NOREA Handreiking ICT-beveiligingsassessment DigiD 3.0

Versie 1.0 – Definitief

25 oktober 2022

Verantwoording

Deze handreiking is uitgegeven door NOREA, de beroepsorganisatie van IT-auditors in Nederland, en is ontwikkeld om Nederlandse gekwalificeerde IT-auditors (Register IT-auditors, RE's) handvatten te bieden om een assurancerapport op te stellen in lijn met de regelgeving rondom het ICT-beveiligingsassessment DigiD.

Postbus 7984, 1008 AD Amsterdam

telefoon: 020-3010380

e-mail: norea@norea.nl www.norea.nl

Versiebeheer		
Versie	**Datum**	**Wijzigingen**
0.1 - 0.9.1	september-oktober 2022	Werkversies
0.99	18 oktober 2022	Initiële versie voor consultatie binnen werkgroep
1.0	**25 oktober 2022**	**Definitieve versie**

Inhoud

1 Inleiding

1.1 Doel handreiking

Doelstelling van deze handreiking is om de IT-auditor relevante informatie te verstrekken en een uniform toetsbaar normenkader te bieden voor het zorgvuldig uitvoeren van een ICT-beveiligingsassessment DigiD (*hierna: DigiD-assessment*). De handreiking geeft de bandbreedte aan waarbinnen de IT-auditor de werkzaamheden verricht. Hiermee wordt voorkomen dat er grote verschillen ontstaan in de scope en mate van diepgang bij uitvoering van de audits en het beoordelen van afwijkingen. Waar mogelijk/ wenselijk wordt ook duidelijk gemaakt wat gedaan zou moeten worden om tot een redelijke mate van zekerheid te komen. Het blijft echter de professionele verantwoordelijkheid van de IT-auditor om op basis van een deugdelijke grondslag tot een oordeel te komen per norm. Richtlijn 3000D van NOREA is daarbij leidend.

De voorliggende versie 3.0 betreft een volledige update van versie 2.0 d.d. uit 2016. In versie 3.0 zijn alle sindsdien uitgebrachte updates en richtlijnen opgenomen. De Frequently Asked Questions (FAQ) is en blijft het mechanisme om IT-auditors tussentijds van belangrijke wijzigingen of aandachtspunten op de hoogte te stellen. Tot en met FAQ versie 1.4 d.d. 8 november 2021 zijn de Frequenly Asked Questions in deze handreiking verwerkt.

Voor deze handreiking en de bijbehorende normenkaders geldt dat de beschreven auditwerkzaamheden voor een belangrijk deel zijn gebaseerd op de richtlijnen van Logius[1].

1.2 Achtergrond en doelstelling DigiD-assessment

De aanleiding voor het uitvoeren van de ICT-beveiligingsassessments bij organisaties die gebruik maken van DigiD is de brief van de minister van BZK aan de Tweede Kamer 'Lekken in een aantal gemeentelijke websites' d.d. 11

[1]. Het ministerie van BZK stelt het DigiD normenkader vast. Logius is door de Minister van Binnenlandse Zaken aangewezen als toezichthouder. Logius houdt toezicht op de naleving van de assessmentplicht en beoordeelt de IT-auditrapportage (assessment-rapportage).

oktober 2011 met kenmerk 2011-2000454268. De minister van BZK zegt hier onder punt 3 toe dat '… alle DigiD gebruikende organisaties … hun ICT-beveiliging getoetst dienen te hebben op basis van een ICT-beveiligingsassessment.'. Verder is bepaald dat de ICT-beveiligingsassessments jaarlijks herhaald dienen te worden en dat het moet worden uitgevoerd door een onafhankelijke EDP-auditor die is aangesloten bij de Nederlandse Organisatie van Register EDP-auditors (NOREA).

Het door het ministerie van BZK vastgestelde normenkader vindt zijn oorsprong in de door het Nationaal Cyber Security Centrum uitgegeven *ICT-Beveiligingsrichtlijnen voor Webapplicaties*.

1.2.1 Object en scope van onderzoek

Het perspectief van de burger die inlogt met DigiD en zijn verwachting dat hetgeen daarna gebeurt onder hetzelfde (strenge) beveiligingsregime van het DigiD assessment valt, bepaalt feitelijk de scope en de objecten van onderzoek bij een DigiD assessment. Dit zijn, samengevat, de internet-facing webpagina's waarmee de interactie naar de gebruiker plaatsvindt nadat 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 webapplicatie 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.

1.2.2 Aspecten van onderzoek

De onderzochte aspecten zijn volgens het Ministerie van Binnenlandse Zaken (BZK) exclusiviteit en integriteit. Beschikbaarheid wordt wel als belangrijk gezien voor de dienstverlening aan burgers, maar het bekend worden van vertrouwelijke gegevens of ongeautoriseerd wijzigen/ verwijderen van gegevens zal het vertrouwen van de burger in de digitale overheid veel meer

schaden dan het niet voldoende beschikbaar zijn van het systeem. Zeker voor de grote diensten die gebruik maken is beschikbaarheid wel een belangrijk aspect, maar dit valt buiten de scope van het DigiD assessment.

1.2.3 Norm ICT-beveiligingsassessments DigiD versie 3.0

De Norm versie 3.0 geldt voor assessments vanaf 1 augustus 2022 en verder. Ten opzichte van de Norm versie 2.0, is aan de Norm versie 3.0 de norm B.01 toegevoegd.

1.3 Governance DigiD

1.3.1 Context DigiD stelsel

DigiD is het veilig en betrouwbaar middel waarmee burgers zich digitaal kunnen identificeren. Aansluithouders zoals overheidsorganisaties, of organisaties met een publieke taak geven met DigiD toegang aan burgers tot online-diensten. DigiD geeft zekerheid over de identiteit van de burger.

1.3.2 Beheer

Het beheer van DigiD wordt uitgevoerd door Logius. Logius is onderdeel van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en beheert overheidsbrede ICT-voorzieningen. Naast beheerder is Logius ook aansluithouder op DigiD en toezichthouder op de aansluithouders.

1.3.3 Overeenkomst

Aansluithouders die DigiD afnemen sluiten nu een privaatrechtelijke overeenkomst met Logius af. Aantonen dat de online-diensten conform zijn met het DigiD normenkader is een onderdeel van deze overeenkomst. Het normenkader is door het Ministerie van Binnenlandse Zaken vastgesteld en is gebaseerd op de Webrichtlijnen van het NCSC. Aansluithouders laten op basis van het normenkader jaarlijks een assessment uitvoeren door een Register EDP-auditor van NOREA. Logius als toezichthouder ziet er vervolgens op toe dat aansluithouders zich conformeren aan de gestelde eisen door deze assessments te controleren.

NOREA stelt op basis van het DigiD normenkader de handreiking op waarmee auditors op gelijke wijze het DigiD assessment uitvoeren.

1.3.4 Overleg NOREA met BZK en Logius

NOREA voert meerdere malen per jaar overleg met BZK en Logius over de doorontwikkeling en de uitvoering van het toetsen, volgens het normenkader, van de online-diensten van de huidige en toekomstige aansluithouders en serviceorganisaties.

2 Audit aanpak

2.1 Formele aspecten van de opdracht

De opdrachten inzake de DigiD-beveiligingsassessments worden door RE's uitgevoerd in het kader van het Raamwerk voor Assurance-opdrachten en (dus) overeenkomstig Richtlijn 3000D[2] 'Assurance-opdrachten'.

Zowel voor het assessment bij de aansluithouder van DigiD als bij de serviceorganisatie is een modelrapport opgesteld (zie bijlage 2). Benadrukt wordt dat strikt de structuur en inhoud van de modelrapporten wordt gevolgd en uiterst zorgvuldig de juistheid en volledigheid van identificerende gegevens van het object van onderzoek en gehanteerde assurance-rapporten van derden wordt bepaald.

Daarnaast gelden de Richtlijnen voor opdrachtaanvaarding en rapportage, zoals die van toepassing zijn voor alle professionele diensten die door RE's worden uitgevoerd.

De werkzaamheden in het kader van deze opdrachten richten zich op het geven van oordelen per beveiligingsrichtlijn van de Norm v3.0, over de opzet en het bestaan van de maatregelen gericht op de ICT-beveiliging van de webomgeving van de DigiD aansluiting. Het feit dat de Norm v3.0 een selectie is van beveiligingsrichtlijnen uit de 'ICT-beveiligingsrichtlijnen voor webapplicaties' van Nationaal Cyber Security Centrum (NCSC) impliceert derhalve dat de auditor niet in staat is om één oordeel te verschaffen omtrent de beveiliging van de betreffende DigiD-aansluiting. De auditor geeft een oordeel 'Voldoet' of 'Voldoet niet' per norm. Dit is expliciet in de tekst van de Modelrapporten opgenomen.

Het rapport wordt uitsluitend verstrekt ten behoeve van de betreffende organisatie en Logius. De reden hiervoor is dat anderen, die niet op de hoogte

[2] Aangezien de aansluithouder niet expliciet een uitspraak doet over getrouwheid die beschikbaar is voor de beoogde gebruiker kwalificeert deze opdracht als een 'direct reporting'-opdracht. Daarnaast is 'direct reporting' ook de wens/eis van de toezichthouder Logius.

zijn van de precieze scope, aard en doel van de werkzaamheden, de resultaten onjuist kunnen interpreteren.

In de huidige opzet beperkt de audit zich tot het beoordelen van de opzet en het toetsen van het bestaan van de beheersmaatregelen. Voor een aantal normen is in de praktijk gebleken dat een afwezigheid, het ontbreken van een gebeurtenis of het niet plaatsvinden van een gebeurtenis zich kan voordoen, de zgn. 'Non-occurrence' Bij de betreffende normen is in de testaanpak aangegeven op grond van welke werkzaamheden c.q. (deel)waarnemingen de auditor tot een oordeel 'Voldoet' kan komen met een voorgeschreven voetnoot bij het oordeel (zie ook Par. 2.4).

2.2 Toetsing op werking

Het Ministerie van Binnenlandse Zaken (BZK) heeft recent besloten dat voor een aantal normen de werking zal worden getoetst. Met het besluit van BZK wordt daar nu voor 5 normen ook een toets op werking aan toegevoegd.

De 5 normen die worden getoetst op opzet, bestaan en werking zijn: **U/TV.01; U/WA.02; C.07; C.08 en C.09**.

De invoering van de toetsing op werking omvat een overgangsjaar:

- vanaf inleverperiode 1 januari -1 mei 2024 (over het voorgaande jaar 2023) **mogen** DigiD-aansluithouders de 5 normen laten toetsen op werking.
- Vanaf inleverperiode 1 januari -1 mei 2025 (over het voorgaande jaar 2024) **moeten** DigiD-aansluithouders de 5 normen laten toetsen op werking.

Opmerking: NOREA zal ten aanzien van de toetsing op de werking nog met nadere invulling komen (invulling zal nog nader met Logius worden besproken).

2.3 Serviceorganisaties

In de praktijk komt het regelmatig voor dat de houder van DigiD gebruik maakt van een serviceorganisatie. De volgende varianten komen voor:

- zowel de hosting als het applicatiebeheer plus de implementatie in eigen hand van de houder;
- hosting bij de houder en applicatiebeheer bij de leverancier, die geen verantwoordelijkheid heeft voor de implementatie;
- hosting bij de houder en applicatiebeheer bij de leverancier, die bepaalde verantwoordelijkheid heeft voor wat de implementatie en beheerrechten in de productieomgeving heeft;
- uitbesteding van de applicatiebeheer en de hosting onder aansturing van de houder (geen SAAS omgeving) aan één of twee leveranciers;
- volledige uitbesteding als SAAS oplossing waarbij wijzigingenbeheer en veelal ook het autorisatiebeheer volledig onder de leverancier valt met betrokkenheid van een gebruikersgroep.

Ook andere varianten en vormen van ketensamenwerking zijn mogelijk.

2.3.1 'Carve-out' versus 'Inclusive'

Bij het beoordelen van uitbestede taken heeft de carve-out methode (waarbij de beschrijving van de normen van de houder de normen van de serviceorganisatie uitsluiten) de voorkeur boven de inclusive methode (waarbij de beschrijving van de normen van de houder van haar systeem tevens de normen van de serviceorganisatie omvatten). Bij de carve-out methode ontvangt de houder een assurance-rapport (TPM) van de serviceorganisatie. De auditor van de houder heeft daarbij geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de rapportage van de serviceorganisatie en neemt ook geen verantwoordelijkheid voor de in die rapportage vermelde oordelen.

Dit heeft impact op de allocatie van te testen maatregelen over de verschillende betrokken partijen; aansluithouders, leveranciers, IT-auditor aansluithouder en IT-auditor serviceorganisatie. Dit vraagt bijzondere

aandacht van de IT-auditor van de aansluithouder en de IT-auditor van de serviceorganisatie.

Voor het DigiD-assessment moet per norm worden bepaald welke partij verantwoordelijk is voor een norm. Ruwweg wordt deze indeling aangehouden:

- normen waarvoor de aansluithouder verantwoordelijk is;
- normen waarvoor de serviceorganisatie verantwoordelijk is;
- normen waarvoor beiden een gedeelde verantwoordelijkheid hebben.

Een apart aandachtspunt daarbij vormen de normen waarvoor de serviceorganisatie aanneemt dat ook de houder verantwoordelijkheid draagt (ook wel de 'de user control considerations' genoemd), omdat de normen bij de serviceorganisatie alleen geen voldoende zekerheid bieden voor de beheersing van de DigiD beveiligingsrisico's. Over deze nomen dient goede afstemming te zijn tussen de partijen. In de guidance per norm is aangegeven voor welke normen mogelijk zowel de aansluithouder als de leverancier verantwoordelijk zijn.

