

**DigiD beveiligingsassessment**  
**2025-2026**  
**Gemeente Meierijstad**



**DigiD aansluiting** Meierijstad - Digitaal Loket  
**Aansluitnummer** 1001977  
**Kenmerk** BKBO/250815-02/D4/AR

Rapportdatum 29 april 2026  
Oordeelsdatum 22 april 2026  
Dit assurancerapport heeft 16 pagina's  
[www.bkbo.nl](http://www.bkbo.nl)

## CITAAT

"Binnen de perken zijn de mogelijkheden even onbeperkt als daarbuiten"

Jules Deelder  
(1944- 2019)

## Colofon

Voor u ligt het rapport van het ICT-beveiligingsassessment, dat wij uitvoerden voor de gemeente Meierijstad.

Ons rapport wordt uitgebracht in twee versies: het 'short form' rapport bevat de basiselementen inclusief de bijlagen bedoeld voor de toezichthouder. Het 'long form' rapport bevat aanvullende informatie die uitsluitend bedoeld is voor de gemeente Meierijstad, zoals een overzicht van de getoetste interne beheersmaatregelen, de door ons vastgestelde bevindingen en aanbevelingen plus een nadere beschrijving van het object van onderzoek.

Dit rapport is opgesteld onder verantwoordelijkheid van de heer drs. M.B.H. Ijpelaar RE CEH CISA CIPP/E ingeschreven onder nummer 1252 als actief RE in het register van NOREA en geregistreerd als actief CISA met nummer 0126934 bij ISACA.

## Inhoudsopgave

|       |                                                                    |    |
|-------|--------------------------------------------------------------------|----|
| 1     | Assurancerapport van de onafhankelijke 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  |
| 1.4.1 | Object van onderzoek                                               | 6  |
| 1.4.2 | Serviceorganisaties                                                | 6  |
| 1.4.3 | Norm ICT-beveiligingsassessments DigiD                             | 7  |
| 1.4.4 | Beperkingen met betrekking tot interne beheersmaatregelen          | 7  |
| 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 – Rapport van bevindingen DigiD                          | 10 |
|       | Bijlage B – Object van onderzoek                                   | 11 |
|       | Bijlage C – Totaaloverzicht getoetste normen                       | 12 |
|       | Bijlage D - Totaaloverzicht beveiligingsassessment                 | 15 |
|       | Bijlage E - DigiD RSO Shift2                                       | 16 |

# 1 Assurancerapport van de onafhankelijke auditor

|                 |                                                     |
|-----------------|-----------------------------------------------------|
| Aan:            | Management van de gemeente Meierijstad en Logius    |
| Rapportdatum:   | 29 april 2026                                       |
| Rapportnummer:  | BKBO/250815-02/D4/AR                                |
| Van:            | drs. M.B.H. Ijpelaar RE CEH CISA CIPP/E van BKBO bv |
| Aansluitnummer: | 1001977                                             |
| Aansluitnaam:   | Meierijstad - Digitaal Loket                        |
| Dienstverlener: | de gemeente Meierijstad                             |

## 1.1 Onze oordelen

Wij hebben een DigiD-beveiligingsassessment met redelijke mate van zekerheid uitgevoerd op de webomgeving van DigiD-aansluiting '1001977 - Meierijstad - Digitaal Loket' van de gemeente Meierijstad (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" met de kleur "groen" of "voldoet niet" met de kleur "rood". Hierbij moet "voldoet" ingeval het oordeel is beperkt tot opzet en bestaan 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 22 april 2026". "Voldoet niet" moet ingeval het oordeel is beperkt tot opzet en bestaan 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 22 april 2026".

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 augustus 2025 tot en met 31 januari 2026". "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 augustus 2025 tot en met 31 januari 2026".

