

Bijlage A1 - Rapport van bevindingen DigiD eDiensten Burgerzaken

Bij een ENSIA opdracht geeft de IT auditor assurance op basis van een attest opdracht volgens richtlijn 3000/A op basis van de collegeverklaring en bijlagen. Hoewel de collegeverklaring het object van controle vormt, is de ingevulde en gedocumenteerde zelfevaluatie uit de ENSIA tool en de bijbehorende bewijsstukken voor de IT auditor het basismateriaal waar elke IT auditor vanuit kan en moet gaan.

In het kader van deze assurance opdracht hebben wij de volgende werkzaamheden uitgevoerd:

- Het verkrijgen van inzicht in de relevante kenmerken van de DigiD-webomgeving.
- Het vaststellen van de scope van het assessment, inclusief het vaststellen van de maatregelen die bij de serviceorganisatie moeten worden onderzocht.
- Het houden van (telefonische/video) interviews met de verantwoordelijk functionaris Alexander Zagkotsis – CISO, vooral gericht op het onderkennen van risico's en het onderzoek in hoeverre deze risico's worden afgedekt door maatregelen.
- Het inventariseren van de opzet en het vaststellen van het bestaan van de relevante maatregelen. Dit door middel van het kennis nemen van documentatie, het kennis nemen van de resultaten van de uitgevoerde interne controles, alsmede eigen waarnemingen.
- Het analyseren van de uitkomsten van onze werkzaamheden met als doel het geven van oordelen per beveiligingsrichtlijn van de 'Norm ICT-beveiligingsassessments DigiD' van Logius.

Hieronder treft u een korte beschrijving van de uitgevoerde werkzaamheden en onze oordelen ter verbetering van de DigiD-webomgeving. Onze oordelen zijn verwoord als voldoet/voldoet niet (met reden) per beveiligingsrichtlijn. Om de leesbaarheid van dit rapport te vergroten zijn de oordelen in deze tabel weergegeven als "voldoet" (met de kleur groen) of "voldoet niet" (met de kleur rood). Hierbij moet "voldoet" worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn effectief zijn opgezet en geïmplementeerd op 20 maart 2024". "Voldoet niet" moet worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn niet in alle materiële opzichten effectief zijn opgezet en/of geïmplementeerd op 20 maart 2024".

De uitspraak voldoet of voldoet niet beperkt zich tot de eigen oordeelsvorming van de auditor.

In Bijlage 1 bij de Collegeverklaring is ten dienste van Logius door de gemeente een totaaloverzicht opgenomen van de door ons onderzochte normen en de normen die door de IT-auditor van de serviceorganisatie zijn onderzocht. Uitdrukkelijk merken wij op dat wij geen onderzoek hebben uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de TPM van de serviceorganisatie. Wij kunnen dan ook geen verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Wij verwijzen -daar waar richtlijnen zijn onderzocht door de IT auditor van de dienstverlener Centric Netherlands B.V, naar het rapport en onderzoeksresultaten van Centric Netherlands B.V.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer. <u>Doelstelling:</u> Het zorgen voor specifieke management aandacht in het beveiligingsproces voor de webapplicaties van de organisatie. <u>Betrokken rol(len):</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>Uitleg:</u> <i>De focus ligt op het vaststellen dat het eigenaarschap van de DigiD webapplicatie is georganiseerd en dat de organisatie beschikt over een geactualiseerd (eenmaal in de 4 jaar dan wel bij grote</i>	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V. Onderzoek van de door de gemeente Duiven aangeleverde documenten plus het uitvoeren van gerichte deelwaarnemingen.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM. Vastgesteld is dat een Informatiebeveiligingsplan/-beleid Samenwerking De Liemers 2022-2025, inclusief DigiD uitwerking norm B.01 is aangeleverd. Dit geldt tevens voor de gemeente Duiven. Vastgesteld is dat het informatiebeveiligingsbeleid en/of de bijlagen en/of apart ontwikkeld beleid van de gemeente Duiven voldoet aan de gestelde eisen omdat het beleid: • Actueel is namelijk niet ouder dan vijf jaar. • Formeel is vastgesteld door het hoger management. • Het eigenaarschap van de webapplicatie regelt. • Dataclassificatie van de webapplicatie adresseert. • Toegangsbeheer en -voorziening adresseert. • Kwetsbaarhedenbeheer adresseert. <u>Eigenaarschap webapplicatie</u> Wij hebben vastgesteld dat het eigenaarschap van de webapplicatie eDiensten Burgerzaken is belegd bij M. Heutink (Hoofd afdeling Publiekszaken 1Stroom) en dat het functioneel beheer wordt uitgevoerd door S. Geerts en C. Dahles. <u>PDCA-cyclus</u> De laatste verplichte rapportage over informatiebeveiliging is aangeleverd en wij hebben kunnen vaststellen dat er een PDCA cyclus is met betrekking tot informatiebeveiliging.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	<i>organisatiewijzigingen)</i> <i>informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid bevat (expliciet) het beleid over de bescherming van de eigen informatiehuishouding in relatie tot de eigen delen van de DigiD webapplicatie en/of de infrastructuur voor het netwerksegment met de DigiD webapplicatie.</i>			Aanbeveling voor de gemeente Duiven: Het DigiD assurancerapport van uw leverancier bevat informatie die voor u als gebruikersorganisatie van belang is. Neem daarom kennis van dit rapport en besteed daarbij speciaal aandacht aan het hoofdstuk 'Verantwoordelijkheden gebruikersorganisatie'. Hierin staat per norm beschreven welke maatregelen u zelf dient te nemen om aan de betreffende norm te kunnen voldoen.
