**Rapportage-template DigiD-Assessment**

|  |  |
| --- | --- |
| Aan : | Management DIENSTVERLENER (VOORHEEN AANSLUITHOUDER) en Logius |
| Datum : | RAPPORTDATUM |
| Van : | AUDITOR  KENMERK |
| Aansluiting : | AANSLUITNUMMER  AANSLUITNAAM  DIENSTVERLENER (VOORHEEN AANSLUITHOUDER) |

Inhoudsopgave

1 Assurance-rapport van de onafhankelijke auditor 2

1.1 Onze oordelen <met beperking> 2

1.2 De basis voor onze oordelen <met beperking> 4

1.3 Van toepassing zijnde criteria 5

1.4 Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek 5

1.5 Beoogde gebruikers en doel 8

1.6 Verantwoordelijkheden van de DigiD dienstverlener 8

1.7 Verantwoordelijkheden van de IT-auditor 8

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

B Bijlage B – Object van onderzoek 14

C Bijlage C – Totaaloverzicht getoetste normen ICT-beveiligingsassessment DigiD-aansluiting van [gebruikersorganisatie]. 16

D Bijlage D - Totaaloverzicht ICT-beveiligingsassessment DigiD 22

# Assurance-rapport van de onafhankelijke IT-auditor

|  |  |
| --- | --- |
| Aan : | Management DIENSTVERLENER (VOORHEEN AANSLUITHOUDER) en Logius |
| Datum : | RAPPORTDATUM |
| Van : | AUDITOR  KENMERK |
| Aansluiting : | AANSLUITNUMMER  AANSLUITNAAM  DIENSTVERLENER (VOORHEEN AANSLUITHOUDER) |

Aan: Bestuur <dienstverlener (voorheen houderorganisatie)>

## Onze oordelen

Wij hebben een DigiD-beveiligingsassessment met redelijke mate van zekerheid uitgevoerd op de webomgeving van DigiD-aansluiting AANSLUITNUMMER en AANSLUITNAAM van DIENSTVERLENER (hierna: 'de DigiD Dienstverlener).

Per beveiligingsrichtlijn hebben wij hieronder vermeld of wordt voldaan aan de beveiligingsrichtlijn. Om de leesbaarheid van dit rapport te vergroten zijn de oordelen in deze tabel weergegeven als “voldoet” of “voldoet niet”. Hierbij moet “voldoet” ingeval het oordeel is beperkt tot opzet en bestaan worden geïnterpreteerd als “Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn effectief is opgezet en geïmplementeerd op (OORDEELSDATUM)”. “Voldoet niet” moet ingeval het oordeel is beperkt tot opzet en bestaan worden geïnterpreteerd als “Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn niet in alle materiële opzichten effectief zijn opgezet en/of geïmplementeerd op (OORDEELSDATUM)”.

Bij beveiligingsrichtlijnen waarbij ook de effectieve werking wordt vastgesteld moet “voldoet” worden geïnterpreteerd als “Wij zijn van oordeel dat de getoetste interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn effectief werkten tijdens de controleperiode van [BEGINDATUM] tot [EINDDATUM]”. “Voldoet niet” moet vervolgens worden geïnterpreteerd als “Wij zijn van oordeel dat de getoetste interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn niet in alle materiële opzichten effectief werkten tijdens de controleperiode van [BEGINDATUM] tot [EINDDATUM]”.

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 assurance-rapport zijn uiteengezet.

Instructie voor de auditor: Neem in de onderstaande tabel alleen de normen op die een (deel)verantwoordelijkheid zijn van de dienstverlener en zelf zijn getoetst. Verwijder de overige rijen, óf geef dit per rij aan met ‘n.v.t’ in de beide cellen met oordeel.

