NOTITIE

Aan	:	IT auditors
Datum	:	19 december 2016
Van	:	NOREA Werkgroep DigiD assessments
Betreft	:	Handreiking bij DigiD-assessments V2.0

Aanleiding

Naar aanleiding van een analyse van de resultaten van ICT-beveiligingsassessments DigiD van de afgelopen jaren en het uitbrengen van nieuwe beveiligingsrichtlijnen voor webapplicaties door het NCSC, heeft BZK het normenkader voor het uitvoeren van DigiD ICT-beveiligingsassessments geactualiseerd: Norm ICT-beveiligingsassessments DigiD versie 2.0 (hierna de "DigiD Norm v2.0").

Doel handreiking

Doelstelling van deze handreiking is de IT-auditor een uniform toetsbaar kader te bieden voor het zorgvuldig uitvoeren van een DigiD-assessment op basis van de DigiD Norm 2.0. Dit kader geldt voor controlejaar 2017 en verder. De handreiking geeft de bandbreedte aan waarbinnen de auditor de werkzaamheden verricht. Voorkomen moet worden dat er grote verschillen ontstaan in de mate van diepgang bij uitvoering van de audits als bij het beoordelen van afwijkingen. Waar mogelijk / wenselijk moet ook duidelijk zijn wat minimaal c.q. maximaal gedaan zou moeten worden om tot redelijke zekerheid te komen. Het is daarom uitdrukkelijk niet de bedoeling voor het assessment aanvullende normen van de NCSC richtlijnen af te leiden. De NCSC richtlijnen zijn namelijk primair bedoeld voor het lijnmanagement dat verantwoordelijk is voor het ontwerpen, implementeren en het beheer van webapplicaties en zijn niet primair opgezet als normen voor een audit. Zoals ook gold voor de Norm v1.0, bevat de Norm v2.0 een selectie van de NCSC richtlijnen. NOREA begrijpt en respecteert ook de uitgangspunten van BZK voor wat betreft de inperking van het assessment. Dit doet niet af aan de opvatting van de NOREA dat organisaties er goed aan doen om op basis van een risicoanalyse te bepalen welke overige beveiligingsrichtlijnen geïmplementeerd moeten worden om zodoende de risico's van onbetrouwbare werking van informatiesystemen te beperken.

De handreiking geeft een leidraad voor overleg tussen IT-auditors onderling, met name bij de afstemming tussen de auditor van de houder van een DigiD aansluiting en de auditor van

de serviceorganisatie waar de houder gebruik van maakt. Het blijft echter de professionele verantwoordelijkheid van de IT-auditor om op basis van een deugdelijke grondslag tot een oordeel te komen per norm. De richtlijn 3000 van de NOREA is daarbij leidend. Bij verschillen van inzicht is het primair aan de betrokken auditors om in overleg tot een oplossing te komen. De NOREA werkgroep DigiD assessments kan daarbij eventueel als gesprekspartner deelnemen.

Voor substantiële meningsverschillen heeft de NOREA een procedure vastgesteld waarmee (via de Vaktechnische Commissie) een collegiaal standpunt wordt gegeven.

Achtergrond DigiD-assessment

De aanleiding voor het uitvoeren van de ICT-beveiligingsassessments bij organisaties die gebruik maken van DigiD is de brief van de minister van BZK aan de Tweede Kamer 'Lekken in een aantal gemeentelijke websites' d.d. 11 oktober 2011 met kenmerk 2011-2000454268. De minister van BZK zegt hier onder punt 3 toe dat '… alle DigiD gebruikende organisaties … hun ICT beveiliging getoetst dienen te hebben op basis van een ICT beveiligingsassessment.'. Verder is bepaald dat de ICT-beveiligingsassessments jaarlijks herhaald dienen te worden. Tevens wordt de basisnorm voor de assessment vastgesteld door GOVCERT.NL (nu NCSC) in overleg met VNG/KING. GOVCERT.NL zal de normstelling regelmatig actualiseren. Uit de brief komt een tweetal aandachtsgebieden voor het ICT-beveiligingsassessment naar voren:

- Aanleiding voor het opstellen van de kamerbrief is een aantal lekken / kwetsbaarheden in gemeentelijke websites die vanaf het internet te misbruiken waren. Dit betekent dat een belangrijk aandachtsgebied in ieder geval externe (vanaf het internet) bedreigingen voor de webapplicatie zijn.
- In de brief wordt meerdere malen het belang van het waarborgen van het vertrouwen van de burger in de elektronische overheidsdienstverlening benadrukt. Hierbij wordt specifiek nog het onderscheppen van gegevens van burgers en oneigenlijk gebruik hiervan genoemd. Op hoofdlijnen zijn hiervoor drie aspecten van belang:
    a. de beveiliging van een webapplicatie die gebruik maakt van DigiD moet op orde zijn;
    b. detectieve maatregelen moeten aanwezig zijn waarmee misbruik van een eventuele kwetsbaarheid in de webapplicatie wordt gedetecteerd;
    c. een toereikende incident management procedure dient aanwezig te zijn waarmee adequaat kan worden gereageerd op een incident en gevolgschade kan worden beperkt.

