**Rapportage-template DigiD-Assessment Serviceorganisatie**

|  |  |
| --- | --- |
| Aan : | Management NAAM SERVICEORGANISATIE en Logius |
| Datum : | RAPPORTDATUM |
| Van : | AUDITORKENMERK |
| Aansluiting :  | AANSLUITNUMMERAANSLUITNAAMNAAM AANSLUITHOUDER |

Inhoudsopgave

1 Assurancerapport 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 4

1.4 Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek 5

1.5 Beoogde gebruikers en doel 7

1.6 Verantwoordelijkheden van NAAM SERVICEORGANISATIE 7

1.7 Verantwoordelijkheden van de IT-auditor 7

2 Verantwoordelijkheden gebruikersorganisatie 10

A Bijlage A - Beschrijving van de testresultaten van de auditor 12

B Bijlage B – Object van onderzoek 16

C Bijlage C – Overzicht onderverdeling getoetste normen ICT-beveiligingsassessment DigiD-omgeving van NAAM SERVICEORGANISATIE 18

D Bijlage D - Overzicht ICT-beveiligingsassessment DigiD NAAM SERVICEORGANISATIE 22

# Assurancerapport van de onafhankelijke auditor

|  |  |
| --- | --- |
| Aan : | NAAM SERVICEORGANISATIE |
| Datum : | RAPPORTDATUM |
| Van : | AUDITORKENMERK |
| Aansluiting :  | AANSLUITNUMMERAANSLUITNAAMNAAM AANSLUITHOUDER |

## Aan: Management <NAAM SERVICEORGANISATIE>

## Onze oordelen <met beperking>

Wij hebben een DigiD-beveiligingsassessment met redelijke mate van zekerheid uitgevoerd op de webomgeving van DigiD-aansluiting AANSLUITNUMMER en AANSLUITNAAM. Hier kan ook verwezen worden naar de lijst van namen van aansluithouders.

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 beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn effectief is opgezet en geïmplementeerd op OORDEELSDATUM”. “Voldoet niet” moet 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 is opgezet en/of geïmplementeerd op OORDEELSDATUM”.

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. Ons onderzoek was beperkt tot de beveiligingsrichtlijnen die de verantwoordelijkheid zijn van de serviceorganisatie.

Instructie voor de auditor: per beperking een verwijzing opnemen naar de corresponderende tekst in paragraaf 1.2. Dit betreft elke beperking t.o.v. volledig een 'voldoet' oordeel in opzet en bestaan. Bij meerdere beperkingen dit doorlopend nummeren [1] [2] [etc.].

| Nr | Beschrijving van de beveiligingsrichtlijn | Oordeel |
| --- | --- | --- |
| B.01 | De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer. | Voldoet / Voldoet niet [1] |
| 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. |  |
| 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 is 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 assessments (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. |  |

## De basis voor onze oordelen <met beperking>

Instructie voor de auditor: optionele passage bij beperkingen in oordelen bij een of meerdere beveiligingsrichtlijnen:

[1] Voor beveiligingsrichtlijn XXX hebben wij vastgesteld dat NAAM SERVICEORGANISATIE 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. Relevante audit evidence voor het bestaan van de betreffende beheersmaatregel is verzameld door een deelwaarneming te doen in een proces dat onderworpen is aan dezelfde control (i.c. dezelfde control owner, dezelfde tools, dezelfde registratie, dezelfde workflow, et cetera). Hierdoor zijn wij van oordeel dat de organisatie voldoet aan deze norm.

[xx] Herhaling bij meerdere beperkingen in oordelen

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

[xx] 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.

Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht, waaronder de NOREA Richtlijn 3000D ’Assurance-opdrachten door IT-auditors (Directe-opdrachten)’. 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 NAAM SERVICEORGANISATIE 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 <met beperking>.

## Van toepassing zijnde criteria

Voor deze opdracht heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de richtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact hebben op de veiligheid van DigiD-webapplicaties en heeft deze vermeld in ‘Norm ICT-beveiligingsassessments DigiD’ welk wij hebben gehanteerd bij dit onderzoek.