Instructie voor de auditor: Indien van toepassing Per oordeel een verwijzing opnemen naar de corresponderende tekst in paragraaf 1.2. Dit betreft elke opmerking t.o.v. een 'voldoet' oordeel in opzet en/of bestaan en/of werking. Bij meerdere opmerkingen dit doorlopend nummeren [1] [2] [etc.].

| Nr | Beschrijving van de beveiligingsrichtlijn | Oordeel opzet en bestaan | Oordeel werking |
| --- | --- | --- | --- |
| B.01 | De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatie gerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer. | Voldoet / Voldoet niet | 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 / Voldoet niet/ Voldoet in opzet [1] | N.v.t. |
| 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 niet/ Voldoet in opzet [1] | Voldoet / Voldoet niet / Geen oordeel [2] |
| U/WA.02 | Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. | Voldoet / Voldoet niet/ Voldoet in opzet [1] | Voldoet / Voldoet niet/ Geen oordeel [2] |
| U/WA.03 | De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt. | Voldoet / Voldoet niet | N.v.t. |
| U/WA.04 | De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren. | Voldoet / Voldoet niet | N.v.t. |
| U/WA.05 | De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacy bevorderende en cryptografische technieken. | Voldoet / Voldoet niet | N.v.t. |
| U/PW.02 | De webserver garandeert specifieke kenmerken van de inhoud van de protocollen. | Voldoet / Voldoet niet | N.v.t. |
| U/PW.03 | De webserver is ingericht volgens een configuratie-baseline. | Voldoet / Voldoet niet | 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 / Voldoet niet | N.v.t. |
| U/PW.07 | Voor het configureren van platformen een hardeningsrichtlijn beschikbaar. | Voldoet / Voldoet niet | 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 / Voldoet niet | N.v.t. |
| U/NW.04 | De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen. | Voldoet / Voldoet niet | N.v.t. |
| U/NW.05 | Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd. | Voldoet / Voldoet niet | N.v.t. |
| U/NW.06 | Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar. | Voldoet / Voldoet niet | N.v.t. |
| C.03 | Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope). | Voldoet / Voldoet niet | N.v.t. |
| C.04 | Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope). | Voldoet / Voldoet niet | N.v.t. |
| C.06 | In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. | Voldoet / Voldoet niet | 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 niet | Voldoet / Voldoet niet |
| 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 niet/ Voldoet in opzet [1] | Voldoet / Voldoet niet/ Geen oordeel [2] |
| 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 niet [3] | Voldoet / Voldoet niet |

## De basis voor onze oordelen

Instructie voor de auditor: voor elke norm ‘voldoet niet’ of bij beperking in oordeel of geen oordeel, expliciet aangeven per norm of de afwijking betreft een afwijking in opzet, bestaan en/of werking, en de reden daarvan (wat heeft auditor niet kunnen vaststellen)

[1] Bestaan - Non-occurrence - voldoet in opzet. Voor beveiligingsrichtlijn XXX hebben wij vastgesteld dat NAAM SERVICEORGANISATIE maatregelen heeft ontworpen met betrekking tot deze norm. Vanwege het feit dat zich geen situatie heeft voorgedaan waarop deze maatregel betrekking heeft, hebben wij het bestaan niet kunnen vaststellen. Hierdoor zijn wij van oordeel dat de organisatie niet voldoet aan deze norm.

[xx] Herhaling bij meerdere beperkingen in oordelen

[2] Werking – non-occurrence - geen oordeel. Voor beveiligingsrichtlijn < vul in U/TV.01, U/WA.02, en/of C.08> hebben wij vastgesteld dat de organisatie maatregelen heeft ontworpen (opzet). Wij zijn van oordeel dat de organisatie in opzet (**of**: opzet en bestaan) voldoet aan deze norm. Vanwege non-occurrence kan de effectieve werking niet worden vastgesteld en daarom geven wij daarover geen oordeel.

