NOREA Handreiking ICT-beveiligingsassessment DigiD Versie 2024

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

1.0 – Definitief

17 juni 2024

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 assurance-rapport op te stellen in lijn met de regelgeving rondom het ICT-beveiligingsassessment DigiD.

Deelnemers werkgroep

De volgende personen hebben namens de NOREA werkgroep DigiD-assessments een bijdrage aan deze handreiking geleverd:

Gerben Bergwerff MSc RE CISSP, drs. Wilfred Hanekamp RE, drs. Rene IJpelaar RE CISA CIPP/e, drs. Joep Janssen RE MIM, Frank Kossen RE, ir. Peter Kornelisse RE CISA, Jacko Möhle MSc RE

Coördinatie en redactie versie 2024:

Frank Kossen RE, drs. Rene IJpelaar RE CISA CIPP/e, Jacko Möhle MSc RE

Versiebeheer NOREA Handreiking ICT-beveiligingsassessment DigiD 2024		
Versie	**Datum**	**Wijzigingen**
0.99	17 mei 2024	Final draft versie voor consultatieronde werkgroep DigiD, Vaktechnische Commissie en Logius
1.0	17 juni 2024	Definitief
Belangrijkste wijzigingen in deze versie		
1. Guidance t.a.v. verplichte toetsing op werking vanaf inleverperiode 1 januari – 1 mei 2025 (Paragaaf 2.2 en Bijlage 3)		
2. Frequently Asked Questions (FAQ) versie: 4.0 d.d. 24 april 2024 opgenomen		
3. Consultatieverplichting bij afwijken van de Handreiking/Formats		
4. Bijlage 3 (beheersingsmaatregelen opzet en bestaan) en Bijlage 4 (beheersingsmaatregelen werking) zijn samengevoegd		
5. Aangepaste rapportage templates naar aanleiding van de verplichte toets op werking.		

Postbus 242 2130 AE Hoofddorp
Frame Offices - Pharos Mercuriusplein 3 - 1e verdieping 2132 HA Hoofddorp
Tel: 088-4960380
e-mail: norea@norea.nl
www.norea.nl

Inhoud

1 Inleiding

1.1 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 Binnenlandse Zaken en Koninkrijksrelaties (BZK) aan de Tweede Kamer 'Lekken in een aantal gemeentelijke websites' d.d. 11 oktober 2011 met kenmerk 2011-2000454268[1]. 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 IT-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 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 Handreiking 2024 treedt in werking op 1 juli 2024 en vervangt versie 4.0 (17 juli 2023). In versie 2024 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 de FAQ van 24 april 2024 zijn de Frequenly Asked Questions in deze Handreiking verwerkt. Ten opzichte van de

[1] Kamerstuk 26643, nr. 193 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)

Handreiking 4.0, is in deze Handreiking 2024 de (verplichte) toets op werking opgenomen vanaf inleverperiode 1 januari – 1 mei 2025.

Voor deze Handreiking en de bijbehorende normenkaders geldt als uitgangspunt dat de beschreven auditwerkzaamheden zijn gebaseerd op de richtlijnen van BZK[2].

Aanvullend op het volgen van de NOREA-richtlijnen zijn voor de uitvoering van DigiD-assessments aanvullende voorwaarden gesteld door de stelselhouder van DigiD. De IT-auditor wordt door de stelselhouder verplicht om de regels, templates, formuleringen en voorwaarden zoals opgenomen in deze handreiking, FAQ's[3] en rapportage templates te volgen. Afwijkingen hierop zijn mogelijk, maar dienen door de IT-auditor conform de consultatieverplichting zoals beschreven in paragraaf 2.12 te worden behandeld. Feedback op de beschikbaar gestelde materialen kan worden gedeeld met de NOREA Digid Werkgroep via norea@norea.nl.

1.2.1 Object en scope van onderzoek

Het perspectief van de burger die inlogt met DigiD en zijn verwachting dat hetgeen daarmee 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 als deze is geïdentificeerd en geauthentiseerd via DigiD, de systeemkoppelingen en de infrastructuur die met DigiD gekoppeld is en betrekking heeft op het DigiD identificatie en authenticatieproces. Ook de verschillende vormen van beheer op de 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 BZK vertrouwelijkheid 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

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

[3] Zie sectie publicaties op website NOREA | Werkgroep DigiD-assessments

overheid veel meer schaden dan het niet voldoende beschikbaar zijn van het systeem. Zeker voor de grote diensten die gebruik maken van DigiD 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 ICT-beveiligingsassessments DigiD is bedoeld voor organisaties die DigiD gebruiken en jaarlijks een ICT-beveiligingsassessment moeten doen. De norm is een selectie van richtlijnen uit het document 'ICT-beveiligingsrichtlijnen voor webapplicaties' van het Nationaal Cyber Security Centrum (NCSC). De norm is vastgesteld door BZK in overleg met Logius, AuditDienst Rijk en het NCSC. De Norm versie 3.0 geldt voor assessments vanaf 1 augustus 2022 en verder.

1.3 Governance DigiD

1.3.1 Context DigiD stelsel

DigiD is het veilig en betrouwbare middel waarmee burgers zich digitaal kunnen authenticeren. 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. Het Ministerie van BZK is stelsel beheerder en daarmee verantwoordelijk voor het beleid rondom DigiD.

1.3.2 Beheer

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

1.3.3 Overeenkomst

Totdat in de uitvoeringsregelgeving behorende bij de Wet Digitale Overheid (Wdo) anders is bepaald, sluiten aansluithouders die DigiD afnemen een privaatrechtelijke overeenkomst af met Logius. Het aantonen dat de online-diensten conform zijn met het DigiD normenkader is onderdeel van zowel de Wdo als de overeenkomst. Aansluithouders laten op basis van het normenkader jaarlijks een assessment uitvoeren door een IT-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 IT-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 de DigiD assessments 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 onder verantwoordelijkheid van RE's uitgevoerd in het kader van het stramien voor Assurance-opdrachten en overeenkomstig Richtlijn 3000D[4] 'Assurance-opdrachten'. In afwijking hierop wordt voor de DigiD-beveiligingsassessments bij gemeenten, die vallen onder ENSIA, richtlijn 3000A gehanteerd. Zie hiervoor de ENSIA Handreiking voor IT-auditors.

Zowel voor het assessment bij de aansluithouder van DigiD als bij de serviceorganisatie zijn modelrapporten opgesteld. Deze zijn afzonderlijk door NOREA gepubliceerd. Benadrukt wordt dat de IT-auditor strikt de structuur en inhoud van de modelrapporten dient te volgen en uiterst zorgvuldig de juistheid en volledigheid van de identificerende gegevens van het object van onderzoek en gehanteerde assurance-rapporten van derden moet bepalen.

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, het bestaan en/of de werking 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 individuele beveiligingsrichtlijn. Dit is expliciet in de tekst van de Modelrapporten opgenomen.

Het rapport wordt uitsluitend verstrekt ten behoeve van de betreffende aansluithouder en Logius, en (indien van toepassing) de serviceorganisatie. De reden hiervoor is dat anderen, die niet op de hoogte zijn van de precieze scope, aard en doel van de werkzaamheden, de resultaten onjuist kunnen interpreteren.

[4] Een 'directe opdracht' is de wens/eis van de toezichthouder Logius ten behoeve van consistentie van de te ontvangen assurance-rapporten.

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 B.05, U/TV.01, U/WA.02 en C.08 is in de testaanpak aangegeven op grond van welke werkzaamheden c.q. (deel)waarnemingen de auditor tot een oordeel 'Voldoet' kan komen voor de bestaanscontrole met een voorgeschreven verwijzing bij het oordeel (zie ook paragraaf 2.5).

2.2 Toetsing op werking

Het DigiD assessment beperkte zich tot nu toe tot het beoordelen van de opzet en het toetsen van het bestaan van de beheersingsmaatregelen. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft in 2022 besloten dat voor een aantal normen de werking zal worden getoetst. Met het besluit van BZK wordt 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.**

Bij nieuwe aansluitingen is bij het eerste (initiële) assessment de toetsing op werking niet verplicht. Indien gebruik wordt gemaakt van een serviceorganisatie die is getoetst op werking kan het rapport ook worden gebruikt indien de organisatie van de aansluithouder niet wordt getoetst op werking.