De criteria waarvan gebruik wordt gemaakt bij het uitvoeren van de assurance-opdracht houden 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.

## 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. Hier kan ook verwezen worden naar de lijst van houders van DigiD aansluitingen.

NAAM SERVICEORGANISATIE 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 APPLICATIE> versienummer applicatie

Deze applicatie(s) betreft/betreffen GEHEEL MAATWERK / EEN COMBINATIE VAN MAATWERK EN STANDAARD SOFTWARE / GEHEEL STANDARD PAKKET en worden onderhouden door NAAM SERVICEORGANISATIE/ NAAM SUBSERVICEORGANISATIE-A.

De infrastructuur waarop de applicaties draaien wordt beheerd door NAAM SERVICEORGANISATIE.

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

De NAAM SERVICEORGANISATIE maakt gebruik van de PLATFORM AS A SERVICE/INFRASTRUCTURE AS A SERVICE diensten van:

NAAM SUBSERVICEORGANISATIE-A – NAAM DIENSTVERLENING

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

INDIEN IDENTITY BROKER Voor het verifiëren van de identiteit van de gebruiker maakt NAAM SERVICEORGANISATIE in haar dienstverlening gebruik van NAAM DIENSTVERLENING van NAAM SUBSERVICEORGANISATIE-B.

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.

### Subserviceorganisatie(s)

Instructie voor de auditor:

Indien geen gebruik wordt gemaakt van subserviceorganisaties, vermeldt hier dan: de serviceorganisatie maakt geen gebruik van de diensten van een sub-serviceorganisatie.

optionele passages bij subservice-organisatie(s):

NAAM SERVICEORGANISATIE maakt gebruik van subserviceorganisatie NAAM SUBSERVICEORGANISATIE voor <de aard van de activiteiten die door de subserviceorganisatie worden uitgevoerd>. NAAM SERVICEORGANISATIE maakt voor 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 beheersingsmaatregelen van de subserviceorganisatie uit. Onze werkzaamheden strekken zich dan ook niet uit tot de interne beheersingsmaatregelen 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.

NAAM SERVICEORGANISATIE maakt gebruik van serviceorganisatie NAAM SUBSERVICEORGANISATIE voor <de aard van de activiteiten die door de serviceorganisatie worden uitgevoerd>. NAAM SERVICEORGANISATIE maakt voor 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 beheersingsmaatregelen van de subserviceorganisatie. Onze werkzaamheden strekken zich dan ook uit tot de interne beheersingsmaatregelen van de subserviceorganisatie.

### Norm ICT-beveiligingsassessment DigiD

De ‘Norm ICT-beveiligingsassessments DigiD 3.0’ 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.

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 NAAM SERVICEORGANISATIE 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.

### 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.

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.

Bovendien is het projecteren naar de toekomst van onze oordelen met betrekking tot de opzet en implementatie van interne beheersingsmaatregelen om de richtlijnen 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 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 NAAM SERVICEORGANISATIE.

Instructie voor de auditor. Alleen indien er gebruik is gemaakt van een (of meerdere) subserviceorganisatie(s). Indien dit niet het geval is kunnen bijlage C en D vervallen.

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).

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 subserviceorganisatie(s).

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

Ons assurance-rapport en 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.

## Verantwoordelijkheden van NAAM SERVICEORGANISATIE

Het bestuur van NAAM SERVICEORGANISATIE 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 ICT-beveiligingsassessments DigiD 3.0’.

## 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 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 en bestaan 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 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 evalueren van de uitkomsten van onze werkzaamheden.

PLAATS, RAPPORTDATUM

<EUTL HANDTEKENING>

AUDITOR

# Verantwoordelijkheden gebruikersorganisatie

Bij de opzet en implementatie van interne beheersingsmaatregelen bij de serviceorganisatie neemt deze voor een aantal beveiligingsrichtlijnen van de ‘Norm ICT-beveiligingsassessments DigiD’ aan, dat enkele interne beheersingsmaatregelen door de houderorganisaties zullen worden geïmplementeerd om te voldoen aan deze beveiligingsrichtlijnen.