Instructie voor de auditor: passage bij beperkingen bij C.09:

[3] Afwijkend patch niveau. Bij C.09 is niet voldaan aan de norm. Het oordeel bij C.09 is daarom "voldoet niet". Wij merken op dat <AANTAL> van de componenten van de applicatie niet beschikt over de laatste ondersteunde security patch, waarbij naar het oordeel van de auditor de kwetsbaarheden afdoende zijn beperkt en de organisatie een ter zake doend verbeterplan heeft opgesteld. Alle andere componenten zijn wel voorzien van de laatste ondersteunde security patch. Voor nadere informatie kan Logius zich wenden tot de auditor.

[xx] Herhaling bij meerdere afwijkingen op beveiligingsrichtlijnen

[4] Verschil in getoetste beveiligingsrichtlijnen. Op basis van onze onderzoeksresultaten zijn wij tot de conclusie gekomen dat, in afwijking van hetgeen is vermeld in hoofdstuk 2 (verantwoordelijkheden dienstverlener) van de assurance-rapportage van <serviceorganisatie>, kenmerk rapport <rapport kenmerk>, de norm(en) <Norm x>, <Norm y, enz > wel/niet van toepassing zijn voor de dienstverlener. Wij hebben deze normen derhalve wel/niet getoetst in het kader van dit DigiD assessment.

[xx] Herhaling bij meerdere afwijkingen op beveiligingsrichtlijnen

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 2025 (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 de DigiD Dienstverlener 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 <behalve die normen waarvoor wij geen oordeel konden geven>.

## 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 geselecteerd 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 geselecteerde 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 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;

• de interne beheersingsmaatregelen die verband houden met de beveiligingsrichtlijnen op afdoende wijze zijn opgezet en daadwerkelijk zijn geïmplementeerd;

• de interne beheersingsmaatregelen die verband houden met een selectie van specifieke beveiligingsrichtlijnen gedurende de controleperiode effectief hebben gewerkt.

## Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek

### Object van onderzoek

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

DIENSTVERLENER biedt de volgende functionaliteit aan waarvoor DigiD aansluiting AANSLUITNUMMER en AANSLUITNAAM ter authenticatie wordt gebruikt: <HIGH LEVEL OPSOMMING VAN AANGEBODEN FUNCTIONALITEIT>.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

* <NAAM VAN DE APPLICATIE> versienummer applicatie
* De URL waarop de webapplicatie te bereiken is, betreft: URL applicatie

Deze applicatie betreft <GEHEEL MAATWERK / EEN COMBINATIE VAN MAATWERK EN STANDAARD SOFTWARE / GEHEEL STANDAARD PAKKET>.

Instructie voor de auditor: onderstaande alinea opnemen ingeval gebruik gemaakt wordt van een identity broker

Voor het verifiëren van de identiteit van de gebruiker maakt de DigiD dienstverlener gebruik van de NAAM DIENSTVERLENING van NAAM SERVICEORGANISATIE A.

Instructie voor de auditor: onderstaande alinea opnemen ingeval van hosting

Voor de infrastructuur maakt de DigiD dienstverlener gebruik van NAAM DIENSTVERLENING van NAAM SERVICEORGANISATIE-A. Voor het beheer van deze infrastructuur wordt (mede) gebruik gemaakt van de diensten van NAAM SERVICEORGANISATIE-B OF SUBSERVICEORGANISATIE-C.

Instructie voor de auditor: onderstaande alinea opnemen ingeval van PAAS of IAAS

De DigiD dienstverlener maakt gebruik van de PLATFORM AS A SERVICE/INFRASTRUCTURE AS A SERVICE diensten van:

NAAM SUBSERVICEORGANISATIE-D – NAAM DIENSTVERLENING

Aanvullende assurance waarop wordt ‘gesteund’ is ontleend aan: [TYPE RAPPORT, RAPPORTDATUM, KENMERK, AUDITORGANISATIE, EVT NAAM IT AUDITOR, ONDERZOEKSPERIODE + EVENTUELE BRIDGE LETTER(S) ZODAT DE PERIODES AANSLUITEN). Zie bijlage C en D.

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, 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.

