

# **DigiD assessment serviceorganisatie**

**2024-2025**

**ISAE3000/D**



Serviceorganisatie: Forus Operations B.V.

Betreft: Forus & Me versie v129

Kenmerk: BKBO/200916-1/V5/TPM

Rapportdatum: 21 oktober 2024

Oordeelsdatum: 15 oktober 2024

Dit assurancerapport heeft 21 pagina's

## Heelal

Hoe verder men keek,  
hoe groter het leek.

Jules Deelder

## Colofon

Voor u ligt het assurance rapport van het DigiD ICT beveiligingsassessment dat wij uitvoerden op het betrouwbaar en integer functioneren van de webapplicatie Forus & Me van Forus Operations B.V..

Ons rapport wordt uitgebracht in twee versies: Het 'short form' rapport bevat de basiselementen inclusief de bijlagen bedoeld voor de gebruikersorganisatie en de toezichthouder. Het 'long form' rapport bevat aanvullende informatie die uitsluitend bedoeld is voor Forus Operations B.V., zoals een overzicht van de getoetste interne beheersmaatregelen, de door ons vastgestelde bevindingen en aanbevelingen plus een nadere beschrijving van het object van onderzoek.

Dit rapport is opgesteld onder verantwoordelijkheid van de heer drs. M.B.H. Ijpelaar RE CEH CISA CIPP/e ingeschreven onder nummer 1252 als actief RE in het register van NOREA en geregistreerd als actief CISA met nummer 0126934 bij ISACA.

## Inhoudsopgave

1	Assurancerapport van de onafhankelijke auditor	4
1.1	Onze oordelen	4
1.2	De basis voor onze oordelen	6
1.3	Van toepassing zijnde criteria	6
1.4	Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek	7
1.4.1	Object van onderzoek	7
1.4.2	Subservice organisaties	8
1.4.3	Norm ICT-beveiligingsassessment DigiD	8
1.4.4	Beperkingen met betrekking tot interne beheersmaatregelen	8
1.5	Beoogde gebruikers en doel	9
1.6	Verantwoordelijkheden van Forus Operations B.V.	9
1.7	Verantwoordelijkheid van de IT-auditor	9
2	Verantwoordelijkheden gebruikersorganisatie	11
	Bijlage A – Rapport van bevindingen DigiD	15
	Bijlage B – Object van onderzoek	16
	Bijlage C –Overzicht onderverdeling getoetste normen bij Forus Operations B.V.	17
	Bijlage D - Overzicht ICT-beveiligingsassessment DigiD	20
	Bijlage E – Rapportage penetratietest Defenced	21

# 1 Assurancerapport van de onafhankelijke auditor

Aan: management van Forus Operations B.V. en gebruikersorganisaties

## 1.1 Onze oordelen

Wij hebben een DigiD-beveiligingsassessment met redelijke mate van zekerheid uitgevoerd op de webomgeving van de aansluithouders welke zijn vermeld in paragraaf 1.4.1 Object van onderzoek.

Per beveiligingsrichtlijn hebben wij hieronder vermeld of 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 beheersmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn effectief is opgezet en geïmplementeerd op 15 oktober 2024". "Voldoet niet" moet worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn niet in alle materiële opzichten effectief is opgezet en/of geïmplementeerd op 15 oktober 2024".

Bij beveiligingsrichtlijnen waarbij ook de effectieve werking wordt vastgesteld moet "voldoet" worden geïnterpreteerd als "Wij zijn van oordeel dat de getoetste interne beheersmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn effectief werkten tijdens de controleperiode van 15 maart 2024 tot 15 oktober 2024". "Voldoet niet" moet vervolgens worden geïnterpreteerd als "Wij zijn van oordeel dat de getoetste interne beheersmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn niet in alle materiële opzichten effectief werkten tijdens de controleperiode van 15 maart 2024 tot 15 oktober 2024".

De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel zijn de criteria die zijn beschreven in de sectie 'Van toepassing zijnde criteria'.

