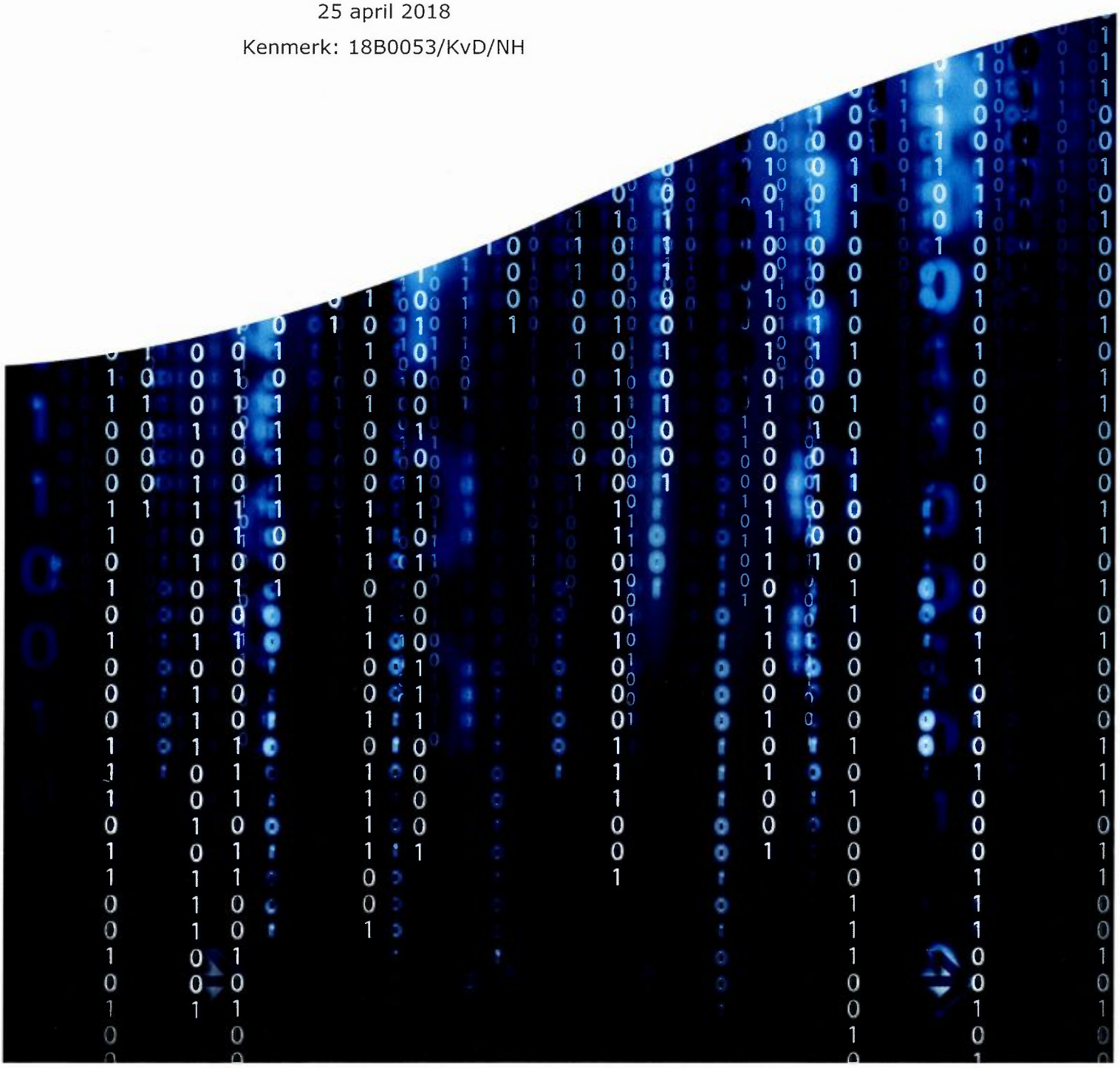
BAKER TILLY
BERK

Gemeente Oude IJsselstreek

ENSIA 2017

25 april 2018

Kenmerk: 18B0053/KvD/NH



BAKER TILLY BERK

INHOUDSOPGAVE

BAKER TILLY BERK

Assurance-rapport van de onafhankelijke auditor

Aan: het College van Burgemeester en Wethouders van de Gemeente Oude IJsselstreek

1.1 Ons oordeel

Wij hebben de bijgevoegde Collegeverklaring ENSIA 2017 inzake informatiebeveiliging van DigiD en Suwinet (inclusief bijlage 1 DigiD en bijlage 2 Suwinet waarnaar in de collegeverklaring wordt verwezen) van gemeente Oude IJsselstreek onderzocht.

