

Onderwerp Digitale veiligheid

Datum	01 juli 2025
Thema programmabegroting	Bedrijfsvoering
Portefeuillehouder	Dorus Klomberg
Zaaknummer	2025-006008

Kennis te nemen van

Geachte leden van de gemeenteraad,

Met deze raadsinformatiebrief informeren wij u graag over de voortgang en status van digitale veiligheid binnen de gemeente Rheden. Onder digitale veiligheid vallen de integrale thema's: cybersecurity (CS), informatiebeveiliging (IB) en gegevensbescherming (privacy).

Aanleiding voor deze brief is drieledig:

- 1) Periodieke rapportage over digitale veiligheid zodat u op de hoogte bent van de gemeentelijk inzet op dit thema en hierop gericht kan sturen. Dit is ook onderdeel van de uitwerking om digitale veiligheid te verbeteren, zoals beschreven in de kadernota.
- 2) Het recente resultaat van ENSIA 2024 en de verplichting van het college u hierover te informeren. Via deze brief legt het college verantwoording af aan de gemeenteraad over informatieveiligheid en datakwaliteit in aanvulling op de paragraaf Bedrijfsvoering in de jaarstukken. Ook informeren wij u over verbeterplannen n.a.v. de resultaten.
- 3) De financiële commissie heeft aangevraagd een raadsinformatiebrief op te stellen m.b.t. cybersecurity en security awareness (beveiligingsbewustzijn).

Kernboodschap

In deze raadsinformatiebrief nemen we u mee in de volgende onderwerpen:

- I. De resultaten van ENSIA 2024
- II. Het algemene beeld op cybersecurity & informatiebeveiliging
- III. Gegevensbescherming (privacy)
- IV. Beveiligingsbewustzijn (awareness)

Inleiding ENSIA

ENSIA is het verantwoordingsinstrument voor informatiebeveiliging binnen gemeenten. Het ondersteunt aantoonbaar grip te houden op informatiebeveiliging en privacy via verplichte verantwoording aan het rijk en toezichthouders. ENSIA is daarnaast een leerinstrument dat ons als organisatie in staat stelt én de ruimte biedt om iteratief te leren en continu te verbeteren.

I. Resultaten ENSIA 2024

Het college is akkoord gegaan met de resultaten voor ENSIA 2024

Het college heeft besloten akkoord te gaan met de resultaten. Als gevolg hiervan is ook akkoord gegaan met het uitvoeren van verbeteringen van de tekortkomingen en het uitvoeren van een her-audit. De resultaten hiervan volgen in een volgende brief.

Het verbeterplan is inmiddels gestart

De verbetermaatregelen zijn belegd en worden gemonitord. Deze verbeteringen zijn noodzakelijk om ENSIA 2024 af te ronden en bieden kansen voor een effectief 2025 traject.

De IT-auditor heeft zijn definitieve Assurancerapport afgegeven met positieve formulering

Hierdoor bestaat een redelijke mate van zekerheid dat de informatie in de collegeverklaring betrouwbaar is voor de DigiD en Suwinet evaluatie. De rest is niet audit plichtig.

De gemeente heeft zich succesvol verantwoord bij de centrale toezichthouders en heeft hiermee aan de wettelijke verplichting om verantwoording af te leggen voldaan.

De resultaten zijn overwegend positief, maar onderstrepen het belang van blijvende alertheid, opvolging en voortdurende aandacht

We voldoen niet aan alle normen binnen onze eigen organisatie. Ook staan de prestaties van een aantal processen onder druk. Deze voldoen weliswaar aan de norm, maar bewegen zich naar de ondergrens. Anderzijds hebben we op onderdelen verbetering van voorgaande jaren vast weten te houden. Om goed resultaat te blijven behalen en naleving met huidige & toekomstige kaders te garanderen is voortdurende aandacht en proactieve verbetering noodzakelijk. Naleving van de kaders beheerst onze digitale veiligheidsrisico's en waarborgt onze dienstverlening en bedrijfsvoering. Onderstaande tabel inventariseert de resultaten ENSIA 2024 op bestuurlijke hoofdlijnen. Voor meer detail, zie bijlage 1 & 2.

