

DigiD ICT-beveiligingsassessment

Rapport voor Gemeente Doesburg (Gemeente Doesburg - Digitaal Loket)

2-Control B.V.

Datum: 21 april 2026
DigiD kenmerk: Gemeente Doesburg - Digitaal Loket
Aansluitnummer: 1001378
Referentie: 2C-2026-868

Versiebeheer

Versie	Datum	Status	Naam
0.1	5 maart 2026	Gereed voor OKB	2-Control B.V.
1.0	21 april 2026	Definitief	2-Control B.V.

Inhoud

1	Assurance-rapport van de onafhankelijke IT-auditor	4
1.1	Onze oordelen	4
1.2	De basis voor onze oordelen	5
1.3	Van toepassing zijnde criteria	5
1.4	Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek	6
1.5	Beoogde gebruikers en doel	7
1.6	Verantwoordelijkheden van de DigiD dienstverlener	8
1.7	Verantwoordelijkheden van de IT-auditor	8
Bijlage A – Beschrijving van de testresultaten van de auditor		9
Bijlage B – Object van onderzoek		10
Bijlage C – Overzicht onderverdeling getoetste normen ICT-beveiligingsassessment DigiD-omgeving van Gemeente Doesburg		11
Bijlage D – Overzicht ICT-beveiligingsassessment DigiD		16

1 Assurance-rapport van de onafhankelijke IT-auditor

Aan: Bestuur Gemeente Doesburg en Logius

Datum: 21 april 2026

Van: 2-Control B.V.

Aansluiting: aansluitnummer: 1001378, aansluitnaam: 'Gemeente Doesburg - Digitaal Loket', dienstverlener Gemeente Doesburg

1.1 Onze oordelen

Wij hebben een DigiD-beveiligingsassessment met redelijke mate van zekerheid uitgevoerd op de webomgeving van DigiD-aansluiting met aansluitnummer: 1001378 en aansluitnaam: "Gemeente Doesburg - Digitaal Loket" van Gemeente Doesburg (hierna: "de DigiD Dienstverlener").

Per beveiligingsrichtlijn hebben wij hieronder vermeld of wordt voldaan aan de beveiligingsrichtlijn. Om de leesbaarheid van dit rapport te vergroten zijn de oordelen in deze tabel weergegeven als "voldoet" of "voldoet niet". 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 is opgezet en geïmplementeerd op 31 december 2025". "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 is opgezet en/of geïmplementeerd op 31 december 2025".

Bij beveiligingsrichtlijnen waarbij ook de effectieve werking wordt vastgesteld moet "voldoet" worden geïnterpreteerd als "Wij zijn van oordeel dat de getoetste interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn effectief werkten tijdens de controleperiode van 1 juli 2025 tot en met 31 december 2025". "Voldoet niet" moet vervolgens worden geïnterpreteerd als "Wij zijn van oordeel dat de getoetste interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn niet in alle materiële opzichten effectief werkten tijdens de controleperiode van 1 juli 2025 tot en met 31 december 2025".

De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel zijn de criteria die zijn beschreven in sectie "1.3 Van toepassing zijnde criteria".

Onze oordelen zijn gevormd op basis van de van de aangelegenheden die in dit assurance-rapport zijn uiteengezet.

Nr.	Beschrijving van de beveiligingsrichtlijn	Oordeel opzet en bestaan	Oordeel werking
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatie gerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.	Voldoet	N.v.t.
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.	Voldoet	N.v.t.
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.	Voldoet in opzet [1]	Geen oordeel [2]
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Voldoet	Voldoet

Nr.	Beschrijving van de beveiligingsrichtlijn	Oordeel opzet en bestaan	Oordeel werking
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Voldoet	N.v.t.
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.	Voldoet	N.v.t.
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet	Voldoet

1.2 De basis voor onze oordelen

[1] Bestaan - non-occurrence - voldoet in opzet. Voor beveiligingsrichtlijn UTV.01 hebben wij vastgesteld dat de Gemeente Doesburg maatregelen heeft ontworpen met betrekking tot deze norm. Vanwege het feit dat zich geen situatie heeft voorgedaan waarop deze maatregel betrekking heeft, hebben wij het bestaan niet kunnen vaststellen. Vanwege non-occurrence kan het bestaan niet worden vastgesteld en daarom geven wij over het bestaan geen oordeel.