Doelstelling DigiD-assessment

Bij de inrichting van het eerste DigiD-assessment in 2012 is gekozen voor het geven van (aanvullende) zekerheid op basis van de NOREA richtlijn 3000 waarbij per norm een oordeel over opzet en bestaan wordt gegeven. Tevens zijn met name operationele richtlijnen geselecteerd die rechtstreeks bijdragen aan de beveiliging van een DigiD webomgeving. Beleidsgerichte onderwerpen die meer indirect en op langere termijn bijdragen aan de beveiliging, zijn in beperkte mate opgenomen. Voor de ICT-beveiligingsassessments voor controlejaar 2017 e.v. is BZK uitgegaan van continuïteit in deze keuzes. BZK heeft als gevolg hiervan de volgende algemene doelstelling voor een DigiD-assessment vanaf controlejaar 2017 geformuleerd:

> *Het verschaffen van aanvullende zekerheid over de opzet en het bestaan in een DigiD webomgeving van een aantal beveiligingsmaatregelen die zijn gebaseerd op een selectie uit de actuele ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC en die gericht zijn op enerzijds de preventie van het optreden van bedreigingen vanaf internet en anderzijds de detectie en de incident response indien deze bedreigingen zich toch manifesteren.*

Norm ICT-beveiligingsassessments DigiD versie 2.0 (de Norm v2.0)

De Norm v2.0 geldt voor het assessment jaar 2017 en verder. Ten opzicht van de Norm v1.0, is in de Norm v2.0 een aantal normen vervangen en is de nummering en terminologie van de nieuwe beveiligingsrichtlijnen gehanteerd. In bijlage 4 is een nadere toelichting op de totstandkoming van het nieuwe normenkader opgenomen en is een omnummeringstabel voor de oude en nieuwe normen opgenomen op basis waarvan een auditdossier kan worden omgezet naar de nieuwe indeling. Uitgangspunt van BZK is dat de audit inspanning voor een DigiD assessment op basis van de Norm v2.0 ten opzicht van de Norm v1.0 gelijk blijft en bij voorkeur zelfs iets minder wordt.

Formele aspecten van de opdracht

De opdrachten inzake de DigiD-beveiligingsassessments worden door RE's uitgevoerd in het kader van het Raamwerk voor Assurance-opdrachten en (dus) overeenkomstig Richtlijn 3000 'Assurance-opdrachten'. Zowel voor het assessment bij de houder van DigiD als bij de serviceorganisatie is een modelrapport opgesteld. Zie bijlage 1. Daarnaast gelden tevens 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 v2.0, over de opzet en het bestaan van de maatregelen gericht op de ICT beveiliging van de webomgeving van DigiD aansluiting. Het feit dat de Norm v2.0 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. Dit is expliciet in de tekst van het Modelrapport opgenomen.

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

In de huidige opzet beperkt de audit zich tot het beoordelen van de opzet en het toetsen van het bestaan van de beheersmaatregelen. Indien bij een beveiligingsrichtlijn wel voldaan is aan de opzet van de interne beheersmaatregel, maar het bestaan niet vastgesteld kan worden omdat de relevante gebeurtenis zich niet heeft voorgedaan in de onderzochte periode dan wordt dit weergegeven als "voldoet". In een voetnoot wordt de volgende zin opgenomen: ''Wij hebben vastgesteld dat deze organisatie maatregelen heeft ontworpen en ingericht met betrekking tot deze norm en hebben deze gevalideerd. Vanwege het feit dat zich geen situatie heeft voorgedaan waarop deze maatregel betrekking heeft, hebben wij het bestaan niet kunnen vaststellen. Wij zijn echter van oordeel dat de organisatie voldoet aan deze norm."

Voor de diepgang van het onderzoek impliceert uitsluitend beoordeling van opzet en bestaan op den duur schijnzekerheid als niet ook de werking in de beoordeling wordt betrokken. NOREA is van mening dat uiteindelijk ook de werking van de beheersmaatregelen beoordeeld dient te worden. NOREA heeft dit eerder onder de aandacht van BZK gebracht. NOREA zal aan de hand van het nieuwe normenkader nagaan voor welke normen dit relevant en toepasbaar is. Er dient echter apart besloten te worden op welk moment ook de werking beoordeeld gaat worden.

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

- zowel de hosting als het applicatiebeheer plus de implementatie in eigen hand van de houder;

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

Ook andere varianten en vormen van ketensamenwerking zijn mogelijk

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

Dit heeft impact op de allocatie van te testen maatregelen over de verschillende betrokken partijen; houders, leveranciers, IT-auditor houder en IT auditor service organisatie. Dit vraagt bijzondere aandacht van de IT-auditor van de houder en de auditor van de leverancier.

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

- normen waarvoor de houder verantwoordelijk is;
- normen waarvoor de leverancier verantwoordelijk is;
- normen waarvoor beiden een gedeelde verantwoordelijkheid hebben.

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

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

Object van onderzoek/Scope

Het DigiD landschap bestaat op hoofdlijnen uit:

1. de centrale DigiD voorziening;
2. de burger als eindgebruiker;
3. een webapplicatie waarmee bijvoorbeeld een gemeente of ziektekostenverzekeraar elektronische dienstverlening aan de burger aanbiedt. De omgeving heeft een aansluiting op de centrale DigiD voorziening en ondersteunt (een deel van) een bedrijfsproces. De omgeving bestaat uit een verzameling van ICT-infrastructuur, systeemkoppelingen, software, data, (beheer-) processen inclusief bijbehorende organisatie(s);
4. het beheer van de webapplicatie.