De IT-auditor dient de afstemming tussen de betrokken partijen actief te faciliteren, zodat geen misverstanden ontstaan over wie welke normen toetst en waarom. Bij twijfel nemen de IT-auditors van de betrokken organisaties contact met elkaar op.

Daarbij dient de auditor van de aansluithouder te controleren of het assurance-rapport van de serviceorganisatie betrekking heeft op dezelfde of hogere versie van het systeem dat in productie is bij de aansluitorganisatie.

De auditor van de aansluithouder vermeldt in bijlage C van het rapport per norm waar deze is getoetst (zie Modelrapport). De aansluithouder stuurt zowel het eigen rapport als het/de rapport(en) van de serviceorganisatie(s) naar Logius.

2.3.2 Gebruik van SOC en ISAE3402 assurance-rapporten

Het is doorgaans niet mogelijk om de oordelen uit 3402 en/of SOC rapporten “inclusive” over te nemen. ISAE3402- en SOC-rapporten zijn gebaseerd op algemeen geformuleerde beheersingsdoelstellingen, terwijl de DigiD testaanpak een concrete inrichting van configuraties vereist. Daarnaast is dossier review bij de ISAE/SOC auditor veelal niet mogelijk, terwijl dit wel vereist is voor een inclusive oordeel, waarbij immers de auditor zelf de verantwoordelijkheid voor de oordeelsvorming neemt. Nu ‘inclusive’ niet mogelijk is, kan de ‘carve-out’ benadering wel een oplossing zijn, maar deze is beperkt tot de IT General Controls, die ook in het DigiD assessment een rol spelen zoals logisch toegangsbeheer, incidentenbeheer, wijzigingsbeheer, et cetera.

In veel gevallen kunnen klanten die Cloud- en (Managed-) hostingdiensten van grote leveranciers afnemen via een platform de relevante actuele ISAE- en/of SOC rapportages downloaden. Voorbeelden hiervan zijn (in willekeurige volgorde, maar niet uitsluitend) Amazon, Cloudflare, Google en Microsoft.

Let op: De toetsing van de ISAE3402/SOC mag niet ouder zijn dan een jaar (het gaat hier om datum oordeel opzet en bestaan, niet om de rapportagedatum (bij een Type I).

In bijlage C wordt dan verwezen naar het ISAE- en/of SOC-rapport, dat in ’short form‘ wordt meegestuurd net als de werkwijze bij een DigiD assurance-rapport. Een verwijzing per DigiD beveiligingsrichtlijn naar het equivalent in de ISAE3402/SOC rapportage is wel vereist omdat de ISAE/SOC rapportage doorgaans een andere nummering kent dan het DigiD normenkader.

Omdat Logius in het ISAE3402/SOC rapport doorgaans niet wordt vermeld als gebruiker van dit type assurance-rapport wordt dit NIET toegestuurd aan Logius tenzij er uitdrukkelijk toestemming is verleend.

2.3.3 Maximale leeftijd assurance-rapport serviceorganisatie (TPM)

Een assurance-rapport van de serviceorganisatie (ook genoemd ‘TPM’) mag niet ouder zijn dan twaalf maanden ten opzichte van de datum van het

assessmentrapport van de DigiD-aansluithouder. Voor vaststelling van de datum van het assurance-rapport is de in paragraaf 1.1 vermelde datum ‘oordelen opzet en bestaan’ leidend. Als de periodes niet aansluiten, kan de serviceorganisatie hier in voorzien door het afgeven van een of meer “bridgeletters”. Als dit van toepassing is, dient de IT-auditor ook de kenmerken van deze “bridgeletters” op te nemen als verwijzing.

Soms verwijst een assurance-rapport via de uitsluitingsmethode naar een onderliggend assurance-rapport. Ook hiervoor geldt dat de desbetreffende getoetste norm(en) niet ouder mogen zijn dan een jaar ten opzichte van het assessmentrapport van de aansluithouder. Bepalend hierbij is de onderzoeksdatum in het assessmentrapport van de serviceorganisatie.

2.3.4 Herhaald gebruik assurance-rapport serviceorganisatie (TPM)

Het assurance-rapport van de serviceorganisatie mag maar één keer gebruikt worden voor het indienen van een DigiD-assessment op de betreffende aansluiting. Voor het assessment van het volgende jaar moet een nieuw assurance-rapport (TPM) worden gebruikt.

2.4 Non-occurrence

Bij een aantal beveiligingsrichtlijnen kan zich de situatie voordoen dat 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. In situaties dat de relevante gebeurtenis zich niet heeft voorgedaan, kan relevante audit evidence voor het bestaan van de betreffende beheersmaatregel worden 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). In dat geval vermeldt de auditor ‘Voldoet’ voor de betreffende beheersmaatregel in de tabel oordelen zonder een opmerking in de toelichtende paragraaf te plaatsen betreffende het toetsen op het bestaan van de beheersmaatregel. Als er geen andere deelpopulatie is waarop hetzelfde proces en dezelfde control van toepassing is waarmee het bestaan van de betreffende beheersmaatregel kan worden vastgesteld, dient de auditor

‘Voldoet’ voor de betreffende beheersmaatregel te vermelden in de tabel oordelen en daarbij met een opmerking in de toelichtende paragraaf in het rapport aan te geven dat het bestaan van de beheersmaatregel niet kon worden getest omdat de relevante gebeurtenis zich niet heeft voorgedaan, noch er een andere deelpopulatie is waarop hetzelfde proces en dezelfde control van toepassing is. Non-occurrence kan zich alleen voordoen bij de normen B.05, U/TV.01, U/WA.02 en C.08.

2.5 Betrouwbaarheidseisen aan de handtekening van een RE-auditor

Met ingang van het jaar 2023 accepteert Logius twee vormen van elektronische handtekeningen in assessmentrapporten:

- De gekwalificeerde elektronische handtekening met een EUTL-certificaat.
- De geavanceerde elektronische handtekening met een EUTL-certificaat

EUTL staat voor European Union Trusted List en is een Europees middel dat wordt gebruikt om de identiteit van de uitgever van de elektronische handtekening te verifiëren. In de eigenschappen van de elektronische handtekening is voor iedereen te zien of de uitgever van het certificaat op de EUTL staat. Dit geeft een hoge betrouwbaarheid.

Met ingang van het jaar 2023 accepteert Logius voor op papier aangeleverde documenten alleen de ‘natte’ handtekening van de RE-auditor.

Tot 2023 is het nog mogelijk om documenten aan te leveren met een gescande handtekening, jpg-handtekening of ‘scribble’. Kenmerkend voor deze handtekeningen is dat ze persoonlijk door de RE-auditor zijn gezet. Een naam uitgeschreven met een computerlettertype, ook wanneer die handgeschreven lijkt, wordt daarom niet geaccepteerd.

Ook een document met een natte handtekening dat gescand wordt ingeleverd wordt tot 2023 nog geaccepteerd.

Let op: assurance-rapporten die worden uitgegeven in het najaar van 2022, ten behoeve van de inleverperiode van 1 januari tot 1 mei 2023, moeten zijn

voorzien van een elektronische handtekening met een EUTL-certificaat, of moeten op papier worden ingeleverd met een ‘natte’ handtekening.

2.6 Meervoudige Aansluiting

In 2020 heeft Logius, als beheerder van het DigiD stelsel, een nieuw soort aansluiting mogelijk gemaakt: de “Meervoudige Aansluiting” (MA). Deze aansluitvorm voorziet in de mogelijkheid dat grote groepen aansluithouders, die gebruik maken van gestandaardiseerde dienstverlening van een leverancier voor het gebruik van DigiD, op een doelmatige wijze kunnen aansluiten op DigiD. Dit betreft een verbetering ten opzichte van de situatie van groepsaansluitingen waarbij personen, die gebruik maken van DigiD, niet kunnen vaststellen met welke organisatie zij contact hebben. Algemeen uitgangspunt is dat de Leverancier van een Meervoudige Aansluiting (LMA) de aansluithouders, die gebruik maken van haar (gestandaardiseerde) dienstverlening, zo veel mogelijk ontzorgt. Voor de volledigheid wordt opgemerkt dat een LMA per definitie ook een SAAS-leveranciers is (echter niet alle SAAS-leveranciers zijn LMA’s).

Logius heeft voor het gebruik van een MA het “DigiD assessment MA” gedefinieerd. De volgende uitgangspunten zijn daarop van toepassing:

- De onder de meervoudig aansluiting geleverde dienstverlening betreft een SaaS-oplossing waarbij de aansluithouders van DigiD aansluitingen als afnemer van de dienst een voldoende homogene doelgroep vormen die onder een gelijke wettelijke bepaling gerechtigd is om het BSN te verwerken.
- De LMA laat een “DigiD assessment MA” uitvoeren dat van toepassing is op al haar afnemers van de gestandaardiseerde dienstverlening.
- De LMA heeft een stelsel van maatregelen ingericht waarmee op doelmatige wijze aanvullende waarborgen zijn aangebracht die erop zijn gericht dat de afnemers de 'Norm ICT-beveiligingsassessment DigiD’ naleven. Hierbij worden waar mogelijk applicatieve maatregelen ingezet. Een voorbeeld is het binnen de functionaliteit van de applicatie toekennen, controleren en intrekken van autorisaties door aansluithouders.

- Het onderzoek wordt door de IT-auditor uitgevoerd bij de LMA, welke door de aansluithouder is gemachtigd om een meervoudig assessment uit te laten voeren conform de 'Handleiding uitvoering ICT-beveiligingsassessment' versie 2.2 van Logius. De machtiging dient de LMA aan te tonen. De LMA zendt het assurancerapport aan Logius, eventueel vergezeld van assurance-rapporten van (sub-)serviceorganisatie(s) waaraan de LMA taken heeft uitbesteed en waar de carve-out methode op van toepassing is.

De in bijlage 4 opgenomen testaanpak geeft aanvullende guidance voor het uitvoeren van een DigiD assessment MA. Waar nodig is de bestaande DigiD testaanpak vertaald op basis van de uitgangspunten van Logius naar de situatie voor een DigiD assessment MA.

2.7 Normen en testaanpak

Voor de uitvoering van een DigiD assessment zijn de normen inclusief testaanpak zoals opgenomen in bijlage 3 leidend. Dit is een selectie van de ICT-Beveiligingsrichtlijnen voor Webapplicaties september 2015, versie verdieping, van het Nationaal Cyber Security Centrum. De oordelen van de IT-auditor dienen gebaseerd te zijn op de testaanpak zoals opgenomen in de guidance per norm en niet op basis van alle achterliggende NCSC-richtlijnen. De normen zijn op zichzelf staand en worden ook als zodanig getoetst. Feitelijk is de testaanpak '*rule based*' en niet '*risk based*'.

In de guidance wordt een indicatie gegeven van het te testen type object (governance, applicatie, infrastructuur proces). Deze typering moet slechts beschouwd worden als een indicatie. De IT-auditor dient zelf vast te stellen welke objecttypering het beste past bij de onderzochte norm. De typering is daarom niet bepalend voor het uit te voeren assessment. In de guidance worden ter indicatie per norm betrokken partij(en) genoemd. De IT-auditor dient zelf vast te stellen welke partij(en) betrokken zijn bij het onderzochte object.

Specifieke aandacht vraagt het uitvoeren van penetratietesten en vulnerabilty assessments bij het onderzoek naar meer technische normen. In de guidance

is per norm onder testaanpak aangegeven voor welke normen dat toepasbaar is. In bijlage 5 worden aandachtspunten gegeven voor het uitvoeren van penetratietesten en vulnerability assessments.

2.8 Bijzondere aanwijzingen van Logius

In bijzondere gevallen kan Logius NOREA verzoeken de IT-auditors een aanwijzing te geven met betrekking tot de testaanpak en/of de rapportage. Voorbeelden uit de afgelopen periode zijn aanwijzingen hoe om te gaan met non-occurrence t.a.v. de normen B.05, U/TV.01, U/WA.02 en C.08. Andere uitzonderingsregels worden door Logius gepubliceerd. Omdat bijzondere aanwijzingen altijd een tijdelijk karakter zullen hebben, worden deze alleen in de FAQ vermeld en niet in de Handreiking.

2.9 Meldpunt auditaangelegenheden DigiD

Bij Logius en de VNG (ENSIA voor onderdeel DigiD) is in de afgelopen jaren de behoefte ontstaan aan een centraal orgaan waarin zij, onder waarborging van de noodzakelijke vertrouwelijkheid – mede gelet op hun positie ten opzichte van de betrokken IT-auditors – aangelegenheden met de uitvoering van de DigiD-assessments kunnen melden. Door dit centrale orgaan kan dan in overleg met alle betrokkenen gekomen moeten worden tot de oplossing van de gesignaleerde aangelegenheden.

Ook bij de andere partijen (opdrachtgevers en betrokken IT-auditors) bestaat een groeiende behoefte aan een dergelijk orgaan. Deze behoefte komt onder meer voort uit de aard en omvang van de discussies en de belemmeringen die worden ervaren rond een open informatie-uitwisseling tussen partijen.

Tegen deze achtergrond heeft NOREA een Meldpunt auditaangelegenheden DigiD ingericht. Het meldpunt is bereikbaar via meldpunt@norea.nl.

2.10 Correctie van assurance-rapporten

Door IT-auditors worden grote aantallen assurance-rapporten afgegeven aan partijen in het maatschappelijk of besloten verkeer. Deze actoren kunnen de assurance-rapporten gebruiken voor onder meer de eigen organisatie, in het

kader van het afleggen van algemene en/ of specifieke verantwoordingen alsmede het voldoen aan ter zake gestelde contractueel overeengekomen verantwoordingen of wettelijk voorgeschreven verantwoordingsrelaties.

