Gemeente Gouda

raadsmemo

aan	de gemeenteraad
onderwerp	ENSIA verantwoording 2024 stand van zaken informatieveiligheid
van	het college van burgemeester en wethouders
datum	25 maart 2025
zaaknummer	1350955

memo

Samenvatting

Het college van burgemeester en wethouders van de gemeente Gouda legt over het jaar 2024 verantwoording af over de stand van zaken op het gebied van informatieveiligheid binnen de gemeentelijke organisatie. Dit gaat op basis van de landelijke en voor gemeenten verplichte Eenduidige Normatiek Single Information Audit (ENSIA) systematiek. We leggen verantwoording af aan de gemeenteraad (horizontale verantwoording) en aan de verschillende toezichthouders (verticale verantwoording).

Doel

De raad informeren over de stand van zaken met betrekking tot informatieveiligheid.

1 Aanleiding

Met ingang van 2017 is er een nieuwe systematiek voor verantwoording van de informatiebeveiliging ingevoerd, ENSIA. De VNG heeft samen met het rijk deze efficiënte verantwoordingssystematiek ontwikkeld: de Eenduidige Normatiek Single Information Audit (ENSIA). ENSIA helpt gemeenten in één keer verantwoording af te leggen over informatieveiligheid. Hiermee kan met één verklaring zowel horizontaal (van het college naar de raad) als verticaal (van het college naar de landelijke toezichthouders) verantwoording worden afgelegd. De verklaring met bijlagen en de rapportage over het Geo-domein (BAG, BGT en BRO) zijn opgesteld aan de hand van landelijke modellen.

Aanvullende informatie

Ontwikkelingen

De NIS2 (Network and Information Systems Directive) is de Europese richtlijn. In NIS2 worden minimale informatiebeveiligingsmaatregelen vereist, die zijn opgenomen in de Baseline Informaliebeveiliging Overheid 2 (BIO2). De BIO2 wordt vervolgens wettelijk verankerd in de nadere regelgeving van de NIS2-implementaitewet (Cyberbeveiligingswet). Zo komt er één basisniveau voor informatiebeveiliging voor alle overheidsorganisaties. Het doel van de richtlijn, de wet en de nieuwe BIO is de cyberbeveiliging van essentiële diensten in EU-lidstaten te verbeteren. De NIS2 richtlijn legt strengere eisen op aan bedrijven en organisaties die cruciale diensten leveren binnen de EU. Alle overheidsorganisaties zijn door de Rijksoverheid aangemerkt als essentiële dienst.

Enkele belangrijke aspecten van de impact van de NIS2/Cbw zijn:

- Verhoogde Veiligheidseisen: De Cbw stelt strengere beveiligingseisen aan gemeenten die als aanbieder van essentiële diensten worden aangemerkt. Gemeenten vallen onder deze categorie, gezien hun rol in het aanbieden van kritieke openbare diensten.
- Meldplicht en Samenwerking: De Cbw introduceert meldplichten voor ernstige incidenten en vereist samenwerking met nationale cybersecurity instanties. Gemeenten moeten in staat zijn om snel en effectief te reageren op cyberincidenten en deze te melden aan relevante autoriteiten.
- Kritieke Infrastructuur Bescherming: De Cbw benadrukt de bescherming van kritieke infrastructuren. Dit omvat vitale diensten zoals brugbediening en digitale diensten die van

cruciaal belang zijn voor het functioneren van de gemeenschap.

- Continuïteit en herstelplannen: Gemeenten moeten robuuste bedrijfscontinuïteitsplannen opstellen, inclusief herstelplannen voor kritieke processen, om de impact van incidenten te minimaliseren en de normale dienstverlening zo snel mogelijk te hervatten.
- Bewustwording: De Cbw benadrukt het belang van bewustwording van medewerkers op het gebied van informatiebeveiliging. Gemeenten dienen structureel programma's te implementeren om cybersecuritybewustzijn te vergroten en het personeel op te leiden om mogelijke dreigingen te herkennen en te voorkomen.
- Risicomanagement: Gemeenten moeten een actief risicomanagementbeleid voeren, waarbij regelmatige risicoanalyses worden uitgevoerd en passende maatregelen worden genomen om deze te mitigeren.
- Verantwoording, toezicht en boetes: Gemeenten moeten zich aantoonbaar kunnen verantwoorden dat ze voldoen aan de eisen van de Cbw en de BIO 2.0 zowel in opzet, bestaan als werking van maatregelen. Er kunnen juridische en financiële consequenties zijn als de organisatie niet voldoet aan de eisen van de NIS2. Dit kan leiden tot boetes of andere sancties, afhankelijk van de ernst van de overtreding.

