gemeente Rheden

ENSIA | Eenduidige Normatiek Single Information Audit

2021

Verbeterplan

DigiD / Suwinet

gemeente Rheden

Inhoudsopgave

gemeente Rheden

Inleiding:

Dit document dient als bijlage van de Collegeverklaring ENSIA (Onderdelen DigiD en Suwinet). Derhalve maakt de inhoud van dit document geen onderdeel uit van de controle door de externe IT-auditor.

Verantwoording over de toepassing van de BIO gebeurt per 2017 via de ENSIA (Eenduidige Normatiek Single Information Audit) verantwoordingssystematiek. Dit naar aanleiding van de aangenomen resolutie “Informatieveiligheid, randvoorwaarde voor de professionele gemeente” op de buitengewone ledenvergadering van de VNG op 29 november 2013. Of we voldoen aan deze Baseline is getoetst door middel van een zelfevaluatie. Voor het jaar 2021 geldt (net als voor het jaar 2020) dat de verantwoording Suwinet (aan Ministerie van SZW) en DigiD (aan Logius) wordt verantwoord door middel van een Collegeverklaring.

Over verantwoordingsjaar 2021 vindt naast de zelfevaluatie over de gehele BIO (Baseline Informatieveiligheid Overheden) een IT Audit (externe toets) plaats op de onderdelen DigiD en Suwinet (Opzet en bestaan, de werking valt buiten de scope). Met ENSIA wordt beoogd om de auditlast te verminderen en het verantwoordingsstelstel voor informatieveiligheid efficiënt en effectief in te richten en te implementeren door het toezicht te bundelen en aan te sluiten op de Planning & Control (P&C)-cyclus.

Uit deze zelfevaluatie blijkt dat binnen onze gemeente op peildatum 31 december 2021 de interne beheersingsmaatregelen in opzet en bestaan niet voldoen aan de geselecteerde normen inzake DigiD en Suwinet. Dit verbeterplan beschrijft welke opvolging (correctieve maatregelen) er door onze gemeente worden getroffen en welke verbetertermijn wordt gehanteerd.

Dit verbeterplan adresseert de bevindingen uit de zelfevaluatie waarover het College verantwoording aflegt door middel van de Collegeverklaring, en de opvolging ervan. Hierbij wordt aangegeven wat de planning is voor uitvoering van de maatregelen.

De classificatie “voldoet niet” wordt meegegeven zodra aan een norm niet voor de volle 100% wordt voldaan.
Normen waaraan wordt voldaan zijn niet meegenomen in dit verbeteringsplan.

Maart 2022,

Roel Harmsen
Chief Information Security Officer (CISO) / Coördinator ENSIA

Gemeentelijk kenmerk collegeverklaring ENSIA:	Rheden-Verbeterplan-2021

gemeente Rheden

Maatregelen DigiD:

Algemeen
In onderstaande wordt expliciet ingegaan op elke norm welke ten tijde van de zelfevaluatie niet voldoet, welke maatregel wordt genomen om dit te corrigeren en welke planning daarvoor geldt.

Aansluiting: DigiD 141579 **Norm: U/PW.03** De webserver is ingericht volgens een configuratie-baseline.		
Bevinding: 1. Bij de leverancier is 1 configuratie als onjuist beoordeeld. De auditor geeft het volgende aan: *'T.a.v. norm U/PW.03 merken we op dat één (1) specifiek onderdeel van de gewenste configuratie-items niet op de juiste wijze is geconfigureerd, waarbij naar het oordeel van de auditor de kwetsbaarheden afdoende zijn beperkt en een verbeterplan is opgesteld waarbij de auditor er kennis van heeft genomen, dat de kwetsbaarheid voor 1 mei 2024 geheel is opgelost. Alle andere configuratie-items zijn wel correct geconfigureerd (bron: FAQ versie: 1.4 d.d. 8 november 2021).'*	**Maatregel:** De actie aan onze kant is de leverancier aansporen de norm in 2022 op orde te hebben en niet pas in 2024.	**Planning:** Q2 start Q2 afronden
Aansluiting: DigiD 1003555 **Normen: B.05, U/TV.01, U/WA.02, U/WA.05, U/NW.06, C.08**		
Bevinding: 1. Bij de leverancier is de audit voor de TPM uitgevoerd per 4 maart 2022. Daar de ENSIA audit over 2021 gaat, dient opzet en bestaan in dat jaar vastgesteld te worden. De TPM is dan ook niet bruikbaar voor deze ENSIA controle, ondanks dat alle normen positief beoordeeld zijn.	**Maatregel:** De leverancier is hiervan op de hoogte gesteld, met als doel de audit over 2022 daadwerkelijk in 2022 plaats te laten vinden. Voor de controle voor 2021 dient een hertest plaats te vinden. Hiervoor is de TPM van 4 maart 2022 wel bruikbaar, waarin alle relevante maatregelen als voldoende beoordeeld zijn.	**Planning:** Q2 start Q2 afronden

Gemeentelijk kenmerk collegeverklaring ENSIA:	Rheden-Verbeterplan-2021

gemeente Rheden

Gemeentelijk kenmerk collegeverklaring ENSIA:	Rheden-Verbeterplan-2021

gemeente Rheden

Maatregelen Suwinet GSD en BRP:

Algemeen
De gemeente Rheden maakt gebruik van Suwinet inkijk en DKD-inlezen, middels de applicatie. De niet Suwinet taken zijn ook meegenomen in onderstaand verbeterplan.