Het is onvermijdelijk dat in uitzonderlijke omstandigheden, zich na datering en afgifte van het assurance-rapport gebeurtenissen voordoen die leiden tot de noodzaak van het uitvoeren van nieuwe en/ of aanvullende werkzaamheden door de IT-auditor. Deze werkzaamheden kunnen leiden tot aanpassingen in het eerder afgegeven assurance-rapport.

Voor alle betrokkenen dient helder te zijn welke verantwoordelijkheden zij hebben bij het uitvoeren van de hier beschreven werkzaamheden alsmede welke stappen hierbij dienen te worden doorlopen.

Met de 'Handreiking Correctie van assurance-rapporten' wordt invulling gegeven aan een voor alle partijen inzichtelijke en eenduidige correctieprocedure.

Bijlage 1 – Begrippenkader DigiD assessments

In de hiernavolgende bijlage 1 worden enkele kernbegrippen bij DigiD assessments toegelicht.

Applicatieleverancier	Een organisatie die een webapplicatie levert en die conform gemaakte afspraken verantwoordelijk is voor het onderhoud en de eventuele doorontwikkeling aan de software.
Bestaan	Het functioneren van een stelsel van informatiebeveiligings- en beheersingsmaatregelen conform beschrijving op of rond een peildatum.
Carve-out methode	Bij de carve-out methode wordt in een assurance-rapport (zoals een DigiD assessment rapportage) een verwijzing opgenomen naar de TPM van een leverancier. De auditor van het assurance-rapport en de auditor van de TPM houden ieder zelfstandig hun vaktechnische verantwoordelijkheid. De eerste auditor dient wel vast te stellen dat de scope van beide rapportages in voldoende mate op elkaar aansluit.
Hosting leverancier	Een organisatie die conform gemaakte afspraken ICT-infrastructuur inclusief internettoegang aanbiedt waarop een webapplicatie kan worden uitgevoerd en kan worden aangeboden aan gebruikers.
Aansluithouder van een DigiD aansluiting	De organisatie die bij Logius staat geregistreerd als de verantwoordelijke voor een specifieke DigiD aansluiting. Iedere DigiD aansluiting wordt gekenmerkt door een uniek aansluitnummer. Per aansluitnummer is er een aansluithouder.
Inclusive methode	Bij de inclusive methode worden alle beheersmaatregelen in een assurance-rapport overgenomen en er wordt dus niet verwezen naar assurance-rapporten waar eventueel gebruik van is gemaakt. De auditor van het assurance-rapport is vaktechnisch volledig verantwoordelijk en voert eigen werkzaamheden (zoals bijv. deelwaarnemingen en een dossierreview) uit voor een TPM waarvan de resultaten worden overgenomen.

Leverancier Meervoudige aansluiting (LMA)	De leverancier van een platform dat meerdere aansluithouders aansluit op DigiD en ervoor zorgt dat de aansluithouders zowel technisch als administratief ontzorgd wordt en bij het tot stand komen van de aansluiting op DigiD.
Assessment Meervoudige Aansluiting (MA)	Het assessment waarbij de Serviceorganisatie (de LMA) door Logius is geaccrediteerd om gebruik te mogen maken van de meervoudige aansluiting.
Opzet	De beschrijving van een stelsel van informatiebeveiligings- en beheersingsmaatregelen.
Penetratietest	Dit is een specifieke vorm van een vulnerability-assessment. Het is een proces waarbij met behulp van technische hulpmiddelen specifieke componenten of specifieke delen van de ICT-infrastructuur op zwakheden gecontroleerd worden. (NCSC) In de context van het DigiD assessment wordt met een penetratietest een technisch beveiligingsonderzoek bedoeld dat vanaf het internet wordt uitgevoerd door een (ervaren) penetratietester en waarbij scantools worden ingezet en aanvullende handmatige onderzoek werkzaamheden worden uitgevoerd.
SAAS-leverancier	Een organisatie die een webapplicatie als online dienst aanbiedt waarbij de klanten de software niet hoeven aan te schaffen. De aanbieder draagt zorg voor onderhoud en doorontwikkeling van (de software van) de applicatie, hosting en applicatiebeheer.
Third Party Mededeling (TPM)	De term 'TPM' wordt in de context van het DigiD-assessment gebruikt om specifiek het assurance-rapport van een leverancier (serviceorganisatie) te duiden waarbij de doelgroep van het rapport een andere is dan de serviceorganisatie en de assurance wordt gegeven door een onafhankelijke auditor.
Vulnerability assessment	Dit is een proces waarbij met behulp van technische hulpmiddelen wordt nagegaan in hoeverre in de ICT-componenten kwetsbaarheden voorkomen waarvan ongeautoriseerden gebruik zouden kunnen maken. (NCSC) In de context van het DigiD assessment wordt een (bij voorkeur geautomatiseerde) scan bedoeld die vanaf een intern netwerksegment zo dicht mogelijk bij de server wordt uitgevoerd op bekende kwetsbaarheden en ontbrekende patches.

Werking	Het functioneren van een stelsel van informatiebeveiligings- en beheersingsmaatregelen conform beschrijving gedurende een bepaalde periode.

Bijlage 2 - Model assurance-rapporten (aansluithouder en serviceorganisatie)

2.1 Model assurance-rapport aansluithouder op volgende pagina

Het modelrapport is tevens als Word bestand beschikbaar.

Rapportage-template DigiD-Assessment (versie 3.0)

Aan	:	Management AANSLUITHOUDER en Logius
Datum	:	RAPPORTDATUM
Van	:	AUDITOR
		KENMERK
Aansluiting	:	AANSLUITNUMMER
		AANSLUITNAAM
		AANSLUITHOUDER

Inhoudsopgave

1. Assurancerapport van de onafhankelijke IT-auditor

Aan	:	Management AANSLUITHOUDER en Logius
Datum	:	RAPPORTDATUM
Van	:	AUDITOR
		KENMERK
Aansluiting	:	AANSLUITNUMMER
		AANSLUITNAAM
		AANSLUITHOUDER

Aan: Bestuur <houderorganisatie>

1.1. Onze oordelen <met beperking>

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

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" 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.

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 webapplicatie gerelateerde 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 privacy bevorderende 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.	

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel
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.	

1.2. 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 de DigiD Aansluithouder 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.

[xx] Herhaling bij meerdere beperkingen in oordelen

Instructie voor de auditor: optionele passage bij beperkingen bij U/PW.03:

[xx] Bij U/PW.03 is niet volledig voldaan aan de verplichtingen van de CSP. Het oordeel voor U/PW.03 is daarom "voldoet niet". Wij merken op dat daarmee één (1) specifiek onderdeel van de gewenste configuratie-items niet op de juiste wijze is geconfigureerd conform de handreiking. Naar het oordeel van de auditor zijn de daardoor aanwezige risico's afdoende beperkt door andere beheersingsmaatregelen en is door de DigiD Aansluithouder een realistisch en effectief verbeterplan opgesteld om voor 1 mei 2024 deze kwetsbaarheden te hebben opgelost. Alle andere configuratie-items zijn wel correct geconfigureerd. 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 de DigiD Aansluithouder 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>.

1.3. 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 'het DigiD normenkader ICT-beveiligingsassessments DigiD 3.0' welke wij hebben gehanteerd bij dit onderzoek. Het DigiD Normenkader 3.0 bestaat uit 21 richtlijnen die zijn gebaseerd op de ICT-Beveiligingsrichtlijnen voor Webapplicaties. De versie 3.0 geldt vanaf 1 augustus 2022 en is vastgesteld door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De 21 beveiligingsrichtlijnen uit het Normenkader worden in het dagelijks gebruik de 21 normen genoemd.

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.

1.4. Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek

1.4.1. Object van onderzoek

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

AANSLUITHOUDER 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

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 aansluithouder 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 aansluithouder 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 aansluithouder 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 webapplicaties, alle onderliggende ICT-componenten die binnen een samenhangende procesketen en een logische afhankelijkheid van DigiD worden ingezet tijdens en na de DigiD authenticatie en ondersteunende processen conform de 'Norm ICT-beveiligingsassessments DigiD 3.0' van het Ministerie van BZK.

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

1.4.2. Service organisaties

Instructie voor de auditor: optionele passages bij serviceorganisatie(s):

De DigiD aansluithouder maakt gebruik van serviceorganisatie ORGANISATIE-A voor <de aard van de activiteiten die door de serviceorganisatie worden uitgevoerd>. De DigiD aansluithouder maakt voor het verschaffen van zekerheid over haar volledige webomgeving zoals beschreven onder het object van onderzoek gebruik van de uitsluitingsmethode ('carve-out method'). De beschrijving van de serviceorganisatie van haar systeem sluit daarmee de interne beheersingsdoelstellingen en daarmee verband houdende interne beheersingsmaatregelen van de serviceorganisatie uit. Onze werkzaamheden strekken zich dan ook niet uit tot de interne beheersingsmaatregelen van de serviceorganisatie.

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

1.4.3. Norm ICT-beveiligingsassessments 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 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 aansluithouder om in aanvulling op de richtlijnen in de vigerende 'Norm ICT-beveiligingsassessments DigiD', ook de andere richtlijnen uit de 'ICT-beveiligingsrichtlijnen voor webapplicaties' van het NCSC te adopteren. Wij wijzen u erop dat, indien wij aanvullende beveiligingsrichtlijnen zouden hebben onderzocht wellicht andere onderwerpen zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen.

1.4.4. Beperkingen met betrekking tot interne 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.

1.5. Beoogde gebruikers en doel

Ons assurance-rapport is uitsluitend bestemd voor de DigiD aansluithouder 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 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).

De bijlagen A en B zijn alleen bestemd voor de DigiD aansluithouder.

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).

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

1.6. Verantwoordelijkheden van de DigiD aansluithouder

Het bestuur van de DigiD aansluithouder 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'.

1.7. 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 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

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

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 (datum)". "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 (datum)".

Instructie voor de auditor: alleen indien gebruik wordt gemaakt van een of meerdere serviceorganisatie(s):

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 aanbevelingen
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatie gerelateerde onderwerpen zoals dataclassificatie,		Voldoet / Voldoet niet

Nr	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en eventuele aanbevelingen
	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.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		

Nr	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en eventuele aanbevelingen
	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.		

Nr	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en eventuele aanbevelingen
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.		

Bijlage B – Object van onderzoek

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

De functionaliteit wordt geboden door de volgende webapplicatie:

- <NAAM VAN DE APPLICATIE> versienummer applicatie indien beschikbaar

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

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

Voor het verifiëren van de identiteit van de gebruiker maakt de DigiD aansluithouder gebruik van de NAAM DIENSTVERLENING van NAAM IDENTITY BROKER.

Instructie voor de auditor: onderstaande alinea opnemen ingeval van hosting

Voor de infrastructuur maakt de DigiD aansluithouder gebruik van NAAM DIENSTVERLENING van NAAM SERVICEORGANISATIE2. Voor het beheer van deze infrastructuur wordt (mede) gebruik gemaakt van de diensten van NAAM SERVICEORGANISATIE2 OF SERVICEORGANISATIE3.

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

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

NAAM SERVICEORGANISATIE4 – NAAM DIENSTVERLENING

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

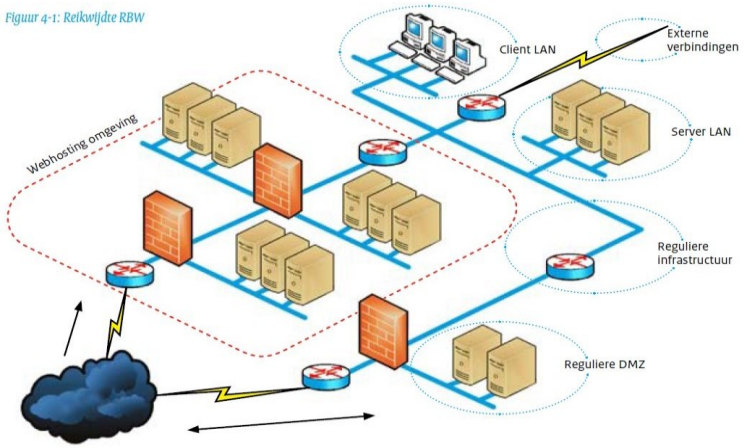
Instructie voor de auditor: onderstaande alinea opnemen ingeval van een serviceorganisatie die een geldige DigiD TPM heeft.

De DigiD aansluithouder heeft een deel van de 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 hetzelfde 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.

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 ondersteunende processen conform de 'Norm ICT-beveiligingsassessments DigiD' van Logius.

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



De DigiD aansluithouder 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.

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

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

Deze bijlage richt zich op het ten dienste van Logius inzichtelijk maken van de wijze waarop AANSLUITHOUDER gebruik heeft gemaakt van service organisaties 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):

Kenmerk	Omschrijving assurancerapportage	Serviceorganisatie en bijbehorende subserviceorganisaties	Bij serviceorganisatie getoetste beveiligingsrichtlijnen	Referentie / rapportnummer	Afgiftedatum	Ondertekend door naam RE
	DigiD assurancerapportage/ ISAE 3402/ SOC1 assurancerapportage/ ISAE 3000/ SOC2 assurancerapportage/ ISAE 3000 assurancerapportage	[Naam] Serviceorganisatie software/ Serviceorganisatie infrastructuur/ Serviceorganisatie SaaS/ Serviceorganisatie Identity Broker/ Subserviceorganisatie …				

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 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
- Default nee invullen

Nr	Beschrijving van de norm	Getoetst bij leverancier 1 Referentie / rapportnr	Getoetst bij leverancier 2 Referentie / rapportnr	Aanvullende beheersmaatregelen gebruikersorganisatie [3]	Getoetst bij gebruikers-organisatie
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.	Voldoet / Voldoet niet		Ja / Nee	Ja / Nee
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/W A.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.				
U/W A.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.				
U/W A.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.				
U/W A.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.				