Naar ons oordeel is bijgevoegde Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging van DigiD en Suwinet (inclusief bijlage 1 DigiD en bijlage 2 Suwinet waarnaar in de collegeverklaring wordt verwezen) van gemeente Oude IJsselstreek in alle van materieel belang zijnde aspecten, juist.

De Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging van DigiD en Suwinet (hierna Collegeverklaring ENSIA 2017) omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0, op het openbare deel van de websites van het ministerie van BZK) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI en bijlage 1 van de notitie verantwoordingsstelsel op website ENSIA voor de selectie van normen). Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel omtrent DigiD en Suwinet. De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel staan beschreven in de collegeverklaring.

1.2 Benadrukking aangelegenheden

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed vallen buiten de reikwijdte van de collegeverklaring en dit assurance-rapport. Wij hebben wel vastgesteld dat onze assurance bij deze collegeverklaring en de assurance bij de verantwoording van de dienstverlener aan wie de beheersingsmaatregelen zijn uitbesteed tezamen de geselecteerde normen inzake DigiD afdekken.

In de collegeverklaring is vermeld dat op de uitzonderingen gerichte beheersingsmaatregelen in verbeterplannen zijn opgenomen, zijn belegd en worden gemonitord. Voor het inzicht van de gebruiker van dit assurance-rapport achten wij het wenselijk om de in de collegeverklaring opgenomen uitzonderingen in dit rapport te benadrukken.

Door de gemeente geconstateerde beperkingen betreffende SUWI:

#	Norm	Criterium	Beperking
1.	B.01	De Afnemer heeft voor de aansluiting op Suwinet expliciet aandacht besteed aan het stelsel van beveiligingsmaatregelen in zijn informatiebeveiligingsbeleid, of hiervoor een apart aansluitingsbeleid ontwikkeld.	Voldoet niet: regie functie ten aanzien van de aan Laborijn uitbestede taken ontbreekt.
2.	B.04	De Afnemer heeft een Beveiligingsfunctie Suwinet (GeVS) benoemd en taken en verantwoordelijkheden vastgesteld.	De beveiligingsfunctie voor Suwi ontbreekt.
3.	C.06	De log-informatie wordt regelmatig gemonitord (signaleren, analyseren rapporteren en bijsturen).	Zichtbare vastlegging van de controle op de logging ontbreekt.
4.	C.07	De Afnemer voert periodiek evaluaties op de technische en organisatorische beoordelingsrapportages en neemt noodzakelijke verbeteracties.	Zichtbare vastlegging van de controle op de logging ontbreekt.

Baker Tilly Berk N.V.
voor
waarmerkingsdoeleinden
paraaf AD datum 25-04-2018

Ons onderzoek heeft zich niet gericht op de verbeterplannen en het beleggen en monitoring hiervan.

Deze aanvullende informatie is niet bedoeld om afbreuk te doen aan ons oordeel.

1.3 De basis voor ons oordeel

Wij hebben onze assurance-opdracht met betrekking tot de Collegeverklaring ENSIA 2017 uitgevoerd volgens Nederlands recht, waaronder de Richtlijn 3000 (Herzien) 'Assuranceopdrachten door IT-auditors' van NOREA. Deze assurance-opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Onze verantwoordelijkheden voor de assurance-opdracht betreffende de Collegeverklaring ENSIA 2017'.

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

Wij vinden dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor ons oordeel.

1.4 Beperking in gebruik en verspreidingskring

Dit assurance-rapport is bestemd voor gebruikers van de Collegeverklaring ENSIA 2017. De Collegeverklaring ENSIA 2017 is opgesteld voor de gemeenteraad en voor de departementen die toezien op de veiligheid van DigiD en Suwinet. Doel van de Collegeverklaring ENSIA 2017 is om de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet te informeren over het in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigiD en Suwinet. Ons assurance-rapport is derhalve uitsluitend bestemd voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet en dient niet te worden verspreid aan of te worden gebruikt door anderen.