Indien de auditor tot het oordeel komt dat de werking niet voldoet, dient, indien mogelijk, het bestaan te worden vastgesteld met een deelwaarneming van tenminste één.

2.2.1 Controleperiode

De controleperiode voor de inleverperiode 1 januari – 1 mei 2025 is door Logius bepaald op 6 maanden. Dit is minimaal 6 maanden aaneengesloten voorafgaand aan de audit waarbij de laatste dag van de controleperiode wordt door Logius wordt gezien/ gehanteerd als de gespecificeerde datum waarop de opzet en het bestaan is getoetst (=de oordeelsdatum). De controleperiode mag variëren tussen de verschillende normen, bijvoorbeeld bij norm X zes maanden en bij norm Y 12 maanden.

Voor ENSIA assessments is en blijft de oordeelsdatum 31 december. Dat betekent automatisch dat de controleperiode voor het DigiD deel van de ENSIA de periode 1 juli (of eerder) – 31 december van het verantwoordingsjaar wordt.

De controleperiode voor serviceorganisaties (en sub-serviceorganisaties) ten aanzien van de werking is uiteraard ook minimaal 6 maanden. De serviceorganisatie zal bij het bepalen van de controleperiode rekening houden met de wensen en afspraken van aansluithouders om aan hun verplichtingen te kunnen voldoen. Hierbij kan de controleperiode vanwege een andere rapportageperiode van die (sub)serviceorganisatie anders zijn dan de laatste 6 maanden voorafgaand aan de oordeelsdatum assurance-rapport van de desbetreffende aansluithouder.

2.2.2 Verbijzonderde interne controle (VIC)

In Bijlage 4 is bij de testaanpak voor de normen die getoetst worden op werking vermeld: *'Inspecteer of in de organisatie gedurende de gehele controleperiode verbijzonderde interne controle heeft plaatsgevonden op het naleven van de beheersingsmaatregel'.* De verbijzonderde interne (2e-lijns) controle is vooralsnog een wenselijkheid en geen verplichting. Het DigiD assessment blijft vooralsnog een directe opdracht[5] waarbij de IT-auditor het onderzoeksobject meet of evalueert ten opzichte van de criteria. De auditee kan ook zelf meten, waarbij de IT-auditor dan zoveel mogelijk aan zal sluiten op en gebruik zal maken van de resultaten van de werkzaamheden in het kader van verbijzonderde interne controle en/of management bewering van de auditee.

2.3 Serviceorganisaties

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

- zowel de hosting als het applicatiebeheer plus de implementatie in eigen hand van de aansluithouder;
- hosting bij de aansluithouder en applicatiebeheer bij de leverancier, die geen verantwoordelijkheid heeft voor de implementatie;
- hosting bij de aansluithouder 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 aansluithouder (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.

[5] Bij een directe opdracht wordt volgens de 3000 (D) Richtlijn direct over het onderzoeksobject en de van toepassing zijnde criteria door de IT-auditor gerapporteerd.

Ook andere varianten en vormen van ketensamenwerking zijn mogelijk. Te denken valt hierbij aan het gebruik van een 'identity-provider' die een routeer functie vervult naar de verschillende digitale authenticatie-diensten zoals DigiD, eHerkenning en eIDAS.

2.3.1 'Carve-out' versus 'Inclusive'

Bij het beoordelen van uitbestede taken heeft de uitsluitingsmethode ('carve-out methode') waarbij de beschrijving van de normen van de aansluithouder de normen van de (sub)serviceorganisatie uitsluiten de voorkeur boven de opname methode ('inclusive methode') waarbij de beschrijving van de normen van de aansluithouder van haar systeem tevens de normen van de (sub)serviceorganisatie omvatten. Bij de carve-out methode ontvangt de aansluithouder een assurance-rapport van de serviceorganisatie (ook wel met een verouderde term genoemd: TPM). De auditor van de aansluithouder 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. In paragraaf 1.1 van het auditrapport voor de aansluithouder worden daarom alleen oordelen gegeven over de normen die door de auditor zelf getoetst zijn (bij de aansluithouder en/of de serviceorganisatie ('inclusive')).

De auditor van de aansluithouder dient te toetsen of het assurance-rapport van de serviceorganisatie bruikbaar[6] is om naar te verwijzen in het assurance-rapport van de aansluithouder.

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.

Indien de **carve-out methode wordt gehanteerd door de aansluithouder**, neemt de auditor in de rapportage (paragraaf 1.4.2 'serviceorganisatie'), de volgende zin op:

Aansluithouder maakt gebruik van serviceorganisatie [NAAM SERVICEORGANISATIE] voor [de aard van de activiteiten die door de serviceorganisatie worden uitgevoerd]. 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 Aansluithouder van haar systeem sluit daarmee de interne beheersingsdoelstellingen en daarmee

[6] Onder 'bruikbaar' wordt in dit verband verstaan dat het assurance-rapport in lijn is met de DigiD-Handreiking, waaronder een passende scope vermeldt (waaronder versienummer/software/ middleware), diepgang, de toetsingsperiode/toetsingsdatum niet ouder is dan een jaar, en dat het rapport is afgegeven door een RE (of vergelijkbaar bij een internationaal assurance rapport). Hierover staat het e.e.a. op de website van Logius: IT-auditrapportage voor DigiD | Logius.

verband houdende interne beheersingsmaatregelen van de serviceorganisatie uit. Onze werkzaamheden strekken zich dan ook niet uit tot de interne beheersingsmaatregelen van de serviceorganisatie. Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de genoemde assurance-rapportage van de serviceorganisatie. Wij kunnen dan ook geen enkele verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Indien de **carve-out methode wordt gehanteerd door de serviceorganisatie**, neemt de auditor in de rapportage (paragraaf 1.4.2 'sub-serviceorganisatie'), de volgende zin op:

[NAAM SERVICEORGANISATIE] maakt gebruik van sub-serviceorganisatie [NAAM SUB-SERVICEORGANISATIE] voor [de aard van de activiteiten die door de sub-serviceorganisatie worden uitgevoerd]. [NAAM SERVICEORGANISATIE] 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 [NAAM SERVICEORGANISATIE] van haar systeem sluit daarmee de interne beheersingsdoelstellingen en daarmee verband houdende interne beheersingsmaatregelen van de sub-serviceorganisatie uit. Onze werkzaamheden strekken zich dan ook niet uit tot de interne beheersingsmaatregelen van de sub-serviceorganisatie. Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de genoemde assurance-rapportage van de sub-serviceorganisatie. Wij kunnen dan ook geen enkele verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Indien de **inclusive-methode wordt gehanteerd door de aansluithouder**, neemt de auditor in de rapportage (paragraaf 1.4.2 'serviceorganisatie'), de volgende zin op:

Aansluithouder maakt gebruik van serviceorganisatie [NAAM SERVICEORGANISATIE] voor [de aard van de activiteiten die door de serviceorganisatie worden uitgevoerd]. Aansluithouder maakt voor het verschaffen van zekerheid over haar volledige webomgeving zoals beschreven onder het object van onderzoek gebruik van de opname methode ('inclusive method'). De beschrijving van de aansluithouder 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.

Indien de **inclusive-methode wordt gehanteerd door de serviceorganisatie**, neemt de auditor in de rapportage (paragraaf 1.4.2 'sub-serviceorganisatie'), de volgende zin op:

[NAAM SERVICEORGANISATIE] maakt gebruik van sub-serviceorganisatie [NAAM SUB-SERVICEORGANISATIE] voor [de aard van de activiteiten die door de sub-

serviceorganisatie worden uitgevoerd]. [NAAM SERVICEORGANISATIE] maakt voor het verschaffen van zekerheid over haar volledige webomgeving zoals beschreven onder het object van onderzoek gebruik van de opname methode ('inclusive method'). De beschrijving van de serviceorganisatie van haar systeem omvat daarmee de interne beheersingsdoelstellingen en daarmee verband houdende interne beheersingsmaatregelen van de sub-serviceorganisatie. Onze werkzaamheden strekken zich dan ook uit tot de interne beheersingsmaatregelen van de sub-serviceorganisatie.

