Assurance-rapport
NOREA Richtlijn 3000D

Verantwoording betreffende het gebruik van
de Gezamenlijke elektronische Voorzieningen Suwi
(GeVS)

[SERVICEORGANISATIE]

Opgesteld voor de gemeente: [XYZ]

Inhoud

Colofon

Voor u ligt het Assurancerapport inzake het onderzoek dat wij uitvoerden op de betrouwbare en integere verwerking van Suwinet gegevens door [SERVICEORGANISATIE]. Het ‘short form’ rapport bevat de basiselementen. Het ‘long form’ rapport bevat in Bijlage A aanvullende informatie die uitsluitend bedoeld is voor [SERVICEORGANISATIE], zoals een overzicht van de getoetste interne beheersmaatregelen en de door ons vastgestelde bevindingen en aanbevelingen.

1 Assurancerapport van de onafhankelijke auditor

1.1 Opdracht

Ingevolge het feit dat wij gebruik maken van [SERVICEORGANISATIE] hebben wij vanuit onze verantwoordelijkheid een onderzoek laten uitvoeren naar de opzet en het bestaan van interne beheersingsmaatregelen per [DATUM] voor het waarborgen van de vertrouwelijkheid van de Suwinet-gegevens die worden verwerkt.

Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen en brengen daarover geen oordeel tot uitdrukking.

1.2 Opdrachtomschrijving

Voor de uitvoering van de ta(a)k(en) [OPSOMMING VAN DE TAKEN DIE DE SERVICEORGANISATIE VOOR DE GEMEENTE UITVOERT] maakt [SERVICEORGANISATIE] gebruik van Suwinet-inkijk | Suwinet Inlezen | DKD Inlezen. [deze tabel is in principe limitatief]

Type	Gegevensverwerking
Carve-out via [SERVICEORGANISATIE]	Werk en Inkomen (o.a. uitvoering P-wet, IOAW/IOAZ)
Carve-out via [SERVICEORGANISATIE]	Werk en Inkomen (uitvoering sociale recherche taken)
Carve-out via [SERVICEORGANISATIE]	Werk en Inkomen (uitvoering bijzondere bijstand)
Carve-out via [SERVICEORGANISATIE]	Werk en Inkomen (uitvoering Besluit Bijstand Zelfstandigen)
Carve-out via [SERVICEORGANISATIE]	Dwanginvordering lokale belastingen
Carve-out via [SERVICEORGANISATIE]	Schuldhulp (Wet gemeentelijke schuldhulpverlening)

Gemeenten passen de Eenduidige Normatiek Single Information Audit (ENSIA) toe om invulling te geven aan een gestroomlijnde informatievoorziening over informatieveiligheid. Gemeenten moeten in het kader van ENSIA vaststellen dat aan alle relevante Suwinet vereisten wordt voldaan, dus de opzet en het bestaan van interne beheersingsmaatregelen per [DATUM] voor het waarborgen van de vertrouwelijkheid van de Suwinet-gegevens die worden verwerkt door [SERVICEORGANISATIE] .

Dit wordt gerealiseerd op basis van de ontvangen assurance rapportages, verantwoordingsinformatie van samenwerkingspartijen en door gemeenten in eigen beheer uitgevoerde werkzaamheden.

1.3 Gebruik van deze rapportage

Het Ministerie van Sociale Zaken en Werkgelegenheid (hierna: SZW) verwacht van gemeenten dat zij ook in het geval van uitbesteding en/ of samenwerking met andere organisaties de bestuurlijke verantwoordelijkheid blijven nemen en daarover verantwoording afleggen. Voorliggende rapportage kan door gemeente [XYZ] worden gebruikt om invulling te geven aan deze verantwoordelijkheid.

Gemeente [XYZ] verzoekt - voorafgaand aan de invulling van het self-assessment - aan de serviceorganisatie om middels een assurance-rapport aan te tonen dat de interne

beheersingsmaatregelen ter waarborging van de vertrouwelijkheid van de Suwinet-gegevens in opzet en bestaan voldoen aan de criteria. Gemeente [XYZ] neemt deze rapportage vervolgens bij de rapportering in ENSIA in aanmerking en past hierbij de 'carve-out' methodiek toe. Ten slotte stelt gemeente [XYZ] deze rapportage ter beschikking aan haar ENSIA auditor en wel in het kader van de ENSIA audit werkzaamheden.

In bijlage A is een overzicht opgenomen van de getoetste interne beheersingsmaatregelen en de door ons vastgestelde bevindingen en aanbevelingen.

