NOTITIE

Aan	:	Betrokkenen bij de testaanpak DigiD-assessments
Datum	:	20 november 2020
Van		NOREA Werkgroep DigiD assessments
Status	:	Versie 1.0
Betreft	:	Update DigiD assessment met Meervoudige Aansluiting 2020

Context en toelichting

Logius heeft als beheerder van het DigiD stelsel een nieuw soort aansluiting mogelijk gemaakt: de “Meervoudige Aansluiting” (MA). Deze aansluitvorm voorziet in de mogelijkheid dat grote groepen gerechtigden, die gebruik maken van gestandaardiseerde dienstverlening van een leverancier (afnemers), voor het gebruik van DigiD op een doelmatige wijze kunnen aansluiten op DigiD. Dit betreft een verbetering ten opzichte van de huidige situatie van groepsaansluitingen waarbij burgers, die gebruik maken van DigiD, niet kunnen vaststellen (op basis van het PKIoverheid certificaat) met welke organisatie zij contact hebben. Algemeen uitgangspunt is dat de Leverancier van een Meervoudige Aansluiting (LMA) de aansluithouders, die gebruik maken 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). Ook voor de MA blijft het normenkader 'Norm ICT-beveiligingsassessment DigiD’ onverkort van toepassing.

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

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

Deze update van de testaanpak maakt het mogelijk om een DigiD assessment MA uit te voeren. Het merendeel van de testaanpak is gelijk aan die van een regulier DigiD Assessment. Waar nodig is de bestaande DigiD testaanpak vertaald op basis van de uitgangspunten van Logius naar de situatie voor een DigiD assessment MA.

Het onderzoek wordt door de auditor uitgevoerd bij de LMA, welke door de houderorganisatie is gemachtigd om een meervoudig assessment uit te laten voeren conform de ‘Handleiding uitvoering ICT-beveiligingsassessment’ versie 2.1 van Logius.’ De machtiging dient de LMA aan te tonen. De LMA zendt het assurancerapport aan Logius, eventueel vergezeld van assurancerapporten van (sub-) service organisatie(s), waaraan de LMA taken heeft uitbesteed en waar de carve-out methode op van toepassing is.

In 2019 heeft NOREA een aanvullende handreiking voor non-occurrence gepubliceerd (9 januari 2019) en in de “Update van de testaanpak DigiD-assessment 2.0” van 26 mei 2020 de testaanpak en verwachte technische maatregelen geactualiseerd. Deze update is in werking getreden op 1 juni 2020. De update is besproken in de NOREA werkgroep DigiD assessments en afgestemd met de Logius. De doelstelling van de NOREA is om met de handreiking aan te geven wat de minimale testaanpak voor de auditor moet zijn voor een DigiD assessment.

Naast een beperkt aantal tekstuele verbeteringen en verduidelijkingen zijn de belangrijkste wijzigingen:

- **U/WA.05:** minimaal de TLS instellingen die het NCSC als ‘Goed’ of ‘Voldoende’ heeft aangemerkt dienen te worden gebruikt.
- **U/PW.03:** de minimale configuratie en het gebruik van HSTS, X-Content-Type-Options, Content-Security-Policy (aangescherpt), en Referrer-Policy is verplicht.

Non-occurrence[1]**:** Voor de normen B.05, U/TV.01, U/WA.02 en C.08 kan de situatie zich voordoen dat dat wel voldaan is aan de opzet van de interne beheersmaatregel, maar het bestaan niet vastgesteld kan worden omdat de relevante gebeurtenis zich niet heeft voorgedaan in de onderzochte periode.

Het normenkader voor het DigiD assessment, zoals gepubliceerd op de Logius website onder '*Norm ICT-beveiligingsassessments DigiD, versie 2.0*' d.d. 16 december 2016 blijft ongewijzigd.