Het object van onderzoek van een ICT-beveiligingsassessment is een webapplicatie die gebruik maakt van DigiD voor de identificatie en authenticatie van (een deel van) de gebruikers. Specifiek zijn in scope de internet-facing webpagina's, systeemkoppelingen en de infrastructuur die met DigiD gekoppeld zijn en betrekking hebben 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. Aan deze afbakening ligt een afweging ten grondslag tussen enerzijds het beperken van de scope van het onderzoek waardoor het uitvoerbaar blijft voor alle partijen en anderzijds het risico (blijven) lopen dat DigiD bij een houder alsnog kwetsbaar is via een kwetsbare andere applicatie, die niet bij het DigiD proces is betrokken. In de praktijk dienen zich veel verschillende vormen van digitale dienstverlening en de inzet van DigiD als authenticatiemiddel aan. Dit vereist dat de IT-auditor voorafgaand aan de feitelijke audit zorgvuldig de scope en de afhankelijkheden van het te onderzoeken object in beeld brengt.

Onderzoeksaspecten

De onderzochte aspecten zijn volgens BZK exclusiviteit en integriteit. Beschikbaarheid wordt wel als belangrijk gezien voor de dienstverlening aan burgers, maar het bekend worden van vertrouwelijke gegevens of ongeautoriseerd wijzigen / verwijderen van gegevens zal het vertrouwen van de burger in e-overheid veel meer schaden dan het niet voldoende beschikbaar zijn van het systeem. Zeker voor de grote diensten die gebruik maken is

beschikbaarheid wel een belangrijk aspect, maar dit valt buiten de scope van het DigiD assessment.

Uitvoering DigiD assessment

Voor de uitvoering van een DigiD assessment zijn de normen inclusief guidance zoals opgenomen in bijlage 2 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 test aanpak zoals opgenomen in de guidance per norm en niet op basis van alle achterliggende NCSC richtlijnen. Daarbij neemt de IT-auditor het risicoprofiel van de DigiD aansluiting in aanmerking en test of de IST situatie voldoet aan de SOLL situatie. De geschetste guidance is een gemiddelde. De normen mogen niet beschouwd worden als af te vinken resultaatverplichtingen. 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 3 worden aandachtspunten gegeven voor het uitvoeren van penetratietesten en vulnerability assessments. In bijlage 5 worden verder enkele kernbegrippen bij DigiD assessments toegelicht.

ENSIA voor gemeenten

Een ontwikkeling die relevant is voor de DigiD assessments is ENSIA (Eenduidige Normatiek Single Information Audit). Dit is een gezamenlijk project van het Ministerie van Binnenlandse Zaken, gemeenten, het ministerie van SZW, het ministerie van I&M en de VNG. Het project heeft tot doel het verantwoordingsproces over de informatiebeveiliging bij gemeenten verder te helpen professionaliseren door het verdeelde toezicht te bundelen en aan te laten sluiten op de gemeentelijke P&C-cyclus. Mogelijk worden DigiD assessments voor gemeenten als gevolg van ENSIA voor controlejaar 2017 op een andere wijze uitgevoerd. Voor andere partijen verandert de werkwijze niet. Meer hierover is te vinden op de site www.ensia.nl.

Bijlage 1. Modelrapporten voor DigiD assessment

a. Houder van DigiD

Separaat opgenomen.

b. Serviceorganisatie

Separaat opgenomen.

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Bijlage 2. Guidance bij de te onderzoeken normen

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

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
B.05	B0-14	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 partij(en): • Applicatie-, hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting. 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 diensten die onder het contract vallen; • de van toepassing zijnde leveringsvoorwaarden; • informatiebeveiligingeisen met de relevante eisen vanuit het beveiligingsbeleid; • het melden van beveiligingsincidenten en datalekken; • 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 sub-leveranciers.

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
				Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspectie van het beveiligingsbeleid. • Inspectie van contracten met leveranciers, SLAs en andere gerelateerde documenten.
U/TV.01	B0-12 (2)	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.[1] 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.	Applicatie Infrastructuur Proces	Betrokken partij(en): • Applicatie-, hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting. Scope: • De DigiD webapplicatie., Digid webservers en beheerinterfaces van de firewalls, routers, IDS/IPS, etc. Nadere toelichting: De focus ligt op de beheerprocessen. Dit betreft enerzijds toegang tot de DigiD-applicatie en anderzijds toegang tot de webservers die een koppeling hebben met de DigiD omgeving van Logius, de routers en de firewalls. Aandachtspunten hierbij zijn: • 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, etc.). Test aanpak: • Interview de verantwoordelijke functionarissen. • 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

[1] In het document RICHTLIJNEN september 2015 van het NCSC staat een afwijkende omschrijving. Deze is onjuist.

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
				deelwaarneming van ten minste één.
U/WA.02	N.v.t.	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. Doelstelling: Effectief en veilig realiseren van de dienstverlening.	Applicatie Proces	Betrokken partij(en): • Applicatie of SAAS leverancier. • Houder van de DigiD-aansluiting. Scope: • De DigiD webapplicatie. Nadere toelichting: Deze norm richt zich meer op de procesmatige aspecten van het functioneel en het applicatiebeheer. Aandachtspunten hierbij zijn: • Beschrijving van taken, verantwoordelijkheden en bevoegdheden van de verschillende beheerrollen. • Autorisatiematrix waarin tot uitdrukking komt welke autorisaties aan welke beheerrollen (b.v. administrator, publicist, auteur,redacteur) worden toegekend. • Autorisatiebeheerproces voor het onderhouden en toekennen van beheerrollen. • Uitvoeren van een periodieke review. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer de functie/taakbeschrijvingen van beheerders, de autorisatiematrix en het autorisatiebeheerproces. • Inspecteer de toegekende autorisaties en de resultaten en opvolging van de periodieke review.
U/WA.03	B3-1	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 partij(en): • Applicatie- of SAAS leverancier. Scope: • De DigiD webapplicatie en webserver. Nadere toelichting: Ongecontroleerde (ongevalideerde) invoer van gebruikers is een belangrijke dreiging voor een webapplicatie. Als invoer van gebruikers rechtstreeks wordt gebruikt in HTML-uitvoer, cookie-waarden, 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.

