**Rapportage-template DigiD-Assessment (versie 2.0)**

|  |  |
| --- | --- |
| Aan : | LOGIUS |
| Datum : |  |
| Van : | KENMERK |
| Aansluiting :  |  |

Inhoudsopgave

1 Assurancerapport van de onafhankelijke auditor 2

1.1 Opdracht 2

1.2 Verantwoordelijkheden van de ORGANISATIE 2

1.3 Verantwoordelijkheden van de auditor 2

1.4 Beperkingen 3

1.5 Oordelen 4

1.6 Beoogde gebruikers en doel 6

2 Criteria 8

3 Object van onderzoek 9

A Bijlage A - Beschrijving van de testresultaten van de auditor 10

B Bijlage B – Object van onderzoek 20

C Bijlage C – Totaaloverzicht getoetste normen ICT-beveiligingsassessment DiGiD-aansluiting van [gebruikersorganisatie]. 21

# Assurancerapport van de onafhankelijke auditor

## Opdracht

Ingevolge de opdracht van hebben wij een DigiD-beveiligingsassessment uitgevoerd op de webomgeving van DigiD-aansluiting en van zoals gespecificeerd in hoofdstuk 3 Object van onderzoek. Het onderzoek wordt conform de ‘Handleiding uitvoering ICT-beveiligingsassessment’ versie 2.1 van Logius uitgevoerd.

Wij hebben de regelgeving van de NOREA voor kwaliteitsbeheersing toegepast en onderhouden een inzichtelijk stelsel van kwaliteitsbeheersing met inbegrip van gedocumenteerde beleidslijnen en procedures met betrekking tot het naleven van ethische voorschriften, professionele Richtlijnen en van toepassing zijnde, door wet- of regelgeving gestelde, vereisten.

De opdracht omvatte het onderzoeken van de opzet en het bestaan van maatregelen en procedures gericht op de ICT-beveiliging van de webomgeving van de DigiD-aansluiting en .

HOUDERORGANISATIE maakt gebruik van serviceorganisatie voor <de aard van de activiteiten die door de serviceorganisatie worden uitgevoerd>. maakt voor haar beschrijving gebruik van de uitsluitingmethode (‘carve-out method’). De beschrijving van de serviceorganisatie van haar systeem sluit daarmee de interne beheersingsdoelstellingen en daarmee verband houdende interne beheersingsmaatregelen van de serviceorganisatie uit. Onze werkzaamheden strekken zich dan ook niet uit tot de interne beheersingsmaatregelen van de serviceorganisatie.

## Verantwoordelijkheden van de

 is verantwoordelijk voor de beschrijving van het object van onderzoek, het verlenen van DigiD-diensten, het onderkennen van de beveiligingsrisico’s van de DigiD-webomgeving en het opzetten en implementeren van interne beheersingsmaatregelen om te voldoen aan de ‘Norm ICT-beveiligingsassessments’ DigiD van Logius.

## Verantwoordelijkheden van de auditor

Onze verantwoordelijkheid is, op basis van onze werkzaamheden, per beveiligingsrichtlijn van de ‘Norm ICT-beveiligingsassessments DigiD’ van Logius een oordeel te geven over de opzet en het bestaan van de maatregelen gericht op de ICT beveiliging van de webomgeving van DigiD aansluiting en .

We hebben onze opdracht uitgevoerd overeenkomstig Nederlands recht, en de NOREA Richtlijn 3000, ‘Richtlijn Assurance-opdrachten door IT-auditors’. 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.

Een assurance-opdracht om te rapporteren over opzet en bestaan van interne beheersingsmaatregelen bij een organisatie omvat het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie over de opzet en het bestaan van interne beheersingsmaatregelen. 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 interne beheersingsmaatregelen niet op afdoende wijze zijn opgezet of niet bestaan.

Zoals hierboven staat vermeld, hebben wij geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen die bij de beschrijving waren inbegrepen; wij brengen derhalve daarover geen oordelen tot uitdrukking.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om daarop een onderbouwing voor onze oordelen te bieden.