In de onderstaande tabel wordt aangegeven voor welke beveiligingsrichtlijn(en) deze aanname is gedaan en welke gewenste interne beheersingsactiviteit bij de gebruikersorganisaties kunnen worden geïmplementeerd om te voldoen aan de desbetreffende beveiligingsrichtlijn van de 'Norm ICT-beveiligingsassessments DigiD' van Logius.

De geschiktheid van de opzet en het bestaan van deze aanvullende interne beheersingsmaatregelen van een gebruikersorganisatie hebben wij niet geëvalueerd. Aan de beveiligingsrichtlijnen van de ‘Norm ICT-beveiligingsassessments DigiD’ wordt alleen voldaan, indien aanvullende interne beheersingsmaatregelen van een gebruikersorganisatie samen met de interne beheersingsmaatregelen van de serviceorganisatie op afdoende wijze zijn opgezet en geïmplementeerd.

Instructie voor de auditor: afhankelijk van de risico’s en de aard van de dienstverlening kan het voorkomen dat de gebruikersorganisatie meer of minder beheersingsmaatregelen zou moeten nemen waardoor een afwijkende lijst (User Control Considerations) wordt aangegeven. Motiveer dit in voor de aansluithouder herkenbare termen.

| Nr | Beschrijving van de beveiligingsrichtlijn | Gewenste interne beheersingsmaatregelen van de gebruikersorganisatie |
| --- | --- | --- |
| B.01 | De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer. |  |
| 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. |  |
| 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.05 | De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken. |  |
| U/NW.06 | Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar. |  |
| C.08 | Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd. |  |

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

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 oordelen 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 effectief is opgezet en geïmplementeerd op OORDEELSDATUM”. “Voldoet niet” moet 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 is opgezet en/of geïmplementeerd op OORDEELSDATUM”.

De uitspraak voldoet of voldoet niet beperkt zich tot de eigen oordeelsvorming van de auditor.

Instructie voor de auditor optioneel op te nemen met hanteren van identieke nummering [1] etc. zoals opgenomen in hoofdstuk 1 :

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.01 | De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangs-voorziening en kwetsbaarheden-beheer. |  | Voldoet / Voldoet niet |
| 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. |  |  |
| 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 is 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 assessments (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 AANSLUITNUMMER en AANSLUITNAAM. Hier kan ook de lijst van aangesloten houders van DigiD worden opgenomen.

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

• <NAAM APPLICATIE> versienummer applicatie indien beschikbaar

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

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

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

INDIEN IDENTIY BROKER Voor het verifiëren van de identiteit van de gebruiker maakt NAAM SERVICEORGANISATIE in haar dienstverlening gebruik van de NAAM DIENSTVERLENING van NAAM SUBSERVICEORGANISATIE-B.

Het object van onderzoek was de webomgeving van DigiD aansluiting DIGID KOPPELING (‘DigiD webomgeving’). Het onderzoek heeft zich gericht op de webapplicatie, de URLs waarmee deze kan 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.

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



Instructie voor de auditor: indien de serviceorganisatie gebruik maakt van een subserviceorganisatie die ook een DigiD TPM heeft èn waarbij de carve-out methodiek wordt toegepast, het onderstaande opnemen:

NAAM SERVICEORGANISATIE heeft een deel DigiD webomgeving uitbesteed aan NAAM SUBSERVICEORGANISATIE. Als gevolg hiervan is een aantal maatregelen belegd bij deze subserviceorganisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT auditor van deze subserviceorganisatie. 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 subserviceorganisatie. In bijlage C is de onderverdeling van normen opgenomen.

1. Bijlage C –Overzicht onderverdeling getoetste normen ICT-beveiligingsassessment DigiD-omgeving van [serviceorganisatie].