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
				• 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. • Observeer het gedrag van de webapplicatie op ongeldige invoer. Voer hierbij een representatieve deelwaarneming uit op de invoermogelijkheden die de applicatie biedt.
U/WA.04	B3-4	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 partij(en): • 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. • Observeer het gedrag van de webapplicatie op voor wat betreft onveilige uitvoer. Voer hierbij een representatieve deelwaarneming uit op de uitvoervelden van de applicatie.
U/WA.05	B5-3	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en	Applicatie Infrastructuur Proces	Betrokken partij(en): • Applicatie-, hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting.

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
		cryptografische technieken. Doelstelling: Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie		Scope: • De DigiD webapplicatie en webserver en bijbehorende infrastructuur. Nadere toelichting Deze norm raakt diverse aspecten van privacybevorderende 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 conform de WBP 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 alle voor gegevens die in hetzelfde 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. 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.
U/PW.02	B3-02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen. Doelstelling: Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.	Applicatie	Betrokken partij(en): • Applicatie-, hosting- of SAAS leverancier. Scope: • De webserver. Nadere toelichting: HTTP headers moeten de risico's beperken van inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie. Aandachtspunten hierbij zijn: • behandel alleen HTTP-requests waarvan de gegevens een correct type, lengte, formaat, tekens en patronen hebben; • behandel alleen HTTP-requests van initiators met een correcte authenticatie en autorisatie; • sta alleen de voor de ondersteunde webapplicaties benodigde HTTP-requestmethoden

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
				(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.
U/PW.03	B3-16	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 partij(en): • 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 worden niet ondersteund; • cookie flags staan op 'HttpOnly' en 'Secure'; • bij alle HTTP-responses wordt de HTTP-headers 'Content-Security-Policy: frame-ancestors' en (tijdelijk) 'X-Frame-Options' verstuurd. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer de configuratie-baseline van de webserver. • Observeer de mogelijk tot het maken van directory listings, de cookies flags en de HTTP response headers.
U/PW.05	B2-1	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd	Infrastructuur Proces	Betrokken partij(en): • Hosting- of SAAS leverancier.

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
		conform het operationeel beleid voor platformen. Doelstelling: Voorkomen van misbruik van beheervoorzieningen.		Scope: • De webserver en andere servers in het DMZ van de DigiD webapplicatie. Nadere toelichting: • Dit betreft het gebruik van veilige netwerkprotocollen. Indien beheerinterfaces via het internet te benaderen zijn moet dit door middel van sterke authenticatie (zoals IP Sec VPN) 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 dat o.a. de volgende: elementen bevat. Aandachtspunten voor deze norm zijn: Het gebruik van veilige protocollen (conform industriestandaarden) voor het benaderen van beheermechanismen (beheerinterfaces). • Het gebruik 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 het DMZ.
U/PW.07	B0-6	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 partij(en): • Hosting- of SAAS leverancier. Scope: • De webserver en andere servers in het DMZ van de DigiD webapplicatie. Nadere toelichting: Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar. Hierbij kan worden verwezen naar actuele hardenings-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 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

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
				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 hardeningsstandaarden. • Inspecteer de configuratiebestanden en de uitkomsten van de penetratietest.
U/NW.03	B1-1	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 partij(en): • Hosting- of SAAS leverancier. Scope: • Het DMZ van de DigiD webapplicatie. Nadere toelichting: DMZ en compartimentering d.m.v. (2 virtuele) firewalls. Deze eis zowel materieel (feitelijk bestaan en inrichting van DMZ) als formeel qua opzet (netwerkschema of tekening) beoordelen, eventueel op basis van een adequate beschrijving. Overigens zal de organisatie moeten aantonen dat zij voldoende inzicht heeft in de architectuur, zowel van het DMZ als van de systemen die zich daarin bevinden. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer het netwerkarchitectuur schema inclusief de toegestane verkeersstromen tussen netwerksegenten. • Inspectie van configuratie files, firewall regels en de uitkomsten van de penetratietest.
U/NW.04	B7-1	De netwerkcomponenten en het netwerkverkeer worden beschermd door	Infrastructuur	Betrokken partij(en):

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
		middel van detectie- en protectiemechanismen. <u>Doelstelling:</u> Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.		• Hosting- of SAAS leverancier. <u>Scope:</u> • Het DMZ van 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. 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. Overigens heeft het de voorkeur om gebruik te maken van een Intrusion Prevention Systeem (IPS) dat automatisch preventieve maatregelen neemt tegen bedreigingen of een gecombineerde IDS/IPS. Ook wordt aanbevolen om het IDS of IPS te plaatsen **na** decryptie van het oorspronkelijk versleuteld netwerkverkeer omdat anders de inhoud van de berichten niet kan worden beoordeeld door het systeem. Aandachtpunten hierbij zijn: • Het gebruik van een IDS of IPS waarmee netwerkverkeer naar / van het Het DMZ van de DigiD webapplicatie wordt gemonitored. • 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. <u>Test aanpak</u>: • 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 regel-set.
U/NW.05	B1-2	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	Infrastructuur Proces	<u>Betrokken partij(en):</u> • Hosting- of SAAS leverancier. <u>Scope:</u>