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

### Service organisatie(s)

Instructie voor de auditor:

Indien geen gebruik wordt gemaakt van serviceorganisaties, vermeld hier dan: de dienstverlener maakt geen gebruik van de diensten van (een) serviceorganisatie.

optionele passages bij serviceorganisatie(s):

De DigiD dienstverlener maakt gebruik van SERVICEORGANISATIE-A voor <de aard van de activiteiten die door de serviceorganisatie worden uitgevoerd>. De DigiD dienstverlener 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 dienstverlener 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. 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.

De DigiD dienstverlener maakt gebruik van SERVICEORGANISATIE-A voor <de aard van de activiteiten die door de serviceorganisatie worden uitgevoerd>. De DigiD dienstverlener maakt voor het verschaffen van zekerheid over haar volledige webomgeving zoals beschreven onder het object van onderzoek gebruik van de opname methode (‘inclusive methode’). De beschrijving van de dienstverlener van haar systeem omvat daarmee de interne beheersingsdoelstellingen en daarmee verband houdende interne beheersingsmaatregelen van de serviceorganisatie. Onze werkzaamheden strekken zich dan ook uit tot de interne beheersingsmaatregelen van de serviceorganisatie.

### Norm ICT-beveiligingsassessments DigiD

Het 'Normenkader 3.0 voor ICT-beveiligingsassessments DigiD' bevat 21 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 de DigiD dienstverlener om in aanvulling op de richtlijnen in de vigerende ‘Norm ICT-beveiligingsassessments DigiD’, ook de andere richtlijnen uit de ‘ICT-beveiligingsrichtlijnen voor webapplicaties versie 2015’ 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.

### Beperkingen met betrekking tot interne beheersingsmaatregelen

Interne beheersingsmaatregelen 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 beheersingsmaatregelen 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 beheersingsmaatregelen om de doelstellingen te bereiken, onderhevig aan het risico dat interne beheersingsmaatregelen ineffectief kunnen worden.

Ons oordeel is niet aangepast als gevolg van deze aangelegenheden.

## Beoogde gebruikers en doel

Ons assurance-rapport is uitsluitend bestemd voor de DigiD dienstverlener 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 de DigiD dienstverlener.

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).

Instructie voor de auditor: onderstaande alinea opnemen ingeval het onderzoek volledig volgens de 'inclusive methode' is uitgevoerd:

Dit rapport bevat geen bijlage C, aangezien geen gebruik is gemaakt van rapporten inzake serviceorganisatie(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 serviceorganisatie(s).

Ons assurance-rapport en bijlagen mogen enkel worden gebruikt door de beoogde gebruikers en/ of verspreidingskring voor het doel waarvoor deze zijn opgesteld en dient niet te worden verspreid aan of te worden gebruikt door anderen.

## Verantwoordelijkheden van de DigiD dienstverlener

Het bestuur van de DigiD dienstverlener 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 beheersingsmaatregelen om te voldoen aan de vigerende norm ‘Normenkader 3.0 voor ICT-beveiligingsassessments DigiD '.

## Verantwoordelijkheden 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 het door ons af te geven oordelen over de opzet en implementatie van interne beheersingsmaatregelen 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 beheersingsmaatregelen 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.

PLAATS, RAPPORTDATUM

<EUTL HANDTEKENING>

AUDITOR

1. Bijlage A - Beschrijving van de testresultaten van de auditor

Per beveiligingsrichtlijn hebben wij hieronder vermeld of wordt voldaan aan de beveiligingsrichtlijn. Om de leesbaarheid van dit rapport te vergroten zijn de oordelen in deze tabel weergegeven als “voldoet” of “voldoet niet”. Hierbij moet “voldoet” ingeval het oordeel is beperkt tot opzet en bestaan worden geïnterpreteerd als “Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn effectief is opgezet en geïmplementeerd op (OORDEELSDATUM)”. “Voldoet niet” moet ingeval het oordeel is beperkt tot opzet en bestaan worden geïnterpreteerd als “Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn niet in alle materiële opzichten effectief zijn opgezet en/of geïmplementeerd op (OORDEELSDATUM)”.