[2] Werking - non-occurrence - geen oordeel. Voor beveiligingsrichtlijn UTV.01 hebben wij vastgesteld dat de Gemeente Doesburg maatregelen heeft ontworpen (opzet). Wij zijn van oordeel dat de organisatie in opzet voldoet aan deze norm. Vanwege non-occurrence kan de effectieve werking niet worden vastgesteld en daarom geven wij daarover geen oordeel.

Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht, waaronder de NOREA Richtlijn 3000D 'Assurance-opdrachten door IT-auditors (Directe-opdrachten)' en de nadere regels zoals opgenomen in de 'Handreiking DigiD 2025 (versie 1.0)' van NOREA. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Verantwoordelijkheden van de IT-auditor'.

Wij zijn onafhankelijk van DigiD dienstverlener en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor onze oordelen.

1.3 Van toepassing zijnde criteria

Voor deze opdracht hanteren wij het "Normenkader 3.0 voor ICT-beveiligingsassessments DigiD" dat door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is vastgesteld. Het Ministerie BZK heeft uit de "NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties versie 2015" de 21 beveiligingsrichtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact op de veiligheid van DigiD-webapplicaties hebben en heeft deze vermeld in het "Normenkader 3.0 ICT-beveiligingsassessments DigiD". De versie 3.0 geldt vanaf 1 augustus 2022. De geselecteerde 21 beveiligingsrichtlijnen worden tevens aangeduid als de 21 DigiD-normen.

De criteria waarvan gebruik wordt gemaakt bij het uitvoeren van de assurance-opdracht houden in dat:

1. de risico's die het voldoen aan de beveiligingsrichtlijnen in gevaar brengen en daarmee de betrouwbaarheid van DigiD aantasten, werden onderkend;
2. de onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het voldoen aan beveiligingsrichtlijnen niet zouden verhinderen;
3. de interne beheersingsmaatregelen die verband houden met de beveiligingsrichtlijnen op afdoende wijze zijn opgezet en daadwerkelijk zijn geïmplementeerd;
4. de interne beheersingsmaatregelen die verband houden met een selectie van specifieke beveiligingsrichtlijnen gedurende de controleperiode effectief hebben gewerkt.

1.4 Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek

1.4.1 *Object van onderzoek*

Het object van onderzoek was de webomgeving van DigiD aansluiting "Gemeente Doesburg - Digitaal Loket" (aansluitnummer 1001378).

Gemeente Doesburg biedt de volgende functionaliteit aan waarvoor DigiD aansluiting "Gemeente Doesburg - Digitaal Loket" (aansluitnummer 1001378) ter authenticatie wordt gebruikt: Een digitaal loket voor burgers met onder meer het inzien van gegevens en het indienen van formulieren. Deze functionaliteit wordt geboden door de volgende webapplicatie:

- SIMform en PIP versie 1.97 (SIMform) en 2.130 (PIP);
- De URL waarop de webapplicatie te bereiken is, betreft: mijn.doesburg.nl.

Deze applicatie betreft een geheel standaard pakket en wordt aangeboden in de vorm van SaaS. De applicatie wordt onderhouden door Shift2.

Het onderzoek heeft zich gericht op de webapplicatie die gebruik maakt van DigiD voor de identificatie en authenticatie van de gebruikers. Specifiek zijn in scope de internet-facing webpagina's waarmee de interactie naar de gebruiker plaatsvindt als deze is geïdentificeerd en geauthentiseerd via DigiD, de systeemkoppelingen en de infrastructuur die met DigiD gekoppeld is en betrekking heeft op het DigiD identificatie en authenticatieproces. Ook de verschillende vormen van beheer op de webapplicaties zijn in scope voor zover relevant voor de doelstelling van de audit.

De URL www.digid.nl, de token uitwisseling tussen Logius en de webserver, de systemen die gegevens leveren of ophalen uit de webapplicatie, zoals backoffice informatiesystemen vallen buiten de scope. Subsystemen en koppelvlakken zijn in scope indien de primaire authenticatie van het systeem op basis van DigiD tot stand is gekomen.

In bijlage B geven wij u een meer gedetailleerde beschrijving van het object van onderzoek.