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
		Doelstelling: Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.		• 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.
U/NW.06	B0-6	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 partij(en): • Hosting- of SAAS leverancier. Scope: • De webserver en andere servers in het DMZ van de DigiD webapplicatie. Nadere toelichting: Voor het configureren van netwerkcomponenten is een hardeningrichtlijn beschikbaar. Hierbij kan worden verwezen naar actuele hardeningrichtlijnen 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

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
				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. Test aanpak: • Interview de verantwoordelijke functionarissen. • Inspecteer de netwerkarchitectuur schema en hardeningrichtlijnen. • Inspecteer de configuratiebestanden en de uitkomsten van de penetratietest.
C.03	B0-9	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope). Doelstelling: Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de webapplicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	Infrastructuur Proces	Betrokken partij(en): • 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 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. • De scope van het vulnerability assessment omvat ten minste 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.

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
				• Inspecteer het vulnerability assessment rapport, het actieplan naar aanleiding van de vulnerability assessment en het statusrapport met betrekking tot de bevindingen.
C.04	B0-8	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 partij(en): • Applicatie-, hosting- of SAAS leverancier. Scope: • De DigiD webapplicatie, de webserver en andere servers in het 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. • De penetratietest dient minimaal eenmaal per jaar te worden uitgevoerd en na significante wijzigingen. • De scope van het vulnerability assessment omvat ten minste 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. Testaanpak: • 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	B7-1	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. Doelstelling: Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te	Infrastructuur Proces	Betrokken partij(en): • Hosting- of SAAS leverancier. Scope: • De infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting 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.

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
		kunnen vaststellen.		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. Aandachtspunten bij C.06 zijn: • Het definiëren van alarm situaties en drempelwaarden. • Het configureren van de alarm situaties en drempelwaarden in het IDS/IPS en het genereren van de bijbehorende alerts. • De inbedding van alert afhandeling in het incidentenbeheerproces inclusief escalatieprocedure. <u>Test aanpak</u>: • Interview de verantwoordelijke functionarissen. • Inspectie van de Use Cases en drempelwaarden. • Inspectie van alerts en de opvolging daarvan.
C.07	B7-8	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. <u>Doelstelling:</u> 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	<u>Betrokken partij(en):</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. 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 hoe 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; - ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden; - toegangslogs.

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
				• 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. <u>Test aanpak</u>: • Interview de verantwoordelijke functionarissen. • Inspectie van de procedurebeschrijving met betrekking tot de logging. • Inspectie van de vastlegging van de periodiek review van de logging, periodieke rapportage aan het management en follow-up acties naar aanleiding van review en analyse van de logging.
C.08	B0-5	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd. <u>Doelstelling:</u> Zeker stellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.	Applicatie Infrastructuur Proces	<u>Betrokken partij(en):</u> • Applicatie-, hosting- of SAAS leverancier. • Houder van DigiD aansluiting. <u>Scope:</u> • De DigiD webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. <u>Nadere toelichting:</u> De focus ligt op het vaststellen dat het proces wijzigingsbeheer zodanig is opgezet en geïmplementeerd dat alle wijzigingen altijd eerst worden getest voordat deze in productie worden genomen en via wijzigingsbeheer worden doorgevoerd. In sommige gevallen kunnen formulieren worden gebouwd die beveiligingsrisico's introduceren en valt wijzigingenbeheer met betrekking tot formulieren wel in scope van de DigiD-assessment. Is dit niet het geval dan valt wijzigingenbeheer met betrekking tot formulieren niet in scope. Welke specifieke situatie zich voordoet hangt af van de applicatie (formulierengenerator) en de wijze waarop deze wordt 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).

Ref	Ref oud	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> • Interview de verantwoordelijke functionarissen. • 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.
C.09	B0-7	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen. <u>Doelstelling:</u> Zeker stellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	Applicatie Infrastructuur Proces	<u>Betrokken partij(en):</u> • Hosting- of SAAS leverancier. <u>Scope:</u> • Hypervisor (VM Ware, etc.). • Operating system (Windows, etc.). • Databases. • Netwerk componenten. • Firewall. <u>Nadere toelichting:</u> De focus is op het patching proces. Dit proces kan gedifferentieerd zijn naar bijvoorbeeld het OS, DBMS en netwerk. Applicaties en systemen dienen periodiek gepatcht te worden. Een maandelijks patching cyclus is aanvaardbaar tenzij er security alerts zijn. Voor internet facing systemen dienen de laatste stabiele beveiligingspatches te zijn geïnstalleerd. Indien patching niet mogelijk is in verband met een legacy applicatie die niet meer zou functioneren na patching, zal dit risico aantoonbaar moeten zijn afgewogen. Aandachtpunten hierbij zijn: • Het beschrijven van patchmanagementbeleid waarin is aangegeven hoe de organisatie omgaat met updates: hoe snel implementeert de organisatie een 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.

Ref	Ref oud	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
				<u>Test aanpak:</u> • Interview de verantwoordelijke functionarissen. • Inspectie van het patchmanagementbeleid. • Inspectie van configuratie files en de uitkomsten van de penetratietest.