[3] naar het oordeel van de auditor van de serviceorganisatie

U/P W.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.				
U/P W.03	De webserver is ingericht volgens een configuratie-baseline.				
U/P W.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/P W.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.				
U/N W.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/N W.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.				
U/N W.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.				
U/N W.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.				

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

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.

Instructie voor de auditor: de eerste drie kolommen te allen tijde invullen (de velden zijn dezelfde als in de assurancerapportage). De laatste kolommen alleen invullen indien er sprake is van een of meerdere assurancerapportages van (sub)serviceorganisaties.

Aansluiting	Auditor aansluithouder	Object van onderzoek	Serviceorganisatie A	Serviceorganisatie B
Aansluitnummer AANSLUITNUMMER Aansluitnaam AANSLUITNAAM Aansluithouder AANSLUITHOUDER	Auditor AUDITOR Kenmerk rapport KENMERK Oordeelsdatum OORDEELSDATUM Rapportdatum RAPPORTDATUM	Webapplicatie <NAAM VAN DE APPLICATIE> versienummer applicatie Deze webapplicatie betreft <GEHEEL MAATWERK / EEN COMBINATIE VAN MAATWERK EN STANDAARD SOFTWARE / GEHEEL	Naam ORGANISATIE-A Auditor AUDITOR S-A Kenmerk rapport KENMERK S-A Oordeelsdatum OORDEELSDATUM S-A Rapportdatum RAPPORTDATUM S-A Webapplicatie	Naam ORGANISATIE-B Auditor AUDITOR S-B Kenmerk rapport KENMERK S-B Oordeelsdatum OORDEELSDATUM S-B Rapportdatum RAPPORTDATUM S-B Webapplicatie

Aansluiting	Auditor aansluithouder	Object van onderzoek	Serviceorganisatie A	Serviceorganisatie B
		STANDAARD PAKKET>.	<NAAM VAN DE APPLICATIE> versienummer applicatie	<NAAM VAN DE APPLICATIE> versienummer applicatie

2.2 Model-rapport serviceorganisatie op volgende pagina.

Het modelrapport is tevens als Word bestand beschikbaar.

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Rapportage-template DigiD-Assessment Serviceorganisatie(versie 3.0)

Aan	:	Management NAAM SERVICEORGANISATIE A en Logius
Datum	:	RAPPORTDATUM
Van	:	AUDITOR
		KENMERK
Aansluiting	:	AANSLUITNUMMER
		AANSLUITNAAM
		NAAM AANSLUITHOUDER

Inhoudsopgave

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

1. Assurancerapport van de onafhankelijke auditor

Aan	:	NAAM SERVICEORGANISATIE-A
Datum	:	RAPPORTDATUM
Van	:	AUDITOR
		KENMERK
Aansluiting	:	AANSLUITNUMMER
		AANSLUITNAAM
		NAAM AANSLUITHOUDER

Aan: Management <NAAM SERVICEORGANISATIE-A>

1.1. 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]

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.	
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 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.	

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel
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.	

1.2. 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-A 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.

[xx] Herhaling bij meerdere beperkingen in oordelen

Instructie voor de auditor: optionele passage bij beperkingen bij U/PW.03:

[xx] Bij U/PW.03 is niet volledig voldaan aan de verplichtingen van de CSP. Het oordeel voor U/PW.03 is daarom "voldoet niet". Wij merken op dat daarmee één (1) specifiek onderdeel van de gewenste configuratie-items niet op de juiste wijze is geconfigureerd conform de handreiking. Naar het oordeel van de auditor zijn de daardoor aanwezige risico's afdoende beperkt door andere beheersingsmaatregelen en is door NAAM SERVICEORGANISATIE-A een realistisch en effectief verbeterplan opgesteld om voor 1 mei 2024 deze kwetsbaarheden te hebben opgelost. Alle andere configuratie-items zijn wel correct geconfigureerd.

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-A 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>.

1.3. 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.

1.4. Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek

1.4.1. Object van onderzoek

Het object van onderzoek was de webomgeving van 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.

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

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-A in haar dienstverlening gebruik van NAAM DIENSTVERLENING van NAAM SUBSERVICEORGANISATIE-B.

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.

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

1.4.2. Subservice organisaties

Instructie voor de auditor: optionele passages bij subserviceorganisatie(s):

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

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

1.4.3. Norm ICT-beveiligingsassessment DigiD

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.

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-A om in aanvulling op de richtlijnen in de 'Norm ICT-beveiligingsassessments DigiD', ook de andere richtlijnen uit de 'ICT-beveiligingsrichtlijnen voor webapplicaties' van het NCSC te adopteren. Wij wijzen u erop dat, indien wij aanvullende beveiligingsrichtlijnen zouden hebben onderzocht wellicht andere onderwerpen zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen.

1.4.4. Beperkingen met betrekking tot interne 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.

1.5. 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.

De bijlagen A en B zijn alleen bestemd voor NAAM SERVICEORGANISATIE-A.

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). 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.

1.6. Verantwoordelijkheden van NAAM SERVICEORGANISATIE-A

Het bestuur van NAAM SERVICEORGANISATIE-A 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 vingerende 'Norm ICT-beveiligingsassessments DigiD'.

1.7. Verantwoordelijkheid van de IT-auditor

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van ons onderzoek dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor 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

2. 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 kan het voorkomen dat de gebruikersorganisaties meer interne beheersingsmaatregelen zou moeten nemen waardoor een afwijkende lijst (User control considerations) wordt aangegeven.

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.	

Nr	Beschrijving van de beveiligingsrichtlijn	Gewenste interne beheersingsmaatregelen van de gebruikersorganisatie
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.	
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	

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		

Nr	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en eventuele adviezen
	(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.		

Nr	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en eventuele adviezen
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.		

Nr	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en eventuele adviezen
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		

Nr	Beschrijving van de beveiligingsrichtlijn	Korte beschrijving van de uitgevoerde werkzaamheden	Oordeel en eventuele adviezen
	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.		

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 .

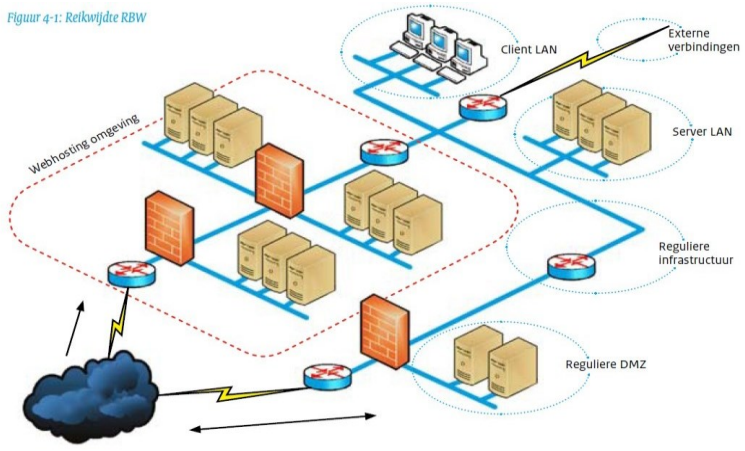
Instructie voor de auditor: onderstaande alinea opnemen ingeval van een identity broker

INDIEN IDENTIY BROKER Voor het verifiëren van de identiteit van de gebruiker maakt NAAM SERVICEORGANISATIE-A 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.

Figuur 4-1: Reikwijdte RBW



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 SUB-SERVICEORGANISATIE. Als gevolg hiervan zijn er een aantal maatregelen belegd bij deze sub-service organisatie. Het onderzoeken van deze maatregelen is dan ook

uitgevoerd door de IT auditor van deze sub-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 sub-service organisatie. In bijlage C is de onderverdeling van normen opgenomen.

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):

Kenmerk	Omschrijving assurancerapportage	Subserviceorganisaties	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] Serviceorganisatie software/ Serviceorganisatie infrastructuur/ Serviceorganisatie SaaS/ Serviceorganisatie Identity Broker/ Subserviceorganisatie …				

Kenmerk	Omschrijving assurancerapportage	Subserviceorganisaties	Bij subserviceorganisatie getoetste beveiligingsrichtlijnen	Referentie / rapportnummer	Afgiftedatum	Ondertekend door naam RE

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 1 Referentie / rapportnr	Getoetst bij leverancier 2 Referentie / rapportnr
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.	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 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.		

Bijlage D - Overzicht ICT-beveiligingsassessment DigiD NAAM SERVICEORGANISATIE A

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

Instructie voor de auditor: de eerste drie kolommen invullen indien er sprake is van een subserviceorganisatie. De laatste kolom alleen invullen indien er sprake is van meerdere assurancerapportages van subserviceorganisaties.

Auditor serviceorganisatie	Object van onderzoek	Sub-serviceorganisatie B	Sub-serviceorganisatie C
Auditor AUDITOR Kenmerk rapport KENMERK Oordeelsdatum OORDEELSDATUM Rapportdatum RAPPORTDATUM	HIGH LEVEL OPSOMMING VAN AANGEBODEN FUNCTIONALITEIT	Naam NAAM SUBSERVICEORGANISATIE-B Auditor AUDITOR SUB-B Kenmerk rapport KENMERK SUB-B Oordeelsdatum OORDEELSDATUM SUB-B Rapportdatum RAPPORTDATUM SUB-B Webapplicatie/ infrastructuur <de aard van de activiteiten die door de serviceorganisatie worden uitgevoerd>	Naam Auditor Kenmerk rapport Oordeelsdatum Rapportdatum Webapplicatie/ infrastructuur <de aard van de activiteiten die door de serviceorganisatie worden uitgevoerd>

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Bijlage 3 - Guidance bij de te onderzoeken DigiD beheersingsmaatregelen

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
B.01	De organisatie formuleert een informatie-beveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatie-gerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer. <u>Doelstelling:</u> Het zorgen voor specifieke management aandacht in het beveiligingsproces voor de webapplicaties van de organisatie.	Governance	<u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS-leverancier. • Aansluithouder van de DigiD aansluiting. <u>Scope:</u> • De DigiD webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. <u>Nadere toelichting:</u> De focus ligt op het vaststellen dat het eigenaarschap van de DigiD webapplicatie is georganiseerd, bevoegdheden aan de eigenaar zijn toegekend en dat de organisatie beschikt over een geactualiseerd (minimaal eenmaal in de 5 jaar dan wel bij grote organisatiewijzigingen en/of wijzingen in de ICT) informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid bevat (expliciet) het beleid over de bescherming van de eigen Informatiehuishouding in relatie tot de eigen delen van

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			de DigiD webapplicatie en/of de infrastructuur voor het netwerksegment met de DigiD webapplicatie. Test aanpak: • Stel vast dat de houder van de DigiD aansluiting het eigenaarschap t.a.v.de DigiD webapplicatie adequaat op een hoog organisatorisch niveau heeft ingericht en dat de eigenaar passende bevoegdheden heeft. • Stel vast dat in het informatiebeveiligingsbeleid, of in een hiervoor apart ontwikkeld beleid, expliciet aandacht is besteed aan het stelsel van beveiligingsmaatregelen t.a.v. webapplicaties en/of de infrastructuren voor de netwerksegmenten met webapplicaties in het algemeen, en DigiD en andere authenticatie- en identificatiediensten in het bijzonder. • Stel vast dat dataclassificatie (zie U/WA.05), toegangsvoorziening (zie U/TV.01) en kwetsbaarhedenbeheer (zie U/PW.07, U/NW.06, C.03 en C.09) zijn geadresseerd. • Stel vast dat het informatiebeveiligingsbeleid door het verantwoordelijk hoger management is vastgesteld en actief wordt uitgedragen, alsmede

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			bekend is bij functionarissen betrokken bij webapplicatie gerelateerde onderwerpen. • Stel vast dat het verantwoordelijk hoger management periodiek rapportages ontvangt inzake informatiebeveiliging en indien nodig hierop acteert. • Stel vast dat het informatiebeveiligingsbeleid wordt geüpdatet conform de beleidscyclus van de organisatie, doch minimaal eens in de 5 jaar. Bij (tussentijdse) grote wijzigingen dient het informatiebeveiligingsbeleid te worden geactualiseerd. • Interview de verantwoordelijke functionarissen.
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>Doelstelling:</u> Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de	Governance	<u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS-leverancier. • Aansluithouder van de DigiD aansluiting. <u>Scope:</u> De contracten en/of Service Level Agreements voor de levering hosting-, applicatie- of SAAS-diensten. <u>Nadere toelichting:</u> De organisatie dient een, door beide partijen ondertekend, contract te hebben waarin tenminste de volgende zaken zijn opgenomen:

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	webapplicatie is uitbesteed aan een andere organisatie.		• een beschrijving van de te leveren diensten die onder het contract vallen; • de van toepassing zijnde leveringsvoorwaarden; • informatiebeveiligingseisen met de relevante eisen vanuit het beveiligingsbeleid; • het melden van beveiligingsincidenten; • de behandeling van gevoelige gegevens; • wanneer en hoe de leverancier toegang tot de systemen / data van de aansluithouder mag hebben; • Service Level Reporting inclusief noodzakelijke vervolgacties door het management van de houder van de DigiD aansluiting; • het jaarlijks uitvoeren van audits bij de leverancier(s); • beding dat deze voorwaarden back-to-back worden doorgegeven aan mogelijke subleveranciers. <u>Test aanpak:</u> • Interview de verantwoordelijke functionarissen. • Inspectie van het beveiligingsbeleid. • Inspectie van contracten met leveranciers, SLA's en andere gerelateerde documenten.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			Nonoccurrence (voor het onderdeel Service Level Reporting): • T.a.v. Service Level Reporting, kan de situatie zich voordoen dat er nog geen rapportering heeft plaatsgevonden, terwijl dit contractueel wel is overeengekomen. In dit geval dient op basis van (deel)waarnemingen binnen een proces dat onderworpen is aan dezelfde control te worden vastgesteld dat Service Level Reporting plaatsvindt.
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 de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken. Doelstelling: Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze	Applicatie Infrastructuur Proces	Betrokken rol(len): • Applicatie-, hosting- of SAAS-leverancier. • Aansluithouder van de DigiD aansluiting. Scope: De DigiD webapplicatie, DigiD webservers en de firewalls, IDS/IPS, etc. Nadere toelichting: De focus ligt op de beheerprocessen. Dit betreft enerzijds toegang tot de DigiD-applicatie en anderzijds toegang tot de DigiD webservers en de firewalls, IDS/IPS, etc. die een koppeling hebben met de DigiD omgeving. Aandachtspunten hierbij zijn: • Toekennen, wijzigen en intrekken van autorisaties.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit.		• Eisen aan wachtwoordinstellingen. • Aantoonbare controle op joiners/movers/leavers. • Wijzigen van de standaard wachtwoorden van administrator accounts. • Beperken eventuele shared accounts. Specifieke aandacht gaat uit naar wachtwoorden die leveranciers hebben om toegang tot de systemen en data van de houder van de DigiD aansluiting te krijgen (wie hebben die wachtwoorden, hoe worden die opgeslagen en wie hebben toegang. Hoe vaak worden ze gewijzigd, et cetera). In het geval van een TPM kan het zijn dat de SAAS leverancier het gehele functionele (toegangs-) beheer verzorgt, inclusief het testen van de applicatie. Als de auditor van de service organisatie vaststelt, dat de aansluithouder geen beheerders noch gebruikers heeft binnen de DigiD scope, ligt het voor de hand dat U/TV-01 niet in hoofdstuk 4 wordt opgenomen van de TPM. Het blijft de verantwoordelijkheid van de auditor van de aansluithouder om te bepalen of U/TV.01 getest moet worden bij de aansluithouder. <u>Test aanpak</u>:

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor

			• Inspecteer het beveiligingsbeleid, de joiners/ movers/ leavers procedure, de autorisatieprocedure, afspraken met leveranciers met betrekking tot toegang tot systemen en data en andere gerelateerde documenten.
			• Stel voor elk van deze processen en systemen, het bestaan vast met een deelwaarneming van tenminste één.
			• Inspecteer de toegekende autorisaties en de resultaten en opvolging van de periodieke review.
			• Interview de verantwoordelijke functionarissen.
			
			<u>Nonoccurrence (deels):</u>
			• Alleen voor de processen 'Toekennen, controleren en intrekken van autorisaties' en 'Uitvoeren periodieke reviews' waarbij geldt dat:
			  • Controle op joiners / movers / leavers wel aantoonbaar dient te hebben plaatsgevonden.
			  • De periodieke review dient te zijn opgenomen in een planning.

U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Applicatie Proces	<u>Betrokken rol(len):</u> • Applicatie of SAAS-leverancier. • Aansluithouder van de DigiD aansluiting.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	Doelstelling: Effectief en veilig realiseren van de dienstverlening.		Scope: De DigiD webapplicatie. Nadere toelichting: Deze norm richt zich meer op de procesmatige aspecten van het functioneel en het applicatiebeheer. Aandachtspunten hierbij zijn: • Beschrijving van taken, verantwoordelijkheden en bevoegdheden van de verschillende beheerrollen. • Een incidentenprocedure is opgesteld. • Meldingen van het NCSC of IBD of Z-CERT of andere CERTS worden geanalyseerd en zo nodig opgevolgd. • Incidenten worden geregistreerd, geanalyseerd, opgevolgd en afgehandeld. • Er is een periodieke rapportage aan het management inzake beveiligingsincidenten. Test aanpak: • Inspecteer de functie/taakbeschrijvingen van beheerders. • Inspecteer het incidentproces, de uitgevoerde analyse, de managementrapportage en opvolging van beveiligingsincidenten. • Interview de verantwoordelijke functionarissen.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			Nonoccurrence (voor het onderdeel opvolging van beveiligingsincidenten): • Voor het proces 'incidentmanagement', waarbij geldt dat op basis van (deel)waarnemingen binnen een proces dat onderworpen is aan dezelfde control, vastgesteld moet worden dat een incidentenprocedure effectief is geïmplementeerd. • Voor het proces 'periodieke rapportage aan het management', waarbij geldt dat op basis van (deel)waarnemingen t.a.v. een plaatsgevonden incident binnen een proces dat onderworpen is aan dezelfde control, vastgesteld moet worden dat rapportages aan het management inzake beveiligingsincidenten structureel plaatsvinden.
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt. Doelstelling: Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of	Applicatie	Betrokken rol(len): Applicatie- of SAAS-leverancier. Scope : De DigiD webapplicatie en webserver. Nadere toelichting: Ongecontroleerde (ongevalideerde) invoer van gebruikers is een belangrijke dreiging voor een

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	beschikbaarheid van de webapplicatie aangetast worden.		webapplicatie. Als invoer van gebruikers rechtstreeks wordt gebruikt in HTML-uitvoer, cookiewaarden, SQL-queries, etc., bestaat er een (grote) kans dat een kwaadwillende de webapplicatie compromitteert. Een gebrek aan invoervalidatie kan tot kwetsbaarheden zoals XSS, commando- en SQL-injectie leiden. • HTTP request voor alle invoermethodes zoals gespecificeerd in de ICT Beveiligingsrichtlijnen van NCSC moeten worden gevalideerd (testen op type, lengte, formaat en karakters van invoer en speciale tekens (bv. <, >, ', ", & , /, --, etc.). <u>Test aanpak:</u> Om deze beveiligingsrichtlijn volledig te testen is een source code review nodig. Er is echter niet gekozen voor een verplichte code review als onderdeel van de DigiD assessment. Een andere manier om dit te testen is bijvoorbeeld een penetratietest. Indien uit de test grote tekortkomingen naar voren komen wordt een code review wel aanbevolen. • Observeer het gedrag van de HTTP headers en responses. Voer hierbij een representatieve deelwaarneming uit op de invoer- en uitvoermogelijkheden die de applicatie biedt.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren. Doelstelling: Voorkom manipulatie van het systeem van andere gebruikers.	Applicatie	Betrokken rol(len): Applicatie- of SAAS-leverancier. Scope: De DigiD webapplicatie. Nadere toelichting: Als een webapplicatie onvoldoende controles uitvoert op de uitvoer die het terugstuurt naar de gebruiker, kan het gebeuren dat er zich onbedoelde of ongewenste inhoud in de uitvoer bevindt. Uitvoervalidatie voorkomt dat de webapplicatie ongewenste opdrachten geeft aan de client, bijvoorbeeld in het geval van XSS. • De webapplicatie codeert dynamische onderdelen in de uitvoer waarbij mogelijke gevaarlijke tekens (bv. <, >, ', ", & , /, --, etc.) worden genormaliseerd. Test aanpak: Om deze beveiligingsrichtlijn volledig te testen is een source code review nodig. Er is echter niet gekozen voor een verplichte code review als onderdeel van de DigiD assessment. Een andere manier om dit te testen is bijvoorbeeld een penetratietest. Indien uit de test

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			grote tekortkomingen naar voren komen wordt een code review wel aanbevolen. • Observeer het gedrag van de webapplicatie op voor wat betreft onveilige uitvoer. Voer hierbij een representatieve deelwaarneming uit op alle typen uitvoervelden van de applicatie.
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken. Doelstelling: Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.	Applicatie Infrastructuur Proces	Betrokken rol(len): • Applicatie-, hosting- of SAAS-leverancier. • Aansluithouder van de DigiD aansluiting. Scope: De DigiD webapplicatie en webserver en bijbehorende infrastructuur. Nadere toelichting: Deze norm raakt diverse aspecten van privacy bevorderende en cryptografische technieken. Dit betreft de classificatie van gegevens, de encryptie van gevoelige gegevens tijdens de opslag en de encryptie van gegevens tijdens transport. Aandachtspunten hierbij zijn: • De classificatie van gegevens door de houder van de DigiD aansluiting op basis van een risicoanalyse.

Bijlage 3 - Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• Mogelijke versleuteling of hashing van gevoelige gegevens. Het gaat hier in ieder geval om het BSN als bijzonder persoonsgegeven. Overigens geldt dit alleen voor gegevens die in dezelfde DMZ worden opgeslagen als waar de webapplicatie draait. Gegevens die in de backoffice worden opgeslagen vallen buiten de scope van dit onderzoek. • De HTTPS- en de TLS-configuratie. De publicatie in 2019 door het NCSC van de vernieuwde ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)v2 is aanleiding om de richtlijnen voor TLS aan te scherpen. Concreet dienen minimaal de TLS instellingen die het NCSC als 'Goed' of 'Voldoende' heeft aangemerkt te worden gebruikt. <u>Test aanpak:</u> • Inspecteer de classificatie van gegevens en daaraan gerelateerde risicoanalyse, de netwerkarchitectuur en het inrichtingsdocument waar de encryptie van gegevens in staat beschreven. • Observeer de encryptie van gegevens. Inspecteer de HTTPS- en TLS configuraties. • Interview de verantwoordelijke functionarissen.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen. Doelstelling: Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.	Applicatie	Betrokken rol(len): Applicatie-, hosting- of SAAS-leverancier. Scope: De webserver. Nadere toelichting: HTTP headers moeten de risico's beperken van inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie. Aandachtspunten hierbij zijn: • Behandel alleen HTTP-requests waarvan de gegevens een correct type, lengte, formaat, tekens en patronen hebben. • Behandel alleen HTTP-requests van initiators met een correcte authenticatie en autorisatie. • Sta alleen de voor de ondersteunde webapplicaties benodigde HTTP-requestmethoden (GET, POST, etc.) toe en blokkeer de overige niet noodzakelijke HTTP-requestmethoden. • Verstuur alleen HTTP-headers die voor het functioneren van HTTP van belang zijn.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• Toon in HTTP-headers alleen de hoogstnoodzakelijke informatie die voor het functioneren van belang is. • Bij het optreden van een fout wordt de informatie in een HTTP-response tot een minimum beperkt. Een eventuele foutmelding zegt wel dat er iets is fout gegaan, maar niet hoe het is fout gegaan. Test aanpak: • Observeer het gedrag van de HTTP-headers en responses. Voer hierbij een representatieve deelwaarneming uit op de invoer- en uitvoermogelijkheden die de applicatie biedt.
U/PW.03	De webserver is ingericht volgens een configuratie-baseline. Doelstelling: Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.	Applicatie infrastructuur	Betrokken rol(len): Hosting- of SAAS-leverancier. Scope: De webserver en andere servers in de DMZ. Nadere toelichting: Deze norm richt zich enerzijds op de aanwezigheid van een configuratie-baseline voor de webserver en op de feitelijke configuratie van de webserver. Aandachtspunten hierbij zijn:

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• Directory listings Te configureren waarde: Directory listings worden niet ondersteund. • Cookie flags Te configureren waarde: Cookies die sessie en/of persoonsgevoelige informatie bevatten, dienen de flags 'HttpOnly' en 'Secure' te bevatten. HTTP security headers bieden steeds meer en fijnmazigere controle over de toegang tot, en het delen van, informatie. Het correct gebruik van security headers levert een extra beveiligingslaag op: • X-Frame-Options & Frame-Ancestors De X-Frame-Options & de Frame-Ancestors headers voorkomen dat de pagina in een iFrame wordt geladen, waarmee gegevens kunnen worden gestolen, pagina's worden aangepast of gebruikers worden misleid. Frame-Ancestors vervangt de X-Frame-Options header. Met het doel zoveel mogelijk (versies van) browsers te ondersteunen dienen zowel de X-Frame-Options header als de Frame-Ancestors header aanwezig te zijn en onderling consistent te zijn geconfigureerd. Te configureren waarden:

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			– X-Frame-Options: deny & Frame-Ancestors: none – OF X-Frame-Options: sameorigin & Frame-Ancestors: self • Strict-Transport-Security (HSTS) HTTP Strict Transport Security (HSTS) zorgt ervoor dat browsers alleen over TLS communiceren met de webapplicatie. Door het forceren van HTTPS beschermt deze header gebruikers tegen afluisteren en Man-in-the-Middle (MitM)-aanvallen. HSTS voorkomt het gebruik van gemengde HTTP en HTTPS inhoud, beschermt tegen fouten van webservers zoals het laden van JavaScript via een onveilige verbinding en voorkomt dat gebruikers waarschuwingen over ongeldige certificaten kunnen negeren. Minimaal te configureren waarde: max-age=31536000 • X-Content-Type-Options De X-Content-Type-Options header voorkomt dat de browser het MIME-type van een bestand bepaalt op basis van kenmerken (sniffing). Wanneer deze header is ingesteld op nosniff, vertrouwt de browser

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			het MIME-type dat door de server wordt meegegeven en zal de browser de bron blokkeren als deze fout is. Dit voorkomt spoofing van resources zoals CSS stylesheets en Javascript-bestanden die over HTTP worden verstuurd. Te configureren waarde: nosniff • Content-Security-Policy De Content-Security-Policy (CSP) geeft de browser instructies over welke resources vanaf welke locatie mogen worden ingeladen en hoe deze mogen worden gebruikt. Een CSP kan fijnmazige instructies bevatten per soort resource, zoals afbeeldingen, stylesheets en scripts. Bij het gebruik van een CSP zijn standaard de uitvoering van inline scripts en de eval()-functie uitgeschakeld Te configureren waarden: default-src 'self'; frame-src 'self'; frame-ancestors 'self'; Sta geen onveilige configuratie toe door het gebruik van 'unsafe-inline' (tenzij gebruik wordt gemaakt van een nonce) en 'unsafe-eval'. Het is niet toegestaan bronnen beginnend met http:// te whitelisten. • Referrer-Policy