Onze oordelen zijn gevormd op basis van de van de aangelegenheden die in dit assurancerapport zijn uiteengezet. Ons onderzoek was beperkt tot de beveiligingsrichtlijnen die de verantwoordelijkheid zijn van de serviceorganisatie.

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel opzet & bestaan	Oordeel werking
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.	Voldoet	n.v.t.
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	Voldoet	n.v.t.

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel opzet & bestaan	Oordeel werking
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.	Voldoet	Voldoet
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Voldoet	Voldoet
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Voldoet	n.v.t.
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	Voldoet	n.v.t.
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Voldoet	n.v.t.
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Voldoet	n.v.t.
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	Voldoet	n.v.t.
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.	Voldoet	n.v.t.
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.	Voldoet	n.v.t.
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.	Voldoet	n.v.t.
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.	Voldoet	n.v.t.
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	Voldoet	n.v.t.
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.	Voldoet	n.v.t.
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie.	Voldoet	n.v.t.
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie.	Voldoet	n.v.t.
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	Voldoet	n.v.t.
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.	Voldoet	Voldoet



Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel opzet & bestaan	Oordeel werking
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet	Voldoet
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.	Voldoet	Voldoet

## 1.2 De basis voor onze oordelen

Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht, waaronder de NOREA Richtlijn 3000D 'Assurance-opdrachten door IT-auditors (Directe-opdrachten)' en de nadere regels zoals opgenomen in de Handreiking DigiD 2024 (versie 1.0) van NOREA. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Verantwoordelijkheden van de IT-auditor'.

Wij zijn onafhankelijk van Forus Operations B.V. en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor onze oordelen.

## 1.3 Van toepassing zijnde criteria

Voor deze opdracht hanteren wij het Normenkader 3.0 voor ICT-beveiligingsassessments DigiD dat door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is vastgesteld. Het Ministerie BZK heeft uit de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties versie 2015 de 21 beveiligingsrichtlijnen tot norm gemaakt waarvan zij vindt dat deze de hoogste impact op de veiligheid van DigiD hebben en heeft deze vermeld in het Normenkader 3.0 voor ICT-beveiligingsassessments DigiD'. Het Normenkader 3.0 voor ICT-beveiligingsassessments DigiD bestaat uit 21 richtlijnen die zijn gebaseerd op de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties versie 2015. De versie 3.0 geldt vanaf 1 augustus 2022. De door BZK tot norm gemaakte 21 beveiligingsrichtlijnen worden tevens aangeduid als de 21 DigiD-normen.

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

- de risico's die het voldoen aan de beveiligingsrichtlijnen in gevaar brengen en daarmee de betrouwbaarheid van DigiD aantasten, werden onderkend;
- de onderkende interne beheersmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het voldoen aan beveiligingsrichtlijnen niet zouden verhinderen;
- de interne beheersmaatregelen die verband houden met de beveiligingsrichtlijnen op afdoende wijze zijn opgezet en daadwerkelijk zijn geïmplementeerd;
- de interne beheersmaatregelen die verband houden met een selectie van specifieke beveiligingsrichtlijnen gedurende de controleperiode effectief hebben gewerkt.

## 1.4 Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek

### 1.4.1 Object van onderzoek

Het object van onderzoek was de webomgeving van de volgende DigiD aansluitingen:

Houder DigiD aansluiting	DigiD aansluitnummer	DigiD aansluitnaam
Gemeente Nijmegen	1005507	Gemeente Nijmegen – Vergoedingen
Gemeente Westerkwartier	1005551	Gemeente Westerkwartier – Potjeswijzer2
Gemeente Groningen	1003635	Gemeente Groningen – Stadjerpas
Gemeente Geertruidenberg	1005591	Gemeente Geertruidenberg – Kindregeling
Gemeente Waalwijk	1005525	Gemeente Waalwijk – Paswijzer 2
Gemeente Schagen	1005555	Gemeente Schagen – Meedoen
Gemeente Eemsdelta	1005491	Gemeente Eemsdelta – Kansshop

Forus Operations B.V. biedt de volgende functionaliteit aan waarvoor DigiD aansluiting ter authenticatie wordt gebruikt:

De webapplicatie Forus & Me wordt door de inwoners/burgers van de klanten van Forus Operations B.V. gebruikt voor de aanvraag van sociale regelingen.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Forus & Me v129. De serviceorganisatie maakt gebruik van Continuous Deployment met behulp van versienummers in het software uitleveringsproces.

