Bijlage 1 DigiD - VRIS - 1003809

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting VRIS met aansluitnummer 1003809

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

- Via xxllnc Belastingen kunnen burgers diverse online-diensten aanvragen, zoals het opvragen van WOZ-gegevens en het indienen van bezwaar bij betreffende gemeenten..

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Naam: xxllnc Heffen + Innen (voormalig VRiS)
- Versie: 7.2408

Deze webapplicatie is extern benaderbaar via het volgende internetadres:

- https://www.belastingloket.overbetuwe.nl/.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting VRIS. 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 versie 3.0” van Logius.

Deze webapplicatie betreft Geheel standaardpakket. De webapplicatie wordt onderhouden door xxllnc.

DigiD-aansluiting VRIS bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door xxllnc met beheervorm Saas Leverancier.

Gemeente Overbetuwe heeft de DigiD web-omgeving uitbesteed aan:

- xxllnc.

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.

De DigiD-webomgeving moet aan het gehele normenkader 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 voor de periode:

Aansluithouder	
Oordeelsdatum:	31-12-2024
Controleperiode:	01-07-2024 - 31-12-2024

De overige normen worden afgedekt door onderstaande TPM / assurancerapportage(s) van de (toe)leverancier(s):

SaaS-leverancier	
Naam SaaS-leverancier:	xxllnc
Referentie/rapportnummer:	TPM: ITAA/DIGID/OVER09122024 Sub-TPM: N.v.t.
Oordeelsdatum:	TPM: 06-12-2024 Sub-TPM: N.v.t.
Controleperiode:	TPM: 06-06-2024 tot en met 06-12-2024 Sub-TPM: N.v.t.

SaaS-leverancier	
Naam RE-auditor	TPM: Achmed Bouazza RE CISA (Forvis Mazars) Sub-TPM: N.v.t.
Ondertekend door RE-auditor:	TPM: Ja Sub-TPM: N.v.t.

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportages van onze serviceorganisatie(s) het gehele normenkader afdekken. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk OVE242528.

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

		Aansluithouder	SaaS-leverancier	
DigiD-norm	**Toetsing op**	**Oordeel**	**Oordeel TPM**	**Totaaloordeel**
B.01 Informatiebeveiligingsbeleid	*Opzet en bestaan*	Voldoet	Voldoet	Voldoet
B.05 Contractmanagement	*Opzet en bestaan*	Voldoet	Voldoet	Voldoet
U/TV.01 Identificatie en authenticatie	*Opzet en bestaan*	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	Voldoet niet	Voldoet niet
U/WA.02 Webapplicatiebeheerproces	*Opzet en bestaan*	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	Voldoet niet	Voldoet niet
U/WA.03 Automatische data-invoercontrole	*Opzet en bestaan*	Niet van toepassing	Voldoet	Voldoet
U/WA04. Normaliseren uitvoer	*Opzet en bestaan*	Niet van toepassing	Voldoet	Voldoet
U/WA.05 Cryptografie/ Privacybevordering	*Opzet en bestaan*	Voldoet	Voldoet	Voldoet
U/PW.02 Garanderen webprotocollen	*Opzet en bestaan*	Niet van toepassing	Voldoet	Voldoet
U/PW.03 Configureren webserver	*Opzet en bestaan*	Niet van toepassing	Voldoet	Voldoet
U/PW.05 Toegang tot beheermechanismen	*Opzet en bestaan*	Niet van toepassing	Voldoet	Voldoet
U/PW.07 Hardening van platformen	*Opzet en bestaan*	Niet van toepassing	Voldoet	Voldoet
U/NW.03 DMZ	*Opzet en bestaan*	Niet van toepassing	Voldoet	Voldoet
U/NW.04 Protectie- en detectiemechanismen	*Opzet en bestaan*	Niet van toepassing	Voldoet	Voldoet
U/NW.05 Scheiding beheer- en productieomgeving	*Opzet en bestaan*	Niet van toepassing	Voldoet	Voldoet
U/NW.06 Hardening van netwerken	*Opzet en bestaan*	Voldoet	Voldoet	Voldoet
C.03 Vulnerability-assessments	*Opzet en bestaan*	Niet van toepassing	Voldoet niet	Voldoet niet
C.04 Penetratietesten	*Opzet en bestaan*	Niet van toepassing	Voldoet	Voldoet
C.06 Signaleringsfuncties	*Opzet en bestaan*	Niet van toepassing	Voldoet	Voldoet
C.07 Monitoringfuncties	*Opzet en bestaan*	Niet van toepassing	Voldoet	Voldoet
	Werking	Niet van toepassing	Voldoet niet	Voldoet niet
C.08 Wijzigingenbeheer	*Opzet en bestaan*	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	Voldoet niet	Voldoet niet
C.09 Patchmanagement	*Opzet en bestaan*	Niet van toepassing	Voldoet	Voldoet
	Werking	Niet van toepassing	Voldoet niet	Voldoet niet