

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Rotterdam

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Rotterdam

Doel en achtergrond verklaring

Met deze verklaring geven wij, het college van burgemeester en wethouders, aan in welke mate Gemeente Rotterdam voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet.

Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA¹ en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen. De inhoud wordt getoetst door een onafhankelijke IT-auditor.

De verklaring is bestemd voor de stelselhouders van DigiD en Suwinet, te weten het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Sociale Zaken en Werkgelegenheid.

Reikwijdte en diepgang verklaring

De toetsing gaat over de opzet en het bestaan van de beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD en Suwinet op 31 december 2021.

De beheersingsmaatregelen inzake DigiD en Suwinet die zijn uitbesteed aan dienstverlener(s) worden niet getoetst door de interne auditor. Deze collegeverklaring en de verantwoording van de dienstverlener(s) dekken tezamen de normen inzake DigiD en Suwinet af. Het overzicht van normen en eventuele afwijkingen en waar deze belegd zijn, is opgenomen in de bijlagen:

- Bijlage 1 DigiD met kenmerk M2204-1211
- Bijlage 2 Suwinet met kenmerk M2204-1211

Verklaring college

Het college verklaart dat voor DigiD en Suwinet niet aan alle normen wordt voldaan. Wij hebben een verbeterplan opgesteld om aan de normen te voldoen, de acties zijn belegd en worden gemonitord.

¹ ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Overheid (BIO), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten (PUN, PNIK), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige Topografie (BGT), Basisregistratie Ondergrond (BRO), de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet) en de Wet Onroerende Zaken (WOZ).

Samenvattend beeld

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in [aan] verbeterplan(nen) opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD 1000161 (Mijnloket)	Nee	Ja
DigiD 1001269 (Mijn KBR)	Ja	Niet van toepassing
DigiD 1001749 (Edison)	Nee	Ja
DigiD 1002211 (E-Suite)	Ja	Niet van toepassing
Suwinet voor SUWI-taken	Nee	Ja
Suwinet voor niet-SUWI-taken	Ja	Niet van toepassing

Rotterdam, 19 april 2022

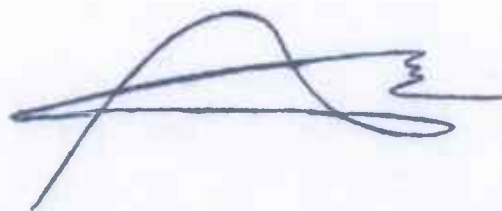
College van B&W gemeente Gemeente Rotterdam

De secretaris,



V.J.M. Roozen

De burgemeester,



A. Aboutaleb

Naam auditfirma:

Concern Auditing, Gemeente Rotterdam

Naam auditor:

De heer, J.P. Volker

Datum

26-04-2022



Ter ident. f. c. a. t. i. e
JP Volker RE
26-04-2022

Bijlage 1 DigiD - Mijn KBR - 1001269

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Mijn KBR met aansluitnummer 1001269

Rotterdam biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Mijn KBR voor authenticatie wordt gebruikt: Als platform waar burgers op een centrale plek gemeentelijke diensten en ondersteuning kan aanvragen voor schulddienstverlening.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door Innovadis en Previder

Deze applicatie is extern benaderbaar via [de] [het] volgende internetadres(sen):

DigiD aansluiting Mijn KBR bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Previder en Innovadis

Applicatie De applicatie in combinatie met de hosting wordt door Innovadis als SAAS aangeboden door Innovadis en het betreft een standaardpakket wordt onderhouden door Innovadis

De fysieke en virtuele infrastructuur en services die door Previder worden beheerd betreffen de volgende diensten:

- Hostingplatform
- Systeembeheer
- Managed Firewall
- Servicemanagement

Het object van zelfevaluatie is de web-omgeving van DigiD aansluiting Mijn KBR. 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 Rotterdam heeft een deel van de DigiD web-omgeving uitbesteed aan Previder en Innovadis. 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] / Assurance rapportages van de gemeentelijke serviceorganisaties:

ICT-leverancier	
Naam serviceorganisatie:	Innovadis en Previder
Referentie/rapportnummer:	AAS2021-1195 Rapport dienst van Innovadis AAS2021-1243 Rapport dienst van Previder
Afgiftedatum:	AAS2021-1243 – 5 November-2021 AAS2021-1195 - 11-Oktober-2021
Naam RE-auditor:	Accoris Audit Services
Ondertekend door RE-auditor:	J.R. Möhle RE

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / Assurance rapportage(s) 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 (zogenaaamde gedeelde norm).