Deze applicatie betreft een geheel standaard pakket en wordt onderhouden door Forus Operations B.V.

De infrastructuur waarop de applicatie draait wordt beheerd door Forus Operations B.V.

Forus Operations B.V. maakt gebruik van de subserviceorganisatie Amazon Web Services, Inc. voor het PaaS-platform.

Daarnaast maakt Forus Operations B.V. gebruik van de subserviceorganisatie Fortra voor het beheer van het IDS/IPS Alert Logic.

Het onderzoek heeft zich gericht op de webapplicatie die gebruik maakt van DigiD voor de identificatie en authenticatie van de gebruikers. Specifiek zijn in scope de internet-facing webpagina's waarmee de interactie naar de gebruiker plaatsvindt als deze is geïdentificeerd en geauthentiseerd via DigiD, de systeemkoppelingen en de infrastructuur die met DigiD gekoppeld is en betrekking heeft op het DigiD identificatie en authenticatieproces. Ook de verschillende vormen van beheer op de webapplicaties zijn in scope voor zover relevant voor de doelstelling van de audit. De URL [www.digid.nl](http://www.digid.nl), de token uitwisseling tussen Logius en de webserver, de systemen die gegevens leveren of ophalen uit de webapplicatie, zoals backoffice informatiesystemen vallen buiten de scope. Subsystemen en koppelvlakken zijn in scope indien de primaire authenticatie van het systeem op basis van DigiD tot stand is gekomen.

### 1.4.2 Subservice organisaties

Forus Operations B.V. maakt gebruik van subserviceorganisatie Amazon Web Services, Inc. voor het PaaS-platform. Forus Operations B.V. maakt voor het verschaffen van zekerheid over haar volledige webomgeving zoals beschreven onder het object van onderzoek gebruik van de uitsluitingsmethode ('carve-out method'). De beschrijving van de serviceorganisatie van haar systeem sluit daarmee de interne beheersingsdoelstellingen en daarmee verband houdende interne beheersmaatregelen van de subserviceorganisatie uit. Onze werkzaamheden strekken zich dan ook niet uit tot de interne beheersmaatregelen van de subserviceorganisatie. Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de genoemde assurance-rapportage(s). Wij kunnen dan ook geen enkele verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Forus Operations B.V. maakt gebruik van subserviceorganisatie Fortra voor het beheer van het IDS/IPS Alert Logic. Forus Operations B.V. maakt voor het verschaffen van zekerheid over haar volledige webomgeving zoals beschreven onder het object van onderzoek gebruik van de 'inclusive methode'. De beschrijving van de serviceorganisatie van haar systeem omvat daarmee de interne beheersingsdoelstellingen en daarmee verband houdende interne beheersmaatregelen van de subserviceorganisatie(s). Onze werkzaamheden strekken zich dan ook uit tot de interne beheersmaatregelen van de subserviceorganisatie(s).

Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de genoemde assurance-rapportage(s). Wij kunnen dan ook geen enkele verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

### 1.4.3 Norm ICT-beveiligingsassessment DigiD

Het Normenkader 3.0 voor ICT-beveiligingsassessments DigiD bevat 21 beveiligingsrichtlijnen en is een selectie van beveiligingsrichtlijnen uit de 'ICT-beveiligingsrichtlijnen voor webapplicaties versie 2015' van het Nationaal Cyber Security Centrum (NCSC). Daarom zijn we niet in staat om één overkoepelend oordeel af te geven met betrekking tot de beveiliging van de DigiD-aansluiting. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft de richtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact hebben op de veiligheid van DigiD-webapplicaties. Logius houdt in opdracht van BZK toezicht op het naleven van de Voorwaarden DigiD, waaronder de uitvoering van DigiD-assessments. Wij adviseren Forus Operations B.V. om in aanvulling op de richtlijnen in de 'Norm ICT-beveiligingsassessments DigiD', ook de andere richtlijnen uit de 'ICT-beveiligingsrichtlijnen voor webapplicaties' van het NCSC te adopteren. Wij wijzen u erop dat, indien wij aanvullende beveiligingsrichtlijnen zouden hebben onderzocht wellicht andere onderwerpen zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen.