Norm: 6.1.2 Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.		
Bevinding: 1. Er is geen autorisatie-matrix beschikbaar om als SOLL positie te dienen. Gebruikers worden op basis van inzicht van managers gecontroleerd.	**Maatregel:** Inzichtelijk maken hoeveel gebruikers in welke Suwi applicatie zitten en hier een matrix voor opstellen bij meer dan 10 gebruikers. Deze matrix dient in de procedure ingeschreven te worden en bijgehouden te worden.	**Planning:** Q2 start Q3 afronden

Norm: 7.2.2 Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.		
Bevinding: 1. Er is in 2021 geen beleid of procedure beschikbaar waarin is vastgelegd dat periodiek aandacht besteed wordt aan bewustwording. 2. Er hebben ad hoc awareness trainingen plaatsgevonden. Wij hebben niet vast kunnen stellen dat er een opzet is waaruit blijkt dat structureel en planmatig elke nieuwe medewerker binnen 3 maanden een awareness training dient te volgen.	**Maatregel:** Procedure awareness training beschrijven in het beveiligingsbeleid. Awareness trainingen uit laten voeren door nieuwe medewerkers en de resultaten bijhouden.	**Planning:** Q2 start Q3 afronden

Norm: 9.2.1 Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
Norm: 9.2.2 Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
Norm: 9.2.5 Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.

Gemeentelijk kenmerk collegeverklaring ENSIA:	Rheden-Verbeterplan-2021

gemeente Rheden

Norm: 9.2.6 De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.		
Bevinding: 1. De periodieke controles zijn mede uitgevoerd door de applicatiebeheerder, waardoor in de controle functiescheiding ontbreekt. 2. De periodieke controles zijn niet op de juiste momenten in het jaar uitgevoerd. Deze dienen minimaal 2 x per jaar over gelijke delen uitgevoerd te worden. 3. Het aanmaken en verwijderen van accounts wordt niet op een aantoonbare manier uitgevoerd. Er is beperkte tot geen vastlegging beschikbaar. 4. Er zijn verschillende processen, waaronder de autorisatieprocudure, in diverse documenten beschreven. Hierdoor is het onduidelijk welke procedure/beschrijving/beleid geldig is. Zie opmerking auditor: *In het Suwinet beveiligingsbeleid is op meerdere plekken tekst opgenomen ten aanzien van autorisaties (beheer, verantwoordelijkheden, proces, controles) eveneens is een nieuwe autorisatieprocedure voor Suwinet opgesteld. Door op verschillende plekken iets op te nemen over de autorisatieprocedure ontstaat het risico dat documenten elkaar gaan tegen spreken en/of dat er onduidelijkheid ontstaat over het proces en de verantwoordelijkheden. Wij geven de overweging mee om het Suwinet beveiligingsbeleid en de nieuwe autorisatieprocedure kritisch door te nemen op inhoud en leesbaarheid.*	**Maatregel:** Functiescheiding tussen applicatiebeheerder en controle uitvoerder realiseren. Accounts tijdig verwijderen en bewijs vastleggen. Autorisatieproces herzien en periodieke controles zorgvuldiger uitvoeren. Autorisatieprocedure duidelijker en eenduidig formuleren.	**Planning:** Q2 start Q3 afronden

Gemeentelijk kenmerk collegeverklaring ENSIA:	Rheden-Verbeterplan-2021

gemeente Rheden

Norm: 12.4.1 en 12.4.2 Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.		
Bevinding: Ten aanzien van Liaan: 1. De betrouwbaarheid en volledigheid van de logging is niet vastgesteld. 2. De logging is niet periodiek juist beoordeeld en de periodieke beoordeling is niet aan het management gerapporteerd. 3. Er is niet vastgesteld of toegang tot de database beperkt is tot onafhankelijke medewerkers. 4. Wijzigingsbeheer ten aanzien van Liaan is niet ingericht. Er is geen wijzigingslog beschikbaar. Er is geen procedure wijzigingsbeheer beschikbaar.	**Maatregel:** Logging van Liaan periodiek beoordelen op betrouwbaarheid en volledigheid. Deze periodieke beoordeling aan het MT rapporteren. Vaststellen dat toegang tot de database beperkt is tot onafhankelijk medewerkers. Wijzigingsbeheerprocedure ten aanzien van Liaan opstellen, implementeren en bewijs bijhouden.	**Planning:** Q2 start Q3 afronden

Norm: 18.1.4 Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.		
Bevinding: Suwinet is niet in het verwerkingsregister opgenomen	**Maatregel:** Suwinet opnemen in het verwerkingsregister. Het beleid ten aanzien van de toegang tot de logging en de controle daarvan wordt opnieuw geëvalueerd en aangepast.	**Planning:** Q2 start Q3 afronden