## Beperkingen

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.

De ‘Norm ICT-beveiligingsassessments DigiD’ is een selectie van beveiligingsrichtlijnen uit de ‘ICT-beveiligingsrichtlijnen voor webapplicaties’ van het Nationaal Cyber Security Centrum (NCSC). Daarom zijn we niet in staat om een overall oordeel te verschaffen omtrent de beveiliging van de DigiD-aansluiting.

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

Logius heeft de richtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact hebben op de veiligheid van DigiD-webapplicaties. Wij adviseren de organisatie 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.

In de volgende paragraaf geven wij onze oordelen ten aanzien van de ‘Norm ICT-beveiligingsassessments DigiD’.

## Oordelen

Onze oordelen zijn gevormd op basis van de werkzaamheden zoals ze zijn beschreven in deze rapportage. Per beveiligingsrichtlijn van de ‘Norm ICT-beveiligingsassessments DigiD’ van Logius wordt een oordeel gegeven over de opzet en het bestaan per . De criteria waarvan wij gebruik hebben gemaakt, zijn opgenomen in onderstaande tabel en een toelichting is te vinden in hoofdstuk 2.

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 op die regel aangegeven beveiligingsrichtlijn 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 beveiligingsrichtlijn 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. Ons onderzoek was beperkt tot de beveiligingsrichtlijnen die de verantwoordelijkheid zijn van de houderorganisatie en waarvan de auditor van de serviceorganisatie heeft aangegeven dat, om te voldoen aan deze beveiligingsrichtlijnen, interne beheersingsmaatregelen door de gebruikersorganisaties dienen worden geïmplementeerd. In Bijlage C is ten dienste van de assessmentbeoordeling door Logius een totaaloverzicht opgenomen van de door ons onderzochte normen en de normen die door de IT-auditor van de serviceorganisatie zijn onderzocht. Uitdrukkelijk merken wij op dat we geen onderzoek hebben uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de rapportage van de serviceorganisatie. Wij kunnen dan ook geen verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Indien bij een beveiligingsrichtlijn wel voldaan is aan de opzet van de interne beheersmaatregel, maar het bestaan niet vastgesteld kan worden omdat de relevante gebeurtenis zich niet heeft voorgedaan in de onderzochte periode, dan wordt dit weergegeven als “voldoet”. In een voetnoot wordt de volgende zin opgenomen: ‘‘Wij hebben vastgesteld dat deze organisatie maatregelen heeft ontworpen en ingericht met betrekking tot deze norm en hebben deze gevalideerd. Vanwege het feit dat zich geen situatie heeft voorgedaan waarop deze maatregel betrekking heeft, hebben wij het bestaan niet kunnen vaststellen. Wij zijn echter van oordeel dat de organisatie voldoet aan deze norm.”

| Nr | Beschrijving van de beveiligingsrichtlijn | Oordeel |
| --- | --- | --- |
| 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 / Voldoet niet |
| 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. |  |
| U/WA.02 | Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. |  |
| U/WA.03 | De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt. |  |
| U/WA.04 | De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren. |  |
| U/WA.05 | De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken. |  |
| U/PW.02 | De webserver garandeert specifieke kenmerken van de inhoud van de protocollen. |  |
| U/PW.03 | De webserver is ingericht volgens een configuratie-baseline. |  |
| 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. |  |
| U/PW.07  | Voor het configureren van platformen een hardeningsrichtlijn beschikbaar. |  |
| 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. |  |
| U/NW.04 | De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen. |  |
| U/NW.05 | Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd. |  |
| U/NW.06 | Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar. |  |
| C.03 | Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope). |  |
| C.04 | Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope). |  |
| C.06 | In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. |  |
| 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. |  |
| C.08 | Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd. |  |
| C.09 | Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen. |  |

## Beoogde gebruikers en doel

De minister van BZK wil een structurele en forse impuls geven aan de kwaliteitsverhoging van ICT-beveiliging bij overheidsorganisaties die gebruik maken van DigiD. Deze organisaties moeten jaarlijks een ICT beveiligingsassessment laten verrichten onder verantwoordelijkheid van een gekwalificeerde IT-auditor (RE), teneinde de DigiD gebruikende organisaties en Logius inzicht te geven in de ICT beveiliging van de webomgeving van DigiD aansluiting.