### 1.4.4 Beperkingen met betrekking tot interne beheersmaatregelen

Interne beheersmaatregelen bij een serviceorganisatie kunnen, vanwege hun aard, niet alle fouten of omissies voorkomen of ontdekken en corrigeren.

Voor wat betreft de werking hebben wij alleen werkzaamheden uitgevoerd naar de interne beheersmaatregelen zoals aangegeven in 'Normenkader 3.0 voor ICT-beveiligingsassessments DigiD' voor zover van toepassing binnen de scope van ons onderzoek.

Bovendien is het projecteren naar de toekomst van onze oordelen met betrekking tot de interne beheersmaatregelen om de doelstellingen te bereiken, onderhevig aan het risico dat interne beheersmaatregelen ineffectief kunnen worden.



Ons oordeel is niet aangepast als gevolg van deze aangelegenheden.

## 1.5 Beoogde gebruikers en doel

Ons assurancerapport is uitsluitend bestemd voor de houder(s) van de DigiD-aansluiting van de webomgeving, haar cliënten en hun auditors en Logius om inzicht te geven in de ICT beveiliging van de webomgeving van DigiD aansluiting. Logius kan hiermee toezicht houden op de koppeling van DigiD met de webapplicatie van een aangesloten organisatie voor het vertrouwen in en de integriteit van elektronische (overheids)dienstverlening.

Bijlage A bevat de beschrijving van de uitgevoerde (test)werkzaamheden en onze oordelen en aanbevelingen ter verbetering van de DigiD-webomgeving.

Bijlage B bevat de (uitgebreide) beschrijving van het 'Object van onderzoek'.

De bijlagen A en B zijn alleen bestemd voor Forus Operations B.V.

Bijlage C is bedoeld om Logius een totaaloverzicht te verschaffen ('volledigheid van de scope') over de resultaten van verschillende assessments, indien gebruik is gemaakt van rapporten inzake subserviceorganisatie(s).

Bijlage D is bedoeld om Logius een totaaloverzicht te verschaffen ('identificatie') over de identificerende kenmerken van het DigiD-assessment, ongeacht of gebruik is gemaakt van rapporten inzake subserviceorganisatie(s).

Ons assurancerapport inclusief bijlagen mag enkel worden gebruikt voor het doel waarvoor het is opgesteld door de beoogde gebruikers en dient niet te worden verspreid aan of te worden gebruikt door anderen.

## 1.6 Verantwoordelijkheden van Forus Operations B.V.

Het management van Forus Operations B.V. is verantwoordelijk voor het verlenen van DigiD-diensten, het onderkennen van de beveiligingsrisico's van de DigiD-webomgeving en het opzetten en implementeren van interne beheersmaatregelen om te voldoen aan de vigerende 'Norm ICT-beveiligingsassessments DigiD 3.0'.

## 1.7 Verantwoordelijkheid van de IT-auditor

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van ons onderzoek dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor de door ons af te geven oordelen over de opzet en implementatie van interne beheersmaatregelen die verband houden met de beveiligingsrichtlijnen in overeenstemming met de hiervoor vermelde criteria.

Ons onderzoek is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens ons onderzoek niet alle materiële fouten en fraude ontdekken.


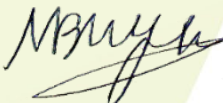
Wij passen de 'Reglement Kwaliteitsbeheersing NOREA' (RKBN) toe. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van ethische voorschriften, professionele standaarden en andere relevante wet- en regelgeving.