Van iedere in het rapport genoemde (sub)serviceorganisatie moet worden opgenomen of deze inclusive, carve-out, dan wel buiten scope is van het DigiD-assessment.

In het geval dat een (sub)serviceorganisatie een SOC 1 of SOC 2[7] rapportage ter beschikking heeft, moet worden omschreven over welke normen door eigen onderzoek een oordeel is gegeven, en welke normen uit de SOC rapportage als 'carve out' zijn beschouwd.

(Sub)serviceorganisaties die als carve out zijn vermeld in onderliggende assurance rapporten hoeven (mogen) niet nogmaals worden opgenomen in het bovenliggende assurance rapport, d.w.z. ieder rapport beperkt zich tot de directe serviceorganisaties.

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 beide een gedeelde verantwoordelijkheid hebben.

Een apart aandachtspunt daarbij vormen de normen waarvoor de serviceorganisatie aanneemt dat ook de aansluithouder verantwoordelijkheid draagt (ook wel 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 is per norm aangegeven voor welke normen mogelijk zowel de aansluithouder als de serviceorganisatie verantwoordelijk zijn. In de praktijk komen situaties voor waarbij de aansluithouder een deel van de beheersingsmaatregelen die onder de 'user control considerations' vallen, weer heeft uitbesteed aan een andere (sub)serviceorganisatie.

[7] Opgemerkt wordt dat een SOC 3 rapport niet geschikt is voor gebruik bij het DigiD assessment omdat de rapportage de detailinformatie mist die hiervoor vereist is.

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. Indien de IT-auditor van de aansluithouder afwijkt van de 'user controls' vermeldt hij/zij deze afwijking als opmerking in paragraaf 1.2 en de normentabel van bijlage C van het assurance-rapport. In de opmerking wordt expliciet opgenomen dat tot de afwijking is gekomen in overleg met IT-auditor van de serviceorganisatie. Zie ook paragraaf 2.4.

Daarbij dient de auditor van de aansluithouder, naast de hiervoor genoemde aspecten, te controleren of het assurance-rapport van de serviceorganisatie bruikbaar is, dit omvat onder meer of deze betrekking heeft op dezelfde of lagere versie van het systeem dat in productie is bij de aansluitorganisatie op de laatste dag van de controleperiode.

Indien de serviceorganisatie gebruik maakt van Continuous Delivery in het softwareontwikkelingsproces en geen gebruik wordt gemaakt van versienummers dient de auditor van de serviceorganisatie dit aan te geven in het object van onderzoek. Het versienummer wordt in die gevallen vervangen voor de datum van de laatste dag van de controleperiode waarop het onderzoek betrekking heeft gehad.

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 (sub)serviceorganisatie(s) naar Logius voorzover het DigD assurance-rapporten zijn waarin Logius ook als beoogd gebruiker van het rapport is vermeld.

2.3.2 Gebruik van SOC (1 of 2) en vergelijkbare assurance-rapporten

Hoewel strikt genomen een SOC rapportage niet gebruikt mag worden, daar deze doorgaans niet is gebaseerd op het DigiD normenkader, de NOREA-handreiking en DigiD rapportage templates en in sommige gevallen ook niet is ondertekend door een RE-auditor (zie de Logius aansluitvoorwaarden DigiD artikel 5.5 en 5.6), staat Logius het gebruik wel toe. Hieraan zijn onderstaande voorwaarden verbonden.

Het is doorgaans niet mogelijk om de oordelen uit SOC rapporten "inclusive" over te nemen. SOC rapporten zijn gebaseerd op algemeen geformuleerde beheersingsdoelstellingen, terwijl de DigiD testaanpak een concrete inrichting van configuraties vereist. Daarnaast is dossier review bij de 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 beveiligingsbeleid (B.01), logisch toegangsbeheer U/TV.01), incidentenbeheer (U/WA.02), wijzigingsbeheer (C.08) en patching (C.09), et cetera. De auditor dient daarbij vast te stellen of de voor het DigiD assessment relevante webapplicatie (en onderliggende infrastructuur) als object van onderzoek in het SOC rapport genoemd wordt en de op deze webapplicatie van toepassing zijnde IT General Controls dezelfde beheersingsmaatregelen omvatten als de DigiD normen.

In veel gevallen kunnen klanten die Cloud- en (Managed-) hostingdiensten van grote leveranciers afnemen via een platform de relevante actuele SOC rapportages downloaden. Voorbeelden hiervan zijn Amazon, Cloudflare, Google en Microsoft.

Let op: De laatste dag van de controleperiode van de toetsing van de SOC mag niet ouder zijn dan een jaar (het gaat hier om datum oordeel opzet en bestaan of de laatste dag van de controleperiode in het SOC-rapport). Peildatum is de oordeelsdatum[8] (en bij toetsing op werking: laatste dag controleperiode) van het assurance-rapport van de aansluithouder.

In bijlage C wordt dan verwezen naar het SOC assurance-rapport. Omdat Logius in het 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. Een verwijzing per DigiD beveiligingsrichtlijn naar het equivalent in de SOC rapportage is wel vereist omdat de SOC rapportage doorgaans een andere nummering kent dan het DigiD normenkader.

2.3.3 Overwegingen voor het gebruik van SOC assurance-rapporten

1. <u>Gebruik van SOC assurance-rapporten</u>

Voor de infrastructuur wordt in toenemende mate gebruik gemaakt van (multinationale) Cloud leveranciers waarbij het (ten dele) niet mogelijk is om 'inclusive' onderzoek uit te voeren en zelf een dossier op te bouwen. Voor een deel van het DigiD onderzoek is een SOC assurance-rapportage uitstekend 'carve-out' te gebruiken mits:

- de controleperiode aansluit bij de termijnen die Logius hieraan stelt, en
- de diensten zoals omschreven in de SOC assurance-rapportage overeenkomen met de diensten die auditee daadwerkelijk van de (sub)serviceorganisatie afneemt en kan worden vastgesteld dat deze daadwerkelijk zijn geconfigureerd.

[8] Zie voor een toelichting op het begrip 'oordeelsdatum' Bijlage 1: Begrippenkader.

Specifiek voor Cloud providers geldt dat uitsluitend gebruik mag worden gemaakt van de ITGC's (waaronder in dit geval de normen B.01, U/WA.02 (voor wat betreft het incidentenbeheer), U/TV.01, C.08 en C.09 omdat in de SOC rapportage doorgaans geen rekening wordt gehouden met specifieke vereisten ten aanzien van de diepgang van het normenkader DigiD. Uitzondering hierop zijn altijd mogelijk. Bijvoorbeeld ingeval van een Cloud WAF-leverancier kan randvoorwaardelijk ook 'carve out' worden gesteund voor de normen U/NW.04, C.06 en/of C.07.
Ook ingeval van het afnemen van een PaaS oplossing kunnen U/PW.05 en/of U/PW.07 deels ontleend worden aan een SOC assurance-rapportage.
In de praktijk zal op basis van 'professional judgement' deels conform de carve-out systematiek naar een SOC assurance-rapportage gerefereerd kunnen worden, maar bij geen enkele norm volledig. (Deels) Inclusive onderzoek blijkt altijd noodzakelijk.