Bij beveiligingsrichtlijnen waarbij ook de effectieve werking wordt vastgesteld moet “voldoet” worden geïnterpreteerd als “Wij zijn van oordeel dat de getoetste interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn effectief werkten tijdens de controleperiode van [BEGINDATUM] tot [EINDDATUM]”. “Voldoet niet” moet vervolgens worden geïnterpreteerd als “Wij zijn van oordeel dat de getoetste interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn niet in alle materiële opzichten effectief werkten tijdens de controleperiode van [BEGINDATUM] tot [EINDDATUM]”.

Instructie voor de auditor:

* Eventuele voetnoten hier terug laten komen in overeenstemming met paragraaf 1.1

| Nr | Beschrijving van de beveiligingsrichtlijn | Korte beschrijving van de uitgevoerde werkzaamheden | Oordeel en eventuele aanbevelingen |
| --- | --- | --- | --- |
| B.01 | De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatie gerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer. |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  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. |  | **Opzet en bestaan**  Voldoet / Voldoet niet / Voldoet in opzet [1]  **Werking**  N.v.t. |
| 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 en bestaan**  Voldoet / Voldoet niet / Voldoet in opzet [1]  **Werking**  Voldoet / Voldoet niet / Geen oordeel [2] |
| U/WA.02 | Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. |  | **Opzet en bestaan**  Voldoet / Voldoet niet / Voldoet in opzet [1]  **Werking**  Voldoet / Voldoet niet / Geen oordeel [2] |
| U/WA.03 | De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt. |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  N.v.t. |
| U/WA.04 | De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren. |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  N.v.t. |
| U/WA.05 | De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken. |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  N.v.t. |
| U/PW.02 | De webserver garandeert specifieke kenmerken van de inhoud van de protocollen. |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  N.v.t. |
| U/PW.03 | De webserver is ingericht volgens een configuratie-baseline. |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  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. |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  N.v.t. |
| U/PW.07 | Voor het configureren van platformen een hardeningrichtlijn beschikbaar. |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  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. |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  N.v.t. |
| U/NW.04 | De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen. |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  N.v.t. |
| U/NW.05 | Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd. |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  N.v.t. |
| U/NW.06 | Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar. |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  N.v.t. |
| C.03 | Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope). |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  N.v.t. |
| C.04 | Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope). |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  N.v.t. |
| C.06 | In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  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. |  | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  Voldoet / Voldoet niet |
| C.08 | Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd. |  | **Opzet en bestaan**  Voldoet / Voldoet niet / Voldoet in opzet [1]  **Werking**  Voldoet / Voldoet niet |
| C.09 | Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen. |  | **Opzet en bestaan**  Voldoet / Voldoet niet / Voldoet niet [3]  **Werking**  Voldoet / Voldoet niet |

1. Bijlage B – Object van onderzoek

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

DIENSTVERLENER biedt de volgende functionaliteit aan waarvoor DigiD aansluiting AANSLUITNUMMER en AANSLUITNAAM ter authenticatie wordt gebruikt: <HIGH LEVEL OPSOMMING VAN AANGEBODEN FUNCTIONALITEIT>.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

<NAAM VAN DE APPLICATIE> versienummer applicatie

De URL waarop de webapplicatie te bereiken is, betreft: URL applicatie

Deze applicatie betreft <GEHEEL MAATWERK / EEN COMBINATIE VAN MAATWERK EN STANDAARD SOFTWARE / GEHEEL STANDAARD PAKKET>.

Instructie voor de auditor: onderstaande alinea opnemen ingeval gebruik gemaakt wordt van een identity broker

Voor het verifiëren van de identiteit van de gebruiker maakt de DigiD dienstverlener gebruik van de NAAM DIENSTVERLENING van NAAM SERVICEORGANISATIE A.