De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het Assurance rapport met kenmerk 202201211

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		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

Bijlage 1 DigiD - Digitaal Loket - 1002211

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Digitaal Loket met aansluitnummer 1002211

Rotterdam biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting [REDACTED] Rotterdam voor authenticatie wordt gebruikt:

- Een digitaal loket voor burgers en bedrijven met daarin formulieren EN
- Een producten en diensten catalogus (PDC)

Deze functionaliteit wordt geboden door de volgende webapplicatie: [REDACTED]

De applicatie betreft standaard software en wordt ontwikkeld en onderhouden door Atos.

De infrastructuur waarop de applicatie draait wordt beheerd door SSC Twente in de vorm van fysieke hosting. Deze applicatie is extern benaderbaar via [de] [het] volgende internetadres(sen):

[REDACTED]
Het object van zelfevaluatie is de web-omgeving van [REDACTED] Rotterdam. 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 Rotterdam heeft een deel van de DigiD web-omgeving uitbesteed aan 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.

Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie. 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] / Assurance rapportage[s] van de gemeentelijke serviceorganisatie[s]:

ICT-leverancier	
Naam serviceorganisatie:	Dimpact
Referentie/rapportnummer:	2111R.AH149
Afgiftedatum:	11-11-2021
Naam RE-auditor:	3angles B.V.
Ondertekend door RE-auditor:	drs. A.J.A. Hassing RE RA

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / Assurance rapportage(s) 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 Assurance rapport met kenmerk 202201211

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		Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer		Voldoet	Voldoet
U/WA.05	Cryptografie/ Privacy bevordering	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

Bijlage 1 DigiD - Mijn Loket - 1000161

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Mijn Loket met aansluitnummer 1000161

Rotterdam biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Rotterdam - "Mijn Loket" voor authenticatie wordt gebruikt:

- Als platform waar burgers op een centrale plek gemeentelijke diensten en ondersteuning kan aanvragen, zoals afspraak bij stadswinkels, gemeentelijke belastingen, vergunningen en subsidies.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

[REDACTED]

Deze applicatie betreft geheel maatwerk en wordt onderhouden door Gemeente Rotterdam. Deze applicatie is extern benaderbaar via het volgende internetadres:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

DigiD-aansluiting Gemeente Rotterdam - "Mijn Loket" bevindt zich in de Demilitariseerde Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt deels beheerd door Gemeente Rotterdam in de vorm van fysieke hosting, deels door leverancier Mendix in de vorm van fysieke hosting.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Rotterdam - "Mijn Loket". 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 Rotterdam heeft een deel van de DigiD web-omgeving uitbesteed aan Mendix. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie. 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 / Assurance rapportage van de gemeentelijke serviceorganisatie:

ICT-leverancier	
Naam serviceorganisatie:	Mendix
Referentie/rapportnummer:	844FD8A2-7805-4557-A326-80754C462C5E
Afgiftedatum:	29 november 2021
Naam RE-auditor:	Mazars N.V.
Ondertekend door RE-auditor:	N. Verhagen RE AA

De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het Assurance rapport met kenmerk 202201211