Ons onderzoek om te rapporteren over opzet, bestaan en voor de van toepassing zijnde beveiligingsrichtlijnen uit Normenkader 3.0 voor ICT-beveiligingsassessment DigiD de werking van interne beheersmaatregelen bestond onder andere uit:

- het verkrijgen van inzicht in de relevante kenmerken van de DigiD-webomgeving;
- het vaststellen van de scope van de assessment, inclusief het vaststellen van de maatregelen die bij de service organisatie 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 evalueren van de opzet, het vaststellen van het bestaan en voor de van toepassing zijnde beveiligingsrichtlijnen uit Normenkader 3.0 voor ICT-beveiligingsassessment DigiD 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 en uitgevoerde pentesten, alsmede eigen waarnemingen;
- het evalueren van de uitkomsten van onze werkzaamheden.

Vlijmen d.d. 21 oktober 2024

BKBO b.v.

	
V.C.W.M. Pajmans MA CIPP/e CISA, auditor	drs. M.B.H. Ijpelaar RE CEH CISA CIPP/e, directeur

## 2 Verantwoordelijkheden gebruikersorganisatie

Bij de opzet en implementatie van interne beheersmaatregelen bij de serviceorganisatie neemt deze voor een aantal beveiligingsrichtlijnen van het 'Normenkader 3.0 voor ICT-beveiligingsassessments DigiD' aan, dat enkele interne beheersmaatregelen door de gebruikersorganisaties zullen worden geïmplementeerd om te voldoen aan deze beveiligingsrichtlijnen.

In de onderstaande tabel wordt aangegeven voor welke beveiligingsrichtlijn(en) deze afweging is gemaakt en welke gewenste interne beheersactiviteit bij de gebruikersorganisaties kunnen worden geïmplementeerd om te voldoen aan de desbetreffende beveiligingsrichtlijn van het 'Normenkader 3.0 voor ICT-beveiligingsassessments DigiD'.

De geschiktheid van de opzet, het bestaan en/of de werking van deze aanvullende interne beheersmaatregelen van een gebruikersorganisatie hebben wij niet geëvalueerd. Aan de beveiligingsrichtlijnen van het 'Normenkader 3.0 voor ICT-beveiligingsassessments DigiD' wordt alleen voldaan, indien aanvullende interne beheersmaatregelen van een gebruikersorganisatie samen met de interne beheersmaatregelen van de serviceorganisatie op afdoende wijze zijn opgezet en geïmplementeerd.

Nr	Beschrijving van de beveiligingsrichtlijn	Gewenste interne beheersmaatregelen van de gebruikersorganisatie
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.	<p>Deze beveiligingsrichtlijn valt deels onder verantwoordelijkheid van de serviceorganisatie en is voor dat deel onderzocht. Voor het overige valt dit onder verantwoordelijkheid van de gebruikersorganisatie.</p> <p>De gebruikersorganisatie dient ervoor zorg te dragen dat:</p> <ul style="list-style-type: none"> <li>- het eigenaarschap t.a.v. de DigiD webapplicatie adequaat op een hoog organisatorisch niveau is inricht;</li> <li>- de eigenaar passende bevoegdheden heeft;</li> <li>- in het informatiebeveiligingsbeleid, of in een hiervoor apart ontwikkeld beleid, expliciet aandacht is besteed aan het stelsel van beveiligingsmaatregelen t.a.v. het functioneel beheer van de webapplicatie</li> <li>- toegangsvoorziening (U/TV.01),</li> <li>- dataclassificatie (U/WA.05) en kwetsbaarhedenbeheer (U/NW.06, t.a.v. DNSSEC) hierin zijn geadresseerd.</li> </ul>
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	<p>De gebruikersorganisatie moet de afspraken met Forus Operations B.V. vastleggen in een overeenkomst waarbij o.a. de volgende zaken zijn opgenomen:</p> <ul style="list-style-type: none"> <li>• een beschrijving van de te leveren diensten die onder het contract vallen;</li> <li>• de van toepassing zijnde leveringsvoorwaarden;</li> <li>• informatiebeveiligingseisen met de relevante eisen vanuit het beveiligingsbeleid;</li> <li>• het melden van beveiligingsincidenten;</li> <li>• de behandeling van gevoelige gegevens;</li> <li>• wanneer en hoe de leverancier toegang tot de systemen/ data van de gebruikersorganisatie mag hebben;</li> </ul>