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Bijlage 3 Procesmatige kwaliteitsaspecten bij DigiD penetratietesten

Van toepassing op norm C.04:

Beveiligingsrichtlijn 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).

Kwaliteitsaspecten:

Randvoorwaarden

- Penetratietester staat onafhankelijk ten opzichte van het te onderzoeken object.
- Penetratietester heeft aantoonbare eerdere ervaringen van de penetratietester met DigiD penetratietesten.
- Overeengekomen opdracht met doel, vraagstelling, normen, scope, stappenplan, doorlooptijd en budget.
- Penetratietest vrijwaring ondertekend door opdrachtgever en evt. betrokken derden zoals hosting partij.
- Afspraak over beschikbaarheid van penetratietesters en beheerders bij de onderzochte organisatie.
- Afspraak tussen auditor en penetratietester over het gebruik van penetratietesttools.
- Gedocumenteerde afspraken over communicatie tussen penetratietesters en contactpersonen bij de opdrachtgevende organisatie.
- Instemming opdrachtgever met uit te voeren penetratietest.

Scope en normstelling

- Vastgesteld object (versienummer) van het onderzoek relevant voor DigiD.
- Vastgestelde Logius normen voor DigiD (subset uit de NCSC normen), minimaal OWASP top 10, eventueel aangevuld met SANS 25, WASC criteria, GHDB en leveranciers-specifieke normen en baselines.
- Voor DigiD audit is een black box/grey box 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 van standaard configuratie functionaliteit zijn ontwikkeld altijd testen.
- Indien standaard formulieren worden gebruikt, waarbij alleen functionele aanpassingen doorgevoerd kunnen worden, kan volstaan worden met vaststellen van de betrouwbare werking van de formulierengenerator (o.b.v. de TPM van de service provider).

Verkenningsfase (vaststellen ingang criteria)

- Inventarisatie gebruikte (webfacing) infrastructuur, applicaties, componenten, e.d.
- Infrastructuurtest vindt altijd plaats op de productieomgeving.
- Applicatietest vindt plaats op test omgeving. Opdrachtgever toont aan dat de versie van de applicatie van acceptatieomgeving gelijk is aan die in de productie omgeving.
- Acceptatieomgevingen met representatieve testgegevens zijn beschikbaar.
- DigiD testaccounts zijn beschikbaar en gekoppeld aan testgegevens, evt. gekoppeld aan mobiele nummers penetratietesters.
- Penetratietester(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 cyber security bronnen.
- Selectie van tests voor aantonen van de mogelijke kwetsbaarheden.

Geautomatiseerde tests (dynamisch testen)

- Keuze geschikte penetratietest tools en hun dekkingsgraad van het te testen object (niet ieder penetratietest 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 zal moeten worden getest.
- Doorlopende bewaking door de penetratietester 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 penetratietester(s), eventueel aanwezige certificeringen ter onderbouwing; aantoonbare kennis/ervaring met gebruikte technologieën.
- Technische details van gecontroleerde SSL/TLS-certificaten en 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 gerede twijfel over het gedrag alsnog een code review uitvoeren.
- Dekkingsgraad van de review bepalen (steekproef, volledig, ..?)
- Aantoonbare ervaring van de penetratietester(s) met de programmeertaal en omgeving, eventueel beschikbare certificeringen ter onderbouwing.
- Bij gebruik van tools voor statische testen: dekkingsgraad ten opzichte van de norm.

Risicoanalyse op bevindingen (vaststellen uitgang criteria)

- Risicoafweging van aangetroffen afwijkingen t.o.v. de norm tegen het daadwerkelijk kunnen exploiteren.
- Risico's uitdrukken in kans X impact of erkende risicoclassificatie.
- Onderbouwen van de ernst van de aangetroffen afwijkingen.
- Geen uitspraken over risiconiveau vanuit business perspectief (beoordeling hiervan kan alleen door de opdrachtgever plaatsvinden).

Rapportage

- Conceptrapportage
    - Classificatie van de rapportage conform DigiD normen, beleid opdrachtgever en auditor en eventueel naar publieke standaarden.
    - Beschrijving object van het onderzoek: webfacing infrastructuur, servers, verbindingen.
    - Tijdstip van uitgevoerde testen.
    - Het ip-adres waarvandaan de test is uitgevoerd.
    - 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 o.b.v. 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.
- Afstemming met auditor (review).
    - Versleutelde, 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.
    - Versleuteld, 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.
    - Versleutelde, 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

- Minimaal zal jaarlijkse, ten tijde van de DigiD audit, een penetratietest uitgevoerd moeten worden door een penetratietester die onafhankelijk is ten opzichte van het te onderzoeken object.
- 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. Deze penetratietest zou specifiek gefocust mogen zijn op wijzigingen in de applicatie of de infrastructuur en behoeft niet noodzakelijkerwijs door een penetratietester te worden uitgevoerd die onafhankelijk staat ten opzichte van het te onderzoeken object.
- Het is aan te bevelen om, op basis van en risicoafweging, frequenter penetratietesten uit te (laten) voeren, zodat ingespeeld kan worden op nieuwe bedreigingen.