1.4.2 *Serviceorganisatie(s)*

De DigiD dienstverlener maakt gebruik van Shift2 voor ontwikkeling en hosting van de SaaS-applicatie. De DigiD dienstverlener maakt voor het verschaffen van zekerheid over haar volledige webomgeving zoals beschreven onder het object van onderzoek gebruik van de uitsluitingsmethode ("carve-out method"). De beschrijving van de DigiD dienstverlener van haar systeem sluit daarmee de interne beheersingsdoelstellingen en daarmee verband houdende interne beheersingsmaatregelen van de serviceorganisatie(s) uit. Onze werkzaamheden strekken zich dan ook niet uit tot de interne beheersingsmaatregelen van de serviceorganisatie. Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de genoemde assurance-rapportages. Wij kunnen dan ook geen enkele verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

1.4.3 **Norm ICT-beveiligingsassessment DigiD**

Het “Normenkader 3.0 voor ICT-beveiligingsassessments DigiD” bevat 21 beveiligingsrichtlijnen uit de “ICT-beveiligingsrichtlijnen voor webapplicaties versie 2015” van het Nationaal Cyber Security Centrum (NCSC). Daarom zijn we niet in staat om één overkoepelend oordeel af te geven met betrekking tot de beveiliging van de DigiD-aansluiting.

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft de richtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact hebben op de veiligheid van DigiD-webapplicaties. Logius houdt in opdracht van BZK toezicht op het naleven van de Voorwaarden DigiD, waaronder de uitvoering van DigiD-assessments. Wij adviseren de DigiD dienstverlener om in aanvulling op de richtlijnen in de vigerende “Norm ICT-beveiligingsassessments DigiD”, ook de andere richtlijnen uit de “ICT-beveiligingsrichtlijnen voor webapplicaties versie 2015” van het NCSC te adopteren. Wij wijzen u erop dat, indien wij aanvullende beveiligingsrichtlijnen zouden hebben onderzocht wellicht andere onderwerpen zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen.

1.4.4 **Beperkingen met betrekking tot interne beheersingsmaatregelen**

Interne beheersingsmaatregelen bij een organisatie kunnen, vanwege hun aard, niet alle fouten of omissies voorkomen of ontdekken en corrigeren.

Voor wat betreft de werking hebben wij alleen werkzaamheden uitgevoerd naar de interne beheersingsmaatregelen zoals aangegeven in “Normenkader 3.0 voor ICT-beveiligingsassessments DigiD” voor zover van toepassing binnen de scope van ons onderzoek.

Bovendien is het projecteren naar de toekomst van onze oordelen met betrekking tot de interne beheersingsmaatregelen om de doelstellingen te bereiken, onderhevig aan het risico dat interne beheersingsmaatregelen ineffectief kunnen worden.

Ons oordeel is niet aangepast als gevolg van deze aangelegenheden.

1.5 **Beoogde gebruikers en doel**

Ons assurance-rapport is uitsluitend bestemd voor de DigiD dienstverlener en Logius om inzicht te geven in de ICT beveiliging van de webomgeving van DigiD aansluiting. Logius kan hiermee toezicht houden op de koppeling van DigiD met de webapplicatie van een aangesloten organisatie voor het vertrouwen in en de integriteit van elektronische (overheids)dienstverlening.

Bijlage A bevat de beschrijving van de uitgevoerde (test)werkzaamheden en onze oordelen en aanbevelingen ter verbetering van de DigiD-webomgeving.

Bijlage B bevat de (uitgebreide) beschrijving van het “Object van onderzoek”.

De bijlagen A en B zijn alleen bestemd voor de DigiD dienstverlener.

Bijlage C is bedoeld om Logius een totaaloverzicht te verschaffen (“volledigheid van de scope”) over de resultaten van verschillende assessments, indien gebruik is gemaakt van rapporten inzake serviceorganisatie(s).

Bijlage D is bedoeld om Logius een totaaloverzicht te verschaffen (“identificatie”) over de identificerende kenmerken van het DigiD-assessment, ongeacht of gebruik is gemaakt van rapporten inzake serviceorganisatie(s).

Ons assurance-rapport en bijlagen mag enkel worden gebruikt voor het doel waarvoor het is opgesteld door de beoogde gebruikers en dient niet te worden verspreid aan of te worden gebruikt door anderen.

1.6 Verantwoordelijkheden van de DigiD dienstverlener

Het bestuur van de DigiD dienstverlener is verantwoordelijk voor het verlenen van DigiD-diensten, het onderkennen van de beveiligingsrisico's van de DigiD-webomgeving en het opzetten en implementeren van interne beheersingsmaatregelen om te voldoen aan de vigerende norm "Normenkader 3.0 voor ICT-beveiligingsassessments DigiD".

1.7 Verantwoordelijkheden van de IT-auditor

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van ons onderzoek dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordelen over de opzet en implementatie van interne beheersingsmaatregelen die verband houden met de beveiligingsrichtlijnen in overeenstemming met de hiervoor vermelde criteria.

Ons onderzoek is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens ons onderzoek niet alle materiële fouten en fraude ontdekken.