Nr	Beschrijving van de beveiligingsrichtlijn	Gewenste interne beheersmaatregelen van de gebruikersorganisatie
		<ul style="list-style-type: none"> <li>• Service Level Reporting;</li> <li>• het jaarlijks uitvoeren van audits bij Forus Operations B.V.;</li> <li>• beding dat deze voorwaarden back-to-back worden doorgegeven aan mogelijke sub-leveranciers.</li> </ul>
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.	<p>Deze beveiligingsrichtlijn valt deels onder verantwoordelijkheid van Forus Operations B.V. en is voor dat deel onderzocht. Voor het overige valt dit onder verantwoordelijkheid van de gebruikersorganisatie.</p> <p>De gebruikersorganisatie moet maatregelen ontwerpen, inrichten en tijdens de controleperiode aantoonbaar waarborgen met betrekking tot toegangsbeveiliging en -beheer. Hierbij valt te denken aan:</p> <ul style="list-style-type: none"> <li>• het toekennen, controleren en intrekken van autorisaties;</li> <li>• het stellen van eisen aan de wachtwoordinstellingen;</li> <li>• een aantoonbare controle op joiners/movers/leavers;</li> <li>• het wijzigen van de standaard wachtwoorden van administrator accounts;</li> <li>• het beperken eventuele shared accounts.</li> <li>• Het uitvoeren periodieke (minimaal jaarlijkse) reviews.</li> </ul> <p>Alle accounts dienen individueel te zijn en er dient door de houder van de DigiD-aansluiting een autorisatiematrix te worden opgesteld en beheerd.</p> <p>Onder gebruikersorganisatie kan de DigiD aansluithouder worden verstaan maar ook een (sub)serviceorganisatie die door de aansluithouder is ingeschakeld.</p>
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	<p>Deze beveiligingsrichtlijn valt deels onder verantwoordelijkheid van Forus Operations B.V. en is voor dat deel onderzocht. Voor het overige valt dit onder verantwoordelijkheid van de gebruikersorganisatie.</p> <p>De gebruikersorganisatie moet maatregelen ontwerpen, inrichten en tijdens de controleperiode aantoonbaar waarborgen met betrekking tot:</p> <ul style="list-style-type: none"> <li>• de beschrijving van taken, verantwoordelijkheden en bevoegdheden van de verschillende beheerrollen;</li> <li>• het opstellen van een incidentenprocedure;</li> <li>• het registreren, analyseren, opvolgen en afhandelen van incidenten;</li> </ul>