Onze schriftelijke rapportage met bijlage C is alleen bestemd voor , haar cliënten en hun auditors en Logius aangezien anderen, die niet op de hoogte zijn van de precieze scope, aard en doel van de werkzaamheden, de resultaten onjuist kunnen interpreteren. De rapportage (al dan niet met bijlagen), onderdelen of samenvattingen daarvan mogen niet mondeling of schriftelijk aan derden beschikbaar worden gesteld zonder onze voorafgaande schriftelijke toestemming. De bijlagen A en B zijn alleen bestemd voor . 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 serviceorganisatie(s).

Voor zover het en Logius 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.

,

# Criteria

Logius heeft de richtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact hebben op de veiligheid van DigiD-webapplicaties. In dit onderzoek zullen wij ons derhalve op de ‘Norm ICT-beveiligingsassessments DigiD’ richten. De criteria waarvan gebruik wordt gemaakt bij het uitvoeren van de assurance-opdracht hielden in dat:

* de interne beheersingsmaatregelen die verband houden met de beveiligingsrichtlijnen op afdoende wijze zijn opgezet en daadwerkelijk zijn geïmplementeerd;
* de risico’s die het voldoen aan de beveiligingsrichtlijnen in gevaar brengen en daarmee de betrouwbaarheid van DigiD aantasten, werden onderkend;
* de onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico’s het voldoen aan beveiligingsrichtlijnen niet zouden verhinderen.

# Object van onderzoek

Het object van onderzoek was de webomgeving van DigiD aansluiting en .

 biedt de volgende functionaliteit aan waarvoor DigiD aansluiting en ter authenticatie wordt gebruikt: <HIGH LEVEL OPSOMMING VAN AANGEBODEN FUNCTIONALITEIT>. Deze functionaliteit wordt geboden door de volgende webapplicatie:

* <NAAM VAN DE APPLICATIE>

Deze applicatie betreft <GEHEEL MAATWERK / EEN COMBINATIE VAN MAATWERK EN STANDAARD SOFTWARE / GEHEEL STANDARD PAKKET> en worden onderhouden door <NAAM SERVICEORGANISATIE 1>. De infrastructuur waarop de applicaties draaien wordt beheerd door <NAAM SERVICEORGANISATIE 2>.

Het onderzoek heeft zich gericht op de webapplicaties, de URLs waarmee deze applicaties kunnen worden benaderd, de infrastructuur (binnen de DMZ waar webapplicaties zich bevinden) en een aantal ondersteunende processen conform de ‘Norm ICT-beveiligingsassessments DigiD’ van Logius.

HOUDER heeft een deel DigiD webomgeving uitbesteed aan <SERVICE ORGANISATIE 1 en SERVICE ORGANISATIE 2>. Als gevolg hiervan zijn er een aantal maatregelen belegd bij deze service organisatie. Het onderzoeken van deze maatregelen bij deze service organisatie is dan ook uitgevoerd door een gekwalificeerde IT auditor op basis van dezelfde beveiligingsrichtlijnen en met hantering van het zelfde onderzoekprotocol als ons onderzoek. De richtlijnen waar deze maatregelen betrekking op hebben zijn door ons dan ook niet onderzocht en niet opgenomen in ons rapport. Waar relevant maken wij, per richtlijn, specifieke verwijzingen naar het rapport van de IT auditor van de service organisatie.

In bijlage B geven wij u een meer gedetailleerde beschrijving van het object van onderzoek.

1. 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 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 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 en uitgevoerde pentesten, alsmede eigen waarnemingen.
* Het analyseren van de uitkomsten van onze werkzaamheden met als doel het geven van oordelen per beveiligingsrichtlijn van de ‘Norm ICT-beveiligingsassessments DigiD’ van Logius.