2. Bepalen relevantie controls in de SOC assurance-rapportage voor het DigiD-assessment

Niet alle controls in een SOC assurance-rapport zijn relevant voor een DigiD-assessment. Het is belangrijk om alleen die controls te selecteren die relevant zijn voor de diensten die worden gebruikt in het kader van de DigiD-audit. Dit moet worden bepaald op basis van overeenkomsten, subscriptions en walkthrough met de auditee. *Voorbeeld: in de praktijk hebben meerdere serviceorganisaties controls opgenomen in de SOC assurance-rapportage over Security Information & Event Management (SIEM) en/of Security Operations Center (SOC) dienstverlening. Het is aan de auditor om te bepalen of deze SIEM/SOC dienstverlening daadwerkelijk gebruikt wordt voor de verkeersstromen van de DigiD-webapplicatie.*

3. Vaststellen of aan de SOC assurance-rapportage voldoende bewijsvoering kan worden ontleend dat aan de relevante DigiD-normen wordt voldaan

Het is niet automatisch zo dat de controls in een SOC assurance-rapportage met voldoende diepgang zijn onderzocht om als bewijs te kunnen worden aanvaard voor een DigiD-assessment. Het is belangrijk om goed af te bakenen tot hoever de verantwoordelijkheden van de serviceorganisatie gaan en op de hoogte te zijn van de toepassing van de controls van de serviceorganisatie in relatie tot het object van onderzoek. Daarnaast moeten de geselecteerde controls voldoende gedetailleerd zijn beschreven in de SOC assurance-rapportage zodat de gehanteerde diepgang beoordeeld kan worden.
Voorbeeld: in de praktijk wordt in SOC assurance-rapportages aangegeven dat de serviceorganisatie beschikt over een IDS/IPS. Deze IDS/IPS is echter in veel gevallen ter bescherming van het (cloud)platform van de serviceorganisatie zelf, niet ter

bescherming van de webapplicatie van de klant. In dit geval dient de klant zelf een IDS/IPS te implementeren en mag niet gerefereerd worden aan de SOC control over het IPS/IDS. Ook kan o.b.v. de enkelvoudige mededeling dat een SIEM/SOC aanwezig is, niet zonder meer worden vastgesteld dat aan de specifieke eis wordt voldaan dat de inhoud van de berichten afdoende kan worden beoordeeld door het systeem (decrypted).

In alle gevallen dient bewijsmateriaal te worden verzameld om zeker te stellen dat daadwerkelijk gebruik wordt gemaakt van een dienst en dat deze dienst ook adequaat is geconfigureerd voor de aansluithouder/service organisatie.

4. Vereiste vastlegging/documentatie voor het 'carve-out' steunen op een SOC assurance-rapportage

Bij gebruik van een SOC assurance-rapportage conform de 'carve-out' systematiek is de auditor verplicht de volgende elementen op te nemen in het assurance-rapport:

- de identificerende kenmerken van het SOC2 rapport en afgevende auditorganisatie of RE;
- de controleperiode (het tijdvak dat de auditor heeft onderzocht om de werking te toetsen waarbij de oordeelsdatum de laatste dag van de controleperiode is). Indien deze oordeelsdatum ruim ligt voor de oordeelsdatum van het eigen onderzoek dienen de identificerende gegevens van 1 of meer bridgeletters[9] te worden opgenomen om dit te overbruggen;
- de gebruikte diensten van de serviceorganisatie (op basis van het contract tussen gebruikersorganisatie en de serviceorganisatie;
- een specificatie van de relevante SOC controls per DigiD norm in de eerste tabel in Bijlage C.

2.3.4 Maximale leeftijd assurance-rapport serviceorganisatie

Een assurance-rapport van de serviceorganisatie mag niet ouder zijn dan twaalf maanden ten opzichte van de oordeelsdatum van het assessmentrapport van de DigiD-aansluithouder. Voor vaststelling van de oordeelsdatum van het assurance-rapport van de serviceorganisatie is de in paragraaf 1.1 vermelde datum 'oordelen opzet en bestaan' leidend. Dit valt samen met de laatste dag van de periode waarover de werking is getoetst. Alleen voor SOC-rapporten (zie 2.3.3) kan de

[9] Het gebruik van 'bridgeletters' is doorgaans beperkt tot een periode van maximaal 9 maanden vanaf de oordeelsdatum van het SOC-rapport. Afhankelijk van de aard en omvang van de uitbestede dienstverlening aan de (sub)serviceorganisatie kan de toezichthouder (Logius) beperkingen stellen aan de maximale termijn waarover 'bridgeletters' zullen worden geaccepteerd.

gebruiksduur van een ouder rapport met een of meer ‘bridgeletters’ worden verlengd. Als dit van toepassing is, dient de IT-auditor ook de kenmerken van deze ’bridgeletters‘ op te nemen als referentie.

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

2.3.5 Herhaald gebruik assurance-rapport van de serviceorganisatie

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 van de serviceorganisatie worden gebruikt.

2.4 Afwijken van user controls

De IT-auditor van de aansluithouder kan op basis van zijn/haar onderzoek afwijken van hetgeen in het hoofdstuk 2 (user controls) door de IT-auditor van de serviceorganisatie in zijn/haar assurance-rapport is aangegeven. Dit kan ongeacht of het te maken heeft met opzet, bestaan of werking. De IT-auditor van de aansluithouder stemt dit af met de IT-auditor van de serviceorganisatie en vermeldt deze afwijking als opmerking zowel in paragraaf ‘1.2 De basis voor onze oordelen’ als in bijlage C in het assurance-rapport.

Hierbij wordt de volgende tekst opgenomen:

Op basis van onze onderzoeksresultaten zijn wij tot de conclusie gekomen dat, in afwijking van hetgeen is vermeld in hoofdstuk 2 (verantwoordelijkheden aansluithouder) van het assurance-rapport van <serviceorganisatie>, kenmerk rapport <rapport kenmerk>, de norm(en) <Norm x>, <Norm y, enzv > wel/niet van toepassing zijn voor de aansluithouder. Wij hebben deze normen derhalve wel/niet getoetst in het kader van dit DigiD assessment. Deze afwijking(en) is/zijn afgestemd met de IT-auditor van <serviceorganisatie>.

2.5 Non-occurrence

2.5.1 Non-occurrence bij opzet en bestaan

Bij een aantal beveiligingsrichtlijnen kan zich de situatie voordoen dat wel voldaan is aan de opzet van de interne beheersingsmaatregel, 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 beheersingsmaatregel 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 beheersingsmaatregel in de tabel oordelen zonder een opmerking in de toelichtende paragraaf te plaatsen betreffende het toetsen op het bestaan van de beheersingsmaatregel. Als er geen andere deelpopulatie is waarop hetzelfde proces en dezelfde control van toepassing is waarmee het bestaan van de betreffende beheersingsmaatregel kan worden vastgesteld, dient de auditor 'Voldoet niet' voor de betreffende beheersingsmaatregel 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 beheersingsmaatregel 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.

2.5.2 Non-occurrence bij werking

Anders dan bij de bestaanscontrole kan bij het toetsen van de werking een non-occurrence voor het verkrijgen van voldoende zekerheid over de effectiviteit van de maatregelen NIET de scope van de test worden uitgebreid tot een ander systeem of proces of procedure waar wel relevante gebeurtenissen hebben plaatsgevonden. Daarmee zou de populatie wijzigen en wordt de effectiviteit van een andere procedure, proces of systeem gemeten; de populatie kan niet worden bepaald noch de omvang van de deelwaarneming.
In de situatie dat de volledigheid van de populatie niet kan worden vastgesteld, maar de maatregelen in opzet (en eventueel bestaan voor een andere deelpopulatie) geen afwijkingen hebben laten zien, wordt de volgende tekst als opmerking in paragraaf 1.2 van het assurance-rapport opgenomen:

[1] Werking. Voor beveiligingsrichtlijn(en) <vul in U/TV.01, U/WA.02 en/of C.08> hebben wij na een controle vastgesteld dat de organisatie maatregelen heeft ontworpen (opzet) [optioneel indien getoetst voor andere deelpopulatie: en ingericht

*(bestaan)] met betrekking tot deze norm en wij hebben deze gevalideerd. Er zijn hierbij geen afwijkingen door ons geconstateerd. Wij zijn van oordeel dat de organisatie in opzet (**of**: opzet en bestaan) voldoet aan deze norm. Vanwege non-occurrence kan de effectieve werking niet worden vastgesteld en daarom geven wij daarover geen oordeel.*

2.6 Betrouwbaarheidseisen aan de handtekening van een RE-auditor

Vanaf 1 januari 2024 is het niet meer mogelijk om documenten bij Logius op papier aan te leveren. Vanaf die datum accepteert Logius alleen de zogenoemde EUTL-handtekening[10] als elektronische handtekening voor alle digitaal ingediende documenten in de assessmentrapportage.