[1] Bij een aantal beveiligingsrichtlijnen kan zich de situatie kan voordoen dat wel voldaan is aan de opzet van de interne beheersmaatregel, maar het bestaan niet vastgesteld kan worden omdat de relevante gebeurtenis zich niet heeft voorgedaan in de onderzochte periode. In situaties dat de relevante gebeurtenis zich niet heeft voorgedaan, kan relevante audit evidence voor het bestaan van de betreffende beheersmaatregel worden verzameld door een deelwaarneming te doen in een proces dat onderworpen is aan dezelfde control (i.c. dezelfde control owner, dezelfde tools, dezelfde registratie, dezelfde workflow, et cetera). In dat geval vermeldt de auditor 'Voldoet' voor de betreffende beheersmaatregel in de tabel oordelen zonder een voetnoot te plaatsen betreffende het toetsen op het bestaan van de beheersmaatregel Als er geen andere deelpopulatie is waarop hetzelfde proces en dezelfde control van toepassing is waarmee het bestaan van de betreffende beheersmaatregel kan worden vastgesteld, dient de auditor 'Voldoet' voor de betreffende beheersmaatregel te vermelden in de tabel oordelen en daarbij met een voetnoot in het rapport aan te geven dat het bestaan van de beheersmaatregel niet kon worden getest omdat de relevante gebeurtenis zich niet heeft voorgedaan, noch er een andere deelpopulatie is waarop hetzelfde proces en dezelfde control van toepassing is. Nonoccurrence kan zich alleen voordoen bij de normen B.05, U/TV.01, U/WA.02 en C.08.

Bijlage. Testaanpak bij de te onderzoeken normen

Tabel beveiligingsrichtlijnen met aandachtspunten (Richtlijnen uit: ICT-Beveiligingsrichtlijnen voor Webapplicaties. Versie VERDIEPING. Nationaal Cyber Security Centrum. September 2015)

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
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. Doelstelling: 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	Betrokken rol(len): • Applicatie-, hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting. • Leverancier Meervoudige Aansluiting (LMA). Scope: • De contracten en/of Service Level Agreements voor de levering hosting-, applicatie- of SAAS diensten. Nadere toelichting: 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 gebruikersorganisatie mag hebben; • Service Level Reporting; • het jaarlijks uitvoeren van audits bij de leverancier(s); • beding dat deze voorwaarden back-to-back worden doorgegeven aan mogelijke subleveranciers. Aanvullend voor assessment Meervoudige Aansluiting: • De LMA is door Logius geregistreerd als aanbieder van een Meervoudige Aansluiting. • Beschrijving van verantwoordelijkheidsverdeling in het contract tussen LMA en houder.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			• 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 voldoende homogene doelgroep vormen die onder een gelijke wettelijke bepaling gerechtigd zijn het BSN te verwerken. Initieel stelt Logius dit vast als onderdeel van de accreditatie. Tijdens de DigiD assessment toont de LMA aan de auditor aan dat de dienstverlening nog steeds aan de uitgangspunten voor een Meervoudige Aansluiting voldoet. • Bepaling in contract dat een houder wordt afgesloten van de dienstverlening door de LMA als deze de noodzakelijke beheersingsmaatregelen t.b.v. het DigiD assessment niet naleeft. • De houder accepteert de gegevensclassificatie zoals opgesteld door de LMA. • De LMA verantwoordt zich jaarlijks schriftelijk aan de houders over (veranderingen in) gegevensclassificatie en de naleving van gerelateerde maatregelen. <u>Test aanpak</u>: • Interview de verantwoordelijke functionarissen. • Inspectie van het beveiligingsbeleid. • Inspectie van contracten met leveranciers, SLA's en andere gerelateerde documenten. <u>Aanvullend voor assessment Meervoudige Aansluiting:</u> • Onderzoek onder nadere toelichting genoemde aanvullende punten. <u>Non-occurrence (voor het onderdeel Service Level Reporting en schriftelijke verantwoording gegevensclassificatie door LMA):</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. • T.a.v. schriftelijke verantwoording gegevensclassificatie door LMA aan houders kan bij de 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 voetnoot 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	Applicatie Infrastructuur Proces	<u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting. • Leverancier Meervoudige Aansluiting (LMA) <u>Scope:</u> • De DigiD webapplicatie, DigiD webservers en de firewalls, IDS/IPS, etc.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
	het automatiseren van arbeidsintensieve taken. Doelstelling: Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit.		Nadere toelichting: De focus ligt op de beheerprocessen. Dit betreft enerzijds toegang tot de DigiD-applicatie en anderzijds toegang tot de DigiD webservers en de firewalls, IDS/IPS, etc. die een koppeling hebben met de DigiD omgeving. Aandachtspunten hierbij zijn: • Toekennen, controleren 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. • Uitvoeren periodieke reviews. Specifieke aandacht gaat uit naar wachtwoorden die leveranciers hebben om toegang tot de systemen of data van de houder van de DigiD aansluiting te krijgen (wie hebben die wachtwoorden, hoe worden die opgeslagen en wie hebben toegang. Hoe vaak worden ze gewijzigd, et cetera). Aanvullend voor assessment Meervoudige Aansluiting: • 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 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 LMA bewaakt dit proces. Eventueel kan de LMA er voor kiezen een houder te blokkeren zolang deze verplichte controle niet is uitgevoerd. Voor de 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 blokkade van gebruik van een gebruikersaccount door meerdere personen voor zover dit laatste technisch mogelijk is. Test aanpak: • Interview de verantwoordelijke functionarissen.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor

			• Inspecteer het beveiligingsbeleid, joiners/movers/leavers procedure, de autorisatieprocedure, afspraken met leveranciers met betrekking tot toegang tot systemen en data en andere gerelateerde documenten.
			• Stel voor elk van deze processen en systemen, het bestaan vast met een deelwaarneming van tenminste één.
			• de toegekende autorisaties en de resultaten en opvolging van de periodieke review.
			<u>Aanvullend voor assessment Meervoudige Aansluiting:</u>
			• Onderzoek onder nadere toelichting genoemde aanvullende punten.
			
			<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> Effectief en veilig realiseren van de dienstverlening.	Applicatie Proces	<u>Betrokken rol(len):</u> • Applicatie of SAAS leverancier. • Houder van de DigiD-aansluiting. <u>Scope</u>: • De DigiD webapplicatie. <u>Nadere toelichting</u>: Deze norm richt zich meer op de procesmatige aspecten van het functioneel en het applicatiebeheer. Aandachtspunten hierbij zijn: • Beschrijving van taken, verantwoordelijkheden en bevoegdheden van de verschillende beheerrollen. • Een incidentenprocedure is opgesteld. • Meldingen van het NCSC of IBD of Z-CERT of andere CERTS worden geanalyseerd en zo nodig opgevolgd. • Incidenten worden geregistreerd, geanalyseerd, opgevolgd en afgehandeld. • Er is een periodieke rapportage aan het management inzake beveiligingsincidenten. <u>Test aanpak</u>: • Interview de verantwoordelijke functionarissen. • Inspecteer de functie/taakbeschrijvingen van beheerders.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			• Inspecteer het incidentproces, de uitgevoerde analyse, de managementrapportage en opvolging van beveiligingsincidenten. Non-occurrence (voor het onderdeel opvolging van beveiligingsincidenten): • Voor het proces 'incidentmanagement', waarbij geldt dat op basis van (deel)waarnemingen binnen een proces dat onderworpen is aan dezelfde control , vastgesteld moet worden dat een incidentenprocedure effectief is geïmplementeerd. • Voor het proces 'periodieke rapportage aan het management', waarbij geldt dat op basis van (deel)waarnemingen t.a.v. een plaatsgevonden incident binnen een proces dat onderworpen is aan dezelfde control, vastgesteld moet worden dat rapportages aan het management inzake beveiligingsincidenten structureel plaatsvinden.
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt. Doelstelling: Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.	Applicatie	Betrokken rol(len): • Applicatie- of SAAS leverancier. Scope: • De DigiD webapplicatie en webserver. Nadere toelichting: Ongecontroleerde (ongevalideerde) invoer van gebruikers is een belangrijke bedreiging 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 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.). 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. Indien uit de test grote tekortkomingen naar voren komen wordt deze 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.