Hieronder treft u een korte beschrijving van de uitgevoerde werkzaamheden en onze oordelen ter verbetering van de DigiD-webomgeving. Onze oordelen zijn verwoord als voldoet/voldoet niet (met reden) per 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 op die regel aangegeven beveiligingsrichtlijn 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 beveiligingsrichtlijn 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. Ons onderzoek was beperkt tot de beveiligingsrichtlijnen die de verantwoordelijkheid zijn van de houderorganisatie en waarvan de auditor van de serviceorganisatie heeft aangegeven dat, om te voldoen aan deze beveiligingsrichtlijnen, interne beheersingsmaatregelen door de gebruikersorganisaties dienen worden geïmplementeerd. In Bijlage C is ten dienste van de assessmentbeoordeling door Logius een totaaloverzicht opgenomen van de door ons onderzochte normen en de normen die door de IT-auditor van de serviceorganisatie zijn onderzocht. Uitdrukkelijk merken wij op dat we geen onderzoek hebben uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de rapportage van de serviceorganisatie. Wij kunnen dan ook geen verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Indien bij een beveiligingsrichtlijn wel voldaan is aan de opzet van de interne beheersmaatregel, maar het bestaan niet vastgesteld kan worden omdat de relevante gebeurtenis zich niet heeft voorgedaan in de onderzochte periode dan wordt dit weergegeven als “voldoet”. In een voetnoot wordt de volgende zin opgenomen: ‘‘Wij hebben vastgesteld dat deze organisatie maatregelen heeft ontworpen en ingericht met betrekking tot deze norm en hebben deze gevalideerd. Vanwege het feit dat zich geen situatie heeft voorgedaan waarop deze maatregel betrekking heeft, hebben wij het bestaan niet kunnen vaststellen. Wij zijn echter van oordeel dat de organisatie voldoet aan deze norm.”

| Nr | Beschrijving van de beveiligingsrichtlijn | Korte beschrijving van de uitgevoerde werkzaamheden | Oordeel en eventuele adviezen |
| --- | --- | --- | --- |
| 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 / Voldoet niet |
| 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. |  |  |
| U/WA.02 | Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. |  |  |
| U/WA.03 | De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt. |  |  |
| U/WA.04 | De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren. |  |  |
| U/WA.05 | De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken. |  |  |
| U/PW.02 | De webserver garandeert specifieke kenmerken van de inhoud van de protocollen. |  |  |
| U/PW.03 | De webserver is ingericht volgens een configuratie-baseline. |  |  |
| 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. |  |  |
| U/PW.07  | Voor het configureren van platformen een hardeningrichtlijn beschikbaar. |  |  |
| 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. |  |  |
| U/NW.04 | De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen. |  |  |
| U/NW.05 | Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd. |  |  |
| U/NW.06 | Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar. |  |  |
| C.03 | Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope). |  |  |
| C.04 | Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope). |  |  |
| C.06 | In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. |  |  |
| 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. |  |  |
| C.08 | Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd. |  |  |
| C.09 | Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen. |  |  |

1. Bijlage B – Object van onderzoek

Het object van onderzoek was de webomgeving van DigiD aansluiting en .

 biedt de volgende functionaliteit aan waarvoor DigiD aansluiting voor authenticatie wordt gebruikt: <HIGH LEVEL OPSOMMING VAN AANGEBODEN FUNCTIONALITEIT>. Deze functionaliteit wordt geboden door de volgende webapplicatie:

• <NAAM VAN APPLICATIE>

Deze applicatie betreft <GEHEEL MAATWERK / EEN COMBINATIE VAN MAATWERK EN STANDAARD SOFTWARE / GEHEEL STANDARD PAKKET> en wordt onderhouden door < / NAAM SERVICE PROVIDER>.