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld. <u>Doelstelling:</u> Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie. <u>Betrokken rol(len):</u> - Applicatie-, hosting- of SAAS leverancier. - Houder van de DigiD-aansluiting. <u>Scope:</u> - De contracten en/of Service Level Agreements voor de levering hosting-, applicatie- of SAAS diensten. <u>Uitleg:</u> <i>De gemeente Duiven dient een, door beide partijen ondertekend, contract te hebben waarin tenminste de volgende zaken zijn opgenomen:</i>	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V. Onderzoek van de door de gemeente Duiven aangeleverde documenten plus het uitvoeren van gerichte deelwaarnemingen.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM. Vastgesteld is dat er een formele overeenkomst is, welke op het juiste (organisatorische) niveau is <i>vastgesteld/geaccordeerd</i> tussen RID De Liemers (voor de gemeente Duiven) en leverancier met als doel te garanderen dat er geen misverstanden bestaan tussen betrokken partijen. Geconstateerd is dat in het contract c.q. de bijlagen met Centric Netherlands B.V het volgende is opgenomen: - de van toepassing zijnde leveringsvoorwaarden; - informatiebeveiligingseisen 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); - een beding dat deze voorwaarden back-to-back worden doorgegeven aan mogelijke sub-leveranciers. Centric Netherlands B.V verwerkt persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming. Er is een verwerkersovereenkomst in de zin van AVG opgesteld en geformaliseerd tussen partijen.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	• 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); • een beding dat deze voorwaarden back-to-back worden doorgegeven aan mogelijke sub-leveranciers.			<u>SLR</u> Service Level Reporting is een van de afspraken in de SLA tussen RID De Liemers (voor de gemeente Duiven) en Centric Netherlands B.V. Er is een rapportage aangeleverd over de prestaties van Centric Netherlands B.V.
