Bijlage 1 DigiD - iBurgerzaken - 1003811

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Roxit zaaksysteem met aansluitnummer 141579

Gemeente Rheden biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting iBurgerzaken voor authenticatie wordt gebruikt:
Het generen van aanvraagformulieren voor verschillende producten die de gemeente aan haar inwoners aanbied via het iBurgerzaken portal van PinkRoccade zoals het doorgeven of aanvragen van:

- Verhuizingen.
- Vermissing reisdocument.
- Wijzigingen in naamgebruik.
- Verstrekkingsbeperking.
- Stempas.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- iBurgerzaken

De webapplicatie betreft een standaard pakket in de vorm van Software as a Service (SaaS) en wordt onderhouden door PinkRoccade. De infrastructuur waarop de applicatie draait wordt eveneens beheerd door PinkRoccade.

Deze applicatie is extern benaderbaar via de volgende URL:
https://rheden.gem.iburgerzaken.nl/

DigiD-aansluiting Gemeente Rheden bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Visma Roxit in de vorm van SAAS.
Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Roxit zaaksysteem. 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.

Gemeente Rheden heeft een deel van de DigiD web-omgeving uitbesteed aan .
Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie(s). Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie(s). 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(s) van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM’s / assurancerapportages van de leverancier(s):

ICT-leverancier	
Naam serviceorganisatie:	PinkRoccade Local Government B.V.
Referentie/rapportnummer:	20211026 DBA-PRLG
Afgiftedatum:	26-10-2021
Naam RE-auditor:	Duijnborgh Audit B.V.
Ondertekend door RE-auditor:	Frank Kossen RE

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

Gemeentelijk kenmerk collegeverklaring ENSIA:	Rheden-Digid-2021

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 2203-09998.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm inclusief de normen die getoetst zijn bij leverancier.

DigiD-norm		Getoetst bij gemeente	Getoetst bij ICT-leverancier	Totaaloordeel 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-invoercontrole	N.v.t.	Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer	N.v.t.	Voldoet	Voldoet
U/WA.05	Cryptografie/ Privacybevordering	Voldoet	Voldoet	Voldoet
U/PW.02	Garanderen webprotocollen	N.v.t.	Voldoet	Voldoet
U/PW.03	Configureren webserver	N.v.t.	Voldoet	Voldoet
U/PW.05	Toegang tot beheermechanismen	N.v.t.	Voldoet	Voldoet
U/PW.07	Hardening van platformen	N.v.t.	Voldoet	Voldoet
U/NW.03	DMZ	N.v.t.	Voldoet	Voldoet
U/NW.04	Protectie- en detectiemechanismen	N.v.t.	Voldoet	Voldoet
U/NW.05	Scheiding beheer- en productieomgeving	N.v.t.	Voldoet	Voldoet
U/NW.06	Hardening van netwerken	Voldoet	Voldoet	Voldoet
C.03	Vulnerability-assessments	N.v.t.	Voldoet	Voldoet
C.04	Penetratietesten	N.v.t.	Voldoet	Voldoet
C.06	Signaleringsfuncties	N.v.t.	Voldoet	Voldoet
C.07	Monitoringfuncties	N.v.t.	Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement	N.v.t.	Voldoet	Voldoet