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			De Referrer-Policy beperkt het ongevraagd delen van privacygevoelige informatie bij het doen van verzoeken aan, en bij het doorsturen van de gebruiker naar, een andere website. Gebruik de instelling 'same-origin', zodat de referrer-header alleen wordt meegestuurd bij verzoeken binnen het eigen domein. Dit voorkomt het lekken van privacygevoelige informatie bij omleiden naar externe domeinen. De striktere instelling 'no-referrer' kan ook worden gebruikt, zodat de referrer-header nooit wordt meegestuurd. <u>Test aanpak:</u> • Observeer de mogelijk tot het maken van directory listings, de cookies flags. • Inspecteer de configuratie-baseline van de webserver m.b.t. X-Frame-Options, Strict-Transport-Security (HSTS), X-Content-Type-Options, Content-Security-Policy en Referrer-Policy. • Interview de verantwoordelijke functionarissen.
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie) protocollen voor het ontsluiten van beheermechanismen en	Infrastructuur Proces	<u>Betrokken rol(len):</u> • Hosting- of SAAS-leverancier.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	wordt uitgevoerd conform het operationeel beleid voor platformen. <u>Doelstelling:</u> Voorkomen van misbruik van beheervoorzieningen.		<u>Scope:</u> • De webserver en andere servers in de DMZ. <u>Nadere toelichting:</u> Dit betreft het gebruik van veilige netwerkprotocollen. Indien beheerinterfaces via het internet te benaderen zijn moet dit door middel van twee factor authenticatie, zoals de combinatie van een wachtwoord en source IP filtering, in combinatie met een veilig (communicatie) protocol worden afgehandeld. Er mag geen gebruik worden gemaakt van backdoors om de systemen te benaderen (ook niet voor noodtoegang). Daarnaast wordt een beknopt operationeel beleid verwacht. Aandachtspunten voor deze norm zijn: • Het gebruik van veilige protocollen (conform industrie standaarden) voor het benaderen van beheermechanismen (beheerinterfaces). • Het gebruik van sterke authenticatie voor zowel technisch als functioneel beheerders. <u>Test aanpak</u>: • Inspecteer het operationele beleid met betrekking tot het gebruik van beheervoorzieningen en de daarbij vereiste authenticatie.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• Observeer de protocollen die kunnen worden gebruikt voor het benaderen van beheerinterfaces en de authenticatiemethoden die daarbij worden afgedwongen. • Inspecteer de configuratie ten aanzien van de wachtwoordvereisten van de webserver en voor een deelwaarneming van minimaal één van de andere servers in de DMZ. • Interview de verantwoordelijke functionarissen.
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar. Doelstelling: Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS-leverancier. Scope: • De webserver en andere ICT-componenten binnen de DMZ. Nadere toelichting: Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar. Hierbij kan worden verwezen naar actuele hardening-richtlijnen van de leverancier(s)/SANS/NIST/CIS met een vermelding van “pas toe of leg uit”. Hierbij spelen de geïdentificeerde risico’s in de “pas toe of leg uit” afweging een

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			bepalende rol. Het gaat echter niet alleen om de hardeningsrichtlijn zelf, maar ook om het concreet toepassen ervan. De hardening van de DigiD webomgeving dient stringent te zijn geregeld: alles wat open staat moet een reden hebben en alles wat open staat moet secure worden aangeboden. De hardening van interne systemen mag minder stringent. Wel moeten de beheer functies secure zijn en mogen er geen onveilige protocollen worden gebruikt, moeten standaard wachtwoorden zijn gewijzigd. Voorbeeld applicaties moeten zijn verwijderd als deze niet daadwerkelijk worden gebruikt. Aandachtspunten hierbij zijn: • Inrichting van ICT-componenten (aantoonbaar) volgens de instructies en procedures van de leverancier. • Bijhouden van een actueel overzicht bij van de noodzakelijke protocollen, services en accounts voor de op het platform geïnstalleerde applicaties. • Deactiveren of verwijderen van alle protocollen, services en accounts op het platform als die niet volgens het ontwerp noodzakelijk zijn. • Periodiek toetsen of de in productie zijnde ICT-componenten niet meer dan de vanuit het ontwerp

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			noodzakelijke functies bieden (statusopname). Afwijkingen worden hersteld. Test aanpak: • Inspecteer de architectuur en hardening standaarden. • Inspecteer de configuratiebestanden en de uitkomsten van de penetratietest. • Interview de verantwoordelijke functionarissen.
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. Doelstelling: Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.	Infrastructuur	Betrokken rol(len): • Hosting- of SAAS-leverancier. Scope: • De DMZ van de DigiD webapplicatie. Nadere toelichting: DMZ en compartimentering d.m.v. (2 virtuele) firewalls. Deze eis zowel materieel (feitelijk bestaan en inrichting van DMZ) als formeel qua opzet (netwerkschema of tekening) beoordelen, eventueel op basis van een adequate beschrijving. Overigens zal de organisatie moeten aantonen dat zij voldoende inzicht heeft in de

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			architectuur, zowel van de DMZ als van de systemen die zich daarin bevinden. Test aanpak: • Inspecteer het netwerkarchitectuur schema inclusief de toegestane verkeersstromen tussen netwerksegmenten. • Inspectie van configuratie files, firewall regels en de uitkomsten van de penetratietest. • Interview de verantwoordelijke functionarissen.
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen. Doelstelling: Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	Infrastructuur	Betrokken rol(len): Hosting- of SAAS-leverancier. Scope: De DMZ van de DigiD webapplicatie. Nadere toelichting: Beveiligingsrichtlijnen U/NW.04, C.06 en C.07 hangen nauw met elkaar samen: - U/NW.04 richt zich op de implementatie en het gebruik van IDS/IPS. - C.06 richt zich op het tijdig signaleren van aanvallen.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			- C.07 richt zich op periodieke analyse van de logging. Inkomend en uitgaand verkeer moet worden gemonitord om mogelijke aanvallen tijdig te detecteren en hier acties op te kunnen ondernemen. Hiervoor zal de organisatie een Intrusion Detection Systeem (IDS) moeten implementeren. Aanbevolen wordt om tevens gebruik te maken van een Intrusion Prevention Systeem (IPS) dat automatisch preventieve maatregelen neemt tegen bedreigingen of een gecombineerde IDS/IPS. Het IDS of IPS dient geplaatst te worden **na** decryptie van het oorspronkelijk versleuteld netwerkverkeer omdat anders de inhoud van de berichten niet afdoende kan worden beoordeeld door het systeem. Een Web Application Firewall (WAF) kan dienen als alternatief voor de situatie dat een organisatie geen IPS heeft, bijvoorbeeld omdat men gebruik maakt van cloud webhosting. Aandachtpunten hierbij zijn: • Het gebruik van een IDS, IPS of WAF waarmee netwerkverkeer naar / van de DMZ van de DigiD webapplicatie wordt gemonitord.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• Een inrichtingsdocument en een beheerprocedure waarin is vastgelegd waar en hoe de IDS / IPS of WAF wordt ingezet. • Het gebruik van een adequate ruleset (b.v. Snort, Suricata, ETPro, etc.) die periodiek (= minimaal wekelijks) wordt geactualiseerd. <u>Test aanpak:</u> • Inspecteer het netwerkarchitectuur schema, de inrichtingsdocumentatie en de beheerprocedure van het IDS/IPS of WAF. • Inspecteer de configuratiefiles van het IDS/IPS of WAF en de signature datum van de regelset. • Interview de verantwoordelijke functionarissen.
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd. <u>Doelstelling:</u> Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	Infrastructuur Proces	<u>Betrokken rol(len):</u> Hosting- of SAAS-leverancier. <u>Scope:</u> Het netwerksegment met de webservers die een koppeling hebben met de DigiD omgeving van Logius inclusief de toegang vanuit internet.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			Nadere toelichting: Door middel van fysieke scheiding, veilige VPN verbindingen (zoals IPSec) of VLANs is het beheer- en productieverkeer van elkaar gescheiden. Deze beveiligingsrichtlijn is nauw verbonden met U/PW.05 omdat voor het beheer uitsluitend veilige netwerkprotocollen mogen worden gebruikt. Aandachtspunten hierbij zijn: • Er is een inrichtingsdocument waaruit blijkt op welke wijze content beheer (web- en database-content), applicatiebeheer en technisch beheer worden uitgeoefend. • Door het gebruik van fysieke scheiding, veilige VPN verbindingen (zoals IPSec) of VLANs is het beheer- en productieverkeer van elkaar gescheiden. Test aanpak: • Inspecteer het netwerkarchitectuurschema inclusief de toegestane verkeersstromen tussen netwerksegmenten. • Inspecteer de configuratie files, firewall regels en de uitkomsten van de penetratietest. • Interview de verantwoordelijke functionarissen.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar. Doelstelling: Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS-leverancier. • Aansluithouder van de DigiD aansluiting. Scope: De webserver en andere ICT-componenten binnen de DMZ. Nadere toelichting: Voor het configureren van netwerkcomponenten is een hardeningrichtlijn beschikbaar. Hierbij kan worden verwezen naar actuele hardening-richtlijnen van de leverancier(s)/SANS/NIST/CIS met een vermelding van “pas toe of leg uit”. Hierbij spelen de geïdentificeerde risico’s in de “pas toe of leg uit” afweging een bepalende rol. Het gaat echter niet alleen om de hardeningrichtlijn zelf, maar ook om het concreet toepassen ervan. De hardening van de DigiD omgeving dient stringent te zijn geregeld: alles wat open staat moet een reden hebben en alles wat open staat moet secure worden aangeboden. De hardening van interne systemen mag minder stringent. Wel moeten de beheer functies secure zijn en mogen er geen onveilige protocollen worden gebruikt, moeten standaard

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			wachtwoorden zijn gewijzigd. Voorbeeld applicaties moeten zijn verwijderd als deze niet daadwerkelijk worden gebruikt. Door de vitale rol die het Domain Name System speelt in het bereikbaar houden van webapplicaties, verdient de beveiliging van DNS-services extra aandacht. Onder deze beveiligingsrichtlijn valt dan ook het verplicht gebruik van DNSSEC (DNS Security Extensions) voor de URL van het object van onderzoek. Met DNSSEC wordt de authenticiteit van DNS-antwoorden geverifieerd om misbruik te voorkomen. Wanneer een aansluithouder gebruik maakt van een (cloud) dienstverlener zonder ondersteuning voor DNSSEC, zal DNSSEC via derden geregeld moeten worden. Aandachtspunten hierbij zijn: • Bijhouden van een actueel overzicht van de noodzakelijke netwerkprotocollen, -poorten en -services. • Uitschakelen van alle netwerkprotocollen, -poorten en -services op de netwerkcomponenten, behalve de noodzakelijke. • Aanpassen van de (beveiligings)configuraties van netwerkprotocollen, -poorten en -services op de netwerkcomponenten conform richtlijnen.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			Test aanpak: • Inspecteer het netwerkarchitectuurschema en de hardening-richtlijnen. • Inspecteer de configuratiebestanden en de uitkomsten van de penetratietest. • Interview de verantwoordelijke functionarissen.
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT- componenten van de webapplicatie (scope). Doelstelling: Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de webapplicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS-leverancier. Scope: • De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting: Deze netwerk based scan dient zich ten minste gericht te hebben op de resultaten van de hardening en patching van de infrastructuur en het detecteren van mogelijke kwetsbaarheden op de infrastructuur. Aandachtspunten hierbij zijn: • Vulnerability assessments vinden intern plaats, minimaal een keer per jaar en vaker op basis van een risicoafweging zoals bijvoorbeeld bij wijziging van de configuratie van de DMZ.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• De scope van het vulnerability assessment omvat tenminste de infrastructuur voor het netwerksegment met de DigiD webapplicatie. • Naar aanleiding van de resultaten van de vulnerability assessment is een actieplan opgesteld om de tekortkomingen op te heffen. • Er is voldoende voortgang geboekt in het opvolgen van bevindingen gezien de aard en complexiteit van de bevindingen. <u>Test aanpak</u>: • Inspecteer het netwerkarchitectuur schema en de opdracht tot het uitvoeren van vulnerability assessment. • Inspecteer het vulnerability assessment rapport, het actieplan naar aanleiding van de vulnerability assessment en het statusrapport met betrekking tot de bevindingen. • Interview de verantwoordelijke functionarissen.
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	Applicatie Infrastructuur Proces	<u>Betrokken rol(len)</u>: • Applicatie-, hosting- of SAAS-leverancier. <u>Scope</u>:

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	Doelstelling: Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).		• De DigiD webapplicatie, de webserver en andere servers in de DMZ van de DigiD webapplicatie. Nadere toelichting: De voorkeur heeft het op basis van een risicoafweging enkele keren per jaar een penetratietest te laten uitvoeren, zodat ingespeeld kan worden op nieuwe bedreigingen. Aandachtspunten hierbij zijn: • De penetratietest dient minimaal eenmaal per jaar te worden uitgevoerd en na significante wijzigingen, zoals vervanging applicatie, nieuwe versie, migratie webservers, database migratie, et cetera. • De scope van de penetratietest omvat tenminste de webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. • Naar aanleiding van de resultaten van de penetratietest is een actieplan opgesteld om de tekortkomingen op te heffen. • Er is voldoende voortgang geboekt in het opvolgen van bevindingen gezien de aard en complexiteit van de bevindingen. Zie ook Bijlage 5 van deze Handreiking (Toetsingscriteria penetratietesten)