Tabel 1: Resultaten ENSIA 2024 op hoofdlijnen

ENSIA onderdeel	Onderwerp	Score	Toelichting
	DigiD		Niet alle aansluitingen voldoen aan alle verplichte normen. Verbetertraject en her-audit is noodzakelijk.
	Burgerzaken		Voldoet niet op sommige verplichte normen.
	Belastingbalie		Goede score op alle verplichte normen.
	Zaaksysteem		Voldoet niet op sommige verplichte normen.
	Zaaksysteem2		Dit jaar niet verantwoordingsplichtig. Om volgend jaar voldoende te scoren moeten stappen gezet worden.
	Suwinet		Goede score voor alle onderdelen op alle normen. De prognose voor volgend jaar is positief.
	GEO-basisregistraties		Alle onderdelen scoren dit jaar voldoende.
	BAG		Voldoende, maar proactieve verbetering noodzakelijk. Beweging naar ondergrens toe. Aanzienlijke daling in prestaties op proces & organisatie. Risico voor kwaliteit dienstverlening en beleidsvorming.
	BGT		Scoort al jaren op rij perfect.
	BRO		Voldoende, maar proactieve verbetering noodzakelijk. Ondergrens bijna bereikt. Prestaties op proces & organisatie gedaald naar onder de norm. Risico voor kwaliteit dienstverlening en beleidsvorming.
	BRP & Reisdocumenten		Score in lijn met landelijke gemiddelde.
	BRP		Voldoende, maar sub thema: naleving, scoort lager dan rest. Reden voor monitoren en op termijn verbeteren.
	Reisdocumenten		Voldoende, maar sub thema: naleving, scoort lager dan rest. Reden voor monitoren en op termijn verbeteren.
	Baseline informatiebeveiliging (BIO)		Richt zich niet uitsluitend op de ENSIA scope, maar gemeente brede implementatie van de BIO (alle

& Verhogen Digitale Weerbaarheid (VDW)		gemeentelijke processen en systemen). Score binnen ENSIA scope is veelal voldoende. Score buiten ENSIA scope is regelmatig onvoldoende. Risico voor kwaliteit & continuïteit dienstverlening en bedrijfsvoering.
--	---	--

Planning ENSIA 2025

Verbeterplannen ENSIA 2024 vormen de basis voor succes in 2025

Om het verantwoordingstraject voor 2025 succesvol af te ronden worden de verbeterplannen van 2024 verwerkt in het plan van aanpak voor 2025. Op deze manier leren we van het voorgaande jaar, verbeteren we, en wordt het gehele proces effectiever en efficiënter. De verbeteringen voor DigiD betreffen identificatie- & authenticatiebeheer, wijzigingsbeheer en incidentbeheer. Verbeteringen van de GEO-basisregistraties BAG en BRO staan in het teken van de kwaliteit van registraties en onze interne processen & organisatie daaromheen.

De beschreven activiteiten in de paragrafen hieronder hebben als doel het bijdragen aan de doelstellingen voor digitale veiligheid, alsmede het verzorgen van naleving aan de kaders waaronder ENSIA. Náást de verbeteringen, moet ook het niveau en de kwaliteit van de nu voldoende beoordeelde structurele taken worden vastgehouden.

II. Cybersecurity & informatiebeveiliging

Goede cybersecurity, informatiebeveiliging en privacy vereist inzet bovenop ENSIA

Het totale kader voor digitale veiligheid is groter dan wat binnen de scope van ENSIA valt (zie tabel 1 BIO & VDW). Daarnaast is de implementatie van dit totale kader vereist voor een scope van gemeentelijke processen, organisatie en systemen breder waar ENSIA op focust.

Binnen de scope van ENSIA is de gemeente goed op weg met de informatiebeveiliging en gegevensbescherming. Deze kennis en kunde kan uitgebreid - & breder toegepast worden en de controle hierop gelijkwaardig ingericht worden om gemeente breed de passende implementatie van het totale kader te verzorgen.

Enkele basiszaken moeten nog aangepakt worden en verdere ontwikkeling is noodzakelijk om informatiebeveiliging te kunnen managen, bovenop de huidige goede prestaties

De gemeente heeft de afgelopen jaren zeker niet stilgezeten. Er is al veel bereikt op het versterken van de digitale veiligheid. De wereld om ons heen zit helaas ook niet stil. Risico's trekken aan en aanvullende wettelijke verplichtingen komen onze kant op. Om mee te kunnen komen is het noodzakelijk een goed management systeem werkend te krijgen. De verschillende initiatieven hier rondom moeten nog één werkend geheel gaan vormen.

De strategie is gericht op het realiseren van een gepast werkend ISMS

Het operationeel krijgen van een goed management systeem voor informatiebeveiliging helpt ons naar een systematische aanpak voor het risico gebaseerd managen van informatiebeveiliging in het teken van continu verbeteren. Vanuit daar kunnen we voldoen aan de basis van de normen en doorwerken naar optimalisatie.

Dit helpt ons ook aan huidige & toekomstige kaders te voldoen. Denk hierbij aan de cyberbeveiligingswet (Cbw) die vanuit de Europese NIS2 richtlijn dit jaar wettelijk verplicht wordt, alsmede het bredere programma Digital Decade. Het maakt het voldoen aan huidige kaders makkelijker en efficiënter.

