NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Toelichting:

In de onderstaande tabel is aangegeven bij welke beveiligingsrichtlijnen 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 (zgn. 'non occurence').

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.

Non occurence kan zich alleen voordoen bij de normen B.05, U/TV.01, U/WA.02 en C.08.

#	Normtekst	Verwachte documentatie (opzet)	Non occurence mogelijk m.b.t. 'Bestaan'?
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.	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);	**Deels** T.a.v. *Service Level Reports*, 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.

#	Normtekst	Verwachte documentatie (opzet)	Non occurence mogelijk m.b.t. 'Bestaan'?
		• beding dat deze voorwaarden back-to-back worden doorgegeven aan mogelijke subleveranciers.	
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken. Doelstelling: Het efficiënter maken van het identiteiten-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, etc.).	**Deels** 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. Doelstelling: Effectief en veilig realiseren van de dienstverlening.	Nadere toelichting: Deze norm richt zich meer op de procesmatige aspecten van het functioneel en het applicatiebeheer. Aandachtspunten hierbij zijn: • Beschrijving van taken, verantwoordelijkheden en bevoegdheden van de verschillende beheerrollen. • Een incidentenprocedure is opgesteld. • Meldingen van het NCSC of IBD of Z-CERT of andere CERTS worden geanalyseerd en zo nodig opgevolgd. • Incidenten worden geregistreerd, geanalyseerd, opgevolgd en afgehandeld. • Er is een periodieke rapportage aan het management inzake beveiligingsincidenten.	**Deels** 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.

#	Normtekst	Verwachte documentatie (opzet)	Non occurence mogelijk m.b.t. 'Bestaan'?
U/WA 03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Nadere toelichting: Ongecontroleerde (ongevalideerde) invoer van gebruikers is een belangrijke dreiging voor een webapplicatie. Als invoer van gebruikers rechtstreeks wordt gebruikt in HTML-uitvoer, cookiewaarden, SQL-queries, etc., bestaat er een (grote) kans dat een kwaadwillende de webapplicatie compromitteert. Een 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.).	**Nee**
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	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.	**Nee**
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	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 door de houder van de DigiD aansluiting op basis van een risicoanalyse; • mogelijke versleuteling of hashing van gevoelige gegevens. Het gaat hier in ieder geval om het BSN als bijzonder persoonsgegeven. Overigens geldt dit alleen voor gegevens die in dezelfde DMZ worden opgeslagen als waar de webapplicatie draait. Gegevens in de backoffice vallen buiten de scope van dit onderzoek; • de HTTPS configuratie en de TLS configuratie. TLS kent veilige en minder veilige instellingen. Het NCSC maakt onderscheid in 'Goede', 'Voldoende'	**Nee**

#	Normtekst	Verwachte documentatie (opzet)	Non occurence mogelijk m.b.t. 'Bestaan'?
		en 'Onvoldoende' instellingen. Voor de DigiD webserver geldt dat minimaal de op dat moment als 'Voldoende' bestempelde instellingen vereist zijn.	
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	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 HTTPrequestmethoden; • 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.	**Nee**
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	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 worden zowel de HTTP-headers 'Content-Security-Policy: frameancestors' als de 'X-Frame-Options' verstuurd.	**Nee**
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.	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	**Nee**

#	Normtekst	Verwachte documentatie (opzet)	Non occurence mogelijk m.b.t. 'Bestaan'?

		om de systemen te benaderen (ook niet voor noodtoegang). Daarnaast wordt een beknopt operationeel beleid verwacht.
		• Aandachtspunten voor deze norm zijn:
		  ○ Het gebruik van veilige protocollen (conform industrie standaarden) voor het benaderen van beheermechanismen (beheerinterfaces).
		  ○ Het gebruik van sterke authenticatie voor zowel technisch als functioneel beheerders.	

U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar.	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 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 beheerfuncties 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.	**Nee**
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.	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	**Nee**

#	Normtekst	Verwachte documentatie (opzet)	Non occurence mogelijk m.b.t. 'Bestaan'?
		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.	
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van protectie- en detectiemechanismen.	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.	**Nee**
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	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.	**Nee**
U/NW.06	Voor het configureren van netwerken is een	Nadere toelichting:	**Nee**

#	Normtekst	Verwachte documentatie (opzet)	Non occurence mogelijk m.b.t. 'Bestaan'?
	hardeningrichtlijn beschikbaar.	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 beheerfuncties 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.	
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	<u>Nadere toelichting:</u> 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 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.	**Nee**

#	Normtekst	Verwachte documentatie (opzet)	Non occurence mogelijk m.b.t. 'Bestaan'?
		• 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.	
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	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, zoals vervanging applicatie, nieuwe versie, migratie webservers, database migratie, etc.. • 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.	**Nee**
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	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. 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.	**Nee**
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord	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;	**Nee**

#	Normtekst	Verwachte documentatie (opzet)	Non occurence mogelijk m.b.t. 'Bestaan'?

	(bewaakt, geanalyseerd) en de bevindingen gerapporteerd.	– C.07 richt zich op periodieke analyse van de logging.
		De logging- en detectie-informatie en de conditie van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.
		
		Aandachtpunten hierbij zijn:
		• Procedurebeschrijving met daarin beschreven op welke wijze en wanneer controles op logging moeten plaatsvinden en hoe taken op dit gebied belegd zijn.
		• Het uitvoeren van periodieke controles op:
		  ○ wijzigingen aan de configuratie van webapplicaties;
		  ○ optreden van verdachte gebeurtenissen en eventuele schendingen van de beveiligingseisen;
		  ○ ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden;
		  ○ 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.	

C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	<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.	**Ja** Waarbij 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.

#	Normtekst	Verwachte documentatie (opzet)	Non occurence mogelijk m.b.t. 'Bestaan'?
		Aandachtspunten hierbij zijn: • Wijzigingsbeheer procedure, waarbij zo nodig onderscheid wordt gemaakt tussenwijzigingen 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.	
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT-voorzieningen.	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.	**Nee**