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken. <u>Doelstelling:</u> Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit. <u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting.	Er is kennis genomen van de door de de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	<u>Scope:</u> - De DigiD webapplicatie., DigiD webservern en beheerinterfaces van de firewalls, routers, IDS/IPS, etc. <u>Uitleg:</u> De focus ligt op de beheerprocessen. Dit betreft enerzijds toegang tot de DigiD-applicatie en anderzijds toegang tot de DigiD webservern en de firewalls, IDS/IPS, etc. die een koppeling hebben met de DigiD omgeving. <u>Aandachtspunten hierbij zijn:</u> - 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. <i>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.).</i>			
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. <u>Doelstelling:</u> Effectief en veilig realiseren van de dienstverlening.	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V. Onderzoek van de door de gemeente Duiven aangeleverde documenten plus		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM. <u>Applicatiebeheer</u> Het applicatiebeheer wordt uitgevoerd door Centric Netherlands B.V. <u>Functioneel beheer</u> Vastgesteld is dat functioneel beheer wordt uitgevoerd door Centric Netherlands B.V. Zo voert Centric de gebruikersacceptatietest uit.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	Betrokken rol(len): • Applicatie of SAAS leverancier. • Houder van de DigiD-aansluiting. Scope: • De DigiD webapplicatie. Uitleg: <i>Deze norm richt zich meer op de procesmatige aspecten van het functioneel en het applicatiebeheer.</i> 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.	het uitvoeren van gerichte deelwaarnemingen.		Incidentenbeheer Er is een incidentenprocedure opgesteld, waarbij o.a. meldingen vanuit de eigen organisatie, de IBD of andere CERTS worden geanalyseerd en zo nodig opgevolgd. Incidenten worden geregistreerd, geanalyseerd, opgevolgd en afgehandeld. Beveiligingsincident Er is een relevant incident aangeleverd waardoor de effectiviteit van de procedure positief kon worden bepaald. Voor het registreren van incidenten wordt gebruik gemaakt van Topdesk. Rapportage Er is een periodieke rapportage aan het management inzake beveiligingsincidenten aangeleverd. Aanbeveling voor de gemeente Duiven: • Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft vastgesteld dat deze norm getoetst gaat worden op werking. Hierbij wordt een overgangsjaar gebruikt. Voor aansluitouders betekent dit het volgende: ○ Vanaf inleverperiode 1 januari - 1 mei 2024 (over het voorgaande jaar 2023) mogen deze en de overige vier betrokken normen op werking worden getoetst. ○ Vanaf inleverperiode 1 januari - 1 mei 2025 (over het voorgaande jaar 2024) moet deze en de overige vier betrokken normen op werking worden getoetst. Zorg ervoor dat u de afhandeling van alle mogelijke (beveiligings)incidenten gedurende een jaar voorafgaand aan het assessment achteraf aan kunt tonen.
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt. Doelstelling: Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden. <u>Betrokken rol(len):</u> • Applicatie- of SAAS leverancier. <u>Scope:</u> De DigiD webapplicatie en webserver.			
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren. <u>Doelstelling:</u> Voorkom manipulatie van het systeem van andere gebruikers. <u>Betrokken rol(len):</u> • Applicatie- of SAAS leverancier. <u>Scope:</u> • De DigiD webapplicatie.	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacy bevorderende en cryptografische technieken. <u>Doelstelling:</u> Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie. <u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS leverancier. • Houder van de DigiD-aansluiting. <u>Scope:</u> • De DigiD webapplicatie en webserver	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V. Onderzoek van de door de gemeente Duiven aangeleverde documenten plus het uitvoeren van gerichte deelwaarnemingen.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM. De gemeente Duiven/RID De Liemers heeft <i>zelf een</i> adequate gegevens- en risicoanalyse uitgevoerd en daarin vastgesteld dat: • Er (bijzondere of daaraan gelijkgestelde) persoonsgegevens worden verwerkt. • Er persoonsgegevens buiten de scope van het DigiD assessment worden opgeslagen. • Er dus geen bijzondere persoonsgegevens worden opslagen binnen de scope. • Alle gegevens zijn geclassificeerd. • Er alleen persoonsgegevens worden gecached gedurende de verbinding tussen de browser van betrokkene en het digitaal loket.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	en bijbehorende infrastructuur. <i>Uitleg:</i> 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. <i>Aandachtspunten hierbij zijn:</i> - de classificatie van gegevens door de houder van de DigiD aansluiting op basis van een risico analyse; - mogelijke versleuteling of hashing van gevoelige gegevens. Het gaat hier in ieder geval om het BSN als bijzonder persoonsgegevens. 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' en 'Onvoldoende' instellingen². Voor de DigiD webserver geldt dat minimaal de op dat moment als 'Voldoende' bestempelde instellingen vereist zijn. Compromittering of verlies van cryptografische sleutels kan de vertrouwelijkheid, authenticiteit en/of integriteit van informatie in gevaar brengen. Deze compromittering is te vergelijken met			De risico's in voldoende mate worden beperkt doordat de berichten via de webapplicatie direct worden doorgestuurd via beveiligd berichtenverkeer naar een apart netwerkdomein buiten de scope van het DigiD assessment. <u>TLS</u> Er is geconstateerd voor de webserver dat de HTTPS en de TLS configuratie aan de meest recente industriestandaard voldoet.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	<i>de recente Heart Bleed bug in OpenSSL. Criminelen kunnen via de private key een valse website in de lucht brengen die doet alsof hij de originele website is, compleet dus met een volledig betrouwbare versleutelde verbinding.</i>			
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen. <u>Doelstelling:</u> Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie. <u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS leverancier. <u>Scope:</u> • De webserver.	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.
