

Bijlage 1 DigiD - iBurgerzaken - 1001685

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting iBurgerzaken met aansluitnummer 1001685

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

- Digitale aanvragen voor Burgerzaken.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- iBurgerzaken.

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door PinkRoccade Local Government B.V..

Deze applicatie is extern benaderbaar via het volgende internetadres(sen):
<https://iburgerzaken.overbetuwe.nl>

DigiD-aansluiting iBurgerzaken bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door PinkRoccade Local Government B.V. in de vorm van SaaS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting iBurgerzaken. 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 Overbetuwe heeft een deel van de DigiD web-omgeving uitbesteed aan PinkRoccade Local Government B.V..

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 / assurancerapportage van de leverancier(s):

SaaS-leverancier	
Naam serviceorganisatie:	PinkRoccade Local Government B.V.
Referentie/rapportnummer:	20231012 DBA-PRLG
Afgiftedatum:	12-10-2023.
Naam RE-auditor:	Frank Kossen RE Laurens van Thiels CISA CISSP Drs. Mohamed El Aarbaoui RE
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportage(s) van onze leverancier(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 OVE232528.

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

DigiD-norm		Getoetst bij aansluithouder	Getoetst bij SaaS-leverancier	Totaaloordeel norm
B.01	Informatiebeveiligingsbeleid	Voldoet	Voldoet	Voldoet
B.05	Contractmanagement	Voldoet	Voldoet	Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet	Voldoet	Voldoet
U/WA.02	Webapplicatiebeheerproces	Voldoet	Voldoet	Voldoet
U/WA.03	Automatische data-invoercontrole		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	Monitoringfuncties		Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement		Voldoet	Voldoet