Bovenstaande aspecten vormen een belangrijk onderdeel van de brede inspanningen die we moeten ondernemen om te voldoen aan de eisen van de Cbw en om de algehele informatiebeveiliging van onze organisatie te versterken. Hierbij wordt opgemerkt dat gemeente Gouda ook een verantwoordelijkheid heeft ten opzichte van 4 regiogemeenten en per 1 januari 2025 de GR JW doordat gemeente Gouda de IT-infrastructuur voor deze organisaties beheert.

ENSIA-verantwoording
Onderstaande tabellen geven per ENSIA-onderdeel een korte toelichting, bevindingen en de stand van zaken weer. Voor de leesbaarheid is per onderdeel met behulp van kleuren de algemene status weergegeven.

Legenda:

Ruim voldoende tot goed	*Voldoende*	*Net onvoldoende*	*Onvoldoende*
Het onderdeel is volledig op orde, in control Mogelijk zijn er minimale verbeterpunten	Het onderdeel is globaal op orde, in control Er zijn enkele verbeterpunten	Het onderdeel is net niet in control Er zijn meerdere verbeterpunten	Het onderdeel is niet in control Er zijn veel verbeterpunten, bijsturing is nodig

Verantwoording per ENSIA-stelsel
De onderstaande tabel geeft per stelsel (domein) een korte toelichting, bevindingen en de stand van zaken weer.

ENSIA-stelsel	Toelichting, bevindingen en stand van zaken	Status
Implementatie BIO Baseline Informatiebeveiliging Overheid	Om op het gebied van informatieveiligheid weerbaar te blijven volgen we de landelijke Baseline Informatiebeveiliging Overheid (BIO). Deze BIO is het normenkader waarbij we op basis van een eigen risico-afweging keuzes maken in het implementeren van beheers- en beveiligingsmaatregelen. Hierbij blijft een basispakket aan generieke maatregelen voor iedere (overheid)organisatie verplicht. Het strategisch informatiebeveiligingsbeleid is geldig tot 2027 en in lijn met de voor overheden verplichte landelijke Baseline Informatiebeveiliging Overheid (BIO). Specifiek gekeken naar de borging van informatieveiligheid over het geheel gezien scoren we ons zelf op een voldoende. Deze score komt voort uit resultaten van onder andere de verschillende ENSIA-onderdelen waaronder een externe audit. Hierbij moet worden opgemerkt dat de BIO	

	2.0 strengere (wettelijke) eisen gaat stellen waardoor we alle zeilen moeten bijzetten om een voldoende te blijven scoren. Het voldoen aan de eisen en normen van de BIO is natuurlijk geen doel op zich, maar wel een belangrijke graadmeter van onze volwassenheid als organisatie op het gebied van informatiebeveiliging. Onderstaand de status van de belangrijkste acties m.b.t. de implementatie van de BIO. <u>Bewustwording</u> Uit de risico-inventarisatie is naar voren gekomen dat vooral bewustwording/menselijk gedrag, een aandachtspunt is binnen de gemeente Gouda. Aangezien dit ook een aandachtspunt is uit het landelijk dreigingsbeeld 2023-2024 is dit een belangrijk onderdeel om de weerbaarheid van Gouda te verhogen. Op basis van de resultaten van de nulmeting is een bewustwordingsprogramma opgesteld waarvan de start staat gepland in het 2e kwartaal van 2025. <u>Bedrijfscontinuïteit</u> Gemeente Gouda heeft het continuïteitsmanagement beter ingericht. Hiermee bereidt ze zich voor op mogelijke continuïteitsproblemen. Inmiddels zijn op basis van een dataclassificatie de volgende 6 kritieke processen vastgesteld: • Burgerzaken • IT-infrastructuur (essentiële componenten) • Betaling van uitkeringen • Rioolbeheer • Verkeersregeling • Brugbediening Vervolgens is er een bedrijfscontinuïteitsplan opgesteld inclusief een crisisstructuur voor specifieke calamiteiten met gevolgen voor de bedrijfsvoering van de gemeentelijke organisatie. Hierbij is zoveel mogelijk aangehaakt bij de bestaande veiligheid crisisorganisatie. Voor deze kritieke processen is een Business Impact Analyse (BIA) uitgevoerd en in de loop van 2025 wordt per proces een draaiboek opgesteld met als doel de basistaken van de gemeente te waarborgen bij calamiteiten/crisis zoals een hack, ransomware aanval, brand, extreem weer, lekkage, pandemie, explosies of uitval van (nuts)voorzieningen.	
Suwinet Structuur uitvoeringsorganisatie Werk en Inkomen	Suwinet wordt gebruikt voor het uitvoeren van de Participatiewet, Inkomensvoorziening voor Oudere en gedeeltelijk Arbeidsongeschikte Werknemers (IOAW), Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ), Wet gemeentelijke schuldhulpverlening (Wgs), Uitvoeren bijzonder bijstand , Uitvoeren bezoldiging zelfstandigen en de Sociale recherche. Voor de regiogemeenten Alphen aan den Rijn, Bodegraven-Reeuwijk, Krimpenerwaard, Nieuwkoop, Waddinxveen en Zuidplas voeren wij werkzaamheden uit op het gebied van hulp aan vroegtijdig schoolverlaters door Regionaal Meld- en Coördinatiecentrum (RMC). Voor de uitvoering van deze taken wordt gebruik gemaakt van Suwinet-Inkijk. Vanwege de hoeveelheid en gevoeligheid van (persoons)gegevens binnen Suwinet is bepaald dat iedere gemeente naast de zelfevaluatie ook extern getoetst wordt op naleving van het normenkader. Het uitvoeren van de audit voor Suwinet is een vereiste van de Regeling SUWI. Het onderzoek van de externe auditor geeft aan dat de gemeente Gouda voldoet aan de wettelijk gestelde eisen en normen in het kader van informatieveiligheid rondom het gebruik en beheer van alle Suwinet-aansluitingen.	
DigiD Digitale Persoonsidentificatie	DigiD is voor inwoners de manier om zichzelf digitaal te identificeren. DigiD wordt gebruikt voor de eDiensten Burgerzaken, eZaken en het inwonerportaal Sociaal Domein. Onvoldoende of onjuist beheer van een DigiD-aansluiting kan grote gevolgen hebben voor de landelijke keten en uiteindelijk persoonsinformatie van inwoners. Daarom heeft de toezichthouder	