Instructie voor de auditor: onderstaande alinea opnemen ingeval van hosting

Voor de infrastructuur maakt de DigiD dienstverlener gebruik van NAAM DIENSTVERLENING van NAAM SERVICEORGANISATIE-A. Voor het beheer van deze infrastructuur wordt (mede) gebruik gemaakt van de diensten van NAAM SERVICEORGANISATIE-B OF SUBSERVICEORGANISATIE-C.

Instructie voor de auditor: onderstaande alinea opnemen ingeval van PAAS of IAAS

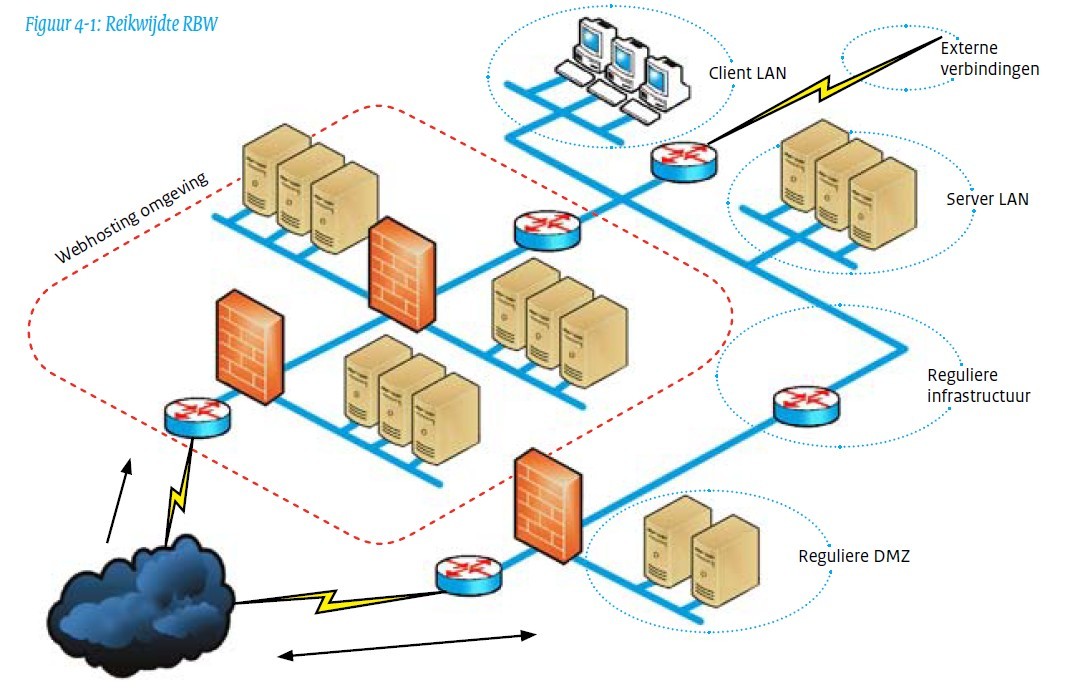
De DigiD dienstverlener maakt gebruik van de PLATFORM AS A SERVICE/INFRASTRUCTURE AS A SERVICE diensten van:

NAAM SUBSERVICEORGANISATIE-D – NAAM DIENSTVERLENING

Aanvullende assurance waarop wordt ‘gesteund’ is ontleend aan: [TYPE RAPPORT, RAPPORTDATUM, KENMERK, AUDITORGANISATIE, EVT NAAM IT AUDITOR, ONDERZOEKSPERIODE + EVENTUELE BRIDGE LETTER(S) ZODAT DE PERIODES AANSLUITEN).

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, 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.

Instructie voor de auditor: vervangen door een specifiek voor de serviceorganisatie schema inclusief systemen, protocollen etc.



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

INSTRUCTIE: Alleen als gebruik wordt gemaakt van een carve-out: Deze bijlage richt zich op het ten dienste van Logius inzichtelijk maken van de wijze waarop NAAM DIENSTVERLENER gebruik heeft gemaakt van serviceorganisaties die betrekking hebben op het object van onderzoek van DigiD-aansluiting AANSLUITNUMMER en AANSLUITNAAM.