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD-norm		Getoetst bij gemeente	Getoetst bij ICT-leverancier	Totaaloordeel norm
B.05	Contractmanagement	Voldoet		Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet Niet	Voldoet	Voldoet Niet
U/WA.02	Webapplicatiebeheer proces	Voldoet	Voldoet	Voldoet
U/WA.03	Automatische data-invoercontrole	Voldoet Niet		Voldoet Niet
U/WA.04	Normaliseren uitvoer	Voldoet		Voldoet
U/WA.05	Cryptografie/ Privacybevordering	Voldoet Niet		Voldoet Niet
U/PW.02	Garanderen webprotocollen	Voldoet		Voldoet
U/PW.03	Configureren webserver	Voldoet Niet	Voldoet	Voldoet Niet
U/PW.05	Toegang tot beheermechanismen	Voldoet	Voldoet	Voldoet
U/PW.07	Hardening van platformen	Voldoet	Voldoet	Voldoet
U/NW.03	DMZ	Voldoet	Voldoet	Voldoet
U/NW.04	Protectie- en detectiemechanismen	Voldoet	Voldoet	Voldoet
U/NW.05	Scheiding beheer- en productieomgeving	Voldoet	Voldoet	Voldoet
U/NW.06	Hardening van netwerken	Voldoet Niet	Voldoet	Voldoet Niet
C.03	Vulnerability-assessments	Voldoet	Voldoet	Voldoet
C.04	Penetratietesten	Voldoet	Voldoet	Voldoet
C.06	Signaleringsfuncties	Voldoet	Voldoet	Voldoet
C.07	Monitoringfuncties	Voldoet	Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement	Voldoet	Voldoet	Voldoet

Bijlage 1 DigiD - Edison W&I Rotterdam - 1001749

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Edison W&I Rotterdam met aansluitnummer 1001749

Gemeente Rotterdam biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting "Edison W&I Gemeente Rotterdam" voor authenticatie wordt gebruikt:

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Deze applicatie wordt onderhouden door Wigo4it. De applicatie Edison is door Wigo4it ontwikkeld en gehost. De combinatie van applicatie en hosting wordt door Wigo4it als SAAS aan gemeente Rotterdam aangeboden

DigiD aansluiting Edison W&I Gemeente Rotterdam bevindt zich in de [REDACTED]
[REDACTED]

Het object van zelfevaluatie is de web-omgeving van DigiD aansluiting Edison W&I Gemeente Rotterdam. 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 Rotterdam heeft een deel van de DigiD web-omgeving uitbesteed aan Wigo4it. 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.

Voor zowel de applicatie als voor de hosting hebben we Wigo4it overeenkomsten afgesloten, waarin onder meer afspraken over informatiebeveiliging in het algemeen en het ICT-beveiligingsassessment DigiD in het kader van ENSIA in het bijzonder zijn gemaakt.

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 / Assurance rapportage van de leverancier(s):

ICT-leverancier	
Naam serviceorganisatie:	Wigo4it
Referentie/rapportnummer:	AAS2022-1317
Afgiftedatum:	18-Maart-2022
Naam RE-auditor:	Accoris
Ondertekend door RE-auditor:	N.M. van der Meij RE

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / Assurance rapportage(s) 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 Assurance rapport met kenmerk 202201211.

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		Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer		Voldoet	Voldoet
U/WA.05	Cryptografie/ privacy bevordering	Voldoet	Voldoet	Voldoet
U/PW.02	Garanderen webprotocollen		Voldoet	Voldoet
U/PW.03	Configureren webserver		Voldoet Niet	Voldoet Niet
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

Identificatie
JP Volker RE
26-04-2022

Bijlage 2 Gebruik van Suwinet

Suwinet-gegevens worden ten behoeve van de dienstverlening aan onze burgers [wel][niet] door serviceorganisaties verwerkt. Hierbij is de eventuele aanwezigheid van IT-serviceorganisaties in aanmerking genomen.

Het college van B en W is als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van Suwinet en legt hierover verantwoording af. Rotterdam heeft een deel van de Suwinet taken uitbesteed aan Wigo4it. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. In de navolgende tabellen is opgenomen of het onderzoeken over het al dan niet voldoen aan deze maatregelen is uitgevoerd door de IT-auditor van deze serviceorganisatie. De controls die betrekking hebben op de taken die belegd zijn bij de serviceorganisatie maken geen onderdeel uit van de zelfevaluatie van onze gemeente, tenzij sprake is van een gedeelde norm. De zelfevaluatie ENSIA voor Suwinet is toegepast op dat deel van het gebruik en normenkader dat niet onder uitbesteding aan onze serviceorganisatie valt.