De raadsinformatiebrief wordt standaard onderdeel van de governance van digitale veiligheid

In control zijn van digitale veiligheid vereist dat het te besturen en te managen is. Het ISMS helpt daarbij. Onderdeel van goede governance van digitale veiligheid betreft de

verantwoordingsstructuren, waar bestuurlijke rapportage een thema is. Daarom gaan wij vaker rapporteren over digitale veiligheid náást enkel de verplichte rapportages.

III. Privacy

Privacy vereist ook uitwerking van basiszaken en verdere aandacht om te waarborgen

Uit het jaarverslag van de functionaris gegevensbescherming (FG) blijkt dat de gemeente al goed op weg is, maar blijvende alertheid, opvolging en voortdurende aandacht noodzakelijk zijn om volledig aan het wettelijke kader te kunnen gaan voldoen. In de geplande toekomstige raadsinformatiebrieven wordt uitgebreider gerapporteerd over de status en voortgang van privacy, zodat ook hier effectiever toezicht op gehouden kan worden.

Beveiligingsbewustzijn, training & opleiding

Belangrijk onderdeel van digitale veiligheid is beveiligingsbewustzijn

Wij hebben als gemeente een security awareness programma. Dit programma is nu nog ingericht op het verzorgen van de basis. De strategie is om het programma, naarmate onze risico management processen meer volwassen zijn in lijn met het ISMS, vorm te geven naar gelang de specifieke context en risico's van de gemeente. Dit houdt ook in dat we op rol en functie gebaseerde awareness gaan verzorgen.

Vervolg & ambitie

Deze rapportage is onderdeel van de strategie om digitale veiligheid structureel bestuurlijk onder de aandacht te houden en de raad in stelling te brengen digitale veiligheid te versterken

De organisatie is van plan periodiek over de integrale thema's binnen digitale veiligheid te rapporteren, afgestemd op de doelgroep (niveau). Het doel is effectieve besturing & management van digitale veiligheid te faciliteren, een belangrijk onderdeel van onze visie op control.

Door periodiek te rapporteren wordt invulling gegeven aan de ambitie om digitale veiligheid als vast onderdeel van het bestuurlijk afwegingskader te positioneren. Hierbij zullen ten minste de volgende thema's aan bod komen:

- Uitslagen van risico management & analyse
- Ontwikkelingen rondom interne & externe incidenten (cyber, informatie, privacy) en bedrijfscontinuïteitskwesties
- Veranderende context zoals wetgeving & risico's, maar ook maatschappelijke invloeden en technologische ontwikkelingen
- Concern rapportage waaronder het behalen van gestelde doelen t.o.v. gealloceerd budget
- Resultaten, status & voortgang van CS, IB en privacy gerelateerde projecten en initiatieven
- Uitslagen van de voornaamste CS, IB en privacy management processen
- Resultaten van interne audits omtrent CS, IB en privacy.
- Resultaten van verantwoordingstrajecten zoals ENSIA en externe audits zoals Wpg.
- Resultaten, status & voortgang van CS, IB en privacy beleidsontwikkeling- en implementatie proces.
- Security awareness trajecten.
- Ontwikkelingen rondom interne veranderende technische context
- Uitslagen van de jaarverslagen CISO en FG.

Uiteindelijk moet dit de raad in stelling brengen de juiste kaders te kunnen stellen om het versterken van de digitale veiligheid binnen de gemeente te faciliteren. Hierdoor verbeteren we onze veiligheid en vanuit daar voldoen we beter aan de kaders.

De raad kan concreet bijdragen aan het versterken van digitale veiligheid

De raad heeft invloed via haar kaderstellende, controlerende en volksvertegenwoordigende rol. In het vaststellen van de kaders voor digitale veiligheid kan ze de spelregels bepalen en doelstellingen formuleren & prioriteren. Daarnaast houdt de raad via haar controlerende functie toezicht, op basis van rapportages en audits over de voortgang van BIO naleving en ISMS prestaties náást het verplichte ENSIA kader. Vanuit deze wisselwerking kan ze middelen beschikbaar stellen (en daarmee prioriteiten vastleggen) om maatregelen uit te voeren en verbeteringen door te voeren. Via haar volksvertegenwoordigende rol kan ze aandacht vragen voor digitale veiligheid en gerelateerde zorgen uit de samenleving signaleren.rol kan ze aandacht vragen voor digitale veiligheid en gerelateerde zorgen uit de samenleving signaleren.

De resultaten van de verbeterplannen ENSIA 2024 volgen

Over de status, voortgang en resultaten van ENSIA 2024 en 2025 wordt gerapporteerd in de volgende raadsinformatiebrief.

Bijlagen

1. Vastgestelde Collegeverklaring ENSIA 2024
2. Besluitenlijst Collegevergadering openbaar 22 april 2025
3. Assurance rapport ENSIA 2024

Met vriendelijke groet,
Burgemeester en wethouders van Rheden,



Carol van Eert,
burgemeester



Bart Drewes,
gemeentesecretaris