Wij passen het "Reglement Kwaliteitsbeheersing NOREA (RKBN)" toe. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van ethische voorschriften, professionele standaarden en andere relevante wet- en regelgeving.

Ons onderzoek om te rapporteren over opzet, bestaan en voor de van toepassing zijnde beveiligingsrichtlijnen uit "Normenkader 3.0 voor ICT-beveiligingsassessment DigiD" de werking van interne beheersingsmaatregelen bestond onder andere uit:

1. Het verkrijgen van inzicht in de relevante kenmerken van de DigiD- webomgeving;
2. Het vaststellen van de scope van het assessment, inclusief het vaststellen van de maatregelen die bij de serviceorganisatie moeten worden onderzocht;
3. Het houden van interviews met verantwoordelijke functionarissen, vooral gericht op het onderkennen van risico's en het onderzoek in hoeverre deze risico's worden afgedekt door maatregelen;
4. Het evalueren van de opzet, het vaststellen van het bestaan en voor de van toepassing zijnde beveiligingsrichtlijnen uit "Normenkader 3.0 voor ICT-beveiligingsassessment DigiD" de werking van de relevante maatregelen. Dit door middel van het kennis nemen van documentatie, het kennis nemen van de resultaten van de uitgevoerde interne controles en uitgevoerde pentesten, alsmede eigen waarnemingen;
5. Het evalueren van de uitkomsten van onze werkzaamheden.

Breda, 21 april 2026

R. Haest

Breda, 21 April 2026
eIDAS Qualified Electronic Signature



R.L.E. Haest RE
2-Control B.V.
Haagsemarkt 1
4813 BA Breda

Bijlage A – Beschrijving van de testresultaten van de auditor

Bijlage B – Object van onderzoek

Bijlage C – Overzicht onderverdeling getoetste normen ICT-beveiligingsassessment DigiD-omgeving van Gemeente Doesburg

Deze bijlage richt zich op het ten dienste van Logius inzichtelijk maken van de wijze waarop Gemeente Doesburg gebruik heeft gemaakt van serviceorganisaties die betrekking hebben op het object van onderzoek van DigiD aansluiting 'Gemeente Doesburg - Digitaal Loket' (aansluitnummer 1001378).

Als input voor de hierna vermelde samenvatting is, naast de voorliggende rapportage, gebruik gemaakt van de volgende rapportage(s):

Omschrijving assurance-rapportage	Serviceorganisatie	Bij serviceorganisatie getoetste beveiligingsrichtlijnen	Referentie / Rapportdatum / Controleperiode	Oordeelsdatum	Ondertekend door naam RE
DigiD assurance-rapportage	1: Shift2 Serviceorganisatie voor SaaS.	B.01, B.05, U/TV.01, U/WA.02, U/WA.03, U/WA.04, U/WA.05, U/PW.02, U/PW.03, U/PW.05, U/PW.07, U/NW.03, U/NW.04, U/NW.05, U/NW.06, C.03, C.04, C.06, C.07, C.08, C.09	214/422400/2025/23962_13 d.d. 15 oktober 2025 over 1 april 2025 tot 30 september 2025	7 oktober 2025	Drs. F.W. Hanekamp RE van Afier IT-Auditors B.V.

Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de genoemde assurance-rapportage(s). Wij kunnen dan ook geen enkele verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Wij hebben kennis genomen van de genoemde assurance-rapportage(s) en hebben ten behoeve van Logius in onderstaande tabel per beveiligingsrichtlijn aangegeven tot welk oordeel de service auditor is gekomen en of in die rapportages sprake is van aanvullende beheersmaatregelen gebruikersorganisatie (de user entity controls) en of wij deze dan ook hebben getoetst bij de houderorganisatie (gebruikersorganisatie).

Nr.	Beschrijving van de norm	Conclusie leverancier(s)	Referentie / rapportnr. Leverancier (s)	Aanvullende beheersmaatregelen gebruikersorganisatie ¹	Conclusie gebruikersorganisatie
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatie gerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Ja	Opzet en bestaan: Voldoet Werking: N.v.t.
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.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Ja	Opzet en bestaan: Voldoet Werking: N.v.t.
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.	Leverancier 1: Opzet en bestaan: Voldoet in opzet [1] Werking: Geen oordeel [2]	Leverancier 1: 214/422400/2025/23962_13	Ja	Opzet en bestaan: Voldoet in opzet [1] Werking: Geen oordeel [2]

¹ Naar het oordeel van de auditor(s) van de serviceorganisatie(s)