Leverancier 1	
Naam serviceorganisatie:	Wigo4it
Referentie/rapportnummer:	AAS2021-1098 (Suwinet DKD Inlezen)
Afgiftedatum:	29 oktober 2021
Naam RE-auditor:	N.M. van der Meij RE
Ondertekend door RE-auditor:	Ja

Gebruik van Suwinet voor SUWI-taken

Voor de volgende taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	TPM/AR
Participatiewet (Pw)	Binnen de gemeente	Ja
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	Binnen de gemeente	Ja
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	Binnen de gemeente	Ja

Gebruik van Suwinet voor niet-SUWI-taken

Voor de volgende niet-SUWI-taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	TPM/AR
Hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC)	Er wordt niet gebruik gemaakt van Suwinet	Nee
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	Er wordt niet gebruik gemaakt van Suwinet	Nee
Adresonderzoek door Burgerzaken	Er wordt niet gebruik gemaakt van Suwinet	Nee

Naleving BIO-maatregelen

Met uitzondering van de volgende maatregelen voldoen de interne beheersingsmaatregelen voor de SUWI-taken op 31 december 2021 in opzet en bestaan aan de doelstellingen uit de verantwoordingsrichtlijn GeVS 2020:

Organisatie	SUWI-taak	BIO-maatregel	Applicatie
Gemeente Rotterdam	Participatiewet (Pw)/IOW/IOAZ	9.2.5 10.1.1 12.1.1 12.4.1	
Gemeente Rotterdam	Participatiewet (Pw)/IOW/IOAZ	7.2.2 9.2.5	

Per 1 februari 2022 voldoen we als Gemeente Rotterdam aan alle bovenstaande BIO normen voor Suwinet. De bevindingen dateren van de stand per 31-12-21, de applicatie GUS is niet meer in gebruik.

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Rotterdam

Collegeverklaring informatiebeveiliging DigiD en Suwinet

Gemeente Rotterdam

Doel en achtergrond verklaring

Met deze verklaring geven wij, het college van burgemeester en wethouders, aan in welke mate Gemeente Rotterdam voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet.

Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA¹ en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen. De inhoud wordt getoetst door een onafhankelijke IT-auditor.

De verklaring is bestemd voor de stelselhouders van DigiD en Suwinet, te weten het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Sociale Zaken en Werkgelegenheid.

Reikwijdte en diepgang verklaring

De toetsing gaat over de opzet en het bestaan van de beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD en Suwinet op 31 december 2021.

De beheersingsmaatregelen inzake DigiD en Suwinet die zijn uitbesteed aan dienstverlener(s) worden niet getoetst door de interne auditor. Deze collegeverklaring en de verantwoording van de dienstverlener(s) dekken tezamen de normen inzake DigiD en Suwinet af. Het overzicht van normen en eventuele afwijkingen en waar deze belegd zijn, is opgenomen in de bijlagen:

- Bijlage 1 DigiD met kenmerk M2204-1211
- Bijlage 2 Suwinet met kenmerk M2204-1211

Verklaring college

Het college verklaart dat voor DigiD en Suwinet niet aan alle normen wordt voldaan. Wij hebben een verbeterplan opgesteld om aan de normen te voldoen, de acties zijn belegd en worden gemonitord.

¹ ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Overheid (BIO), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten (PUN, PNIK), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige Topografie (BGT), Basisregistratie Ondergrond (BRO), de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet) en de Wet Onroerende Zaken (WOZ).