Een EUTL-handtekening is een gekwalificeerde elektronische handtekening met een certificaat dat herleidbaar is naar een uitgevende instantie die vermeld is op de EUTL. De handtekening zorgt voor een hoge betrouwbaarheid. Daarnaast is de controle van de handtekening eenvoudig en snel. Een EUTL-handtekening is persoonsgebonden aan de RE-auditor die een document in de assessmentrapportage ondertekent.

2.7 Meervoudig Assessment

In 2020 heeft Logius een nieuw soort assessmentmethodiek mogelijk gemaakt: het "Meervoudig Assessment" (MA). Het meervoudig assessment is van toepassing op een clusteraansluiting en 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. Een clusteraansluiting 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 Assessment (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).

---

[10] 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.

Logius heeft voor het gebruik van een MA het “DigiD Meervoudig 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 Meervoudig 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 assurance-rapport 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 Meervoudig Assessment MA. Waar nodig is de bestaande DigiD testaanpak vertaald op basis van de uitgangspunten van Logius naar de situatie voor een DigiD Meervoudig Assessment MA.

2.8 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 ieder 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.

2.9 Bijzondere instructies van Logius

In bijzondere gevallen kan Logius NOREA verzoeken de IT-auditors aanvullende instructies 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. Bijzondere aanwijzingen worden door Logius gepubliceerd. Omdat bijzondere aanwijzingen vaak een tijdelijk karakter zullen hebben, worden deze eerst in een FAQ vermeld[11] en worden de structurele onderdelen later opgenomen in de Handreiking.

2.10 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 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.

[11] Zie sectie publicaties op website NOREA | Werkgroep DigiD-assessments

2.11 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 kan voorkomen dat zich, in uitzonderlijke omstandigheden, 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 NOREA 'Handreiking Correctie van assurance-rapporten' wordt invulling gegeven aan een voor alle partijen inzichtelijke en eenduidige correctieprocedure.

2.12 Consultatie

Indien een auditor[12] in het kader van de uitvoering van een DigiD-assessment wil afwijken van Handreikingen / formats voorgeschreven door stelselhouder(s) / stelselbeheerder(s) / toezichthouder(s) of van de onderhavige DigiD-Handreiking en/of de formats assurance-rapporten, dient de auditor dit tijdig af te stemmen met NOREA.

Op basis van een door de auditor concreet uitgewerkt voorstel zal onder verantwoordelijkheid van het bestuur van NOREA door ter zake deskundige leden een beoordeling plaatsvinden. Hierbij zullen, waar nodig, overige gremia binnen NOREA waaronder de Vaktechnische Commissie en het bestuur betrokken worden. Tevens zal, voor aangelegenheden die onder de verantwoordelijkheid van de stelsel- of toezichthouder vallen, afstemming plaatsvinden met stelselhouder(s) / stelselbeheerder(s) / toezichthouder(s).

[12] Hieronder te verstaan auditorganisatie en/of individuele auditor.

De uitkomsten van de beoordeling worden meegedeeld aan de auditor en zijn bindend voor alle betrokken partijen bij de verdere uitvoering van zijn werkzaamheden.

Waar nodig vindt communicatie in breder verband plaats. Denk daarbij aan alle bij de uitvoering van DigiD-opdrachten betrokken auditors / alle leden NOREA (verantwoordelijkheid NOREA) en/of stelselhouder(s) / stelselbeheerder(s) / toezichthouder(s).

Bijlage 1 – Begrippenkader DigiD assessments

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

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.
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.
Beveiligingsincident	Een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatieverwerkende systemen in gevaar is of kan komen.
Carve-out methode	Bij de carve-out methode wordt in een assurance-rapport (zoals een DigiD assessment rapportage) een referentie opgenomen naar het assurance-rapport van een leverancier. De auditor van de aansluithouder en de auditor van de serviceorganisatie houden ieder zelfstandig hun vaktechnische verantwoordelijkheid. De auditor van de aansluithouder dient wel vast te stellen dat de scope van beide rapportages in voldoende mate op elkaar aansluiten.
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.
Identity provider.	Een organisatie die identiteitsgegevens onderhoudt en beheert en tevens authenticatiediensten levert aan afhankelijke toepassingen binnen een federatie of gedistribueerd netwerk.

Inclusive methode (ook: opname methode)	Bij de inclusive methode worden alle beheersingsmaatregelen van de (sub)serviceorganisatie in het assurance-rapport van de aansluithouder opgenomen en er wordt dus niet verwezen naar assurance-rapport(en) waar eventueel gebruik van is gemaakt. De auditor die de inclusive methode toepast is vaktechnisch volledig verantwoordelijk en voert eigen werkzaamheden (zoals bijv. deelwaarnemingen en een dossierreview) uit t.a.v. de beheersingsmaatregelen die een (deel)verantwoordelijkheid zijn van een (sub)serviceorganisatie.
Leverancier Meervoudig Assessment (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.
Meervoudig Assessment (MA)	Het assessment waarbij de serviceorganisatie (de LMA) door Logius is geaccrediteerd om dit (assessment) meervoudig uit te laten voeren voor alle dienstverleners (afnemers van de LMA).
Opzet	De beschrijving van een stelsel van informatiebeveiligings- en beheersingsmaatregelen.
Oordeelsdatum	○ Voor een rapport met alleen een toets op opzet en bestaan geldt: de oordeelsdatum is de datum waarop de opzet en het bestaan worden vastgesteld. ○ Voor een rapport met alleen een toets op werking geldt: de oordeelsdatum is de laatste dag van de controleperiode voor de toets op werking. ○ Voor een rapport met zowel een toets op werking als een toets op opzet en bestaan valt het einde van de controleperiode voor werking samen met de datum waarop opzet en bestaan is vastgesteld. ○ Voor een ENSIA-rapportage geldt dat de oordeelsdatum 31 december is (van het 'ENSIA-jaar').
Patch	Een installatiebestand dat een kwetsbaarheid of fout in een programma herstelt (een soort pleister plakt) of een programma verbetert (bijv. een extra functionaliteit toevoegt).

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. 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.
Serviceorganisatie	de SaaS-, hosting-, applicatieleverancier en/of identity provider
Third Party Mededeling (TPM)	De term 'TPM' is in het verleden in de context van het DigiD-assessment vaak gebruikt om specifiek het assurance-rapport van een (sub)serviceorganisatie te duiden waarbij de doelgroep van het rapport een andere is dan de (sub)serviceorganisatie en de assurance wordt gegeven door een onafhankelijke auditor. De term TPM is niet voldoende eenduidig en verouderd. Hiervoor in de plaats wordt de term 'assurance-rapport van de serviceorganisatie' gebruikt als het een rapport van een (sub)serviceorganisatie betreft.
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. 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.
Wijzigingsbeheer	Wijzigingsbeheer is het op beheerste wijze doorvoeren van wijzigingen in de ICT-infrastructuur, waardoor verstoringen in de dienstverlening als gevolg van wijzigingen worden voorkomen of tot een minimum beperkt blijven.

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

De NOREA werkgroep DigiD heeft ten behoeve van de rapportage verschillende modelrapporten opgesteld:

- Modelrapport/template aansluithouders
- Modelrapport/template serviceorganisaties
- Modelrapport/template Leverancier Meervoudige Assessment (LMA)

De genoemde modelrapporten zijn als Word-bestand beschikbaar op de website van NOREA.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft ten aanzien van het DigiD assessment besloten een toets op werking toe te voegen. Sinds de invoering van het DigiD-assessment zijn de DigiD-normen getoetst op opzet en bestaan. 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.**

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

In onderstaande tabel zijn de normen en de specifieke testwerkzaamheden t.a.v. de werking van bovengenoemde maatregelen geel gearceerd.

LET OP 1: Indien de auditor tot het oordeel komt dat de werking niet voldoet, dient daar bovenop het bestaan te worden vastgesteld met een recente deelwaarneming van tenminste één waarbij geldt dat de toets op bestaan niet de toets op werking vervangt, er zal nog altijd aan de werking moeten worden voldaan.