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

| Omschrijving assurance-rapportage | (Sub)Serviceorganisatie | Bij serviceorganisatie getoetste beveiligingsrichtlijnen | Referentie /  Rapportnummer/ controleperiode | Oordeelsdatum | Ondertekend door naam auditor/ auditeenheid |
| --- | --- | --- | --- | --- | --- |
| DigiD assurance-rapportage/  ISAE 3402/ SOC1 assurance-rapportage/  ISAE 3000/ SOC2 assurance-rapportage/  ISAE 3000 assurance-rapportage | [Naam] Serviceorganisatie  Serviceorganisatie voor webapplicatie/ managed services/ fysieke hosting/ remote support/ SaaS/ identity broker |  | Referentie/ rapportnummer/ controleperiode | Oordeelsdatum |  |
|  | [Naam] Subserviceorganisatie 1  Subserviceorganisatie voor webapplicatie/ managed services/ fysieke hosting/ remote support/ SaaS/ identity broker |  | Referentie/ rapportnummer/ controleperiode |  |  |
|  |  |  |  |  |  |

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.

Wij hebben kennis genomen van de genoemde assurance-rapportage(s) en hebben te behoeve van Logius in onderstaande tabel per beveiligingsrichtlijn aangegeven tot welk oordeel de service auditor is gekomen en of in die rapportages sprake is van aanvullende beheersmaatregelen gebruikersorganisatie (de user entity controls) en of wij deze dan ook hebben getoetst bij de houderorganisatie (gebruikersorganisatie).

Instructie voor de auditor:

* Eventuele voetnoten hier terug laten komen in overeenstemming met paragraaf 1.1
* Default nee invullen

| Nr | Beschrijving van de norm | Getoetst in opdracht van [serviceorganisatie 1]  [rapportkenmerk], [rapportdatum], [i.v.t versienummer]  (inclusief hierbij inclusive getoetste organisaties) | Getoetst in opdracht van [serviceorganisatie 2]  [rapportkenmerk], [rapportdatum], [i.v.t versienummer]  (inclusief hierbij inclusive getoetste organisaties) | Getoetst in opdracht van [NAAM DIENSTVERLENER]  (inclusief hierbij inclusive getoetste organisaties) |
| --- | --- | --- | --- | --- |
| B.01 | De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer. | **Opzet en bestaan**  Voldoet / Voldoet niet  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| 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. | **Opzet en bestaan**  Voldoet / Voldoet niet  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| 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 en bestaan**  Voldoet / Voldoet niet / Voldoet in opzet[1]  **Werking**  Voldoet / Voldoet niet / Geen oordeel [2]  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / Voldoet in opzet[1]  **Werking**  Voldoet / Voldoet niet / Geen oordeel [2]  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / Voldoet in opzet[1]  **Werking**  Voldoet / Voldoet niet / Geen oordeel [2]  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| U/WA.02 | Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. | **Opzet en bestaan**  Voldoet / Voldoet niet / Voldoet in opzet[1]  **Werking**  Voldoet / Voldoet niet / Geen oordeel [2]  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / Voldoet in opzet[1]  **Werking**  Voldoet / Voldoet niet / Geen oordeel [2]  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / Voldoet in opzet[1]  **Werking**  Voldoet / Voldoet niet / Geen oordeel [2]  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| U/WA.03 | De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt. | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| U/WA.04 | De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren. | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| U/WA.05 | De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken. | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| U/PW.02 | De webserver garandeert specifieke kenmerken van de inhoud van de protocollen. | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t |
| U/PW.03 | De webserver is ingericht volgens een configuratie-baseline. | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| 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. | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| U/PW.07 | Voor het configureren van platformen een hardeningsrichtlijn beschikbaar. | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| 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. | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t |
| U/NW.04 | De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen. | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t |
| U/NW.05 | Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd. | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| U/NW.06 | Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar. | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| C.03 | Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope). | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| C.04 | Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope). | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| C.06 | In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t | **Opzet en bestaan**  Voldoet / Voldoet niet / n.v.t | **Opzet en bestaan**  Voldoet / Voldoet niet / 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. | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  Voldoet / Voldoet niet  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  Voldoet / Voldoet niet  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet  **Werking**  Voldoet / Voldoet niet  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| C.08 | Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd. | **Opzet en bestaan**  Voldoet / Voldoet niet / Voldoet in opzet[1]  **Werking**  Voldoet / Voldoet niet / Geen oordeel [2]  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / Voldoet in opzet[1]  **Werking**  Voldoet / Voldoet niet / Geen oordeel [2]  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet / Voldoet in opzet[1]  **Werking**  Voldoet / Voldoet niet / Geen oordeel [2]  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |
| C.09 | Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen. | **Opzet en bestaan**  Voldoet / Voldoet niet [3]  **Werking**  Voldoet / Voldoet niet  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet [3]  **Werking**  Voldoet / Voldoet niet  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] | **Opzet en bestaan**  Voldoet / Voldoet niet [3]  **Werking**  Voldoet / Voldoet niet  [Verwijzing maatregel i.g.v ISAE/ SOC (mapping)] |