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

Onze oordelen zijn gevormd op basis van de aangelegenheden die in dit assurancerapport zijn uiteengezet.

| Nr   | Beschrijving van de beveiligingsrichtlijn                                                                                                                                                                             | Oordeel opzet & bestaan | Oordeel werking |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-----------------|
| B.01 | De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde 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.          |

| Nr      | Beschrijving van de beveiligingsrichtlijn                                                                                                                                         | Oordeel opzet & bestaan | Oordeel werking |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-----------------|
| U/WA.02 | Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.                                | Voldoet                 | Voldoet         |
| U/WA.05 | De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacy bevorderende 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

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 1.7 'Verantwoordelijkheden van de IT-auditor'.

Wij zijn onafhankelijk van de 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 heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de richtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact hebben op de veiligheid van DigiD-webapplicaties en heeft BZK deze vermeld in 'het DigiD normenkader ICT-beveiligingsassessments DigiD 3.0' welke wij hebben gehanteerd bij dit onderzoek. Het DigiD Normenkader 3.0 bestaat uit 21 richtlijnen die zijn gebaseerd op de ICT-Beveiligingsrichtlijnen voor webapplicaties. De versie 3.0 geldt vanaf 1 augustus 2022 en is vastgesteld door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De 21 beveiligingsrichtlijnen uit het Normenkader worden in het dagelijks gebruik de 21 normen genoemd.

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

- de risico's die het voldoen aan de beveiligingsrichtlijnen in gevaar brengen en daarmee de betrouwbaarheid van DigiD aantasten, werden onderkend;
- 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;
- de interne beheersingsmaatregelen die verband houden met de beveiligingsrichtlijnen op afdoende wijze zijn opgezet en daadwerkelijk zijn geïmplementeerd;

- 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 '1001977 Meierijstad - Digitaal Loket'.

De gemeente Meierijstad biedt de volgende functionaliteit aan waarvoor DigiD aansluiting '1001977 Meierijstad - Digitaal Loket' ter authenticatie wordt gebruikt:

- Een Persoonlijke Internet Pagina voor burgers ten behoeve van het inzien van de eigen gegevens en de status van aanvragen.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- PIP met de door ons onderzochte versie 2.133.0.

De webapplicatie is extern benaderbaar via DigiD via de volgende URL:

[https://www.meerijstad.nl/Mijn\\_Meerijstad](https://www.meerijstad.nl/Mijn_Meerijstad)

De webapplicatie betreft een geheel standaard pakket en wordt geleverd als Software As A Service door Shift2.

#### Scope

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](http://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.

Zie voor de aanvullende assurance waarop wordt 'gesteund' de bijlagen C en D.

### 1.4.2 Serviceorganisaties

#### SAAS volgens carve-out methodiek

De gemeente Meierijstad maakt gebruik van serviceorganisatie Shift2 voor de ontwikkeling, beheer en onderhoud en het hosten van de webapplicatie. De gemeente Meierijstad maakt voor het verschaffen van zekerheid over haar volledige webomgeving zoals beschreven onder het object van onderzoek gebruik van de uitsluitingsmethode ('carve-out methodiek'). De beschrijving van de DigiD dienstverlener van haar

systeem sluit daarmee de interne beheersdoelstellingen en daarmee verband houdende interne beheersmaatregelen van de serviceorganisatie uit. Onze werkzaamheden strekken zich dan ook niet uit tot de interne beheersmaatregelen van de serviceorganisatie.

### 1.4.3 Norm ICT-beveiligingsassessments DigiD

Het Normenkader 3.0 voor ICT-beveiligingsassessments DigiD bevat 21 beveiligingsrichtlijnen en is een selectie van 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 gemeente Meierijstad 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 beheersmaatregelen

Interne beheersingsmaatregelen bij een serviceorganisatie 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 assurancerapport en bijlagen mogen enkel worden gebruikt door de beoogde gebruikers en/of verspreidingskring voor het doel waarvoor deze zijn opgesteld 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 beheersmaatregelen om te voldoen aan de vigerende 'Normenkader voor ICT-beveiligingsassessments DigiD 3.0'.

## 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 door ons af te geven oordelen over de opzet en implementatie van interne beheersmaatregelen 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:

- 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(s) moeten worden onderzocht.
- 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.
- 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.

- Het evalueren van de uitkomsten van onze werkzaamheden.