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

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
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. • Houder van de DigiD-aansluiting. • Leverancier Meervoudige Aansluiting (LMA) Scope: • De DigiD webapplicatie en webserver en bijbehorende infrastructuur. Nadere toelichting Deze norm raakt diverse aspecten van privacy bevorderende en cryptografische technieken. Dit betreft de classificatie van gegevens, de encryptie van gevoelige gegevens tijdens de opslag en de encryptie van gegevens tijdens transport. Aandachtspunten hierbij zijn: • De classificatie van gegevens door de houder van de DigiD aansluiting op basis van een risico analyse. • 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 in de backoffice vallen buiten de scope van dit onderzoek. • De HTTPS configuratie en de TLS configuratie. De publicatie in 2019 door het NCSC van de vernieuwde ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)v2 is aanleiding om de richtlijnen voor TLS aan te scherpen. Concreet dienen minimaal de TLS instellingen die het NCSC als 'Goed' of 'Voldoende' heeft aangemerkt te worden gebruikt. Aanvullend voor assessment Meervoudige Aansluiting: • In afwijking van de eerste bullet. 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. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer de classificatie van gegevens en daaraan gerelateerde risico analyse, de netwerkarchitectuur en het inrichtingsdocument waar de encryptie van gegevens in staat beschreven. • Observeer de encryptie van gegevens. Inspecteer de HTTPS en TLS configuraties. Aanvullend voor assessment Meervoudige Aansluiting: • Onderzoek onder nadere toelichting genoemde aanvullende punten.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Applicatie	Betrokken rol(len): • Applicatie-, hosting- of SAAS leverancier.
	Doelstelling: Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.		Scope: • De webserver. Nadere toelichting: HTTP headers moeten de risico's beperken van inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie. Aandachtspunten hierbij zijn: • Behandel alleen HTTP-requests waarvan de gegevens een correct type, lengte, formaat, tekens en patronen hebben. • Behandel alleen HTTP-requests van initiators met een correcte authenticatie en autorisatie. • Sta alleen de voor de ondersteunde webapplicaties benodigde HTTP-requestmethoden (GET, POST, etc.) toe en blokkeer de overige niet noodzakelijke HTTP-requestmethoden. • Verstuur alleen HTTP-headers die voor het functioneren van HTTP van belang zijn. • Toon in HTTP-headers alleen de hoogst noodzakelijke informatie die voor het functioneren van belang is. • Bij het optreden van een fout wordt de informatie in een HTTP-response tot een minimum beperkt. Een eventuele foutmelding zegt wel dat er iets is fout gegaan, maar niet hoe het is fout gegaan. Test aanpak: • Observeer het gedrag van de HTTP headers en responses. Voer hierbij een representatieve deelwaarneming uit op de invoer- en uitvoermogelijkheden die de applicatie biedt.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/PW.03	De webserver is ingericht volgens een configuratie-baseline. Doelstelling: Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.	Applicatie Infrastructuur	Betrokken rol(len): • Applicatie-, hosting- of SAAS leverancier. Scope: • De webserver. 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: Cookie flags staan op 'HttpOnly' en 'Secure'. HTTP security headers bieden steeds meer en fijnmazigere controle over de toegang tot, en het delen van, informatie. Het correct gebruik van security headers levert een extra beveiligingslaag op: • X-Frame-Options De X-Frame-Options header voorkomt dat de pagina in een iFrame wordt geladen, waarmee gegevens kunnen worden gestolen, pagina's worden aangepast of gebruikers worden misleid. Te configureren waarden: deny of sameorigin • Strict-Transport-Security (HSTS) HTTP Strict Transport Security (HSTS) zorgt ervoor dat browsers alleen over TLS communiceren met de webapplicatie. Door het forceren van HTTPS beschermt deze header gebruikers tegen afluisteren en Man-in-the-Middle (MitM)-aanvallen. HSTS voorkomt het gebruik van gemengde HTTP en HTTPS inhoud, beschermt tegen fouten van webservers zoals het laden van JavaScript via een onveilige verbinding en voorkomt dat gebruikers waarschuwingen over ongeldige certificaten kunnen negeren. Minimaal te configureren waarde: max-age=31536000 • X-Content-Type-Options De X-Content-Type-Options header voorkomt dat de browser het MIME-type van een bestand bepaalt op basis van kenmerken (sniffing). Wanneer deze header is ingesteld op nosniff, vertrouwt de browser het MIME-type dat door de server wordt meegegeven en