LET OP 2: De in de testaanpak beschreven verbijzonderde interne (2e-lijns) controle bij de normen die worden getoetst op opzet, bestaan en werking, is vooralsnog een wenselijkheid en geen verplichting (zie ook paragraaf 2.2.2).

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
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	Governance	Betrokken rol(len): • Applicatie-, hosting- of SaaS-leverancier. • Identity provider. • Aansluithouder van de DigiD aansluiting.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer. <u>Doelstelling:</u> Het zorgen voor specifieke management aandacht in het beveiligingsproces voor de webapplicaties van de organisatie.		<u>Scope:</u> • De DigiD webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. <u>Diepgang:</u> • Opzet en bestaan van de beheersingsmaatregelen. <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 de DigiD webapplicatie en/of de infrastructuur voor het netwerksegment met de DigiD webapplicatie. <u>Test aanpak:</u>

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• Stel vast dat de aansluithouder 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 de onderwerpen 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 bekend is bij functionarissen betrokken bij webapplicatie gerelateerde onderwerpen.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• 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 webapplicatie is uitbesteed aan een andere organisatie.	Governance	<u>Betrokken rol(len):</u> • Applicatie-, hosting- of SaaS-leverancier. • Identity provider. • Aansluithouder van de DigiD aansluiting. <u>Scope:</u> De contracten en/of Service Level Agreements voor de levering hosting-, applicatie- of SaaS-diensten. <u>Diepgang:</u> • Opzet en bestaan van de beheersingsmaatregelen. <u>Nadere toelichting:</u>

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			De organisatie dient een, door beide partijen ondertekend, contract te hebben waarin tenminste de volgende zaken zijn opgenomen: • 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 aansluithouder 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.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• Inspectie van contracten met leveranciers, SLA's en andere gerelateerde documenten. <u>Non-occurrence (voor het onderdeel Service Level Reporting):</u> • 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:	Applicatie Infrastructuur Proces	<u>Betrokken rol(len):</u> • Applicatie-, hosting- of SaaS-leverancier. • Identity provider. • Aansluithouder van de DigiD aansluiting. <u>Scope</u>: De DigiD webapplicatie, DigiD webservers en de firewalls, IDS/IPS, etc. <u>Diepgang:</u> Opzet, bestaan en werking van de beheersingsmaatregelen.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	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.		<u>Nadere toelichting</u>: 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. • 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 aansluithouder 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 assurance-rapport van de serviceorganisatie kan het zijn dat de SaaS leverancier het gehele functionele (toegangs-) beheer verzorgt, inclusief het testen van de applicatie. Als de auditor van

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			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 het assurance-rapport van de serviceorganisatie. 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>: • 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. • Inspecteer of in de organisatie gedurende de gehele controleperiode verbijzonderde interne controle heeft plaatsgevonden op het naleven van de beheersingsmaatregelen rondom mutaties van rechten in de gebruikersgroep. • Selecteer conform de tabel omvang deelwaarnemingen het juiste aantal mutaties in de gebruikersgroep (verzameling mutaties met de

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			identificatie en autorisatie van de gebruikers en/of beheerder die in de controleperiode is doorgevoerd) en inspecteer deze op naleving van het identiteits- en toegangsbeheer, waarbij voor elke categorie (joiner, mover èn leaver) tenminste één deelwaarneming wordt uitgevoerd. Inspecteer de toegekende autorisaties en de resultaten en opvolging van de periodieke review. • Interview de verantwoordelijke functionarissen. <u>Non-occurrence (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. <u>Doelstelling:</u>	Applicatie Proces	<u>Betrokken rol(len):</u> • Applicatie-, hosting-, of SaaS-leverancier. • Identity provider. • Aansluithouder van de DigiD aansluiting. <u>Scope:</u>

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	Effectief en veilig realiseren van de dienstverlening.		De DigiD webapplicatie. Diepgang: Opzet, bestaan en werking (alleen voor het proces 'incidentenbeheer') van de beheersingsmaatregelen. 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. • Beveiligingsincidenten worden geregistreerd, geanalyseerd, opgevolgd en afgehandeld. • Er is een periodieke rapportage aan het management inzake beveiligingsincidenten en/of datalekken. Test aanpak: • Inspecteer de functie/taakbeschrijvingen van beheerders.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• Inspecteer het incidentproces, de uitgevoerde analyse, de managementrapportage en opvolging van beveiligingsincidenten. • Inspecteer of in de organisatie gedurende de gehele controleperiode verbijzonderde interne controle heeft plaatsgevonden op het naleven van de beheersingsmaatregelen rondom beveiligingsincidenten. • Selecteer conform de tabel omvang deelwaarnemingen het juiste aantal incidenten (verzameling incidenten met het 'label' beveiligingsincident of datalek dat in de controleperiode is geregistreerd) en inspecteer deze op naleving van het incidentenbeheerproces. • Interview de verantwoordelijke functionarissen. <u>Non-occurrence (voor het onderdeel opvolging van beveiligingsincidenten):</u> • 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.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• 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 beschikbaarheid van de webapplicatie aangetast worden.	Applicatie	Betrokken rol(len): • Applicatie- of SaaS-leverancier. • Identity provider. Scope : De DigiD webapplicatie en webserver. Diepgang: • Opzet en bestaan van de beheersingsmaatregelen. Nadere toelichting: Ongecontroleerde (ongevalideerde) invoer van gebruikers is een belangrijke dreiging voor een 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

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			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.
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	Applicatie	<u>Betrokken rol(len):</u> • Applicatie- of SaaS-leverancier. • Identity provider.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	Doelstelling: Voorkom manipulatie van het systeem van andere gebruikers.		Scope: De DigiD webapplicatie. Diepgang: • Opzet en bestaan van de beheersingsmaatregelen. 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 (opzet, bestaan en werking)			
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. • Identity provider. • Aansluithouder van de DigiD aansluiting. Scope: De DigiD webapplicatie en webserver en bijbehorende infrastructuur. Diepgang: • Opzet en bestaan van de beheersingsmaatregelen. 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

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			van gegevens tijdens transport. Aandachtspunten hierbij zijn: • De classificatie van gegevens door de aansluithouder van de DigiD aansluiting op basis van een risicoanalyse. • 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 2021 door het NCSC van de vernieuwde ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)v2.1 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

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			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.
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen. <u>Doelstelling:</u> Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.	Applicatie	<u>Betrokken rol(len):</u> • Applicatie-, hosting- of SaaS-leverancier. • Identity provider. <u>Scope:</u> De webserver. <u>Diepgang:</u> • Opzet en bestaan van de beheersingsmaatregelen. <u>Nadere toelichting:</u> 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.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• 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. • 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. <u>Test aanpak:</u> • 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.	Applicatie infrastructuur	<u>Betrokken rol(len):</u> • Applicatie-, hosting- of SaaS-leverancier. • Identity provider.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	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.		Scope: De webserver en andere servers in de DMZ. Diepgang: • Opzet en bestaan van de beheersingsmaatregelen. 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: • 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:

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			Bij onderstaande voorgeschreven waarden dient er rekening mee worden gehouden dat er onder de Content Security Policy Level 3 nieuwe en verbeterde directives mogelijk zijn. Het is ondoenlijk om dit in een testaanpak bij te houden. Het is ALTIJD toegestaan om veiligere waarden te gebruiken dan onderstaande. • 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: • X-Frame-Options: deny & Frame-Ancestors: none • OF X-Frame-Options: sameorigin & Frame-Ancestors: self • Strict-Transport-Security (HSTS)

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			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 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

Bijlage 3 - Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• 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 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

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			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.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
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>Doelstelling:</u> Voorkomen van misbruik van beheervoorzieningen.	Infrastructuur Proces	<u>Betrokken rol(len):</u> • Hosting- of SaaS-leverancier. • Identity provider. <u>Scope:</u> • De webserver en andere servers in de DMZ. <u>Diepgang:</u> • Opzet en bestaan van de beheersingsmaatregelen. <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).