1.4 Eventueel zelfstandig gebruik van Suwinet gegevens door gemeente [XYZ]

Indien gemeente [XYZ] naast de uitbestede Suwi-taken ook zelfstandig gebruik maakt van Suwinet gegevens, is zij zelf verantwoordelijk voor het opzetten en implementeren van interne beheersingsmaatregelen ter waarborging van de vertrouwelijkheid van de Suwinet-gegevens. Voor het gebruik van Suwinet en de daarin opgenomen gegevens zijn wettelijke grondslagen vereist. Deze vallen onder de verantwoordelijkheid van de minister van SZW en overige betrokken ministers. Het eventuele zelfstandig gebruik van Suwinet gegevens door gemeente [XYZ] is niet in deze assurance-rapportage betrokken en dient door de IT-auditor(s) van gemeente [XYZ] te worden onderzocht.

1.5 Verantwoordelijkheden [SERVICEORGANISATIE]

[SERVICEORGANISATIE] is verantwoordelijk gemaakt voor het opzetten en implementeren van interne beheersingsmaatregelen ter waarborging van de vertrouwelijkheid van de Suwinet-gegevens die worden verwerkt voor de gemeente [XYZ].

De beheersingsmaatregelen voor het veilige gebruik van Suwinet voorzieningen zijn daarbij leidend. De beheersingsmaatregelen zijn opgenomen in paragraaf 1.10. Indien sprake is van Suwinet-inlezen dan wel Suwinet-DKD, wordt van de serviceorganisatie verwacht dat de effectiviteit van de onderliggende General IT-Controls expliciet kan worden aangetoond.

1.6 Onze onafhankelijkheid en kwaliteitsbeheersing

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

De IT-auditeenheid past het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhoudt het een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en de procedures met betrekking tot de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving.

1.7 Verantwoordelijkheden van de auditor

We hebben onze opdracht uitgevoerd overeenkomstig Nederlands recht, waaronder NOREA Richtlijn 3000D 'Richtlijn Assurance-opdrachten door IT-auditors'.

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van een assurance-opdracht, dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel. Onze assurance-opdracht is uitgevoerd met een redelijke mate van zekerheid, dit betekent een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens onze assurance-opdracht niet alle afwijkingen ontdekken.

De geselecteerde werkzaamheden zijn afhankelijk van de door de auditor van de organisatie toegepaste oordeelsvorming, met inbegrip van het inschatten van de risico's dat de geselecteerde beheersingsmaatregelen niet op afdoende wijze zijn opgezet of niet bestaan. De werkzaamheden bestonden uit een combinatie van het kennisnemen van documentatie, het houden van interviews, het evalueren van de resultaten van de uitgevoerde interne controles en het verrichten van eigen (aanvullende) testwerkzaamheden.

Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de werking van de geselecteerde beheersingsmaatregelen en brengen daarover geen oordeel tot uitdrukking.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om daarop een onderbouwing met een redelijke mate van zekerheid voor ons oordeel te bieden.

1.8 Gehanteerde criteria

Wij hebben bij de uitvoering van onze werkzaamheden gebruik gemaakt van een selectie van beheersingsmaatregelen (gezamenlijk verder aangeduid als ENSIA normenkader) die zijn beschreven in de *'Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2022'* die is vastgesteld door het ketenoverleg van de Gezamenlijke elektronische Voorziening Suwinet (GeVS).

Daarnaast is gebruik gemaakt van de NOREA '*Handreiking ENSIA voor IT-auditors (RE's), versie 4.0 – Update Verantwoordingsjaar 2021 15 oktober 2021'* (Guidance voor de IT-auditors die zich bezighouden met IT-audits betreffende de Eénduidige Normatiek Single Information Audit (ENSIA) voor gemeenten).

Wij achten deze selectie van beheersingsmaatregelen en de guidance relevant en toereikend voor ons onderzoek.

1.9 Beperkingen

Het 'ENSIA normenkader' is een selectie van beheersingsmaatregelen uit de BIO dat is vastgesteld door het ketenoverleg van de Gezamenlijke elektronische Voorziening Suwinet (GeVS). Wij kunnen niet uitsluiten dat, indien wij aanvullende beheersingsmaatregelen zouden hebben onderzocht wellicht andere onderwerpen zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen.

Bovendien is de projectie van oordelen naar de toekomst onderhevig aan het risico dat interne beheersingsmaatregelen bij een serviceorganisatie onderhevig aan het risico dat interne beheersingsmaatregelen bij een serviceorganisatie ineffectief kunnen worden.