Nr	Beschrijving van de beveiligingsrichtlijn	Gewenste interne beheersmaatregelen van de gebruikersorganisatie
		<ul style="list-style-type: none"> <li>het analyseren en zo nodig opvolgen van meldingen van het NCSC of IBD of Z-CERT of andere CERTS;</li> <li>het periodiek rapporteren aan het management inzake beveiligingsincidenten.</li> </ul> <p>Onder gebruikersorganisatie kan de DigiD aansluithouder worden verstaan maar ook een (sub)serviceorganisatie die door de aansluithouder is ingeschakeld.</p>
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	<p>Deze beveiligingsrichtlijn valt deels onder verantwoordelijkheid van Forus Operations B.V. en is voor dat deel onderzocht. Voor het overige valt dit onder verantwoordelijkheid van de gebruikersorganisatie.</p> <p>In ons onderzoek is vastgesteld dat de serviceorganisatie de vereiste maatregelen heeft genomen om de gevoelige gegevens te kunnen beschermen.</p> <p>De gebruikersorganisatie dient zorg te dragen voor:</p> <ul style="list-style-type: none"> <li>het classificeren van de gegevens die met DigiD worden ontsloten conform de vigerende privacywetgeving en zo nodig met de leverancier in overleg te gaan over aanvullende beveiligingsmaatregelen zoals het versleutelen of hashen van gevoelige gegevens.</li> </ul>
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	<p>Onder deze beveiligingsrichtlijn valt het verplicht gebruik van DNSSEC (DNS Security Extensions) voor de URL van het object van onderzoek. Met DNSSEC wordt de authenticiteit van DNS-antwoorden geverifieerd om misbruik te voorkomen.</p> <p>Het regelen van DNSSEC is de verantwoordelijkheid van de gebruikersorganisatie. De gebruikersorganisatie moet maatregelen ontwerpen en zodanig inrichten dat het object van onderzoek wordt beveiligd via DNSSEC.</p>
C.08	Wijzigingsbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	<p>De gebruikersorganisatie dient te beoordelen of wijzigingen van de functionaliteit van de webapplicatie gevolgen hebben voor de eigen administratieve organisatie.</p> <p>Daarom zou de gebruikersorganisatie tijdens de controleperiode aantoonbaar kennis moeten nemen van de releasenotes, handleidingen, cursusmateriaal en overige mededelingen van de serviceorganisatie en zo nodig hierop te handelen.</p>



Nr	Beschrijving van de beveiligingsrichtlijn	Gewenste interne beheersmaatregelen van de gebruikersorganisatie
		De releasenotes zijn door Forus Operations B.V. inzichtelijk gemaakt via <a href="https://github.com/teamforus/forus/releases">https://github.com/teamforus/forus/releases</a>

## **Bijlage A – Rapport van bevindingen DigiD**

Deze bijlage is niet bestemd voor de gebruikersorganisaties en wordt slechts verstrekt aan Forus Operations B.V.

## **Bijlage B – Object van onderzoek**

Deze bijlage is vertrouwelijk en niet bestemd voor de gebruikersorganisatie en wordt slechts verstrekt aan Forus Operations B.V.

Bij het uitbrengen van een nieuwe release van de applicatie of een grote upgrade van het onderliggende platform moet, bij voorkeur door middel van een penetratietest, worden onderzocht of er geen nieuwe kwetsbaarheden zijn geïntroduceerd. Deze penetratietest zou specifiek gefocust mogen zijn op wijzigingen in de applicatie en/of de infrastructuur en hoeft niet noodzakelijkerwijs door een penetratietester te worden uitgevoerd die onafhankelijk staat ten opzichte van het te onderzoeken object.

## Bijlage C –Overzicht onderverdeling getoetste normen bij Forus Operations B.V.

Deze bijlage richt zich op het ten dienste van Logius inzichtelijk maken van de wijze waarop Forus Operations B.V. gebruik heeft gemaakt van subserviceorganisaties die betrekking hebben op het object van onderzoek.

Als input voor de hierna vermelde samenvatting is, naast de voorliggende rapportage, gebruik gemaakt van de volgende rapportage(s):

Omschrijving assurancerapportage	Subservice organisatie	Bij subservice-organisatie getoetste beveiligingsrichtlijnen	Referentie	Oordeelsdatum & controleperiode	Ondertekend door auditor of auditeenheid
SOC2 assurancerapportage	Amazon Web Services, Inc.	B.01, U/WA.02, U/TV.01, C.08 en C.09	System and Organisation Controls 2 (SOC2) Type 2 Report Description of the Amazon Web Services System Relevant to Security, Availability, Confidentiality, and Privacy	Controleperiode: 1 april 2023 tot en met 31 maart 2024 Oordeelsdatum: 14 mei 2024	Ernst + Young LLP
Brugletter SOC2 type 2 rapport	Amazon Web Services, Inc.	B.01, U/WA.02, U/TV.01, C.08 en C.09		Controleperiode: 1 april 2024 tot en met 1 september 2024	Sara Duffer Director, AWS Security Assurance Amazon Web Services

Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de genoemde assurancerapportage(s). Wij kunnen dan ook geen enkele verantwoordelijkheid nemen met betrekking tot de in die rapportage vermelde oordelen.