	bepaald dat iedere DigiD-aansluiting naast een jaarlijkse zelfevaluatie ook (extern) getoetst wordt op naleving van het normenkader. Het onderzoek van de externe auditor geeft aan dat onze processen rondom DigiD op orde zijn. Wij voldoen aan de gestelde informatiebeveiligingsnormen met als kanttekening dat “In 2024 is het nieuw dat naast opzet en bestaan ook de werking wordt getoetst op vijf (5) normen. Voor twee (2) van deze normen heeft de leverancier voor het proces eZaken per 31/12/2024 geen werking kunnen aantonen. Dit is overgenomen in de bijgevoegde collegeverklaring 2024. In januari 2025 heeft een heraudit plaatsgevonden en hiermee wordt door de leverancier aan alle normen voldaan”. Naast het onderzoek rondom organisatorische waarborgen heeft er ook een technische penetratietest plaatsgevonden op www.gouda.nl. Ook deze uitkomst is positief, er zijn geen kwetsbaarheden ontdekt. De veiligheid van DigiD en websites staat onder druk. Het landelijke dreigingsbeeld geeft aan dat digitale risico’s onverminderd groot zijn en cyberaanvallen steeds meer succesvol zijn met alle gevolgen van dien. De beveiliging vraagt steeds meer aandacht waarbij het een uitdaging is om dit huidige niveau vast te houden.	
BRP Basis Registratie Personen Deel 1 bestandscontrole op persoonslijsten	BRP is de basisregistratie waarin alle inwoners zijn geregistreerd. Gemeenten beheren deze BRP voor hun inwoners. Uiteindelijk worden alle BRP-registraties landelijk gekoppeld, zodat overheidsinstanties, zorgverleners en andere dienstverleners die gebruik mogen maken van deze BRP beschikken over de juiste persoonsinformatie. Vanwege het grote landelijke belang rondom de BRP zijn gemeenten verplicht om jaarlijks een zelfevaluatie uit te voeren. ***Bestandscontrole op de persoonslijsten.*** Bij de bestandscontrole in de Basisregistratie personen van 23-11-2024 is 99,99% van de actuele persoonslijsten correct bevonden. Dit is in lijn met eerdere jaren, waarin de score steeds nagenoeg hetzelfde positieve resultaat liet zien. Dit voldoet ruimschoots aan de landelijke norm.	
BRP Deel 2 Inhoudelijke controle op de persoonslijsten	***Een inhoudelijke controle van persoonslijsten.*** Aan de hand van brondocumenten is een steekproefsgewijze controle uitgevoerd naar de juiste verwerking daarvan in de basisregistratie. Op 1 aspect voldoet het resultaat van 97% niet aan de landelijke norm van 98%. De steekproef wordt uitgevoerd aan de hand van brondocumenten die in de afgelopen 10 jaar in de BRP zijn opgenomen. Verbeteringen in het proces en kwaliteit zijn daardoor pas langzaam zichtbaar en hebben geen directe invloed op persoonslijsten uit het verleden. De geconstateerde afwijkingen zijn inmiddels hersteld.	
BRP Deel 3 Uitvoering van de processen	***Een controle op uitvoering van de processen.*** Door middel van een zelfevaluatie vragenlijst is dit onderdeel onderzocht. In de vragenlijst staan vragen over de procedures die gevolgd worden bij het verwerken en beveiligen van persoonsgegevens. De gemeente scoort 80 %. De score is ten opzichte van vorig jaar (85%) verslechterd. Het eindresultaat voor dit onderdeel is net niet voldoende. Meerdere verbeterpunten moeten de komende jaren worden opgepakt.	
PUN Paspoort Uitvoeringsregeling Nederland	Gemeenten verzorgen het aanvragen en het uitreiken van reisdocumenten voor hun inwoners. Reisdocumenten zijn erg waardevol en vaak de sleutel tot identiteitsfraude. De processen rondom het aanvragen en uitreiken zijn daarom strikt. De burgemeester is verantwoordelijk voor de borging van deze processen en moet hierover jaarlijks verantwoording afleggen aan de minister van Binnenlandse Zaken en Koninkrijksrelaties. Via de ENSIA-verantwoording infomeren we ook het eigen bestuur over de stand van zaken. De zelfevaluatie PUN over het jaar 2024 is afgerond met een score van 95% Dit is een goed eindresultaat. Vorig jaar was de score 91%. Processen en	