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			zal de browser de bron blokkeren als deze fout is. Dit voorkomt spoofing van resources zoals CSS stylesheets en Javascript-bestanden die over HTTP worden verstuurd. Te configureren waarde: nosniff • Content-Security-Policy De Content-Security-Policy (CSP) geeft de browser instructies over welke resources vanaf welke locatie mogen worden ingeladen en hoe deze mogen worden gebruikt. Een CSP kan fijnmazige instructies bevatten per soort resource, zoals afbeeldingen, stylesheets en scripts. Bij het gebruik van een CSP zijn standaard de uitvoering van inline scripts en de eval()-functie uitgeschakeld Te configureren waarden: default-src 'self'; frame-src 'self'; frame-ancestors 'self'; Sta geen onveilige configuratie toe door het gebruik van 'unsafe-inline' (tenzij gebruik wordt gemaakt van een nonce) en 'unsafe-eval'. Het is niet toegestaan bronnen beginnend met http:// te whitelisten. • Referrer-Policy De Referrer-Policy beperkt het ongevraagd delen van privacygevoelige informatie bij het doen van verzoeken aan, en bij het doorsturen van de gebruiker naar, een andere website. Gebruik de instelling 'same-origin', zodat de referrer-header alleen wordt meegestuurd bij verzoeken binnen het eigen domein. Dit voorkomt het lekken van privacygevoelige informatie bij omleiden naar externe domeinen. De striktere instelling 'no-referrer' kan ook worden gebruikt, zodat de referrer-header nooit wordt meegestuurd. Test aanpak: • Interview de verantwoordelijke functionarissen. • 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.