Samenvattend beeld

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD 1000161 (Mijnloket)	Nee	Ja
DigiD 1001269 (Mijn KBR)	Ja	Niet van toepassing
DigiD 1001749 (Edison)	Nee	Ja
DigiD 1002211 (E-Suite)	Ja	Niet van toepassing
Suwinet voor SUWI-taken	Nee	Ja
Suwinet voor niet-SUWI-taken	Ja	Niet van toepassing

Rotterdam, 19 april 2022

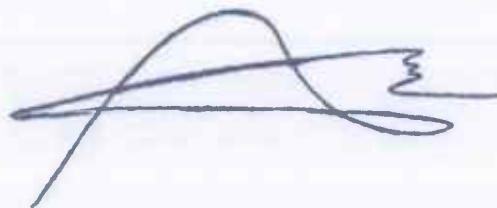
College van B&W gemeente Gemeente Rotterdam

De secretaris,



V.J.M. Roozen

De burgemeester,



A. Aboutaleb

Naam auditfirma:

Concern Auditing, Gemeente Rotterdam

Naam auditor:

De heer, J.P. Volker

Datum

26-04-2022



Ter identificatie
JP Volker RE
26-04-2022

Bijlage 1 DigiD - Mijn KBR - 1001269

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Mijn KBR met aansluitnummer 1001269

Rotterdam biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Mijn KBR voor authenticatie wordt gebruikt: Als platform waar burgers op een centrale plek gemeentelijke diensten en ondersteuning kan aanvragen voor schulddienstverlening.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door Innovadis en Previder

Deze applicatie is extern benaderbaar via [de] [het] volgende internetadres(sen):

DigiD aansluiting Mijn KBR bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Previder en Innovadis

Applicatie De applicatie in combinatie met de hosting wordt door Innovadis als SAAS aangeboden door Innovadis en het betreft een standaardpakket wordt onderhouden door Innovadis

De fysieke en virtuele infrastructuur en services die door Previder worden beheerd betreffen de volgende diensten:

- Hostingplatform
- Systeembeheer
- Managed Firewall
- Servicemanagement

Het object van zelfevaluatie is de web-omgeving van DigiD aansluiting Mijn KBR. 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 Rotterdam heeft een deel van de DigiD web-omgeving uitbesteed aan Previder en Innovadis. 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] / Assurance rapportages van de gemeentelijke serviceorganisaties:

ICT-leverancier	
Naam serviceorganisatie:	Innovadis en Previder
Referentie/rapportnummer:	AAS2021-1195 Rapport dienst van Innovadis AAS2021-1243 Rapport dienst van Previder
Afgiftedatum:	AAS2021-1243 – 5 November-2021 AAS2021-1195 - 11-Oktober-2021
Naam RE-auditor:	Accoris Audit Services
Ondertekend door RE-auditor:	J.R. Möhle RE

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / Assurance rapportage(s) 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 (zogenoemde gedeelde norm).

De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het Assurance rapport met kenmerk 202201211

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		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

Bijlage 1 DigiD - Digitaal Loket - 1002211

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Digitaal Loket met aansluitnummer 1002211

Rotterdam biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting [REDACTED]
Rotterdam voor authenticatie wordt gebruikt:

- Een digitaal loket voor burgers en bedrijven met daarin formulieren EN
- Een producten en diensten catalogus (PDC)

Deze functionaliteit wordt geboden door de volgende webapplicatie: [REDACTED]

De applicatie betreft standaard software en wordt ontwikkeld en onderhouden door Atos.

De infrastructuur waarop de applicatie draait wordt beheerd door SSC Twente in de vorm van fysieke hosting. Deze applicatie is extern benaderbaar via [de] [het] volgende internetadres(sen):
[REDACTED]

Het object van zelfevaluatie is de web-omgeving van [REDACTED] Rotterdam. 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 Rotterdam heeft een deel van de DigiD web-omgeving uitbesteed aan 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.

Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie. 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] / Assurance rapportage[s] van de gemeentelijke serviceorganisatie[s]:

ICT-leverancier	
Naam serviceorganisatie:	Dimpact
Referentie/rapportnummer:	2111R.AH149
Afgiftedatum:	11-11-2021
Naam RE-auditor:	3angles B.V.
Ondertekend door RE-auditor:	drs. A.J.A. Hassing RE RA

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / Assurance rapportage(s) 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 Assurance rapport met kenmerk 202201211

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		Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer		Voldoet	Voldoet
U/WA.05	Cryptografie/ Privacy bevordering	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

Bijlage 1 DigiD - Mijn Locket - 1000161

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Mijn Locket met aansluitnummer 1000161