Deze applicatie is extern benaderbaar via de volgende URL(s): en bevinden zich in een DMZ met ip-reeks <\_\_\_.\_\_\_.\_\_\_.\_\_\_-\_\_\_>. De infrastructuur waar deze applicaties op draaien wordt beheerd door < / NAAM SERVICE PROVIDER> in de vorm van <MANAGED SERVICES / FYSIEKE HOSTING / REMOTE SUPPORT / SAAS >.

Het object van onderzoek was de webomgeving van DigiD aansluiting (‘DigiD webomgeving’). Het onderzoek heeft zich gericht op de webapplicaties, de URLs waarmee deze kunnen worden benaderd, de infrastructuur (binnen de DMZ waar webapplicaties zich bevinden) en een aantal ondersteunende processen conform de “Norm ICT-beveiligingsassessments DigiD” van Logius. Het onderstaande schema toont de webomgeving die is onderzocht door middel van een infrastructurele test.



ORGANISATIE heeft een deel DigiD webomgeving uitbesteed aan . Als gevolg hiervan zijn er een aantal maatregelen belegd bij deze service organisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT auditor van deze service organisatie. De richtlijnen waar deze maatregelen betrekking op hebben zijn door ons dan ook niet onderzocht. Waar relevant geven wij, per richtlijn, specifieke verwijzingen naar het rapport van de service organisatie.

1. Bijlage C – Totaaloverzicht getoetste normen ICT-beveiligingsassessment DiGiD-aansluiting van [gebruikersorganisatie].

In deze bijlage brengen wij de oordelen samen, op basis van de diverse uitgevoerde werkzaamheden / uitgebrachte rapportages. Het doel van deze samenvatting is om Logius een totaaloverzicht te verschaffen over de resultaten vanuit de verschillende assessments t.a.v. de DigiD-aansluiting en .

Volgens de NOREA-handreiking inzake de DigiD-assessments moeten de volgende normen bij de gebruikersorganisatie worden getoetst: B.05, U/TV.01, U/WA.02, U/WA.05. en C.08.

Als input voor de hierna vermelde samenvatting hebben wij, naast de voorliggende rapportage, gebruik gemaakt van de rapportage van [TPM-rapportage van de serviceorganisatie, referentie/rapportnummer, afgiftedatum] ondertekend door [naam RE].

Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de rapportage van [TPM-rapportage van de serviceorganisatie, referentie/rapportnummer, datum]. Wij kunnen dan ook geen verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

| Nr | Beschrijving van de norm | Getoetst bij leverancier | Referentie /rapportnummer | Aanvullende beheersmaatregelen gebruikersorganisatie[[1]](#footnote-1) | Getoetst bij gebruikers-organisatie | Referentie /rapportnummer |
| --- | --- | --- | --- | --- | --- | --- |
| 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 / Voldoet niet |  | Ja / Nee | Voldoet / Voldoet niet |  |
| 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. |  |  |  |  |  |
| U/WA.02 | Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. |  |  |  |  |  |
| U/WA.03 | De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt. |  |  |  |  |  |
| U/WA.04 | De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren. |  |  |  |  |  |
| U/WA.05 | De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken. |  |  |  |  |  |
| U/PW.02 | De webserver garandeert specifieke kenmerken van de inhoud van de protocollen. |  |  |  |  |  |
| U/PW.03 | De webserver is ingericht volgens een configuratie-baseline. |  |  |  |  |  |
| 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. |  |  |  |  |  |
| U/PW.07 | Voor het configureren van platformen een hardeningsrichtlijn beschikbaar. |  |  |  |  |  |
| 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. |  |  |  |  |  |
| U/NW.04 | De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen. |  |  |  |  |  |
| U/NW.05 | Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd. |  |  |  |  |  |
| U/NW.06 | Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar. |  |  |  |  |  |
| C.03 | Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope). |  |  |  |  |  |
| C.04 | Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope). |  |  |  |  |  |
| C.06 | In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. |  |  |  |  |  |
| 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. |  |  |  |  |  |
| C.08 | Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd. |  |  |  |  |  |
| C.09 | Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen. |  |  |  |  |  |

1. naar het oordeel van de auditor van de serviceorganisatie [↑](#footnote-ref-1)