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. Doelstelling: Voorkomen van misbruik van beheervoorzieningen.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • De webserver en andere servers in de DMZ. Nadere toelichting: Dit betreft het gebruik van veilige netwerkprotocollen. Indien beheerinterfaces via het internet te benaderen zijn moet dit door middel van twee factor authenticatie, zoals de combinatie van een wachtwoord en source IP filtering, in combinatie met een veilig (communicatie) protocol worden afgehandeld. Er mag geen gebruik worden gemaakt van backdoors om de systemen te benaderen (ook niet voor noodtoegang). Daarnaast wordt een beknopt operationeel beleid verwacht. Aandachtspunten voor deze norm zijn: • Het gebruik van veilige protocollen (conform industrie standaarden) voor het benaderen van beheermechanismen (beheerinterfaces). • Het gebruik van sterke authenticatie voor zowel technisch als functioneel beheerders. Test aanpak: • Interview de verantwoordelijke functionarissen. • 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.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar. Doelstellingen: Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • De webserver en andere ICT componenten binnen de DMZ. Nadere toelichting: Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar. Hierbij kan worden verwezen naar actuele hardening-richtlijnen van de leverancier(s)/SANS/NIST/CIS met een vermelding van "pas toe of leg uit". Hierbij spelen de geïdentificeerde risico's in de "pas toe of leg uit" afweging een bepalende rol. Het gaat echter niet alleen om de hardeningsrichtlijn zelf, maar ook om het concreet toepassen ervan. De hardening van de DigiD webomgeving dient stringent te zijn geregeld: alles wat open staat moet een reden hebben en alles wat open staat moet secure worden aangeboden. De hardening van interne systemen mag minder stringent. Wel moeten de beheer functies secure zijn en mogen er geen onveilige protocollen worden gebruikt, moeten standaard wachtwoorden zijn gewijzigd. Voorbeeld applicaties moeten zijn verwijderd als deze niet daadwerkelijk worden gebruikt. Aandachtspunten hierbij zijn: • Inrichting van ICT-componenten (aantoonbaar) volgens de instructies en procedures van de leverancier. • Bijhouden van een actueel overzicht bij van de noodzakelijke protocollen, services en accounts voor de op het platform geïnstalleerde applicaties. • Deactiveren of verwijderen van alle protocollen, services en accounts op het platform als die niet volgens het ontwerp noodzakelijk zijn. • Periodiek toetsen of de in productie zijnde ICT-componenten niet meer dan de vanuit het ontwerp noodzakelijke functies bieden (statusopname). Afwijkingen worden hersteld. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer de architectuur en hardening standaarden. • Inspecteer de configuratiebestanden en de uitkomsten van de penetratietest.
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:	Infrastructuur	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • De DMZ van de DigiD webapplicatie.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
	Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.		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: • Interview de verantwoordelijke functionarissen. • Inspecteer het netwerkarchitectuur schema inclusief de toegestane verkeersstromen tussen netwerksegmenten. • Inspectie van configuratie files, firewall regels en de uitkomsten van de penetratietest.
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen. Doelstelling: Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	Infrastructuur	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • De DMZ van de DigiD webapplicatie. Nadere toelichting: Beveiligingsrichtlijnen NW.04, C.06 en C.07 hangen nauw met elkaar samen: - 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. 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. Aandachtpunten hierbij zijn: • Het gebruik van een IDS of IPS 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 ingezet. • Het gebruik van een adequate ruleset (b.v. Snort, Suricata, ETPro, etc.) die periodiek (= minimaal wekelijks) wordt geactualiseerd.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer het netwerkarchitectuur schema, de inrichtingsdocumentatie en de beheerprocedure van de IDS/IPS. • Inspecteer de configuratiefiles van het IDS/IPS en de signature datum van de regelset.
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd. Doelstelling: Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • Het netwerksegment met de webservers die een koppeling hebben met de DigiD omgeving van Logius inclusief de toegang vanuit internet. 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 de voor het beheer uitsluitend veilige netwerkprotocollen mogen worden gebruikt. • Er is een inrichtingsdocument waaruit blijkt op welke wijze content beheer (web- en database-content), applicatiebeheer en technisch beheer worden uitgeoefend. • Het gebruik van fysieke scheiding, veilige VPN verbindingen (zoals IPSec) of VLANs het beheer- en productieverkeer van elkaar gescheiden. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer het netwerkarchitectuurschema inclusief de toegestane verkeersstromen tussen netwerksegmenten. • Inspecteer de configuratie files, firewall regels en de uitkomsten van de penetratietest.