Beperkingen van interne beheersingsmaatregelen

Interne beheersingsmaatregelen kunnen vanwege hun aard niet alle fouten of omissies bij het verwerken of rapporteren van transacties voorkomen of ontdekken.

Werking niet onderzocht

Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen en brengen daarover geen oordeel tot uitdrukking.

1.5 Verantwoordelijkheden van het college van gemeente Oude IJsselstreek

Het college van burgemeester en wethouders van gemeente Oude IJsselstreek is verantwoordelijk voor het opstellen van de Collegeverklaring ENSIA 2017. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet dienen voldoende inzicht te hebben om deze collegeverklaring, samen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die zelf worden uitgevoerd, te beschouwen wanneer zij de risico's van afwijkingen van materieel belang in relatie tot DigiD en Suwinet inschatten.

De criteria waarvan bij het maken van deze verklaring gebruik werd gemaakt hielden in dat:

Baker Tilly Berk N.V.
voor
waarmerkingsdoeleinden

paraaf datum 26-04-2018

- De risico's die het bereiken van de geselecteerde normen DigiD en Suwinet in gevaar brengen, werden geïdentificeerd;
- De onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de vermelde interne beheersingsdoelstellingen niet zouden verhinderen;
- Het college ook verantwoordelijk is voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de collegeverklaring ENSIA 2017 mogelijk te maken zonder afwijkingen van materieel belang als gevolg van fraude of fouten.

1.6 Onze verantwoordelijkheden voor de assurance-opdracht betreffende de collegeverklaring ENSIA 2017

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van een assurance-opdracht dat wij daarmee, met een redelijke mate van zekerheid voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel. Een redelijke mate van zekerheid wil zeggen dat onze assurance-opdracht is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens onze assurance-opdracht niet alle materiële fouten en fraude ontdekken.

Wij passen het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van de ethische voorschriften, professionele standaarden en andere wet- en regelgeving.

Afwijkingen kunnen ontstaan als gevolg van fraude of fouten en zijn materieel indien redelijkerwijs kan worden verwacht dat deze, afzonderlijk of gezamenlijk, van invloed kunnen zijn op de beslissingen die gebruikers op basis van de Collegeverklaring ENSIA 2017 nemen. De materialiteit beïnvloedt de aard, timing en omvang van onze assurance-werkzaamheden en de evaluatie van het effect van onderkende afwijkingen op ons oordeel.

Wij hebben deze assurance-opdracht professioneel kritisch uitgevoerd en hebben waar relevant professionele oordeelsvorming toegepast in overeenstemming met de Richtlijn 3000 (Herzien) 'Assuranceopdrachten door IT-auditors' van NOREA.

Onze assurance-opdracht bestond onder andere uit:

- Het verkrijgen van kennis omtrent de Collegeverklaring ENSIA 2017 en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen. Deze werkzaamheden hebben niet als doel om een oordeel uit te spreken over de effectiviteit van de interne beheersing van de gemeente;
- Het op basis van deze kennis inschatten van de risico's dat de Collegeverklaring ENSIA 2017 onjuistheden van materieel belang bevat als gevolg van fraude en fouten, het in reactie op deze risico's bepalen en uitvoeren van assurance-werkzaamheden en het verkrijgen van assurance-informatie die voldoende en geschikt is als basis voor ons oordeel. Bij fraude is het risico dat een afwijking van materieel belang niet ontdekt wordt groter dan bij fouten. Bij fraude kan sprake zijn van samenspanning, valsheid in geschrifte, het opzettelijk nalaten transacties vast te leggen, het opzettelijk verkeerd voorstellen van zaken of het doorbreken van de interne beheersing;
- Het reageren op de ingeschatte risico's, waaronder het ontwikkelen van een algehele aanpak, en het bepalen van de aard, de tijdsfasering en de omvang van verdere procedures;

- Het uitvoeren van verdere procedures die duidelijk zijn gekoppeld aan de gesignaleerde risico's, waarbij gebruik wordt gemaakt van een combinatie van inspectie, waarnemingen ter plaatse en inwinnen van inlichtingen;
- Het evalueren van de toereikendheid van de assurance-informatie.