Bijlage 3 - Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			Testaanpak: • Inspecteer het netwerkarchitectuur schema en de opdracht tot het uitvoeren van de penetratie test. • Inspecteer het penetratietest rapport, het actieplan naar aanleiding van de penetratietest en het statusrapport met betrekking tot de bevindingen. • Interview de verantwoordelijke functionarissen.
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. Doelstelling: Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	Infrastructuur Proces	Betrokken rol(len): Hosting- of SAAS-leverancier. Scope: De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting: Beveiligingsrichtlijnen NW.04, C.06 en C.07 hangen nauw met elkaar samen: - U/NW.04 richt zich op de implementatie en het gebruik van IDS/IPS. - C.06 richt zich op het tijdig signaleren van aanvallen.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			- C.07 richt zich op periodieke analyse van de logging. Hoewel deze richtlijn een brede reikwijdte heeft, is zij – in overleg met Logius – ingeperkt tot het detecteren van aanvallen met detectiesystemen in de webapplicatie-infrastructuur. Aandachtspunten hierbij zijn: • Het definiëren van alarm situaties en drempelwaarden. • Het configureren van de alarm situaties en drempelwaarden in het IDS/IPS en het genereren van de bijbehorende alerts. • De inbedding van alert afhandeling in het incidentenbeheerproces inclusief escalatieprocedure. <u>Test aanpak:</u> • Inspectie van de Use Cases en drempelwaarden. • Inspectie van alerts en de opvolging daarvan. • Interview de verantwoordelijke functionarissen.
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-	Infrastructuur Proces	<u>Betrokken rol(len):</u> Hosting- of SAAS-leverancier.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd. Doelstelling: Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.		Scope: De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting: Beveiligingsrichtlijnen NW.04, C.06 en C.07 hangen nauw met elkaar samen: - U/NW.04 richt zich op de implementatie en het gebruik van IDS/IPS. - C.06 richt zich op het tijdig signaleren van aanvallen. - C.07 richt zich op periodieke analyse van de logging. De logging- en detectie-informatie en de conditie van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd. Aandachtpunten hierbij zijn: • Procedurebeschrijving met daarin beschreven op welke wijze en wanneer controles op logging moeten plaatsvinden en hoe taken op dit gebied belegd zijn. • Het uitvoeren van periodieke controles op:

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			○ wijzigingen aan de configuratie van webapplicaties; ○ optreden van verdachte gebeurtenissen en eventuele schendingen van de beveiligingseisen; ○ ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden; ○ toegangslogs. • Periodieke analyse op ongebruikelijke situaties (incidenten) die de werking van webapplicaties kunnen beïnvloeden. • Periodieke rapportage van de geanalyseerde en beoordeelde gelogde gegevens aan de systeemeigenaren en/of aan het management. • Opvolging van bevindingen naar aanleiding van de analyse. <u>Test aanpak:</u> • Inspectie van de procedurebeschrijving met betrekking tot de logging. • Inspectie van de vastlegging van de periodiek review van de logging, periodieke rapportage aan het management en follow-up acties naar aanleiding van review en analyse van de logging.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• Interview de verantwoordelijke functionarissen.
C.08	Wijzigingsbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd. Doelstelling: Zeker stellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.	Applicatie Infrastructuur Proces	<u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS-leverancier. • Aansluithouder van DigiD aansluiting. <u>Scope:</u> De DigiD webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. <u>Nadere toelichting:</u> De focus ligt op het vaststellen dat het proces wijzigingsbeheer zodanig is opgezet en geïmplementeerd dat alle wijzigingen altijd eerst worden getest voordat deze in productie worden genomen en via wijzigingsbeheer worden doorgevoerd. In sommige gevallen kunnen formulieren worden gebouwd die beveiligingsrisico's introduceren en valt wijzigingenbeheer met betrekking tot formulieren wel in scope van de DigiD-assessment. Is dit niet het geval dan valt wijzigingenbeheer met betrekking tot formulieren niet in scope. Welke specifieke situatie zich voordoet hangt af van de applicatie (formulierengenerator) en de wijze waarop deze wordt

Bijlage 3 - Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			gebruikt. Het is aan de auditor om te bepalen of er aanleiding is om wijzigingenbeheer ten aanzien van de formulieren in de DigiD-scope op te nemen. Ingeval van SAAS-toepassingen ligt de verantwoordelijkheid voor het testen van wijzigingen aan de applicatie doorgaans bij de leverancier en/of gebruikersgroep. Aandachtspunten hierbij zijn: • Wijzigingsbeheer procedure, waarbij zo nodig onderscheid wordt gemaakt tussen wijzigingen op de applicatie, de servers en de netwerkcomponenten. • Het inrichten van een OTAP-omgeving zodat wijzigingen eerst in een testomgeving worden getest voordat zij in productie kunnen worden genomen (n.b. voor netwerkwijzigingen is een testomgeving vaak niet mogelijk). • Het hanteren van een testscript en de vastlegging van de testresultaten. • Een formele acceptatie voor het in productie nemen van de wijziging. • Het beperken van het aantal personen die wijzigingen in productie kunnen nemen. • Bij het uitbrengen van een nieuwe release van de applicatie of een grote upgrade van het

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			onderliggende platform moet, bij voorkeur door middel van een penetratietest, worden onderzocht of er geen nieuwe kwetsbaarheden zijn geïntroduceerd. <u>Test aanpak:</u> • Inspecteer de wijzigingsprocedure en de inrichting van de OTAP-omgeving. • Inspecteer voor elk type wijziging (applicatie, servers, netwerk), één wijziging en de daaraan gerelateerde documentatie. • Interview de verantwoordelijke functionarissen. <u>Nonoccurrence (voor het onderdeel inspecteren van een doorgevoerde wijziging):</u> Hierbij geldt dat op basis van (deel)waarnemingen binnen een proces dat onderworpen is aan dezelfde control vastgesteld moet worden dat de wijzigingsprocedure effectief is geïmplementeerd.
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste	Applicatie Infrastructuur Proces	<u>Betrokken rol(len):</u> Applicatie-,Hosting- of SAAS-leverancier. <u>Scope:</u>

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	(beveiligings)patches tijdig zijn geïnstalleerd in de ICT-voorzieningen. <u>Doelstelling:</u> Zeker stellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.		• Hypervisor (VM Ware, etc.). • Operating system (Windows, etc.). • Databases. • Netwerk componenten. • Firewall. • Webapplicatie en daarvoor benodigde software componenten. <u>Nadere toelichting:</u> De focus is op het patching proces. Dit proces kan gedifferentieerd zijn naar bijvoorbeeld het OS, DBMS en netwerk. Applicaties en systemen dienen periodiek gepatcht te worden. Een maandelijks patching cyclus is aanvaardbaar tenzij er security alerts zijn. Voor internet facing systemen dienen de laatste stabiele beveiligingspatches te zijn geïnstalleerd. Indien patching niet mogelijk is in verband met een legacy applicatie die niet meer zou functioneren na patching, zal dit risico aantoonbaar moeten zijn afgewogen. Aandachtpunten hierbij zijn: • Het beschrijven van patchmanagementbeleid waarin is aangegeven hoe de organisatie omgaat met updates: hoe snel implementeert de organisatie een

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			kritieke patch en welke stadia moet de patch doorlopen. • Registratie van patches met vastlegging of de patches niet, wel of versneld worden doorgevoerd. • Het tijdig doorvoeren van patches. <u>Test aanpak</u>: • Inspectie van het patchmanagementbeleid. • Inspectie van de registratie van patches. • Stel vast dat het patchmanagementbeleid conform de beschreven periodiciteit wordt uitgevoerd. • Inspecteer de uitkomsten van de penetratietest op de aanwezigheid van (bekende) beveiligingsissues waarvoor een patch beschikbaar is. • Interview de verantwoordelijke functionarissen.

Bijlage 4 – Aanvullende Guidance bij Meervoudige Aansluiting (MA)

De in deze bijlage beschreven testaanpak maakt het mogelijk om een DigiD assessment MA uit te voeren. Het merendeel van de testaanpak is gelijk aan die van een regulier DigiD Assessment. Alleen voor de normen B.01, B.05, U/TV.01, U/WA.05, U/NW.06 en C.08 is de reguliere DigiD testaanpak aangevuld op basis van de uitgangspunten van Logius voor een DigiD assessment MA.

Deze bijlage 4 bevat uitsluitend de aanvullende testaanpak m.b.t. het DigiD assessment MA. Hieruit volgt dat de IT-auditor bij het uitvoeren van een DigiD assessment MA zowel de in Bijlage 3 als de in Bijlage 4 beschreven nadere toelichting en testaanpak dient te volgen.

Bijlage 4 – Aanvullende Guidance bij Meervoudige Aansluiting (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudige Aansluiting)
B.01	De organisatie formuleert een informatie-beveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatie-gerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer. Doelstelling:	Governance	Betrokken rol(len): • Leverancier Meervoudige Aansluiting (LMA). Nadere toelichting: Belangrijk verschil t.o.v. een 'regulier' DigiD assessment is dat de LMA kan worden gezien als vertegenwoordiger van de Aansluithouders Meervoudige Aansluiting (AMA) en dat derhalve het eigenaarschap binnen de organisatie van de LMA zal moeten worden ingericht.

Bijlage 4 – Aanvullende Guidance bij Meervoudige Aansluiting (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudige Aansluiting)
	Het zorgen voor specifieke management aandacht in het beveiligingsproces voor de webapplicaties van de organisatie.		Test aanpak: • Stel vast dat de LMA het eigenaarschap t.a.v.de DigiD webapplicatie adequaat op een hoog organisatorisch niveau heeft ingericht en dat de eigenaar passende bevoegdheden heeft. • Stel vast dat in het informatiebeveiligingsbeleid, of in een hiervoor apart ontwikkeld beleid, expliciet aandacht is besteed aan het stelsel van beveiligingsmaatregelen t.a.v. webapplicaties en/of de infrastructuren voor de netwerksegmenten met webapplicaties in het algemeen, en DigiD en andere authenticatie- en identificatiediensten in het bijzonder. • Stel vast dat dataclassificatie (zie U/WA.05), toegangsvoorziening (zie U/TV.01) en kwetsbaarhedenbeheer (zie U/PW.07, U/NW.06, C.03 en C.09) zijn geadresseerd en er aandacht is geschonken aan de specifieke rolverdeling tussen LMA en de houder. • Stel vast dat het informatiebeveiligingsbeleid door het verantwoordelijk hoger management van de LMA is vastgesteld en actief wordt uitgedragen, alsmede

Bijlage 4 – Aanvullende Guidance bij Meervoudige Aansluiting (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudige Aansluiting)
			bekend is bij functionarissen betrokken bij webapplicatie gerelateerde onderwerpen. • Stel vast dat zowel het verantwoordelijk hoger management van de LMA als de houder periodiek rapportages ontvangt inzake informatiebeveiliging en indien nodig hierop acteert. • Stel vast dat het informatiebeveiligingsbeleid wordt geüpdatet conform de beleidscyclus van de LMA, doch minimaal eens in de 5 jaar. Bij (tussentijdse) grote wijzigingen dient het informatiebeveiligingsbeleid te worden geactualiseerd.
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>Doelstelling:</u> Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de		<u>Betrokken rol(len):</u> • Leverancier Meervoudige Aansluiting (LMA). <u>Nadere Toelichting</u>: • De LMA is door Logius geregistreerd als aanbieder van een Meervoudige Aansluiting. • Beschrijving van verantwoordelijkheidsverdeling in het contract tussen LMA en houder. • De onder de meervoudig aansluiting geleverde dienstverlening betreft, conform de eisen van

Bijlage 4 – Aanvullende Guidance bij Meervoudige Aansluiting (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudige Aansluiting)
	ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.		Logius, een SaaS-oplossing waarbij de houders van DigiD aansluitingen als afnemer van de dienst een voldoende homogene doelgroep vormen die onder een gelijke wettelijke bepaling gerechtigd zijn het BSN te verwerken. Initieel stelt Logius dit vast als onderdeel van de accreditatie. Tijdens de DigiD assessment toont de LMA aan de auditor aan dat de dienstverlening nog steeds aan de uitgangspunten voor een Meervoudige Aansluiting voldoet. • Bepaling in contract dat een houder wordt afgesloten van de dienstverlening door de LMA als deze de noodzakelijke beheersingsmaatregelen t.b.v. het DigiD assessment niet naleeft. • De houder accepteert de gegevensclassificatie zoals opgesteld door de LMA. • De LMA verantwoordt zich jaarlijks schriftelijk aan de houders over (veranderingen in) gegevensclassificatie en de naleving van gerelateerde maatregelen. <u>Testaanpak</u>: • Onderzoek onder nadere toelichting genoemde aanvullende punten.

