Bijlage 1 DigiD - Digitaal loket Gemeente Raalte - 1000313

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Digitaal loket Gemeente Raalte met aansluitnummer 1000313

Gemeente Raalte biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Digitaal loket Gemeente Raalte voor authenticatie wordt gebruikt:

- Digitaal loket voor burgers en bedrijven met daarin formulieren.
- Een Producten en Diensten Catalogus (PDC).

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Atos e-Suite, versie 4.30.

Deze applicatie betreft geheel standaard pakket en wordt onderhouden door Atos.

Deze applicatie is extern benaderbaar via het volgende internetadres: https://dloket.raalte.nl .

DigiD-aansluiting Digitaal loket Gemeente Deventer bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door SSC Twente in de vorm van fysieke hosting. De software wordt ontwikkeld door Atos.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Digitaal loket Gemeente Raalte. 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 Raalte heeft een deel van de DigiD web-omgeving uitbesteed aan Atos ontwikkelaar en Dimpact..
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/Applicatie-leverancier	
Naam serviceorganisatie:	Dimpact (SSC Twente)/Atos softwareontwikkelaar
Referentie/rapportnummer:	2111R.AH147
Afgiftedatum:	11-11-2021
Naam RE-auditor:	Drs. A.J.A. Hassing RE RA
Ondertekend door RE-auditor:	Ja

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).

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 202203ERaalte.

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

Alleen voor identificatie doeleinden
M. Hommes RE

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

Alleen voor identificatie doeleinden
M. Hommes RE