Utrecht, 25 april 2018

Baker Tilly Berk N.V.

C.P. van Diepen RE

Partner IT Advisory

Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet

Het college van burgemeester en wethouders van de gemeente Oude IJsselstreek legt met deze verklaring verantwoording af over geselecteerde informatiebeveiligingsnormen inzake DigiD en Suwinet op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

Het doel van ENSIA is om verantwoording over informatieveiligheid af te leggen aan de gemeenteraad. ENSIA sluit aan op de gemeentelijke planning en controlcyclus voor informatiebeveiliging, neemt de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie. Hierdoor heeft het gemeentebestuur meer overzicht over de informatiebeveiliging van de gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad en andere belanghebbenden.

Zo structureert ENSIA ook de verticale verantwoording van gemeenten richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Reikwijdte verklaring

Deze verklaring betreft de onderdelen van de ENSIA systematiek waarover assurance wordt gevraagd van een onafhankelijke IT auditor. Voor het jaar 2017 betreft dit DigID (aansluitnummer 1000237) en Suwinet. De verklaring omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0, op het openbare deel van de websites van het ministerie van BZK[1]) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI[2] en bijlage 1 van de notitie Verantwoordingsstelsel op website ENSIA[3] voor de selectie van normen). De normen vinden hun basis in internationale standaarden en zijn geschikt voor het doel van deze Collegeverklaring. De Collegeverklaring omvat niet de werking van de maatregelen over 2017.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring "bijlage 1 DigiD" blijkt over welke beheersmaatregelen en DigiD-normen door de dienstverlener aan wie de beheersmaatregelen zijn uitbesteed verantwoording wordt afgelegd. Deze collegeverklaring en de verantwoording van de dienstverlener dekken tezamen de geselecteerde normen inzake DigiD af.

De beheersingsmaatregelen rond het gebruik van Suwinet die belegd zijn bij Laborijn vallen onder de reikwijdte van deze collegeverklaring.

Deze Collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet zijn via bij deze collegeverklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk 1000237) en Suwinet geïnformeerd over de afwijkingen van de normen.

Verklaring college
Het college verklaart dat bij gemeente Oude IJsselstreek op 31 december 2017 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigID. Voor Suwinet wordt niet aan alle geselecteerde normen voldaan.

De op de uitzonderingen gerichte beheersmaatregelen zijn inmiddels verbeterd.

Gendringen, 24 april 2018
College van B en W, gemeente Oude IJsselstreek

mevrouw M.J.P. Verstappen
secretaris

de heer O.E.T. Van Dijk
burgemeester

1 https://www.logius.nl/ondersteuning/digid/beveiligingsassessments/normenkader-v20-voor-2017/
2 https://www.bkwi.nl/nieuws/nieuw-normenkader-voor-gemeenten
3 https://www.ensia.nl/

Bijlage 1. Rapportage DigiD Assessment - ENSIA 2017

Aansluiting no. 1

ZZ-ICTU-10

Vragen vooraf

Vraag	Antwoord
Vraag 1: Bent u aansluithouder van DigiD aansluitingen?	JA
Vraag 2: Hoeveel assessmentplichtige DigiD aansluitingen heeft u?	1 assessmentplichtige DigiD aansluiting

Gegevens DigiD aansluiting(en)	Antwoord
Nummer DigiD aansluiting Vul het Logius aansluitnummer in:	1000237
Naam DigiD aansluiting Vul de aansluitnaam in van de aansluiting:	Zaaksysteem Oude IJsselstreek
Externe infrastructuur-leverancier Maakt u voor deze DigiD aansluiting gebruik van een externe infrastructuur-leverancier?	Ja
Naam leveranciers Geef de namen op van alle leveranciers die betrokken zijn bij deze DigiD aansluiting.	Mintlab
TPM datum Voer hier de datum in van het TPM rapport.	17-11-2017
Applicatieleverancier Maakt u voor deze DigiD aansluiting gebruik van een externe leverancier voor de applicatie?	Nee
Naam leverancier Geef de naam op van de applicatieleverancier.	
TPM datum Vult u hier de datum in van het TPM rapport van de applicatieleverancier.	
TPM kenmerk Vul hier het kenmerk in van het TPM rapport van de applicatieleverancier.	
Bij applicatieleverancier: U kunt de TPM's hier uploaden.	
SaaS-leverancier Maakt u voor deze DigiD aansluiting gebruik van een SaaS-leverancier?	Ja
Naam leverancier Geef de naam op van de SaaS-leverancier.	Mintlab
TPM datum Voer hier de datum in van het TPM rapport.	17-11-2017
TPM kenmerk Voer hier het kenmerk in van het TPM rapport.	MMC/DIGID/GO17112017