Nr.	Beschrijving van de norm	Conclusie leverancier(s)	Referentie / rapportnr. Leverancier (s)	Aanvullende beheersmaatregelen gebruikersorganisatie ¹	Conclusie gebruikersorganisatie
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Ja	Opzet en bestaan: Voldoet Werking: Voldoet
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Nee	Niet getoetst
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Nee	Niet getoetst
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Ja	Opzet en bestaan: Voldoet Werking: N.v.t.
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Nee	Niet getoetst
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Nee	Niet getoetst
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.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Nee	Niet getoetst

Nr.	Beschrijving van de norm	Conclusie leverancier(s)	Referentie / rapportnr. Leverancier (s)	Aanvullende beheersmaatregelen gebruikersorganisatie ¹	Conclusie gebruikersorganisatie
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Nee	Niet getoetst
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.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Nee	Niet getoetst
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Nee	Niet getoetst
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Nee	Niet getoetst
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Ja	Opzet en bestaan: Voldoet Werking: N.v.t.
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Nee	Niet getoetst
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Nee	Niet getoetst

Nr.	Beschrijving van de norm	Conclusie leverancier(s)	Referentie / rapportnr. Leverancier (s)	Aanvullende beheersmaatregelen gebruikersorganisatie ¹	Conclusie gebruikersorganisatie
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	Leverancier 1: Opzet en bestaan: Voldoet Werking: N.v.t.	Leverancier 1: 214/422400/2025/23962_13	Nee	Niet getoetst
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.	Leverancier 1: Opzet en bestaan: Voldoet Werking: Voldoet	Leverancier 1: 214/422400/2025/23962_13	Nee	Niet getoetst
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Leverancier 1: Opzet en bestaan: Voldoet Werking: Voldoet	Leverancier 1: 214/422400/2025/23962_13	Ja	Opzet en bestaan: Voldoet Werking: Voldoet
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.	Leverancier 1: Opzet en bestaan: Voldoet Werking: Voldoet	Leverancier 1: 214/422400/2025/23962_13	Nee	Niet getoetst

[1] Bestaan - non-occurrence - voldoet in opzet. Voor beveiligingsrichtlijn UTV.01 hebben wij vastgesteld dat de leverancier en gebruikersorganisatie maatregelen heeft ontworpen met betrekking tot deze norm. Vanwege het feit dat zich geen situatie heeft voorgedaan waarop deze maatregel betrekking heeft, hebben wij het bestaan niet kunnen vaststellen. Vanwege non-occurrence kan het bestaan niet worden vastgesteld en daarom geven wij over het bestaan geen oordeel.

[2] Werking - non-occurrence - geen oordeel. Voor beveiligingsrichtlijn UTV.01 hebben wij vastgesteld dat de leverancier en gebruikersorganisatie maatregelen heeft ontworpen (opzet). Wij zijn van oordeel dat de organisatie in opzet voldoet aan deze norm. Vanwege non-occurrence kan de effectieve werking niet worden vastgesteld en daarom geven wij daarover geen oordeel.

Bijlage D – Overzicht ICT-beveiligingsassessment DigiD

Hieronder treft u een verkort overzicht aan van de identificerende kenmerken en de gebruikte assessmentrapportages die invulling geven aan het uitgevoerde DigiD-beveiligingsassessment op de webomgeving van de hieronder vermelde DigiD-aansluiting

Aansluiting	Aansluitnummer:	1001378
	Aansluitnaam:	Gemeente Doesburg - Digitaal Loket
	Dienstverlener:	Gemeente Doesburg
Auditor dienstverlener	Auditor:	2-Control B.V. getekend door R.L.E. Haest RE
	Kenmerk rapport	2C-2026-868 d.d. 21 april 2026
	Oordeelsdatum	31 december 2025
	Controleperiode	1 juli 2025 tot en met 31 december 2025
Object van onderzoek	Naam webapplicatie:	SIMform en PIP
	Versienummer:	1.97 (SIMform) en 2.130 (PIP)
	Omschrijving:	Een digitaal loket voor burgers met onder meer het inzien van gegevens en het indienen van formulieren.
Serviceorganisatie 1	Naam serviceorganisatie:	Shift2
	Auditor serviceorganisatie:	Afier IT-Auditors B.V. getekend door Drs. F.W. Hanekamp RE
	Kenmerk rapport:	214/422400/2025/23962_13 d.d. 15 oktober 2025
	Oordeelsdatum:	7 oktober 2025
	Controleperiode:	1 april 2025 tot 30 september 2025