1.10 Oordelen

Onze oordelen zijn gevormd op basis van de werkzaamheden zoals ze zijn beschreven in deze rapportage. Per beheersingsmaatregel van de '*Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2022'* wordt een oordeel gegeven over de opzet en het bestaan per [DATUM]. De criteria waarvan wij gebruik hebben gemaakt, zijn opgenomen in onderstaande vastgestelde tabel. Per beveiligingsrichtlijn hebben wij hieronder vermeld of met redelijke mate van zekerheid wordt voldaan aan de beveiligingsrichtlijn. Om de leesbaarheid van dit rapport te vergroten zijn de conclusies in deze tabel weergegeven als "voldoet" of "voldoet niet". Hierbij moet "voldoet" worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de beheersingsdoelstellingen volgens de criteria genoemd in hoofdstuk 2 in alle materiële opzichten effectief zijn". "Voldoet niet" moet worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beheersingsmaatregel volgens de criteria genoemd in hoofdstuk 2 niet in alle materiële opzichten effectief zijn". De uitspraak voldoet of voldoet niet beperkt zich tot de eigen oordeelsvorming van de auditor.

BIO control	Beheersingsmaatregel	Oordelen
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 / Voldoet niet
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 / Voldoet niet
6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Voldoet / Voldoet niet
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 / Voldoet niet
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 / Voldoet niet
9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Voldoet / Voldoet niet
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 / Voldoet niet
9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	Voldoet / Voldoet niet
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 / Voldoet niet
10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersingsmaatregelen te worden ontwikkeld en geïmplementeerd.	Voldoet / Voldoet niet / Deze norm is niet van toepassing doordat geen gebruik wordt gemaakt

BIO control	Beheersingsmaatregel	Oordelen
		van Suwinet- en/of DKD-inlezen.
12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	Voldoet / Voldoet niet
12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Voldoet / Voldoet niet
12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Voldoet / Voldoet niet / Deze norm is niet van toepassing doordat geen gebruik wordt gemaakt van Suwinet- en/of DKD-inlezen.
18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Voldoet / Voldoet niet
	IT omgeving in service organisatie	
12.1.2	Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	Voldoet / Voldoet niet
12.1.4	Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Voldoet / Voldoet niet
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 / Voldoet niet

1.11 Beoogde gebruikers en doel

Onze schriftelijke rapportage is alleen bestemd voor [SERVICEORGANISATIE], de gemeente [XYZ], haar auditor(s), en het Ministerie van SZW en haar auditors, aangezien anderen, die niet op de hoogte zijn van de precieze reikwijdte, aard en doel van de werkzaamheden, de resultaten onjuist kunnen interpreteren.

De rapportage, onderdelen of samenvattingen daarvan mogen niet mondeling of schriftelijk aan derden beschikbaar worden gesteld zonder onze voorafgaande schriftelijke toestemming.

Voor zover het [SERVICEORGANISATIE] en gemeente [XYZ] is toegestaan het rapport aan derden beschikbaar te stellen, zal het rapport origineel, volledig en ongewijzigd beschikbaar worden gesteld. Indien de producten van onze werkzaamheden aan derden ter beschikking worden gesteld, dient erop te worden gewezen dat zonder onze uitdrukkelijke voorafgaande schriftelijke toestemming geen rechten aan het product kunnen worden ontleend. Het verstrekken van deze toestemming kan omgeven zijn met nadere voorwaarden.

[PLAATS], [DATUM]

[AUDIT ORGANIATIE]

[AUDITOR, RE]

2 Criteria

Het ketenberaad[1] heeft de BIO-controls geselecteerd waarvan zij vindt dat deze de hoogste impact hebben op de vertrouwelijkheid bij de verwerking van Suwinet gegevens. In dit onderzoek zullen wij ons derhalve zoals eerder aangegeven op de '*Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2022*' richten. De criteria waarvan gebruik wordt gemaakt bij het uitvoeren van de Assurance-opdracht houden in dat:.

- de interne beheersingsmaatregelen die verband houden met de beheersingsdoelstellingen op afdoende wijze (robuust) zijn opgezet en daadwerkelijk zijn geïmplementeerd;
- de risico's die het voldoen aan de beheersingsmaatregelen in gevaar brengen en daarmee de vertrouwelijkheid van Suwinet gegevens aantasten, in voldoende mate werden onderkend;
- de onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat onderliggende risico's het toereikend voldoen aan beheersingsmaatregelen niet verhinderen.

[1] Het Suwinet is een aaneenschakeling van systemen van verschillende partijen. Het ketenberaad bestaat uit afgevaardigden van de verschillende partijen. Gezamenlijk worden beslissingen genomen aangaande het Suwinet.