Wij hebben kennisgenomen van de genoemde assurancerapportage(s) en hebben ten behoeve van Logius in onderstaande tabel per beveiligingsrichtlijn aangegeven tot welk oordeel de service auditor is gekomen.

Norm	Beschrijving van de norm	Getoetst Amazon Web Services, Inc.
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.	Opzet & bestaan voldoet Werking n.v.t. AWSCA-1.1 AWSCA-1.2 AWSCA-1.3
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	Nee
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.	Opzet & bestaan voldoet Werking voldoet AWSCA-2.1 AWSCA-2.2 AWSCA-2.3 AWSCA-2.4 AWSCA-2.5 AWSCA-2.6
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Opzet & bestaan voldoet Werking voldoet AWSCA-8.1 AWSCA-8.2
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Nee
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	Nee
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Nee
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Nee
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	Nee
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.	Nee
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.	Nee
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.	Nee
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.	Nee
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	Nee
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	Nee
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	Nee
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	Nee
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	Nee
C.07	De logging- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord	Nee



	(bewaakt, geanalyseerd) en de bevindingen gerapporteerd.	
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Opzet & bestaan voldoet
		Werking voldoet
		AWSCA-6.1
		AWSCA-6.2
		AWSCA-6.3
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.	AWSCA-6.4
		AWSCA-6.5
		AWSCA-6.6
		AWSCA-6.7
		Opzet & bestaan voldoet
		Werking voldoet
		AWSCA-3.16
		AWSCA-6.1
		AWSCA-6.2
		AWSCA-6.3
		AWSCA-6.4
		AWSCA-6.5
		AWSCA-6.6
		AWSCA-6.7

## Bijlage D - Overzicht ICT-beveiligingsassessment DigiD

Bijlage D is bedoeld om Logius een totaaloverzicht te verschaffen ('identificatie') over de identificerende kenmerken van het DigiD-assessment, ongeacht of gebruik is gemaakt van rapporten inzake subserviceorganisatie(s).

<b>Aansluiting</b>	Aansluitnummer	Zie de tabel in paragraaf 1.4.1 Object van onderzoek
	Aansluitnaam	Idem
	Aansluithouder	Idem
<b>Auditor serviceorganisatie</b>	Naam auditor	drs. M.B.H. Ijpelaar RE CEH CISA CIPP/e
	Auditorganisatie	BKBO bv
	Kenmerk rapport	BKBO/200916-1/V5/TPM
<b>Object van onderzoek</b>	Naam webapplicatie	Forus & Me
	Versie	v129
	Omschrijving	De webapplicatie Forus & Me wordt door de inwoners/burgers van de klanten van Forus Operations B.V. gebruikt voor de aanvraag van sociale regelingen.
<b>Subserviceorganisatie A</b>	Subserviceorganisatie A	Amazon Web Services, Inc.
	Auditor subserviceorganisatie A	Ernst + Young LLP
	Kenmerk rapport	SOC2 Type 2 Report 'Description of the Amazon Web Services System Relevant to Security, Availability, Confidentiality, and Privacy'
	Controleperiode	1 april 2023 tot en met 31 maart 2024 inclusief brugletter verlengd tot en met 1 september 2024.
	Rapportdatum	14 mei 2024
<b>Subserviceorganisatie B</b>	Subserviceorganisatie B	Fortra
	Auditor subserviceorganisatie B	drs. M.B.H. Ijpelaar RE CEH CISA CIPP/e
	Kenmerk rapport	BKBO/200916-1/V5/TPM (dit rapport)
	Controleperiode	15 maart 2024 tot 15 oktober 2024
	Rapportdatum	21 oktober 2024

## Bijlage E – Rapportage penetratietest Defenced

Deze bijlage is niet bestemd voor de gebruikersorganisaties en wordt slechts verstrekt aan Forus Operations B.V.