BKBO B.V.

|                                                                                                                                                                                                                                                                                                               |                                                                                    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
|  <div data-bbox="284 730 719 869"> <p><b>M. Ijpelaar</b></p> <p>Vrijmen, 29 April 2026<br/>eIDAS Qualified Electronic Signature</p>  </div> |  |
| <p>drs. M.B.H. Ijpelaar RE CEH CISA CIPP/E,<br/>directeur</p>                                                                                                                                                                                                                                                 | <p>S.H.J. van Buren MSc, auditondersteuner</p>                                     |

## Bijlage A – Rapport van bevindingen DigiD

Deze bijlage is niet bestemd voor de toezichthouder en wordt slechts verstrekt aan de gemeente Meierijstad.

## Bijlage B – Object van onderzoek

Deze bijlage is niet bestemd voor de toezichthouder en wordt slechts verstrekt aan de gemeente Meierijstad.

## Bijlage C – Totaaloverzicht getoetste normen

Deze bijlage richt zich op het ten dienste van Logius inzichtelijk maken van de wijze waarop de gemeente Meerijstad gebruik heeft gemaakt van serviceorganisaties die betrekking hebben op het object van onderzoek van DigiD-aansluiting '1001977 - Meerijstad - Digitaal Loket'.

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

| Omschrijving assurance-rapportage                  | (Sub)service-organisatie | Bij service-organisatie getoetste normen | Referentie en controleperiode                                                  | Oordeelsdatum  | Ondertekend door      |
|----------------------------------------------------|--------------------------|------------------------------------------|--------------------------------------------------------------------------------|----------------|-----------------------|
| ISAE3000/D assurance-rapportage PIP versie 2.122.2 | Shift2                   | Alle DigiD beveiligingsrichtlijnen       | 214/422400/2025/23963_2 met controleperiode 1 april 2025 tot 30 september 2025 | 7 oktober 2025 | drs. W.F. Hanekamp RE |

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 kennisgenomen van de genoemde assurance rapportage(s) en hebben ten behoeve van Logius in onderstaande tabel per beveiligingsrichtlijn aangegeven tot welk oordeel de auditor van de serviceorganisatie is gekomen en of in die rapportages sprake is van aanvullende beheersmaatregelen voor de gebruikersorganisatie (de "user entity controls") en of wij deze dan ook hebben getoetst bij de gemeente Meerijstad.

| Nr      | Beschrijving van de beveiligingsrichtlijn                                                                                                                                                                                                 | Getoetst in opdracht van Shift2<br>214/422400/2025/23963_2<br>15 oktober 2025 | Getoetst in opdracht van de gemeente Meerijstad |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|-------------------------------------------------|
| B.01    | De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.                          | <b>Opzet en bestaan</b><br>Shift2 voldoet                                     | <b>Opzet en bestaan</b><br>voldoet              |
| 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.                     | <b>Opzet en bestaan</b><br>Shift2 voldoet                                     | <b>Opzet en bestaan</b><br>voldoet              |
| 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 | <b>Opzet en bestaan</b><br>Shift2 voldoet in opzet                            | <b>Opzet en bestaan</b><br>n.v.t.               |
|         |                                                                                                                                                                                                                                           | <b>Werking</b><br>Shift2 geen oordeel                                         | <b>Werking</b><br>n.v.t.                        |