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• 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. • 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. <u>Doelstelling:</u>	Infrastructuur Proces	<u>Betrokken rol(len)</u>: • Hosting- of SaaS-leverancier. • Identity provider.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.		Scope: • De webserver en andere ICT-componenten binnen de DMZ. Diepgang: • Opzet en bestaan van de beheersingsmaatregelen. 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 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

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			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 noodzakelijke functies bieden (statusopname). Afwijkingen worden hersteld. <u>Test aanpak</u>: • Inspecteer de architectuur en hardening standaarden. • Inspecteer de configuratiebestanden en de uitkomsten van de penetratietest. • Interview de verantwoordelijke functionarissen.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
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. • Identity provider. Scope: • De DMZ van de DigiD webapplicatie. Diepgang: • Opzet en bestaan van de beheersingsmaatregelen. 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 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.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• 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. <u>Doelstelling:</u> Het detecteren van aanvallen (onder andere (D)DoS) om te vooWArkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	Infrastructuur	<u>Betrokken rol(len):</u> • Hosting- of SaaS-leverancier. • Identity provider. <u>Scope:</u> De DMZ van de DigiD webapplicatie. <u>Diepgang:</u> • Opzet en bestaan van de beheersingsmaatregelen. <u>Nadere toelichting:</u> 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. • C.07 richt zich op periodieke analyse van de logging.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			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. • Een inrichtingsdocument en een beheerprocedure waarin is vastgelegd waar en hoe de IDS / IPS of WAF wordt ingezet.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• 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. • Identity provider. <u>Scope:</u> Het netwerksegment met de webservers die een koppeling hebben met de DigiD omgeving van Logius inclusief de toegang vanuit internet. <u>Diepgang:</u> • Opzet en bestaan van de beheersingsmaatregelen.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
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 netwerk architectuurschema 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 (opzet, bestaan en werking)			
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. • Identity provider. • Aansluithouder van de DigiD aansluiting. Scope: De webserver en andere ICT-componenten binnen de DMZ. Diepgang: • Opzet en bestaan van de beheersingsmaatregelen. 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

Bijlage 3 - Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			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. 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.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• 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. Test aanpak: • Inspecteer het netwerkarchitectuur schema 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	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SaaS-leverancier. • Identity provider. Scope: • De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Diepgang: • Opzet en bestaan van de beheersingsmaatregelen.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	beschermende maatregelen kunnen worden getroffen.		<u>Nadere toelichting</u>: 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. • 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>:

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• 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). Doelstelling: Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).	Applicatie Infrastructuur Proces	Betrokken rol(len): • Applicatie-, hosting- of SaaS-leverancier. • Identity provider. Scope: • De DigiD webapplicatie, de webserver en andere servers in de DMZ van de DigiD webapplicatie. Diepgang: • Opzet en bestaan van de beheersingsmaatregelen. Nadere toelichting: De voorkeur heeft het op basis van een risicoafweging enkele keren per jaar een penetratietest te laten

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor

			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.
			• Wanneer een penetratietest wordt uitgevoerd op de Acceptatie-/Preproductie-omgeving dient deze geheel gelijk/representatief te zijn aan de productieomgeving. De IT-auditor dient dit vast te stellen door de volgende zaken op de geteste omgeving en de productieomgeving te vergelijken:
			  ○ versie nummer van de software;
			  ○ SSL configuratie van de webserver;
			  ○ security-headers hoofdpagina (voor DigiD-inlog);
			  ○ indien gebruik gemaakt wordt van containerization (docker): evidence van de versienummers van de containers;

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			○ indien gebruik gemaakt wordt van een deployment-straat: evidence van de deployments naar acceptatie en productie. • 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) <u>Testaanpak</u>: • 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.	Infrastructuur Proces	<u>Betrokken rol(len):</u> • Hosting- of SaaS-leverancier. • Identity provider.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	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.		Scope: • De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Diepgang: • Opzet en bestaan van de beheersingsmaatregelen. 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. 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.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• 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. Test aanpak: • 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-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-	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SaaS-leverancier. • Identity provider. Scope: • De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Diepgang: • Opzet, bestaan en werking van de beheersingsmaatregelen.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor

	diensten en de status van de componenten waarmee deze worden voortgebracht.		<u>Nadere toelichting:</u>
			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:
			  ○ wijzigingen aan de configuratie van webapplicaties;
			  ○ optreden van verdachte gebeurtenissen en eventuele schendingen van de beveiligingseisen;

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			○ 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. • Inspecteer of in de organisatie gedurende de gehele controleperiode verbijzonderde interne controle heeft plaatsgevonden op het naleven van het bewakings-, analyse-, rapportage- en follow-up-proces en beheersingsmaatregelen rondom de registraties en alarmeringen. • Selecteer conform de tabel omvang deelwaarnemingen het juiste aantal registraties en alarmeringen (die in de controleperiode zijn

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			geregistreerd) en inspecteer deze op naleving van het bewakings-, analyse-, rapportage- en follow-up-proces. • 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	Betrokken rol(len): • Applicatie-, hosting- of SaaS-leverancier. • Identity provider. • Aansluithouder van DigiD aansluiting. Scope: De DigiD webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. Diepgang: Opzet, bestaan en werking van de beheersingsmaatregelen. Nadere toelichting: 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.

Bijlage 3 - Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			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 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).

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• 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 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 of in de organisatie gedurende de gehele controleperiode verbijzonderde interne controle heeft plaatsgevonden op het naleven van de beheersingsmaatregelen rondom wijzigingenbeheer. • Bepaal hoeveel wijzigingen hebben plaatsgevonden gedurende de controleperiode en selecteer conform de tabel in steekproefomvang het juiste aantal samples uit de registratie van wijzigingen. Zorg

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			hierbij voor voldoende spreiding over de verschillende soorten wijzigingen standaard/maatwerk/applicatie/infrastructuur). Inspecteer de geselecteerde wijzigingen en de daaraan gerelateerde documentatie op naleving van de wijzigingsbeheer procedure. • Interview de verantwoordelijke functionarissen. Non-occurrence (voor het onderdeel inspecteren van een doorgevoerde wijziging): 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 (beveiligings)patches tijdig zijn geïnstalleerd in de ICT-voorzieningen. Doelstelling: Zeker stellen dat technische en software kwetsbaarheden tijdig en effectief worden	Applicatie Infrastructuur Proces	Betrokken rol(len): • Applicatie-,Hosting- of SaaS-leverancier. • Identity Provider. Scope: • Hypervisor (VM Ware, etc.). • Operating system (Windows, etc.). • Databases. • Netwerk componenten.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
	aangepakt en zo een stabiele omgeving wordt gecreëerd.		• Firewall. • Webapplicatie en daarvoor benodigde software componenten. <u>Diepgang:</u> Opzet, bestaan en werking van de beheersingsmaatregelen. <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. Mocht om objectief aantoonbare technische redenen het tijdig doorvoeren van een securitypatch niet mogelijk zijn, dan dienen door de organisatie passende mitigerende maatregelen te zijn ingericht, zoals bijvoorbeeld extra monitoring en analyse op kwetsbaarheden.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			De auditor stelt vast of aan de volgende voorwaarden is voldaan: • de technische reden voor het niet kunnen doorvoeren van beveiligingspatches is met rationele argumenten onderbouwd; • er zijn passende mitigerende maatregelen genomen tot het moment waarop patching van alle componenten wel mogelijk is; • de organisatie heeft een verbeterplan opgesteld waarin staat beschreven hoe en wanneer de organisatie zorgt dat alle componenten voorzien kunnen worden van patches. Als dit het geval is beoordeelt de auditor de norm als 'voldoet niet' en neemt in paragraaf 1.1 'Onze oordelen met beperking' bij C.09 een verwijzing op naar de corresponderende tekst in paragraaf 1.2 'De basis voor onze oordelen met beperking' en geeft daar een toelichting, door middel van het opnemen van de volgende tekst: *T.a.v. norm C.09 merken we op dat <AANTAL> van de componenten van de applicatie niet beschikt over de laatste ondersteunde security patch, waarbij naar het oordeel van de auditor de kwetsbaarheden afdoende*

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			zijn beperkt en de organisatie een ter zake doend verbeterplan heeft opgesteld. Alle andere componenten zijn wel voorzien van de laatste ondersteunde security patch. Voor nadere informatie kan Logius zich wenden tot de auditor. *Note:* Details over de kwetsbaarheden worden niet in paragraaf 1.2 vermeld. Aandachtpunten hierbij zijn: • Het beschrijven van patchmanagementbeleid waarin is aangegeven hoe de organisatie omgaat met updates: hoe snel implementeert de organisatie een 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.