Bijlage 4 – Aanvullende Guidance bij Meervoudige Aansluiting (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudige Aansluiting)
			Nonoccurrence: (voor het onderdeel schriftelijke verantwoording gegevensclassificatie door LMA): • T.a.v. schriftelijke verantwoording gegevensclassificatie door LMA aan houders kan bij het initiële assessment de situatie zicht voordoen dat verantwoording nog niet heeft plaatsgevonden, terwijl dit contractueel wel is overeengekomen. In dit geval kan indien de opzet voldoet aan de norm een non occurrence worden gemeld middels een opmerking in de toelichtende paragraaf zoals beschreven onder 'Context en toelichting'.
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 de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.	Applicatie Infrastructuur Proces	Betrokken rol(len): • Leverancier Meervoudige Aansluiting (LMA). Nadere toelichting: • Indien houders toegang hebben tot de applicatie zijn onderstaande zaken van toepassing. • Houders hebben uitsluitend op applicatieniveau toegang tot data. • Wachtwoordinstellingen worden centraal door de LMA beheerd voor de SaaS-oplossing als geheel en

Bijlage 4 – Aanvullende Guidance bij Meervoudige Aansluiting (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudige Aansluiting)
	Doelstelling: Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit.		hebben voldoende sterke instellingen. Wijzigingen in deze instellingen worden vastgelegd in een audittrail (bewaartermijn 7 jaar) • Voor houders wordt het toekennen, controleren en intrekken van autorisaties binnen de applicatie ondersteund en hiervan is een audittrail aanwezig (bewaartermijn 7 jaar). Dit is alleen van toepassing als een houder vanuit functionaliteit toegang heeft tot de applicatie, bijvoorbeeld om mee te kunnen kijken met een burger. • Per houder wordt door een 'power user' een aantoonbare controle op joiners/movers/leavers verplicht 3-maandelijks uitgevoerd als onderdeel van de functionaliteit van de applicatie. Ook hiervan wordt een audittrail bijgehouden. Een kwaliteitsfunctionaris van de LMA bewaakt dit proces. Eventueel kan de LMA er voor kiezen een houder te blokkeren zolang deze verplichte controle niet is uitgevoerd. Voor het assessment is per jaar een samenvattende rapportage beschikbaar. • Technische maatregelen zijn ingericht t.b.v. het correcte gebruik van gebruikersaccounts van de houder: automatisch blokkeren van

Bijlage 4 – Aanvullende Guidance bij Meervoudige Aansluiting (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudige Aansluiting)
			gebruikersaccounts na 6 weken niet gebruik en blokkade van gebruik van een gebruikersaccount door meerdere personen voor zover dit laatste technisch mogelijk is.
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken. Doelstelling: Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie	Applicatie Infrastructuur Proces	Betrokken rol(len): • Leverancier Meervoudige Aansluiting (LMA). Nadere toelichting: In afwijking van een regulier assessment waarbij de houder van de DigiD aansluiting op basis van een risicoanalyse een gegevensclassificatie uitvoert: • De LMA onderhoudt jaarlijks een schriftelijke classificatie van de gegevens. Aan deze classificatie ligt een risicoanalyse en 'legal opinion' van een ter zake kundige medewerker ten grondslag. De wettelijke bepaling op basis waarvan de houders gerechtigd zijn het BSN te verwerken vormt bij deze 'legal opinion' het uitgangspunt. Testaanpak: • Onderzoek onder nadere toelichting genoemde aanvullende punten.

Bijlage 4 – Aanvullende Guidance bij Meervoudige Aansluiting (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudige Aansluiting)
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar. Doelstelling: Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	Infrastructuur Proces	Betrokken rol(len): • Leverancier Meervoudige Aansluiting (LMA). Nadere toelichting: • De LMA heeft een monitoringsoplossing ingericht waarmee maandelijks wordt vastgesteld dat voor de domeinnamen van alle houders DNSSEC correct is geconfigureerd. In geval een nieuwe houder aan de Meervoudige Aansluiting wordt toegevoegd zal deze controle direct plaatsvinden. Hierna gaat deze mee in de maandelijkse cyclus. • Voor het DigiD assessment is jaarlijks een rapportage beschikbaar met de data van de monitoringsoplossing. Testaanpak: • Onderzoek onder nadere toelichting genoemde aanvullende punten.
C.08	Wijzigingsbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van	Applicatie Infrastructuur Proces	Betrokken rol(len): • Leverancier Meervoudige Aansluiting (LMA). Nadere toelichting:

Bijlage 4 – Aanvullende Guidance bij Meervoudige Aansluiting (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudige Aansluiting)
	webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd. Doelstelling: Zeker stellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.		• De houders hebben op operationeel en tactisch niveau geen betrokkenheid bij het wijzigingenproces. Dit sluit niet uit dat er een vertegenwoordigende groep van houders is die bijvoorbeeld met de leverancier de doorontwikkeling van de applicatie bespreekt. <u>Testaanpak:</u> • Onderzoek onder nadere toelichting genoemde aanvullende punten.

Bijlage 5 – Toetsingscriteria penetratietesten

In deze bijlage zijn de (procesmatig, organisatorisch en inhoudelijk) te stellen kwaliteitseisen aan de DigiD penetratietest beschreven.

Algemeen

Het uitvoeren van pentratietest wordt in norm C.04 verplicht gesteld (*Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope)*).

Naast het voldoen aan norm C.04 wordt een penetratietest ook vaak gebruikt om vast te stellen of aan andere DigiD normen wordt voldaan. Te denken valt hierbij aan:

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 privacy bevorderende 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.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar.
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT-voorzieningen.

Voor wat betreft de penetratietest zijn er twee varianten:

1. De penetratietest wordt uitgevoerd als een mogelijk controlemiddel van de IT-auditor en onder diens verantwoordelijkheid. In dit geval dienen de

penetratietest, de documentatie en de rapportage aan de kwaliteitsstandaarden van NOREA te voldoen omdat de pentester immers deelneemt aan het controleteam en de bevindingen worden gebruikt voor de beoordeling en conclusies ten aanzien van bepaalde DigiD normen.

2. De penetratietest wordt uitgevoerd op verzoek van de klant, als controlemiddel van de klant (in lijn met 3000A), mede bedoeld om te voldoen aan norm C.04. In dit geval hoeft de pentest, de documentatie en de rapportage alleen te voldoen aan de kwaliteitsstandaarden van NOREA en de in deze bijlage beschreven Toetsingscriteria penetratietesten in de gevallen dat de IT-auditor deze pentest gebruikt voor zijn bevindingen. Als deze pentest 'alleen' in het licht van C.04 is uitgevoerd, dient de IT-auditor deze te beoordelen op basis van de in norm C.04 beschreven criteria en testaanpak.

In alle gevallen dat de pentest, wordt gebruikt voor de beoordeling en conclusies ten aanzien van bepaalde DigiD normen, zijn de volgende aandachtspunten van belang:

- Er dient zowel bewijs te worden verzameld en gedocumenteerd ten aanzien van de normelementen die niet voldoen, als ten aanzien van de normelementen die wel voldoen.
- Ten behoeve van de navolgbaarheid dient het pentestrapport beschrijvingen te bevatten met betrekking tot de gehanteerde scope, de uitgevoerde testen, testmethodieken en de gebruikte tooling.
- Doordat de IT-auditor feitelijk een uitspraak doet over de productieomgeving, is het noodzakelijk dat belangrijke onderdelen van de pentest zijn gericht op deze omgeving. Indien dat echt niet mogelijk is, dient de IT-auditor de bevindingen die gedaan zijn in de acceptatieomgeving te verifiëren op de productieomgeving (bijvoorbeeld door het inspecteren van de webconfiguratie, de instellingen van cryptografische technieken, etc.)

Organisatorisch

- De pentester staat onafhankelijk ten opzichte van het te onderzoeken object.
- De pentester heeft aantoonbare ervaring met het uitvoeren van pentesten, bij voorkeur met pentesten i.h.k.v. DigiD.
- Opdrachtgever ondertekent een zgn. 'instemmings- en vrijwaringsverklaring' (denk hierbij ook aan evt. betrokken derden zoals hosting partij).
- Beschikbaarheid van pentesters en beheerders bij de onderzochte organisatie wordt overeengekomen.
- Afspraken worden gemaakt over communicatie tussen pentesters en contactpersonen bij de opdrachtgevende organisatie.

- Doorlooptijd en budget wordt overeengekomen.

Scope en normstelling

- Vastgesteld object van het onderzoek relevant voor DigiD.
- Vastgesteld normenkader (DigiD-subset uit de NCSC normen, eventueel aangevuld met OWASP top 10, WASC criteria, GHDB en leveranciers-specifieke normen en baselines).
- Voor DigiD audit is een greybox benadering, waarbij zonder veel voorkennis ingelogd wordt als gebruiker, voldoende.
- Vaststellen met welke functionele scope de volledige technische oplossing wordt afgedekt (bijvoorbeeld een selectie van formulieren waarmee alle componenten worden geraakt), waarbij wordt aangetoond dat de technische oplossing adequaat wordt getest).
- Maatwerk formulieren die niet op basis standaard configuratie functionaliteit zijn ontwikkeld altijd testen.
- Indien standaardformulieren worden gebruikt, waarbij alleen functionele aanpassingen doorgevoerd kunnen worden, kan volstaan worden met vaststellen van de betrouwbare werking van de formulierengenerator (o.b.v. de TPM van de serviceprovider).

Verkenningsfase (vaststellen ingangscriteria)

- Inventarisatie gebruikte (webfacing) infrastructuur, applicaties, componenten, e.d..
- Opdrachtgever toont aan dat de technische inrichting van testomgeving gelijk is aan productie omgeving.
- Testomgevingen met representatieve testgegevens zijn beschikbaar.
- DigiD testaccounts zijn beschikbaar en gekoppeld aan testgegevens, evt. gekoppeld aan mobiele nummers pentesters.
- Pentester(s) zijn bekend met de werking van de applicatie.
- Contactpersonen bij de opdrachtgever zijn bekend met de werking van de applicatie.

Initiële kwetsbaarheden analyse

- Fingerprinting van het object: vaststellen gebruikte merken en versies.
- Inventariseren bekende kwetsbaarheden op basis van publicaties van leveranciers en openbare cybersecurity bronnen.
- Selectie van tests voor aantonen van de mogelijke kwetsbaarheden.

Geautomatiseerde tests (dynamisch testen)

- Keuze geschikte pentest tools en hun dekkingsgraad van het te testen object (niet ieder pentest tool ondersteunt alle technologieën, denk aan AJAX, Silverlight, Java en dergelijke).
- Inzicht in het deel van de norm dat door de tool(s) wordt afgedekt en welk deel afzonderlijk (handmatig) zal moeten worden getest.
- Doorlopende bewaking door de pentester tijdens de uitvoering om schade te voorkomen, bij voorkeur automatisch afbreken van geautomatiseerde testen bij foutmeldingen waaruit een kritiek probleem blijkt.

Handmatige tests

- Adequate expertise van de pentester(s), eventueel aanwezige certificeringen ter onderbouwing; aantoonbare kennis/ervaring met gebruikte technologieën.
- Technische details van gecontroleerde SSL-certificaten en SSL-versleutelde verbindingen.
- Details van gecontroleerde cookies en volledige dekking tijdens de testen.
- Alle bevindingen uit de geautomatiseerde testen zijn handmatig geverifieerd.
- Op basis van bevindingen uit de geautomatiseerde testen zijn handmatige vervolgtesten uitgevoerd.
- Kwetsbaarheden in functionele flows zijn handmatig onderzocht, bijvoorbeeld manipulatie van velden bij meerstaps-formulieren.`

Optioneel: Code review (statisch testen) afhankelijk van de norm

- In principe kunnen alle normen getest worden op basis van het bepalen van het gedrag van de applicatie. Bij twijfel over het gedrag alsnog een code review uitvoeren.
- Dekkingsgraad van de review bepalen (steekproef, volledig, ..).
- Aantoonbare ervaring van de pentester(s) met de programmeertaal en omgeving, eventueel beschikbare certificeringen ter onderbouwing.
- Bij gebruik van tools voor statische testen: dekkingsgraad ten opzichte van de norm.

Rapportage

- Conceptrapportage
    - Classificatie van de rapportage conform DigiD norm, beleid opdrachtgever en auditor en eventueel naar publieke standaarden.
    - Beschrijving object van het onderzoek: webfacing infrastructuur, servers, verbindingen.

    - Indien van toepassing: overzicht van onderdelen die niet of onvoldoende getest konden worden.
    - Overzicht afwijkingen ten opzichte van de norm met bijbehorende mate van risico obv norm en na risicoanalyse.
    - Overzicht en details resultaten en afwijkingen per onderdeel uit de norm.
    - Proof of Concepts of details in rapportage waarmee de bevinding kan worden gereproduceerd.
    - Concrete aanbevelingen per bevinding.
    - Overzicht van de gebruikte pentest tools.
- Afstemming met auditor
    - Versleuteld, beveiligde uitwisseling met de auditor.
    - Controle op volledigheid en consistentie.
    - Controle of met de verkregen diepgang tijdens de testen de norm is afgedekt.
- Melden kritieke bevindingen aan opdrachtgever indien deze naar verwachting in een productieomgeving aanwezig zijn.
    - In overleg met de auditor melden.
    - Proof of Concept of stappen om te reproduceren.
    - Versleutelde, beveiligde uitwisseling details van de kwetsbaarheid.
- Afstemming met opdrachtgever
    - Versleuteld, beveiligde uitwisseling met de auditor.
    - Afstemming over planning van oplossing en hertesten van bevindingen.
- Definitieve rapportage
    - Versleuteld, beveiligde uitwisseling met de opdrachtgever.
    - Bevindingen waarvoor een hertest is uitgevoerd zijn als zodanig opgenomen in het rapport met de uitkomst van de hertest (tbv traceerbaarheid).
- Archiveren rapportage
    - Indien van toepassing: archivering in een afgeschermde omgeving met passende beveiligingsmaatregelen.

Periodiciteit

- Alleen een pentest laten uitvoeren ten tijde van de DigiD audit is minimaal. De voorkeur heeft het dit twee- of meerdere keren per jaar te laten doen, zodat ingespeeld kan worden op nieuwe bedreigingen.

- Bij het uitbrengen van een nieuwe release van de applicatie of een grote upgrade van het onderliggende platform is het wenselijk een pentest te laten uitvoeren.