

Gemeentelijk kenmerk bijlage 1 DigiD:	2021-0046382-1
--	----------------

Naam auditfirma:	BDO Audit & Assurance B.V.
Naam auditor:	Drs. W. Dalhuisen RE CISA
Datum:	

Bijlage 1 DigiD (1)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Sliedrecht - eDiensten en aansluitnummer 1003453

Sliedrecht biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Sliedrecht - eDiensten voor authenticatie wordt gebruikt:

- Het genereren van aanvraagformulieren voor e-diensten burgerzaken.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- eDiensten Burgerzaken

Deze applicatie betreft een combinatie van maatwerk en standaard software en wordt onderhouden door Centric Nederland B.V..

Deze applicatie is extern benaderbaar via het volgende internetadres:
<https://edienstenburgerzaken.sliedrecht.nl>

DigiD aansluiting Gemeente Sliedrecht - eDiensten bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Centric MS Public in de vorm van SAAS.

Het object van zelfevaluatie is de web-omgeving van DigiD aansluiting Gemeente Sliedrecht - eDiensten. De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius.

Sliedrecht heeft een deel van de DigiD web-omgeving uitbesteed aan Centric Nederland B.V.. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie. De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM / Assurancerapportage van de gemeentelijke serviceorganisatie:

Leverancier 1

Naam serviceorganisatie:	Centric Nederland B.V.
Referentie/rapportnummer:	NP9AQ7B_B en REQ5157460_B2
Afgiftedatum:	4 december 2020 en 8 maart 2021
Naam RE-auditor:	Ernst & Young Accountants LLP, ir. Peter Kornelisse RE CISA CIPP
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM / Assurancerapportage van onze serviceorganisatie het gehele normenkader afdekken. Het kan voorkomen dat een norm deels bij een leverancier en deels bij de gemeente getoetst is (zogenaamde gedeelde norm).

De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het Assurancerapport met kenmerk wdn/esc/8108.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier 1	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet	• Voldoet	• Voldoet
U/ TV.01	Identificatie en authenticatie		• Voldoet	• Voldoet
U/ WA.02	Webapplicatiebeheer proces	• Voldoet	• Voldoet	• Voldoet
U/ WA.03	Automatische data invoer controle		• Voldoet	• Voldoet
U/ WA.04	Normaliseren uitvoer		• Voldoet	• Voldoet
U/ WA.05	Cryptografie/ Privacybevordering	• Voldoet	• Voldoet	• Voldoet
U/ PW.02	Garanderen webprotocollen	•	• Voldoet	• Voldoet
U/ PW.03	Configureren webserver	•	• Voldoet niet	• Voldoet niet
U/ PW.05	Toegang tot beheermechanismen	•	• Voldoet	• Voldoet
U/ PW.07	Hardening van platformen	•	• Voldoet	• Voldoet
U/ NW.03	DMZ	•	• Voldoet	• Voldoet
U/ NW.04	Protectie- en detectiemechanismen	•	• Voldoet	• Voldoet
U/ NW.05	Scheiding beheer- en productieomgeving		• Voldoet	• Voldoet
U/ NW.06	Hardening van netwerken	• Voldoet	• Voldoet	• Voldoet
C.03	Vulnerability-assessments	•	• Voldoet	• Voldoet
C.04	Penetratietesten	•	• Voldoet	• Voldoet
C.06	Signaleringsfuncties	•	• Voldoet	• Voldoet
C.07	Monitoring functies	•	• Voldoet	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• Voldoet	• Voldoet
C.09	Patchmanagement	•	• Voldoet	• Voldoet

Bijlage 1 DigiD (2)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Sliedrecht en aansluitnummer 1002817

Sliedrecht biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Sliedrecht voor authenticatie wordt gebruikt:

- Het genereren van aanvraagformulieren voor de gemeentelijke dienstverlening.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- InProces

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door Visma Roxit B.V..

Deze applicatie is extern benaderbaar via het volgende internetadres: loket.sliedrecht.nl.

DigiD-aansluiting Gemeente Sliedrecht bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Visma Roxit B.V. in de vorm van SAAS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Sliedrecht. De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius.

Sliedrecht heeft een deel van de DigiD web-omgeving uitbesteed aan Visma Roxit B.V.. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie. De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM / assurancerapportage van de gemeentelijke serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	Visma Roxit BV
Referentie/rapportnummer:	AC/KV/RSN/09122020.2
Afgiftedatum:	9 december 2020
Naam RE-auditor:	Audit Connect BV , Agnes ter Agter RE
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM / assurancerapportage van onze serviceorganisatie het gehele normenkader afdekken. Het kan voorkomen dat een norm deels bij een leverancier en deels bij de gemeente getoetst is (zogenaamde gedeelde norm).

De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk wdn/esc/8111

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD Norm	Getoetst bij Gemeente	Getoetst bij leverancier 1	Totaal oordeel norm
------------	-----------------------	----------------------------	---------------------

B.05	Contractmanagement	• Voldoet	• Voldoet	• Voldoet
U/ TV.01	Identificatie en authenticatie	• Voldoet	• Voldoet	• Voldoet
U/ WA.02	Webapplicatiebeheer proces	• Voldoet	• Voldoet	• Voldoet
U/ WA.03	Automatische data invoer controle	•	• Voldoet	• Voldoet
U/ WA.04	Normaliseren uitvoer	•	• Voldoet	• Voldoet
U/ WA.05	Cryptografie/ Privacybevordering	• Voldoet	• Voldoet	• Voldoet
U/ PW.02	Garanderen webprotocollen	•	• Voldoet	• Voldoet
U/ PW.03	Configureren webserver	•	• Voldoet	• Voldoet
U/ PW.05	Toegang tot beheermechanismen	•	• Voldoet	• Voldoet
U/ PW.07	Hardening van platformen	•	• Voldoet	• Voldoet
U/ NW.03	DMZ	•	• Voldoet	• Voldoet
U/ NW.04	Protectie- en detectiemechanismen	•	• Voldoet	• Voldoet
U/ NW.05	Scheiding beheer- en productieomgeving	•	• Voldoet	• Voldoet
U/ NW.06	Hardening van netwerken	• Voldoet	• Voldoet	• Voldoet
C.03	Vulnerability-assessments	•	• Voldoet	• Voldoet
C.04	Penetratietesten	•	• Voldoet	• Voldoet
C.06	Signaleringsfuncties	•	• Voldoet	• Voldoet
C.07	Monitoring functies	•	• Voldoet	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• Voldoet	• Voldoet
C.09	Patchmanagement	•	• Voldoet	• Voldoet