	de uitvoering rondom het aanvragen, beheren en uitreiken van reisdocumenten zijn op orde.	
BAG Basisregistratie Adressen en Gebouwen	De BAG bevat gemeentelijke basisgegevens van alle adressen en gebouwen in een gemeente. Kopieën van al deze gegevens zijn verzameld in een landelijke voorziening. Deze voorziening wordt landelijk gebruikt door overheden, organisaties en particulieren. Net als alle andere bronhouders verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BAG. De zelfevaluatie BAG over het jaar 2024 is afgerond met een score van 100%. Hiermee voldoen we aan de landelijk gestelde norm van minimaal 75%. Vorig jaar was de score 92%.	
BGT Basisregistratie Grootschalige Topografie	De BGT is een digitale kaart van Nederland waarop gebouwen, wegen, waterlopen, terreinen en spoorlijnen eenduidig zijn vastgelegd. Kortom: de inrichting van de fysieke omgeving. De BGT is een landelijk uniforme registratie die alleen gemaakt kan worden vanuit een goede samenwerking tussen de diverse bronhouders. Gemeenten zijn als bronhouder medeverantwoordelijk voor de kwaliteit van deze landelijke basisregistratie. Net als alle andere bronhouders verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BGT. De zelfevaluatie BGT over het jaar 2024 is afgerond met een score van 100%. Hiermee voldoen we aan de landelijk gestelde norm van minimaal 75%. Vorig jaar was de score 100%.	
BRO Basisregistratie Ondergrond	De BRO bevat bodem- en ondergrondgegevens. Het gebruik van deze gegevens is de laatste decennia sterk toegenomen. Een goede informatievoorziening over de ondergrond is van wezenlijk belang voor het realiseren van bestuurlijke ambities als het omgevingsplan, de energietransitie, watertoets en dergelijke. Als we willen dat onze inwoners hier ook actief in participeren, moet het fundament hiervoor op orde en goed ingevuld zijn. De BRO is een van de elementen die de verschillende opgaves mogelijk moeten maken. De gemeente is bronhouder voor deze basisregistratie. Net als alle andere bronhouders verantwoorden we ons jaarlijks over de stand van zaken rondom het beheer van deze BRO. De zelfevaluatie BRO over het jaar 2024 is positief afgerond met een score van 80%. Hiermee voldoen we ruim aan de landelijk norm. Vorig jaar was de score 84%. De ENSIA-score van BRO is nog erg theoretisch en moet met enige nuance bekeken worden. Daarom zetten wij onze status zelf op “voldoende”. **Verbeterdoelen ten aanzien van Kwaliteitseisen BRO** Controleurs van ODMH hebben afgelopen jaar een training gehad m.b.t. sonderingen voor controletaken. We sluiten aan bij de ontwikkeling van een landelijke datakwaliteitscontroletool (ministerie BZK, ontwikkeld door RWS). **Verbetermaatregelen ten aanzien van Borging proces BRO** Verdere stappen zetten om de gebruiksplicht van de BRO op te nemen in de werkprocessen van de beleidsafdeling (RBA).	

Bijlagen(n):
-/-