3 Verantwoordelijkheden gebruikersorganisatie

De opzet en implementatie van interne beheersingsmaatregelen bij [SERVICEORGANISATIE] zijn uitsluitend gericht op de Suwi-taken die [SERVICEORGANISATIE] voor gemeente [XYZ] uitvoert.

Indien gemeente [XYZ] daarnaast zelfstandig Suwi-taken uitvoert (hierbij kan gedacht worden aan taken in het kader van de participatiewet en bijzondere bijstand), dan wel Suwinet-gegevens voor andere doeleinden gebruikt (hierbij kan gedacht worden aan het gebruik ten behoeve van Burgerzaken) en daarvoor Suwinet-inkijk, DKD-inlezen, en/of Suwinet-inlezen gebruikt, dient op basis van zelfstandig uit te (laten) voeren onderzoek vast te stellen of de noodzakelijk geachte interne beheersingsmaatregelen door gemeente [XYZ] zijn geïmplementeerd.

OPTIONEEL

Dit rapport geeft inzicht in het interne controlesysteem dat ten grondslag ligt aan onze dienstverlening. [SERVICEORGANISATIE] merkt op dat onderstaande verantwoordelijkheden zijn belegd bij gemeente [XYZ]. Derhalve dienen deze maatregelen door de auditor van de gemeente [XYZ] te worden getoetst en worden meegenomen in de algehele oordeelsvorming.

De verantwoordelijkheden van onze gemeenten omvatten, maar zijn niet beperkt tot, het volgende:

De bijlage van dit rapport is uitsluitend bestemd voor [SERVICEORGANISATIE].

Bijlage A - Beschrijving van de testresultaten van de auditor

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

- Het verkrijgen van inzicht in de relevante kenmerken van de door [SERVICEORGANISATIE] verwerkte Suwinet-gegevens.
- Het vaststellen van de reikwijdte van het onderzoek, inclusief het vaststellen van de beheersingsmaatregelen die moeten worden onderzocht en het vaststellen dat de reikwijdte van de verwerking van Suwinet-gegevens volledig en juist wordt afgedekt.
- 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 vaststellen van het bestaan van de relevante maatregelen. Dit door middel van het kennis nemen van documentatie, het kennis nemen van de resultaten van de uitgevoerde interne controles, alsmede eigen (deel)waarnemingen.
- Het analyseren van de uitkomsten van onze werkzaamheden met als doel het geven van oordelen per beheersingsmaatregel van de Verantwoordingsrichtlijn Informatiebeveiliging GeVS 2022.

BIO control	Beheersingsmaatregel	Werkzaamheden	Oordelen
5. Informatiebeveiligingsbeleid			
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 / Voldoet niet
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 / Voldoet niet
6. Organiseren van informatiebeveiliging			
6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.		Voldoet / Voldoet niet

BIO control	Beheersingsmaatregel	Werkzaamheden	Oordelen
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 / Voldoet niet
7. Veilig personeel			
7.2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.		Voldoet / Voldoet niet
9. Toegangsbeveiliging			
9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.		Voldoet / Voldoet niet
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 / Voldoet niet Voldoet / Voldoet niet
9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.		Voldoet / Voldoet niet
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 / Voldoet niet
10. Cryptografie			
10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersingsmaatregelen te worden ontwikkeld en geïmplementeerd.	(LET OP: ALLEEN VAN TOEPASSING INDIEN GEBRUIK WORDT GEMAAKT VAN SUWINET-INLEZEN EN/OF DKD-INLEZEN)	Voldoet / Voldoet niet / Deze norm is niet van toepassing doordat geen gebruik wordt gemaakt van

BIO control	Beheersingsmaatregel	Werkzaamheden	Oordelen
			Suwinet- en/of DKD-inlezen.
12. Beveiliging bedrijfsvoering			
12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.		Voldoet / Voldoet niet
12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.		Voldoet / Voldoet niet
12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	(LET OP: ALLEEN VAN TOEPASSING INDIEN GEBRUIK WORDT GEMAAKT VAN SUWINET-INLEZEN EN/OF DKD-INLEZEN)	Voldoet / Voldoet niet / Deze norm is niet van toepassing doordat geen gebruik wordt gemaakt van Suwinet- en/of DKD-inlezen.
18. Naleving			
18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.		Voldoet / Voldoet niet
IT omgeving in service organisatie			
12.1.2	Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.		Voldoet / Voldoet niet
12.1.4	Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.		Voldoet / Voldoet niet

BIO control	Beheersingsmaatregel	Werkzaamheden	Oordelen
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 / Voldoet niet