Bijlage D - Totaaloverzicht ICT-beveiligingsassessment DigiD

Hieronder treft u een verkort overzicht aan van de identificerende kenmerken en de gebruikte assessmentrapportage(s) die invulling geeft/ geven aan het uitgevoerde DigiD-beveiligingsassessment op de webomgeving van de hieronder vermelde DigiD-aansluiting.

|  |  |  |
| --- | --- | --- |
| **Aansluiting** | **Aansluitnummer:** | [AANSLUITNUMMER] |
| **Aansluitnaam:** | [AANSLUITNAAM] |
| **Dienstverlener:** | [DIENSTVERLENER] |
| **Auditor aansluithouder** | **Naam auditor:** |  |
| **Auditorganisatie:** | [NAAM AUDITORGANISATIE] |
| **Kenmerk rapport:** | [RAPPORTNUMMER] |
| **Object van onderzoek** | **Naam webapplicatie:** | [NAAM WEBAPPLICATIE] |
| **Versienummer:** | [VERSIENUMMER] |
| **Omschrijving:** | HIGH LEVEL OMSCHRIJVING VAN AANGEBODEN FUNCTIONALITEIT |
| **Serviceorganisatie A** | **SERVICEORGANISATIE :** | [SERVICEORGANISATIE A] (instructie voor de auditor: indien geen gebruik gemaakt wordt van een serviceorganisatie, hier invullen: *N.V.T., er wordt geen gebruik gemaakt van een serviceorganisatie*) |
| **AUDITOR SERVICEORGANISATIE-A:** |  |
| **KENMERK RAPPORT:** | [REF. SERV. AUDITOR] |
| **OORDEELSDATUM:** | (instructie voor de auditor: hier de controleperiode werking (van datum x t/m datum y) opnemen inclusief eventuele bridge letter |
| **(Sub)Serviceorganisatie B** | **(SUB)SERVICEORGANISATIE-B:** | [(SUB)SERVICEORGANISATIE B] (instructie voor de auditor: indien geen gebruik gemaakt wordt van een serviceorganisatie, hier invullen: *N.V.T., er wordt geen gebruik gemaakt van een (sub)serviceorganisatie*) |
| **AUDITOR (SUB)SERVICEORGANISATIE:** |  |
| **KENMERK RAPPORT:** | [REF. SERV. AUDITOR] |
| **OORDEELSDATUM:** | (instructie voor de auditor: hier de controleperiode werking (van datum x t/m datum y) opnemen inclusief eventuele bridge letter |
| **RAPPORTDATUM:** |  |