Rotterdam biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Rotterdam - "Mijn Locket" voor authenticatie wordt gebruikt:

- Als platform waar burgers op een centrale plek gemeentelijke diensten en ondersteuning kan aanvragen, zoals afspraak bij stadswinkels, gemeentelijke belastingen, vergunningen en subsidies.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

Deze applicatie betreft geheel maatwerk en wordt onderhouden door Gemeente Rotterdam. Deze applicatie is extern benaderbaar via het volgende internetadres:

[Redacted address block]

DigiD-aansluiting Gemeente Rotterdam - "Mijn Locket" bevindt zich in de Demilitariseerde Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt deels beheerd door Gemeente Rotterdam in de vorm van fysieke hosting, deels door leverancier Mendix in de vorm van fysieke hosting.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Rotterdam - "Mijn Locket". 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 Rotterdam heeft een deel van de DigiD web-omgeving uitbesteed aan Mendix. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie. 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 / Assurance rapportage van de gemeentelijke serviceorganisatie:

ICT-leverancier	
Naam serviceorganisatie:	Mendix
Referentie/rapportnummer:	844FD8A2-7805-4557-A326-80754C462C5E
Afgiftedatum:	29 november 2021
Naam RE-auditor:	Mazars N.V.
Ondertekend door RE-auditor:	N. Verhagen RE AA

De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het Assurance rapport met kenmerk 202201211

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD-norm		Getoetst bij gemeente	Getoetst bij ICT-leverancier	Totaaloordeel norm
B.05	Contractmanagement	Voldoet		Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet Niet	Voldoet	Voldoet Niet
U/WA.02	Webapplicatiebeheer proces	Voldoet	Voldoet	Voldoet
U/WA.03	Automatische data-invoercontrole	Voldoet Niet		Voldoet Niet
U/WA.04	Normaliseren uitvoer	Voldoet		Voldoet
U/WA.05	Cryptografie/ Privacybevordering	Voldoet Niet		Voldoet Niet
U/PW.02	Garanderen webprotocollen	Voldoet		Voldoet
U/PW.03	Configureren webserver	Voldoet Niet	Voldoet	Voldoet Niet
U/PW.05	Toegang tot beheermechanismen	Voldoet	Voldoet	Voldoet
U/PW.07	Hardening van platformen	Voldoet	Voldoet	Voldoet
U/NW.03	DMZ	Voldoet	Voldoet	Voldoet
U/NW.04	Protectie- en detectiemechanismen	Voldoet	Voldoet	Voldoet
U/NW.05	Scheiding beheer- en productieomgeving	Voldoet	Voldoet	Voldoet
U/NW.06	Hardening van netwerken	Voldoet Niet	Voldoet	Voldoet Niet
C.03	Vulnerability-assessments	Voldoet	Voldoet	Voldoet
C.04	Penetratietesten	Voldoet	Voldoet	Voldoet
C.06	Signaleringsfuncties	Voldoet	Voldoet	Voldoet
C.07	Monitoringfuncties	Voldoet	Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement	Voldoet	Voldoet	Voldoet

Bijlage 1 DigiD - Edison W&I Rotterdam - 1001749

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Edison W&I Rotterdam met aansluitnummer 1001749

Gemeente Rotterdam biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting "Edison W&I Gemeente Rotterdam" voor authenticatie wordt gebruikt:

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Deze applicatie wordt onderhouden door Wigo4it. De applicatie Edison is door Wigo4it ontwikkeld en gehost. De combinatie van applicatie en hosting wordt door Wigo4it als SAAS aan gemeente Rotterdam aangeboden

DigiD aansluiting Edison W&I Gemeente Rotterdam bevindt zich in de [REDACTED]
[REDACTED]

Het object van zelfevaluatie is de web-omgeving van DigiD aansluiting Edison W&I Gemeente Rotterdam. 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 Rotterdam heeft een deel van de DigiD web-omgeving uitbesteed aan Wigo4it. 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.