U/PW.03	De webserver is ingericht volgens een configuratie-baseline. <u>Doelstelling:</u> Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging. <u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS leverancier. <u>Scope:</u> • De webserver.	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	wordt uitgevoerd conform het operationeel beleid voor platformen. <u>Doelstelling:</u> Voorkomen van misbruik van beheervoorzieningen. <u>Betrokken rol(len):</u> • Hosting- of SAAS leverancier. <u>Scope:</u> • De webserver en andere servers in het DMZ van de DigiD webapplicatie.	"gesteund" op de TPM van Centric Netherlands B.V.		
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar. <u>Doelstellingen:</u> Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten. <u>Betrokken rol(len):</u> • Hosting- of SAAS leverancier. <u>Scope:</u> • De webserver en andere servers in het DMZ van de DigiD webapplicatie.	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is. <u>Doelstelling:</u> Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen. <u>Betrokken rol(len):</u> • Hosting- of SAAS leverancier.	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	<u>Scope:</u> Het DMZ van de DigiD webapplicatie.			
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen. <u>Doelstelling:</u> Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed. <u>Betrokken rol(len):</u> - Hosting- of SAAS leverancier. <u>Scope:</u> - Het DMZ van de DigiD webapplicatie.	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd. <u>Doelstelling:</u> Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet. <u>Betrokken rol(len):</u> - Hosting- of SAAS leverancier. <u>Scope:</u> - Het netwerksegment met de webserver die een koppeling hebben met de DigiD omgeving van Logius inclusief de toegang vanuit internet.	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	<u>Doelstelling</u> Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten. <u>Betrokken rol(len):</u> • Hosting- of SAAS leverancier • Houder van de DigiD aansluiting <u>Scope:</u> • De webserver en andere servers in het DMZ van de DigiD webapplicatie. <u>Uitleg:</u> <i>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.</i> <i>DNS is het registratiesysteem van namen en bijbehorende nummers op het Internet. Het is vergelijkbaar met een telefoonboek. De namen van bestemmingen op Internet heten domeinnamen. Iedere computer op Internet is bereikbaar via een eigen uniek IP-adres. Voorbeelden daarvan zijn 192.0.2.26 (IPv4) en 2001:db8:1:26 (IPv6). DNS, een afkorting van Domain Name System, zorgt op de achtergrond voor de vertaling van domeinnamen naar IP-adressen zodat de webbrowser op de juiste bestemming terechtkomt. DNSSEC, een afkorting van Domain Name System Security Extensions, breidt DNS uit</i>	geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V. Onderzoek van de door de gemeente Duiven aangeleverde documenten plus het uitvoeren van gerichte deelwaarnemingen.		Wij hebben geconstateerd dat DNSSEC (DNS Security Extensions) wordt gebruikt voor de URL van het object van onderzoek. Met DNSSEC wordt de authenticiteit van DNS-antwoorden geverifieerd om misbruik te voorkomen. Wij hebben vastgesteld dat de gemeente Duiven verantwoordelijk is voor het regelen van DNSSEC. Wij hebben vastgesteld dat de gemeente Duiven een voorschrift heeft opgesteld dat DNSSEC moet worden toegepast op alle domeinnamen én op DNS-resolvers die clients van de gemeente Duiven direct of indirect van DNS-antwoorden voorzien. Het toepassen van DNSSEC is op basis van de "pas toe of leg uit" lijst van het College Standaardisatie verplicht voor het openbaar bestuur (rijk, provincies, gemeenten en waterschappen en instellingen uit de (semi-)publieke sector). Zie hiervoor https://www.forumstandaardisatie.nl/standaard/dnssec.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	met een extra beveiliging. De vertaling van domeinnaam naar IP-adres wordt daartoe voorzien van een digitale handtekening. Een internetgebruiker kan die handtekening automatisch laten controleren. Dat voorkomt dat hij misleid wordt naar een vals IP-adres. DNSSEC is in het DigiD assessment verplicht gesteld. Voor organisaties die DNSSEC ondersteunen wordt er voor beide partijen direct een sterke beveiliging aan het DNS-systeem toegevoegd. Een valse website of een valse brievenbus wordt dan simpelweg geblokkeerd. Internetgebruikers die nog geen DNSSEC ondersteunen kunnen beveiligde domeinnamen zonder problemen blijven gebruiken. HTTPS wordt voor alle overheidssites overigens ook wettelijk verplicht na invoering van de Wet Generieke Digitale Infrastructuur, waarin digitale overheidsvoorzieningen zoals DigiD en MijnOverheid.nl in worden geregeld.			
