auditconnect
auditors & consultants

Assurance-rapport van de onafhankelijke IT-auditor

ENSIA

Ten behoeve van: gemeente Maastricht

Uitgebracht door	: AuditConnect B.V.
Contactpersoon	: drs. M.R. van der Vliet RE
Uitgebracht aan	: gemeente Maastricht
Contactpersoon	: de heer F. Toonen
Datum	: 07-03-2018
Versie	: 0.1 – Concept – Ter bespreking met opdrachtgever

Contactgegevens

Postadres	:	AuditConnect B.V., Postbus 4355, 7320 AJ Apeldoorn	
Telefoon	:	+31 (0)55 30 10 100	
Contactpersoon	:	De heer M. van der Vliet	
Mobiel	:	+31 (0)62 50 57 951	
E-mail	:	m.vandervliet@auditconnect.nl	
Bankrelatie	:	ABN-AMRO bank Zutphen	NL12ABNA 0517978210
Handelsregister	:	Oost Nederland	08162731
BTW	:	Randmeren / Apeldoorn	NL8184.24.588.B01

Inhoudsopgave

Aan: de heer F. Toonen

Ons oordeel met beperking

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 Maastricht 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 Maastricht 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.

Onderbouwing van ons oordeel met beperking

Zoals in de Collegeverklaring ENSIA 2017 is aangegeven wordt nog niet aan alle normen inzake Suwinet voldaan. Hieronder treft u de nadere uiteenzetting van de normen en waarom hier niet aan is voldaan.

Norm C.04: Het verantwoordelijk management behoort de toegangsrechten van gebruikers / beheerders tot de Suwinet diensten regelmatig te beoordelen in een formeel (cyclisch) proces.
Wij hebben vastgesteld dat niet kon worden aangetoond dat de beoordeling op de toegangsrechten volgens het informatiebeveiligingsplan gedurende 2017 zijn beoordeeld (tweejaarlijks).

Norm C.07: De afnemer voert periodiek evaluaties op de technische en organisatorische beoordelingsrapportages en neemt noodzakelijke verbeteracties.
Wij hebben vastgesteld dat de beoordelingsrapportage beschikbaar is. Er kon echter niet worden vastgesteld dat deze wordt gerapporteerd aan het verantwoordelijk management. Hierdoor hebben wij niet kunnen vaststellen of de rapportage wordt geëvalueerd. Deze evaluatie is noodzakelijk om indien van toepassing passende noodzakelijke verbeteracties te kunnen treffen dan wel passende maatregelen te nemen bij vermoeden van misbruik.

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

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

De basis voor ons oordeel met beperking

Wij hebben onze assurance-opdracht met betrekking tot de Collegeverklaring ENSIA 2017 uitgevoerd volgens Nederlands recht, waaronder de Richtlijn 3000 (Herzien) 'Assuranceopdracht 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.

Beperking in gebruik en verspreidingskring

Dit assurancerapport 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 assurancerapport 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.

Verantwoordelijkheden van het college van gemeente Maastricht

Het college van burgemeester en wethouders van gemeente Maastricht 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 zoals informatie over interne beheersingsmaatregelen, 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:

- 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.

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; en
- het evalueren van de toereikendheid van de assurance-informatie.

[Plaats en datum]

[naam IT-auditeenheid]

[naam IT Auditor RE]

auditconnect
auditors & consultants

AuditConnect B.V.

Bezoekadres:
Jean Monnetpark 11
7336 BA Apeldoorn

Postadres:
Postbus 4355
7320 AJ Apeldoorn

055 - 30 101 00

info@AuditConnect.nl
www.AuditConnect.nl