Bij SaaS-leverancier: U kunt de TPM's hier uploaden	
TPM aanwezigheid Leveren alle leveranciers een TPM op?	Ja
Heeft uw eigen auditor vastgesteld dat deze leverancier aan de DigiD normen voldoet?	Nee
Reikwijdte TPM Hebben de TPM's dezelfde scope als de DigiD aansluiting?	Ja
Reikwijdte TPM Hanteren de TPM's hetzelfde normenkader als het DigiD normenkader 2.0?	Ja
Reikwijdte TPM Zijn de TPM's maximaal 1 jaar oud?	Ja
Reikwijdte TPM Heeft u als coördinator vastgesteld dat de overige normen, buiten de 5 waar u verantwoordelijk voor bent, door de TPM worden afgedekt?	Ja
Reikwijdte TPM Zijn de TPM's eerder gebruikt voor een DigiD assessment voor dezelfde aansluiting?	Ja
Externe auditor bedrijf Vul de namen in van het bedrijf van de externe auditors:	Mazars
Externe auditor Vul de namen in van de externe auditors:	J.H. Matto RE RI Partner-aandeelhouder Mazars Paardekoper Hoffman N.V., A. Bouazza RE CISA, Directeur
Heeft de auditor opmerkingen gemaakt in de TPM van de leverancier over normen die bij de aansluithouder moeten worden onderzocht?	Ja
Kunt u aangeven over welke normen opmerkingen zijn gemaakt in alle aanwezige TPM's en waar u dus zekerheid over moet verkrijgen?	B.05, U/TV.01, U/WA.02, U/WA.05, C.08,

Object van onderzoek

Het object van onderzoek was de webomgeving van DigiD aansluiting 1000237 en Zaaksysteem Oude IJsselstreek.

Gemeente Oude IJsselstreek biedt de volgende functionaliteit aan waarvoor DigiD aansluiting 1000237 voor authenticatie wordt gebruikt: . Deze functionaliteit wordt geboden door de volgende webapplicatie: Zaaksysteem Oude IJsselstreek.

Deze applicatie betreft Zaaksysteem en wordt onderhouden door Mintlab.

Deze applicatie is extern benaderbaar via de volgende URL(s): https://mijn.oude-ijsselstreek.nl. De infrastructuur waar deze applicaties op draaien wordt beheerd door Mintlab in de vorm van een SAAS-oplossing.

Het object van onderzoek was de webomgeving van DigiD aansluiting 1000237 ('DigiD webomgeving'). Het onderzoek heeft zich gericht op de webapplicaties, de URLs waarmee deze kunnen worden benaderd, de infrastructuur (binnen de DMZ waar webapplicaties zich bevinden) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius. Het onderstaande schema toont de webomgeving die is onderzocht door middel van een infrastructurele test.

Gemeente Oude IJsselstreek heeft een deel DigiD webomgeving uitbesteed aan Mintlab. Als gevolg hiervan zijn er een aantal maatregelen belegd bij deze service organisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT auditor van deze service organisatie. De richtlijnen waar deze maatregelen betrekking op hebben zijn door ons dan ook niet onderzocht. Waar relevant geven wij, per richtlijn, specifieke verwijzingen naar het rapport van de service organisatie.

Totaaloverzicht getoetste normen ICT-beveiligingsassessment DiGiD-aansluiting van gemeente Oude IJsselstreek

In deze bijlage brengen wij de oordelen samen, op basis van de diverse uitgevoerde werkzaamheden / uitgebrachte rapportages. Het doel van deze samenvatting is om Logius een totaaloverzicht te verschaffen over de resultaten vanuit de verschillende assessments t.a.v. de DigiD-aansluiting 1000237 en Zaaksysteem Oude IJsselstreek.