Bijlage 4 Toelichting op Norm ICT-beveiligingsassessments DigiD versie 2.0 (de Norm v2.0)

BZK heeft een aantal overwegingen gegeven voor het uitbrengen van de Norm v2.0:

1. Het uitbrengen van nieuwe beveiligingsrichtlijnen voor webapplicaties door NCSC, waar het normenkader voor het ICT beveiligingsassessment DigiD op gebaseerd is;
2. Een geheel nieuwe indeling en nummering van deze nieuwe beveiligings-richtlijnen voor webapplicaties;
3. De initiële opdracht om het normenkader gedurende de tijd te verzwaren of uit te breiden, om zo de effectiviteit en veiligheid van het DigiD stelsel te vergroten;
4. De wens van BZK om de auditlast van de DigiD assessment te verminderen.

Daarnaast hanteert NOREA het standpunt dat uitsluitend beoordeling van opzet en bestaan op den duur schijnzekerheid impliceert als niet ook de werking in de beoordeling wordt betrokken. Het invoeringstraject daarvan vraagt echter de nodige voorbereidingstijd. Vooralsnog blijft de beoordeling in het assessment 2017 beperkt tot op opzet en het bestaan van de beheersmaatregelen.

Kenmerken nieuwe normenkader

De aanpak is volgens BZK meer risicogericht en heeft de belangrijkste, momenteel relevante dreigingen als uitgangspunt;

1. Een groot deel van het normenkader blijft gelijk;
2. Daar waar het normenkader in de loop van de jaren zijn effect heeft gehad, wordt de audit verlicht;
3. Door inbreng van de nieuwe normen worden nieuwe risico's afgedekt en wordt hierdoor het normenkader effectiever en actueler;
4. Het kader wordt aangepast aan de nieuwe NCSC nummering;
5. Door een deel van het kader te wijzigen, hoeft ook maar een deel van de (rapportage)templates, handreikingen etc. aangepast te worden;
6. De doorlooptijd van deze wijziging voor houders, NOREA en Logius is te overzien.

Uitgangspunten bij de Norm v2.0

De focus komt zoveel als mogelijk op technische normen te liggen om zo de overlap met de ISO27001/2 en afgeleiden als de Baseline Informatiebeveiliging Rijk/ Gemeenten e.a. te verkleinen.

De focus ligt op thema's als:

- Normen met betrekking tot logging en monitoring;
- Veilig programmeren normen;
- Normen met betrekking tot incident detectie en opvolging.

Verschillen en overeenkomsten tussen de Norm v1.0 en de Norm v2.0

De Norm v1.0 was gebaseerd op de NCSC ICT-Beveiligingsrichtlijnen voor webapplicaties versie 2012.

De Norm v2.0 is gebaseerd op de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties richtlijnen versie 2015.

Ten opzichte van de Norm v1.0 heeft BZK de volgende normen laten vervallen:

- B0-13 Niet (meer) gebruikte websites en/of informatie moet worden verwijderd.
- B1-03 Netwerktoegang tot de webapplicaties is voor alle gebruikersgroepen op een zelfde wijze ingeregeld.
- B3-05 Voor het raadplegen en/of wijzigen van gegevens in de database gebruikt de webapplicatie alleen geparametriseerde queries.
- B3-15 Een (geautomatiseerde) blackbox scan wordt periodiek uitgevoerd.
- B5-01 Voer sleutelbeheer in waarbij minimaal gegarandeerd wordt dat sleutels niet onversleuteld op de servers te vinden zijn.
- B7-09 Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en response inzake informatiebeveiliging dienen adequaat te zijn vastgesteld.

De Norm v2.0 wijkt inhoudelijk niet al te veel af van de Norm v1.0, wel kent het normenkader een andere indeling. De investeringen van houders en hun leveranciers in de methodiek en de vele doorgevoerde verbeteringen hoeven daardoor niet verloren te gaan. Wel dient een omnummering plaats te vinden en zal het controledossier op onderdelen herschikt moeten worden. Er is een omnummertabel voor de Norm v1.0 naar de Norm v2.0.

In de volgende tabel staan in kolom 1 en 2 de overgebleven beveiligingsrichtlijnen uit de Norm v1.0.

In kolom 3 staat de nummering van de volgens de vertaaltabel van het NCSC.

oude nr.	**Norm v1.0**	**nieuwe nummer V2.0**
B0-05	Alle wijzigingen worden altijd eerst getest voordat deze in productie worden genomen en worden via wijzigings-beheer doorgevoerd.	C.08
B0-06	Maak gebruik van een hardeningsproces, zodat alle ICT-componenten zijn gehard tegen aanvallen.	U/PW.07 en U/NW.06
B0-07	De laatste (beveiligings)patches zijn geïnstalleerd en deze worden volgens een patchmanagement proces doorgevoerd.	C.09
B0-08	Penetratietests worden periodiek uitgevoerd.	C.04
B0-09	Vulnerability assessments (security scans) worden periodiek uitgevoerd.	C.03
B0-12	Ontwerp en richt maatregelen in met betrekking tot toegangsbeveiliging/ toegangsbeheer.	B.02 en U/TV.01
B0-14	Leg afspraken met leveranciers vast in een overeenkomst.	B0.5
B1-01	Er moet gebruik worden gemaakt van een Demilitarised Zone (DMZ), waarbij compartimentering wordt toegepast en de verkeersstromen tussen deze compartimenten wordt beperkt tot alleen de hoogst noodzakelijke.	U/NW.03
B1-02	Beheer- en productieverkeer zijn van elkaar gescheiden.	U/NW.03 en U/NW.05
B2-01	Maak gebruik van veilige beheermechanismen.	U/PW.05
B3-01	De webapplicatie valideert de inhoud van een HTTP-request voor die wordt gebruikt.	U/WA.03
B3-02	De webapplicatie controleert voor elk HTTP verzoek of de initiator geauthenticeerd is en de juiste autorisaties heeft.	U/PW.02
B3-03	De webapplicatie normaliseert invoerdata voor validatie.	U/WA.03
B3-04	De webapplicatie codeert dynamische onderdelen in de uitvoer.	U/WA.04
B3-06	De webapplicatie valideert alle invoer, gegevens die aan de webapplicatie worden aangeboden, aan de serverzijde.	U/WA.03