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. • Houder van de DigiD-aansluiting. • Leverancier Meervoudige Aansluiting (LMA) Scope: • De webserver en andere ICT componenten binnen de DMZ. Nadere toelichting: Voor het configureren van netwerkcomponenten is een hardeningrichtlijn beschikbaar. Hierbij kan worden verwezen naar actuele hardening-richtlijnen van de leverancier(s)/SANS/NIST/CIS met een vermelding van "pas toe of leg uit". Hierbij spelen de geïdentificeerde risico's in de "pas toe of leg uit" afweging een bepalende rol. Het gaat echter niet alleen om de hardeningrichtlijn zelf, maar ook om het concreet toepassen ervan. De hardening van de DigiD omgeving dient stringent te zijn geregeld: alles wat open staat moet een reden hebben en alles wat open staat moet secure worden aangeboden. De hardening van interne systemen mag minder stringent. Wel moeten de beheer functies secure zijn en mogen er geen onveilige protocollen worden gebruikt, moeten standaard 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. Aandachtspunten hierbij zijn: • Bijhouden van een actueel overzicht van de noodzakelijke netwerkprotocollen, -poorten en -services. • Uitschakel op de netwerkcomponenten alle netwerkprotocollen, -poorten en –services uit, behalve de noodzakelijke. • Aanpassen de (beveiligings)configuraties van netwerkprotocollen, -poorten en -services op de netwerkcomponenten aan conform richtlijnen. Aanvullend voor assessment Meervoudige Aansluiting: • De LMA heeft een monitoringsoplossing ingericht waarmee maandelijks wordt vastgesteld dat voor de domeinnamen van alle houders DNSSEC correct is geconfigureerd. In geval een nieuwe houder aan de Meervoudige Aansluiting wordt toegevoegd zal deze controle direct plaatsvinden. Hierna gaat deze mee in de maandelijkse cyclus. • Voor de DigiD assessment is jaarlijks een rapportage beschikbaar met de data van de monitoringsoplossing. Test aanpak:

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			• Interview de verantwoordelijke functionarissen. • Inspecteer de netwerkarchitectuur schema en hardening-richtlijnen. • Inspecteer de configuratiebestanden en de uitkomsten van de penetratietest. <u>Aanvullend voor assessment Meervoudige Aansluiting:</u> • Onderzoek onder nadere toelichting genoemde aanvullende punten.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICTcomponenten van de webapplicatie (scope). Doelstelling: Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de webapplicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting: Deze netwerk based scan dient zich ten minste gericht te hebben op de resultaten van de hardening en patching van de infrastructuur en het detecteren van mogelijke kwetsbaarheden op de infrastructuur. • 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. Test aanpak: • Interview de verantwoordelijke functionarissen. • 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.
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	Applicatie Infrastructuur Proces	Betrokken rol(len): • Applicatie-, hosting- of SAAS leverancier. Scope: • De DigiD webapplicatie, de webserver en andere servers in de DMZ van de DigiD webapplicatie. Nadere toelichting: De voorkeur heeft het op basis van een risicoafweging enkele keren per jaar een penetratietest te laten uitvoeren, zodat ingespeeld kan worden op nieuwe bedreigingen.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
	misbruiken van webapplicatie).		• De penetratietest dient minimaal eenmaal per jaar te worden uitgevoerd en na significante wijzigingen, zoals vervanging applicatie, nieuwe versie, migratie webservers, database migratie, et cetera. • De scope van de penetratietest omvat tenminste de webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. • Naar aanleiding van de resultaten van de penetratietest is een actieplan opgesteld om de tekortkomingen op te heffen. • Er is voldoende voortgang geboekt in het opvolgen van bevindingen gezien de aard en complexiteit van de bevindingen. <u>Testaanpak:</u> • Interview de verantwoordelijke functionarissen. • 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.
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. <u>Doelstelling:</u> Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	Infrastructuur Proces	<u>Betrokken rol(len):</u> • Hosting- of SAAS leverancier. <u>Scope:</u> • De infrastructuur voor het netwerksegment met de DigiD webapplicatie. <u>Nadere toelichting</u> Beveiligingsrichtlijnen NW.04, C.06 en C.07 hangen nauw met elkaar samen: - 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 zijn: • Het definiëren van alarm situaties en drempelwaarden. • Het configureren van de alarm situaties en drempelwaarden in het IDS/IPS en het genereren van de bijbehorende alerts. • De inbedding van alert afhandeling in het incidentenbeheerproces inclusief escalatieprocedure.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspectie van de Use Cases en drempelwaarden. • Inspectie van alerts en de opvolging daarvan.
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICTsystemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd. Doelstelling: Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.	Infrastructuur Proces	Betrokken rol(len): • Hosting- of SAAS leverancier. Scope: • De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting Beveiligingsrichtlijnen NW.04, C.06 en C.07 hangen nauw met elkaar samen: - 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: o wijzigingen aan de configuratie van webapplicaties; o optreden van verdachte gebeurtenissen en eventuele schendingen van de beveiligingseisen; o ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden; o toegangslogs; • Periodieke analyse op ongebruikelijke situaties (incidenten) die de werking van webapplicaties kunnen beïnvloeden. • Periodiek rapportage van de geanalyseerde en beoordeelde gelogde gegevens aan de systeemeigenaren en/of aan het management. • Opvolging van bevindingen naar aanleiding van de analyse. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspectie van de procedurebeschrijving met betrekking tot de logging.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			• Inspectie van de vastlegging van de periodiek review van de logging, periodieke rapportage aan het management en follow-up acties naar aanleiding van review en analyse van de logging.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
C.08	Wijzigingenbeheer 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. • Houder van DigiD aansluiting. • Leverancier Meervoudige Aansluiting (LMA) Scope: • De DigiD webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. 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. 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 netwerk wijzigingen is een testomgeving vaak niet mogelijk). • Het hanteren van een testscript en de vastlegging van de testresultaten. • Een formele acceptatie voor het in productie nemen van de wijziging. • Het beperken van het aantal personen die wijzigingen in productie kunnen nemen. • Bij het uitbrengen van een nieuwe release van de applicatie of een grote upgrade van het onderliggende platform moet, bij voorkeur door middel van een penetratietest, worden onderzocht of er geen nieuwe kwetsbaarheden zijn geïntroduceerd. Aanvullend voor assessment Meervoudige Aansluiting: • 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. Test aanpak: • Interview de verantwoordelijke functionarissen.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
			• Inspecteer de wijzigingsprocedure en de inrichting van de OTAP omgeving. • Inspecteer, voor elk type wijziging (applicatie, servers, netwerk), één wijziging en de daaraan gerelateerde documentatie. <u>Aanvullend voor assessment Meervoudige Aansluiting:</u> • Onderzoek onder nadere toelichting genoemde aanvullende punten. <u>Non-occurrence (voor het onderdeel inspecteren van een doorgevoerde wijziging):</u> Hierbij geldt dat op basis van (deel)waarnemingen binnen een proces dat onderworpen is aan dezelfde control vastgesteld moet worden dat de wijzigingsprocedure effectief is geïmplementeerd.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
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 aangepakt en zo een stabiele omgeving wordt gecreëerd.	Applicatie Infrastructuur Proces	Betrokken rol(len): • Applicatie-,Hosting- of SAAS leverancier. Scope: • Hypervisor (VM Ware, etc.). • Operating system (Windows, etc.). • Databases. • Netwerk componenten. • Firewall. • Webapplicatie en daarvoor benodigde software componenten Nadere toelichting: De focus is op het patching proces. Dit proces kan gedifferentieerd zijn naar bijvoorbeeld het OS, DBMS en netwerk. Applicaties en systemen dienen periodiek gepatcht te worden. Een maandelijks patching cyclus is aanvaardbaar tenzij er security alerts zijn. Voor internet facing systemen dienen de laatste stabiele beveiligingspatches te zijn geïnstalleerd. Indien patching niet mogelijk is in verband met een legacy applicatie die niet meer zou functioneren na patching, zal dit risico aantoonbaar moeten zijn afgewogen. Aandachtpunten hierbij zijn: • Het beschrijven van patchmanagementbeleid waarin is aangegeven hoe de organisatie omgaat met updates: hoe snel implementeert de organisatie een 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. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspectie van het patchmanagementbeleid. • Inspectie van configuratie files en de uitkomsten van de penetratietest.