Deze bijlage richt zich op het ten dienste van Logius inzichtelijk maken van de wijze waarop NAAM SERVICEORGANISATIE gebruik heeft gemaakt van subserviceorganisaties 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 assurancerapportage | Subserviceorganisatie  | Bij subserviceorganisatie getoetste beveiligingsrichtlijnen | Referentie /rapportnummer | Afgiftedatum | Ondertekend door naam RE |
| --- | --- | --- | --- | --- | --- |
| DigiD assurancerapportage/ ISAE 3402/ SOC1 assurancerapportage/ISAE 3000/ SOC2 assurancerapportage/ ISAE 3000 assurancerapportage | [Naam] Subserviceorganisatie 1 |  |  |  |  |
|  | [Naam] Subserviceorganisatie 2 |  |  |  |  |
|  |  |  |  |  |  |

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 m.b.t. de in die rapportage vermelde oordelen.

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

Instructie voor de auditor:

* Eventuele voetnoten hier terug laten komen
* Default nee invullen

| Nr | Beschrijving van de norm | Getoetst bij leverancier 1Referentie /rapportnr | Getoetst bij leverancier 2Referentie /rapportnr |
| --- | --- | --- | --- |
| B.01 | De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer. | Voldoet / Voldoet niet | Voldoet / Voldoet niet |
| 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 / 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. | Voldoet / Voldoet niet | Voldoet / Voldoet niet |
| U/WA.02 | Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. | Voldoet / Voldoet niet | Voldoet / Voldoet niet |
| 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 | Voldoet / Voldoet niet |
| U/WA.04 | De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren. | Voldoet / Voldoet niet | Voldoet / Voldoet niet |
| U/WA.05 | De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken. | Voldoet / Voldoet niet | Voldoet / Voldoet niet |
| U/PW.02 | De webserver garandeert specifieke kenmerken van de inhoud van de protocollen. | Voldoet / Voldoet niet | Voldoet / Voldoet niet |
| U/PW.03 | De webserver is ingericht volgens een configuratie-baseline. | Voldoet / Voldoet niet | Voldoet / Voldoet niet |
| 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 | Voldoet / Voldoet niet |
| U/PW.07 | Voor het configureren van platformen een hardeningsrichtlijn beschikbaar. | Voldoet / Voldoet niet | Voldoet / Voldoet niet |
| 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 | Voldoet / Voldoet niet |
| U/NW.04 | De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen. | Voldoet / Voldoet niet | Voldoet / Voldoet niet |
| U/NW.05 | Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd. | Voldoet / Voldoet niet | Voldoet / Voldoet niet |
| U/NW.06 | Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar. | Voldoet / Voldoet niet | Voldoet / Voldoet niet |
| C.03 | Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope). | Voldoet / Voldoet niet | Voldoet / Voldoet niet |
| C.04 | Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope). | Voldoet / Voldoet niet | Voldoet / Voldoet niet |
| C.06 | In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. | Voldoet / Voldoet niet | Voldoet / Voldoet niet |
| 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 / 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. | Voldoet / Voldoet niet | Voldoet / Voldoet niet |

Bijlage D - Overzicht ICT-beveiligingsassessment DigiD NAAM SERVICEORGANISATIE

Hieronder treft u een verkort overzicht aan van de identificerende kenmerken en de gebruikte assessmentrapportage(s) van subserviceorganisatie(s) die invulling geeft/ geven aan het uitgevoerde DigiD-beveiligingsassessment bij NAAM SERVICEORGANISATIE.

|  |  |  |
| --- | --- | --- |
| **Aansluiting** | **Aansluitnummer:**  | [AANSLUITNUMMER] |
| **Aansluitnaam:** | [AANSLUITNAAM] |
| **Aansluithouder:**  | [AANSLUITHOUDER] |
| **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-A :** | [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:** |  |
| **RAPPORTDATUM:** |  |
| **(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-B:** |  |
| **KENMERK RAPPORT:** | [REF. SERV. AUDITOR] |
| **OORDEELSDATUM:** |  |
| **RAPPORTDATUM:** |  |