oude nr.	Norm v1.0	nieuwe nummer V2.0
B3-07	De webapplicatie staat geen dynamische file includes toe of beperkt de keuze mogelijkheid (whitelisting).	U/WA.03
B3-16	Zet de cookie attributen 'HttpOnly' en 'Secure'.	U/PW.03
B5-02	Maak gebruik van versleutelde (HTTPS) verbindingen.	U/WA.05
B5-03	Sla gevoelige gegevens versleuteld of gehashed op.	U/WA.05
B5-04	Versleutel cookies.	U/WA.05
B7-01	Maak gebruik van Intrusion Detection Systemen (IDS).	U/NW.04 en C.06
B7-08	Voer actief controles uit op logging.	C.07

Het DigiD assessment maakt onderdeel uit van een breder overheidsinitiatief om de veiligheid van digitale dienstverlening te vergroten, maar is zeker niet het enige middel Blijvende management aandacht voor de risico's van digitale dienstverlening en het treffen van de juiste beheersmaatregelen is van groot belang.

Algemeen geaccepteerde beheerskaders als ISO 27001/2, de verschillende Baselines voor Informatiebeveiliging voor overheidsorganisaties en CobiT 5 vormen daarbij belangrijke hulpmiddelen. De IT auditor betrekt deze context (de 'controle omgeving') wel bij zijn audit aanpak, maar voert daar in het kader van het DigiD assessment geen specifiek onderzoek op uit.

Bijlage 5 Begrippenkader

Applicatieleverancier	Een organisatie die een webapplicatie levert en die conform gemaakte afspraken verantwoordelijk is voor het onderhoud en de eventuele doorontwikkeling aan de software.
Bestaan	Het functioneren van een stelsel van informatiebeveiligings- en beheersingsmaatregelen conform beschrijving op of rond een peildatum.
Carve out methode	Bij de carve out methode wordt in een assurance rapport (zoals een DigiD assessment) een verwijzing opgenomen naar de TPM van een leverancier. De auditor van het assurance rapport en de auditor van de TPM houden ieder zelfstandig hun vaktechnische verantwoordelijkheid. De eerste auditor dient wel vast te stellen dat de scope van beide rapportages in voldoende mate op elkaar aansluit.
Hosting leverancier	Een organisatie die conform gemaakte afspraken ICT-infrastructuur inclusief internettoegang aanbiedt waarop een webapplicatie kan worden uitgevoerd en kan worden aangeboden aan gebruikers.
Houder 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 houder.
Inclusive methode	Bij de inclusive methode worden alle beheersmaatregelen in een assurance rapport overgenomen en er wordt dus niet verwezen naar TPM's waar eventueel gebruik van is gemaakt. De auditor van het assurance rapport is vaktechnisch volledig verantwoordelijk en voert indien nodig een dossierreview uit voor een TPM waarvan de resultaten worden overgenomen.
Opzet	De beschrijving van een stelsel van informatiebeveiligings- en beheersingsmaatregelen.
Penetratietest	Dit is een specifieke vorm van een vulnerability-assessment. Het is een proces waarbij met behulp van technische hulpmiddelen specifieke componenten of specifieke delen van de ICT-infrastructuur op zwakheden gecontroleerd worden. (NCSC) In de context van het DigiD assessment wordt met een penetratietest een technisch beveiligingsonderzoek bedoeld dat vanaf het internet wordt uitgevoerd door een (ervaren) penetratietester en waarbij scantools worden ingezet en aanvullende handmatige onderzoekswerkzaamheden worden uitgevoerd.
SAAS leverancier	Een organisatie die een webapplicatie als online dienst aanbiedt waarbij de klanten de software niet hoeven aan te schaffen. De aanbieder draagt zorg voor onderhoud en doorontwikkeling van (de software van) de applicatie, hosting en applicatiebeheer.

Third Party Mededeling (TPM)	Een TPM is een assurance rapport dat betrekking heeft op een leverancier (serviceorganisatie) waarbij de doelgroep van het rapport een andere is dan de serviceorganisatie en de assurance wordt gegeven door een onafhankelijke auditor.
User control considerations (UCC)	In de UCC paragraaf in een TPM (assurance rapport) worden beheersingsmaatregelen (controls) beschreven waarvan de betreffende leverancier aangeeft dat de gebruikersorganisatie (bijvoorbeeld een gemeente) deze moet hebben ingericht teneinde het stelsel van beveiligings- en beheersingsmaatregelen bij de leverancier optimaal te laten functioneren.
Vulnerability assessment	Dit is een proces waarbij met behulp van technische hulpmiddelen wordt nagegaan in hoeverre in de ICT-componenten kwetsbaarheden voorkomen waarvan ongeautoriseerden gebruik zouden kunnen maken. (NCSC) In de context van het DigiD assessment wordt een (bij voorkeur geautomatiseerde) scan bedoeld die vanaf een intern netwerksegment zo dicht mogelijk bij de server wordt uitgevoerd op bekende kwetsbaarheden en ontbrekende patches.