opgevraagde SUWI-gegevens worden d.m.v. GALO rapportages opgeslagen in Socrates.

Socrates
Socrates verzorgt de bijstandsuitkeringen aan burgers van de G4 gemeenten. Socrates ontvangt het (voorstel) besluit van GALO via de Socrates adapter van de ESB, waarna de professional het besluit indien nodig aanvult of aanpast. Hierbij kan de burger via de applicatie TripleForms aanvullende gegevens aanleveren, die worden vastgelegd in Socrates. Nadat de professional een definitief besluit heeft genomen, stuurt Socrates een beschikking aan de burger. Voor de ondersteuning van de besluitvorming door de professional is in de applicatie Socrates een URL beschikbaar die doorverwijst naar Suwinet-Inkijk.
Socrates bevat de historie van genomen besluiten inzake de hoogte van de uitkering en de daarop betrekking hebbende SUWI-gegevens. Daarnaast ontvangt Socrates via MOVEit file transfer van de ESB de IB-signalen van IB, waarin geen SUWI-gegevens zijn opgenomen. Deze signalen vormen werkopdrachten voor de professional, die via Suwinet-Inkijk nieuwe gegevens over arbeid en inkomen opzoekt, hetgeen kan leiden tot wijzigingen in het vermogensbedrag van bijstandsgerechtigden, dat in Socrates is vastgelegd. Socrates levert SUWI-gegevens aan de applicatie Digidos van gemeente Den Haag, aan het DMS van gemeente Rotterdam via het DMS-koppelvlak van de ESB, en aan gemeenten Amsterdam en Utrecht via MoveIT managed file transfer koppelingen.

RMW
In RMW wordt het door de professional uit RMW ontvangen werkzoekende profiel verder aangevuld. De professional kan de SUWI-gegevens van het UWV en het DUO actualiseren door een nieuwe bevraging te doen bij het IB o.b.v. een BSN.
Deze bevraging wordt voor de gemeenten Den Haag, Rotterdam en Utrecht door RMW direct uitgevoerd op het DKD-inlees Koppelvlak van het IB en niet via de ESB.

Digidos
Deze applicatie, die wordt beheerd door gemeente Den Haag en gehost door Wigo4it, ontvangt SUWI-gegevens van de applicatie Socrates (Den Haag). Digidos heeft een eigen koppeling met het DKD-inlees Koppelvlak van IB voor het ontvangen van SUWI-gegevens.

Citrix Sharefile

Citrix Sharefile: Generieke functionaliteit voor uitwisseling van bestanden. Voor SUWI in gebruik voor:

- het maandelijks verstrekken van de SUWI-rapportages aan de G4;
- ondersteuning van de TOZO check, waarbij aan de hand van de door de gemeente verstrekte gegevens drie bronnen worden geraadpleegd (UWV, DUO en KvK) a.d.h.v. BSN's en bij KvK op basis van KvK-nummers. De KvK check en gegevens vormen het overgrote deel van de aanlevering voor deze regeling voor zelfstandige ondernemers en vallen buiten de DKD-keten. De SUWINET-controle behelst het controleren of de aanvrager recht heeft op studiefinanciering (DUO) of op een andere manier inkomen of een financiële regeling ontvangt (SUWICHECK). Door Wigo4it wordt via Sharefile het resultaat van de afweging (binair J/N) en de reden van eventuele uitval teruggegeven. Resultaat en reden van uitval kan bestaan uit 2 onderdelen, de Suwi-check en de KvK-check. Bij beide controles op de bron wordt het moment (timestamp) van controleren vastgelegd. Er worden voor TOZO(1) geen SUWI-gegevens via Sharefile verzonden, maar slechts het resultaat van de Check. Voor TOZO2 en TOZO3 is de informatie uitgebreid met de partner en inkomstentoets, waardoor wel (afgeleide) SUWI-gegevens over inkomen (LB) per maand van de lopende regeling worden aangeleverd aan de gemeente.

In Citrix Sharefile worden de uitgewisselde bestanden na twee weken weer automatisch geschoond. Wigo4it heeft een EU-aansluiting, waardoor de gegevensuitwisseling alleen binnen deze zone kan plaatsvinden.

Bijlage C - Schematisch overzicht van het object van onderzoek