Volgens de NOREA-handreiking inzake de DigiD-assessments moeten de volgende normen bij de gebruikersorganisatie worden getoetst: B.05, U/TV.01, U/WA.02, U/WA.05. en C.08.

Als input voor de hierna vermelde samenvatting hebben wij, naast de voorliggende rapportage, gebruik gemaakt van de rapportage van DigiD-assesment zaaksysteem.nl ten behoeve van Oude IJsselstreek van de serviceorganisatie Mazaars, MMC/DIGID/GO17112017, 17-11-2017 ondertekend door J.H. Matto RE RI Partner-aandeelhouder Mazaars Paardekoper Hoffman N.V., A. Bouazza RE CISA, Directeur.

Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de rapportage van DigiD-assesment zaaksysteem.nl ten behoeve van Oude IJsselstreek van de serviceorganisatie Mazaars, MMC/DIGID/GO17112017, 17-11-2017. Wij kunnen dan ook geen verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Norm	Beschrijving van de norm	Getoetst bij leverancier. Voldoet niet/Voldoet niet van toepassing	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie zijn/zijn niet van toepassing	Getoetst bij gebruiker Voldoet niet/Voldoet niet van toepassing	Referentie / rapportnummer
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	Voldoet	MMC/DIGID/GO17112017	Ja	Voldoet	
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve	Voldoet	MMC/DIGID/GO17112017	Ja	Voldoet	

	mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.					
U/WA .02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Voldoet	MMC/DIGID/GO1 7112017	Ja	Voldoet	
U/WA .03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Voldoet	MMC/DIGID/GO1 7112017	Nee		
U/WA .04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	Voldoet	MMC/DIGID/GO1 7112017	Nee		
U/WA .05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing	Voldoet	MMC/DIGID/GO1 7112017	Ja	Voldoet	

	van privacybevordere nde en cryptografische technieken.					
U/PW .02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Voldoet	MMC/DIGID/GO1 7112017	Nee		
U/PW .03	De webserver is ingericht volgens een configuratie-baseline.	Voldoet	MMC/DIGID/GO1 7112017	Nee		
U/PW .05	Het beheer van platformen maakt gebruik van veilige (communicatie)pr otocollen voor het ontsluiten van beheermechanis men en wordt uitgevoerd conform het operationeel beleid voor platformen.	Voldoet	MMC/DIGID/GO1 7112017	Nee		
U/PW .07	Voor het configureren van platformen een hardeningsrichtlij n beschikbaar.	Voldoet	MMC/DIGID/GO1 7112017	Nee		
U/NW .03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.	Voldoet	MMC/DIGID/GO1 7112017	Nee		

U/NW .04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.	Voldoet	MMC/DIGID/GO1 7112017	Nee		
U/NW .05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	Voldoet	MMC/DIGID/GO1 7112017	Nee		
U/NW .06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	Voldoet	MMC/DIGID/GO1 7112017	Nee		
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	Voldoet	MMC/DIGID/GO1 7112017	Nee		
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	Voldoet	MMC/DIGID/GO1 7112017	Nee		
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief	Voldoet	MMC/DIGID/GO1 7112017	Nee		

	en beveiligd ingericht.					
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.	Voldoet	MMC/DIGID/GO1 7112017	Nee		
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet	MMC/DIGID/GO1 7112017	Ja	Voldoet	
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.	Voldoet	MMC/DIGID/GO1 7112017	Nee		

Bijlage 2 Suwinet

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging DigiD en Suwinet van de gemeente Oude IJsselstreek.

De gemeente heeft de uitvoering van de participatiewet gedeeltelijk uitbesteed aan Laborijn. De uitbestede taken zijn onderdeel van de Collegeverklaring omdat wij voor de uitbestede taken de volledige verantwoordelijkheid dragen.

Afwijkingen van de normen
Met uitzondering van de volgende normen voldoen de interne beheersingsmaatregelen voor de SUWI-taken in opzet en bestaan aan alle geselecteerde normen:

- BIG:10.10.1 en 10.10.2 / Suwinet: C.06, C.07 Suwinet-Inkijk.
- BIG:13.1.2 / Suwinet: B.01, B.04 Suwinet-Inkijk.