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope). <u>Doelstelling:</u> Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de webapplicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen. <u>Betrokken rol(len):</u> • Hosting- of SAAS leverancier. <u>Scope:</u> • De infrastructuur voor het netwerksegment met de DigiD	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	webapplicatie.			
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope). <u>Doelstelling:</u> Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie). <u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS leverancier. <u>Scope:</u> • De DigiD webapplicatie, de webserver en andere servers in het DMZ van de DigiD webapplicatie.	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. <u>Doelstelling:</u> Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen. <u>Betrokken rol(len):</u> • Hosting- of SAAS leverancier. <u>Scope:</u>	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	De infrastructuur voor het netwerksegment met de DigiD webapplicatie.			
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd. <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. <u>Betrokken rol(len):</u> - Hosting- of SAAS leverancier. <u>Scope:</u> - De infrastructuur voor het netwerksegment met de DigiD webapplicatie.	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.
C.08	Wijzigingsbeheer 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. <u>Betrokken rol(len):</u> Applicatie-, hosting- of SAAS leverancier.	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V. Onderzoek van de door de gemeente Duiven aangeleverde documenten plus het uitvoeren van gerichte deelwaarnemingen.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM. De webapplicatie wordt door Centric Netherlands B.V. getest en nieuwe versies worden geaccepteerd voordat deze in de productie worden genomen. Bij het testen worden testscript gehanteerd en de testresultaten vastgelegd. <u>TPM versie</u> Er is slechts één versie van de applicatie in productie. Het betreft een multi-tenant applicatie; de versie van de applicatie komt derhalve overeen of is hoger dan de versie die is vermeld in de TPM. De gemeente Duiven heeft aantoonbaar kennisgenomen van de releasedocumentatie van Centric Netherlands B.V.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	- Houder van DigiD aansluiting. <u>Scope:</u> - De DigiD webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. <u>Uitleg:</u> <i>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.</i> <i>Ingeval van SAAS-toepassingen ligt de verantwoordelijkheid voor het testen van wijzigingen aan de applicatie doorgaans bij de leverancier en/of gebruikersgroep.</i> <u>Aandachtspunten hierbij zijn:</u> - 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			Aanbeveling voor de gemeente Duiven: - Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft vastgesteld dat deze norm getoetst gaat worden op werking. Hierbij wordt een overgangsjaar gebruikt. Voor aansluithouders betekent dit het volgende: - Vanaf inleverperiode 1 januari - 1 mei 2024 (over het voorgaande jaar 2023) mogen deze en de overige vier betrokken normen op werking worden getoetst. - Vanaf inleverperiode 1 januari - 1 mei 2025 (over het voorgaande jaar 2024) moet deze en de overige vier betrokken normen op werking worden getoetst. Zorg ervoor dat u alle releasenotes gedurende een jaar voorafgaand aan het assessment bewaard en achteraf kunt aantonen.

Nr	Beschrijving van de beveiligingsrichtlijn	Uitgevoerde werkzaamheden	Oordeel	Aanbevelingen en/of opmerkingen
	<i>testomgeving worden getest voordat zij in productie kunnen worden genomen (N.B. voor netwerk wijzigingen is een testomgeving vaak niet mogelijk).</i> <i>Het hanteren van een testscript en de vastlegging van de testresultaten.</i> <i>Een formele acceptatie voor het in productie nemen van de wijziging.</i> <i>Het beperken van het aantal personen die wijzigingen in productie kunnen nemen.</i> <i>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.</i>			
C.09	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. <u>Betrokken rol(len):</u> • Applicatie-, hosting- of SAAS leverancier. <u>Scope:</u> • Hypervisor (VM Ware, etc.). • Operating system (Windows, etc.). • Databases. • Netwerk componenten. • Firewall.	Er is kennis genomen van de door de gemeente Duiven overlegde Third Party Mededeling. Deze TPM is beoordeeld als geldig en actueel. Hierbij wordt "gesteund" op de TPM van Centric Netherlands B.V.		De gemeente Duiven heeft de ontwikkeling, beheer en het onderhoud van de webapplicatie plus het beheer van de infrastructuur uitbesteed aan de serviceorganisatie Centric Netherlands B.V. Hiervoor geldt de TPM.