Voor zowel de applicatie als voor de hosting hebben we Wigo4it overeenkomsten afgesloten, waarin onder meer afspraken over informatiebeveiliging in het algemeen en het ICT-beveiligingsassessment DigiD in het kader van ENSIA in het bijzonder zijn gemaakt.

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 / Assurance rapportage van de leverancier(s):

ICT-leverancier	
Naam serviceorganisatie:	Wigo4it
Referentie/rapportnummer:	AAS2022-1317
Afgiftedatum:	18-Maart-2022
Naam RE-auditor:	Accoris
Ondertekend door RE-auditor:	N.M. van der Meij RE

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / Assurance rapportage(s) 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 Assurance rapport met kenmerk 202201211.

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		Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer		Voldoet	Voldoet
U/WA.05	Cryptografie/ privacy bevordering	Voldoet	Voldoet	Voldoet
U/PW.02	Garanderen webprotocollen		Voldoet	Voldoet
U/PW.03	Configureren webserver		Voldoet Niet	Voldoet Niet
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

Identificatie
JP Volker RE
26-04-2022

Bijlage 2 Gebruik van Suwinet

Suwinet-gegevens worden ten behoeve van de dienstverlening aan onze burgers [wel][niet] door serviceorganisaties verwerkt. Hierbij is de eventuele aanwezigheid van IT-serviceorganisaties in aanmerking genomen.

Het college van B en W is als opdrachtgever verantwoordelijk voor de kwaliteit en veiligheid van het gebruik van Suwinet en legt hierover verantwoording af. Rotterdam heeft een deel van de Suwinet taken uitbesteed aan Wigo4it. Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. In de navolgende tabellen is opgenomen of het onderzoeken over het al dan niet voldoen aan deze maatregelen is uitgevoerd door de IT-auditor van deze serviceorganisatie. De controls die betrekking hebben op de taken die belegd zijn bij de serviceorganisatie maken geen onderdeel uit van de zelfevaluatie van onze gemeente, tenzij sprake is van een gedeelde norm. De zelfevaluatie ENSIA voor Suwinet is toegepast op dat deel van het gebruik en normenkader dat niet onder uitbesteding aan onze serviceorganisatie valt.

Leverancier 1	
Naam serviceorganisatie:	Wigo4it
Referentie/rapportnummer:	AAS2021-1098 (Suwinet DKD Inlezen)
Afgiftedatum:	29 oktober 2021
Naam RE-auditor:	N.M. van der Meij RE
Ondertekend door RE-auditor:	Ja

Gebruik van Suwinet voor SUWI-taken

Voor de volgende taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	TPM/AR
Participatiewet (Pw)	Binnen de gemeente	Ja
Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW)	Binnen de gemeente	Ja
Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)	Binnen de gemeente	Ja

Gebruik van Suwinet voor niet-SUWI-taken

Voor de volgende niet-SUWI-taken wordt Suwinet op de volgende plaatsen gebruikt:

Taak	Organisatie	TPM/AR
Hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC)	Er wordt niet gebruik gemaakt van Suwinet	Nee
Onderzoek loonbeslag door Gemeentelijke Belastingdeurwaarders	Er wordt niet gebruik gemaakt van Suwinet	Nee
Adresonderzoek door Burgerzaken	Er wordt niet gebruik gemaakt van Suwinet	Nee

Naleving BIO-maatregelen

Met uitzondering van de volgende maatregelen voldoen de interne beheersingsmaatregelen voor de SUWI-taken op 31 december 2021 in opzet en bestaan aan de doelstellingen uit de verantwoordingsrichtlijn GeVS 2020:

Organisatie	SUWI-taak	BIO-maatregel	Applicatie
Gemeente Rotterdam	Participatiewet (Pw)/IOW/IOAZ	9.2.5 10.1.1 12.1.1 12.4.1	
Gemeente Rotterdam	Participatiewet (Pw)/IOW/IOAZ	7.2.2 9.2.5	

Per 1 februari 2022 voldoen we als Gemeente Rotterdam aan alle bovenstaande BIO normen voor Suwinet. De bevindingen dateren van de stand per 31-12-21, de applicatie GUS is niet meer in gebruik.