Bijlage 3 – Guidance bij de te onderzoeken DigiD beheersingsmaatregelen (opzet, bestaan en werking)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor
			• Inspecteer of in de organisatie gedurende de gehele controleperiode verbijzonderde interne controle heeft plaatsgevonden op het naleven van de beheersingsmaatregelen rondom het patchmanagement. • Selecteer conform de tabel omvang deelwaarnemingen het juiste aantal patchacties (verzameling patches die in een keer is doorgevoerd) en inspecteer deze op naleving van het patchmanagementbeleid en -proces. • Inspecteer de uitkomsten van de penetratietest op de aanwezigheid van (bekende) beveiligingsissues waarvoor een patch beschikbaar is. Interview de verantwoordelijke functionarissen.

Tabel omvang deelwaarnemingen

NOREA heeft op moment van uitbrengen van deze Handreiking geen algemeen toepasbare methodiek voor het bepalen van de omvang van de deelwaarnemingen bij de toetsing van werking. Onderstaande tabel is ter handreiking. Gebruik van andere methoden is toegestaan, mits daar een rationele argumentatie bij gegeven wordt (comply-or-explain). Ondanks dat processen homogeen van aard kunnen zijn over meerdere DigiD-aansluitingen c.q. applicaties is het uitgangspunt om per assurance-onderzoek (per DigiD-aansluiting) onderstaande omvang te hanteren.

Bij het toetsen van de werking bij de aansluithouder of de serviceorganisaties steunt de auditor op uitgevoerde verbijzonderde interne controles op de beheersingsmaatregelen gedurende de gehele controleperiode. De auditor toetst de werking van de beheersingsmaatregelen over een **periode van 6 aaneengesloten maanden.** De populatie van de te onderzoeken aspecten (c.q. deelwaarneming) is daarmee beperkt tot de occurrences binnen de periode van 6 maanden.

Factoren die van invloed zijn op het auditrisico, en daarmee op de omvang van de waarnemingen, zijn onder meer:
- Bevindingen uit het verleden
- Wijzigingen in de uitvoering van de interne controle-activiteiten (o.a. personele wijzigingen)
- Veranderingen in de design van de control
- Zwakke controle omgeving (1e-, 2e- en/of 3e-lijnscontrole)

Sampling o.b.v. Frequentie van de beheersingsmaatregel		Minimale omvang van de te verrichten deelwaarnemingen bij een lager auditrisico	Minimale omvang van te verrichten deelwaarnemingen bij een hoger auditrisico
Frequentie op jaarbasis	Aantal occurences in de onderzoeksperiode		
Jaarlijks	of 1 occurrence	1	1
Eens per kwartaal	of 2-4 occurrences	2	2
Eens per maand	of 5-12 occurrences	2	3
Eens per week	of 13-52 occurrences	5	8
Dagelijks	of 53-249 occurrences	15	25

Meer dan dagelijks (recurring)	≥ 250 occurrences	25	40

Context bij voorgaande tabel
Voor de periodiciteit jaarlijks, eens per kwartaal, eens per maand, eens per week en dagelijks wordt een niet-statistische steekproef (deelwaarneming) gehanteerd[13].

Algemeen uitgangspunt voor de oordeelsvorming bij geconstateerde afwijkingen: Er wordt vanuit gegaan dat in de 1e-, 2e- (en eventueel 3e-) lijns controle eventuele fouten reeds gedetecteerd en gecorrigeerd zijn. Indien de auditor een afwijking heeft gevonden waarvoor de auditee al compenserende maatregel(en) heeft getroffen dient dit in de rapportage te worden opgenomen als 'Voldoet met compenserende maatregel'[14]. Indien een (of meerdere) fout(en) worden gevonden die door de auditee niet zijn opgemerkt en gecorrigeerd leidt binnen de binaire oordeelsmethodiek (Voldoet / Voldoet niet) tot 'Voldoet niet'. De mate waarin een maatregel afdoende een fout compenseert is ter beoordeling van de IT-auditor.

[13] Zie voor een uitleg van een statistische en niet-statistische steekproef Controle Standaard 530 van de NBA.
[14] Gebruik van Voldoet met compenserende maatregelen is alleen toegestaan voor normen die op de werking worden getoetst.

Bijlage 4 – Aanvullende Guidance bij het Meervoudig Assessment (MA)

De in deze bijlage beschreven testaanpak maakt het mogelijk om een DigiD Meervoudig 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 Meervoudig Assessment MA.

Deze bijlage 4 bevat uitsluitend de aanvullende testaanpak m.b.t. het DigiD Meervoudig 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 Assessment (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudig Assessment)
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> • Leverancier Meervoudig Assessment (LMA). <u>Nadere toelichting:</u> Belangrijk verschil t.o.v. een ‘regulier’ DigiD assessment is dat de LMA kan worden gezien als vertegenwoordiger van de Aansluithouders Meervoudige Assessment (AMA) en dat derhalve het eigenaarschap binnen de organisatie van de LMA zal moeten worden ingericht. Test aanpak:

Bijlage 4 – Aanvullende Guidance bij Meervoudige Assessment (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudig Assessment)
			• 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 bekend is bij functionarissen betrokken bij webapplicatie gerelateerde onderwerpen.

Bijlage 4 – Aanvullende Guidance bij Meervoudige Assessment (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudig Assessment)
			• 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 ontwikkeling en/of het beheer van de		<u>Betrokken rol(len):</u> • Leverancier Meervoudig Assessment (LMA). <u>Nadere Toelichting</u>: • De LMA is door Logius geregistreerd als aanbieder van een Meervoudig Assessment. • Beschrijving van verantwoordelijkheidsverdeling in het contract tussen LMA en houder. • De onder de meervoudig aansluiting geleverde dienstverlening betreft, conform de eisen van Logius, een SaaS-oplossing waarbij de houders van DigiD aansluitingen als afnemer van de dienst een

Bijlage 4 – Aanvullende Guidance bij Meervoudige Assessment (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudig Assessment)
	webapplicatie is uitbesteed aan een andere organisatie.		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 Meervoudig Assessment 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. Testaanpak: • Onderzoek onder nadere toelichting genoemde aanvullende punten. Non-occurrence:

Bijlage 4 – Aanvullende Guidance bij Meervoudige Assessment (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudig Assessment)
			(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. Doelstelling:	Applicatie Infrastructuur Proces	<u>Betrokken rol(len):</u> • Leverancier Meervoudig Assessment (LMA). <u>Nadere toelichting:</u> • 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 hebben voldoende sterke instellingen. Wijzigingen in

Bijlage 4 – Aanvullende Guidance bij Meervoudige Assessment (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudig Assessment)
	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.		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 gebruikersaccounts na 6 weken niet gebruik en

Bijlage 4 – Aanvullende Guidance bij Meervoudige Assessment (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudig Assessment)
			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 Meervoudig Assessment (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 Assessment (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudig Assessment)
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 Meervoudig Assessment (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 het Meervoudig Assessment 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 webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Applicatie Infrastructuur Proces	Betrokken rol(len): • Leverancier Meervoudig Assessment (LMA). Nadere toelichting:

Bijlage 4 – Aanvullende Guidance bij Meervoudige Assessment (MA)			
Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT-auditor (aanvullende toelichting en testaanpak Meervoudig Assessment)
	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 penetratietest 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 vaak ook 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 door de volgende zaken op de geteste omgeving en de productieomgeving te vergelijken:
    - versie nummer van de software;
    - SSL configuratie van de webserver;
    - security-headers hoofdpagina (voor DigiD-inlog);
    - indien gebruik gemaakt wordt van containerization (docker): evidence van de versienummers van de containers;
    - indien gebruik gemaakt wordt van een deployment-straat: evidence van de deployments naar acceptatie en productie.

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. het assurance-rapport van de serviceorganisatie.

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.