Bijlage 1 DigiD - Belastingbalie - 1003555

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting belastingbalie met aansluitnummer 1003555

Gemeente Rheden biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting belastingbalie voor authenticatie wordt gebruikt:
Burgers en bedrijven kunnen digitaal hun belastingzaken regelen, waaronder het aanvragen van kwijtscheldingen en het indienen van bezwaren. De burger heeft inzicht in zijn/haar belastingzaken, aanslagen en gegevens via de belastingbalie.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Digitale balie belastingen

Deze applicatie betreft een geheel standaard pakket en wordt onderhouden door de Connectie (Functioneel Beheer) en GouwIT (Applicatie en technische beheer).

Deze applicatie is extern benaderbaar via de volgende URL:

https://belastingen.rheden.nl/

DigiD-aansluiting belastingbalie bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door GouwIT in de vorm van SAAS.
Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting belasting balie. 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 de DigiD web-omgeving uitbesteed aan de Connectie.
Als gevolg hiervan zijn alle 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):

Applicatie	
Naam serviceorganisatie:	De Connectie
Referentie/rapportnummer:	Geen TPM ontvangen over 2021
Afgiftedatum:	
Naam RE-auditor:	
Ondertekend door RE-auditor:	

ICT-leverancier	
Naam serviceorganisatie:	GouwIT
Referentie/rapportnummer:	IAS0988_21_6802
Afgiftedatum:	20-10-2021
Naam RE-auditor:	Inergy Auditservices
Ondertekend door RE-auditor:	D.J.A Koot

Gemeentelijk kenmerk collegeverklaring ENSIA:	Rheden-Digid-2021

De 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).

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 de Connectie	Getoetst bij ICT-leverancier	Totaaloordeel norm
B.05	Contractmanagement	Voldoet niet	Voldoet	Voldoet niet
U/TV.01	Identificatie en authenticatie	Voldoet niet	Voldoet	Voldoet niet
U/WA.02	Webapplicatiebeheer proces	Voldoet niet	Voldoet	Voldoet niet
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 niet	Voldoet	Voldoet niet
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 niet	Voldoet	Voldoet niet
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 niet	Voldoet	Voldoet niet
C.09	Patchmanagement	N.v.t.	Voldoet	Voldoet