| Nr      | Beschrijving van de beveiligingsrichtlijn                                                                                                                                                    | Getoetst in opdracht van<br>Shift2<br>214/422400/2025/2396<br>3_2<br>15 oktober 2025 | Getoetst in opdracht van de gemeente<br>Meierijstad |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------------------------------------|
|         | gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.                                                                                                                  |                                                                                      |                                                     |
| U/WA.02 | Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.                                           | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | <b>Opzet en bestaan</b><br>voldoet                  |
|         |                                                                                                                                                                                              | <b>Werking</b><br>Shift2 voldoet                                                     | <b>Werking</b><br>voldoet                           |
| U/WA.03 | De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.                                                 | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | n.v.t.                                              |
| U/WA.04 | De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.                                                                               | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | n.v.t.                                              |
| U/WA.05 | De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.                                                         | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | <b>Opzet en bestaan</b><br>voldoet                  |
| U/PW.02 | De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.                                                                                                               | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | n.v.t.                                              |
| U/PW.03 | De webserver is ingericht volgens een configuratie-baseline.                                                                                                                                 | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | n.v.t.                                              |
| 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. | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | n.v.t.                                              |
| U/PW.07 | Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.                                                                                                                    | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | n.v.t.                                              |
| 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.                          | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | n.v.t.                                              |
| U/NW.04 | De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.                                                                              | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | n.v.t.                                              |
| U/NW.05 | Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.                                                                                                         | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | n.v.t.                                              |
| U/NW.06 | Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.                                                                                                                   | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | <b>Opzet en bestaan</b><br>voldoet                  |
| C.03    | Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).                                                  | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | n.v.t.                                              |
| C.04    | Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).                                               | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | n.v.t.                                              |
| C.06    | In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht                                                        | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | n.v.t.                                              |
| C.07    |                                                                                                                                                                                              | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | n.v.t.                                              |

| Nr   | Beschrijving van de beveiligingsrichtlijn                                                                                                                                                                    | Getoetst in opdracht van<br>Shift2<br>214/422400/2025/2396<br>3_2<br>15 oktober 2025 | Getoetst in opdracht<br>van de gemeente<br>Meierijstad |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------|
|      | 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. | <b>Werking</b><br>Shift2 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.                            | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | <b>Opzet en bestaan</b><br>voldoet                     |
|      |                                                                                                                                                                                                              | <b>Werking</b><br>Shift2 voldoet                                                     | <b>Werking</b><br>voldoet                              |
| C.09 | Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.                         | <b>Opzet en bestaan</b><br>Shift2 voldoet                                            | n.v.t.                                                 |
|      |                                                                                                                                                                                                              | <b>Werking</b><br>Shift2 voldoet                                                     | n.v.t.                                                 |

## Bijlage D - Totaaloverzicht beveiligingsassessment

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

|                               |                            |                                                                                                                            |
|-------------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Aansluiting</b>            | Aansluitnummer             | 1001977                                                                                                                    |
|                               | Aansluitnaam               | Meierijstad - Digitaal Loket                                                                                               |
|                               | Dienstverlener             | de gemeente Meierijstad                                                                                                    |
| <b>Auditor dienstverlener</b> | Naam auditor               | drs. M.B.H. Ijpelaar RE CEH CISA CIPP/E                                                                                    |
|                               | Auditorganisatie           | BKBO B.V.                                                                                                                  |
|                               | Kenmerk rapport            | BKBO/250815-02/D4/AR                                                                                                       |
| <b>Object van onderzoek</b>   | Naam webapplicatie         | PIP                                                                                                                        |
|                               | Versie                     | 2.133.0                                                                                                                    |
|                               | Omschrijving               | Een Persoonlijke Internet Pagina voor burgers ten behoeve van het inzien van de eigen gegevens en de status van aanvragen. |
| <b>Serviceorganisatie</b>     | Serviceorganisatie         | Shift2                                                                                                                     |
|                               | Auditor serviceorganisatie | Drs. F. W. Hanekamp RE van Afier IT-Auditors B.V.                                                                          |
|                               | Kenmerk rapport            | 214/422400/2025/23963_2                                                                                                    |
|                               | Controleperiode            | 1 april 2025 tot 30 september 2025                                                                                         |
|                               | Rapportdatum               | 15 oktober 2025                                                                                                            |

## Bijlage E - DigiD RSO Shift2

Het assurancerapport van de serviceorganisatie waar naar wordt verwezen in bijlage C moet door de gemeente Meerijstad in PDF/A formaat in dezelfde zending worden aangeboden aan Logius. Let op! Het is mogelijk dat hier ook een aanbiedingsbrief van de auditororganisatie van de serviceorganisatie bij hoort. Zeker als daar de aansluitnaam en aansluitnummer in staan vermeld.