gemeente
Haarlemmermeer

De leden van de gemeenteraad van Haarlemmermeer

Postbus 250
2130 AG Hoofddorp

Bezoekadres:
Taurusavenue 100
Hoofddorp
Telefoon 0900 1852

Verzenddatum
22 SEP. 2026

Cluster Concerncontrol
Inlichtingen Arjen van der Meulen
Telefoon +31235677470
Uw brief
Ons kenmerk XS-26091709.2800
Bijlage(n) Bijlage 1 - Voortgangsrapportage IAF - Eerste en tweede kwartaal 2026 (Bestuurlijke samenvatting)
Onderwerp Voortgangsrapportage Interne Auditfunctie – Auditjaarplan 2026 (eerste halfjaar)

Geachte heer, mevrouw,

Hierbij informeren wij de raad over de voortgang van de uitvoering van het Auditjaarplan 2026 in de eerste helft van dit jaar. Het bijgevoegd document bevat de bestuurlijke samenvatting van de voortgangsrapportage van de interne auditfunctie (IAF). De IAF is de onafhankelijke onderzoeksfunctie binnen de gemeente en onderzoekt of processen, risicobeheersing en governance toereikend functioneren en geeft hierover inzicht en advies aan directie en college. De voortgangsrapportage geeft inzicht in de resultaten en voortgang van de interne audits en onderzoeken, de belangrijkste bestuurlijk relevante uitkomsten en de ontwikkeling van de IAF.

Vanaf 2026 wordt afzonderlijk gerapporteerd over de IAF en de verbijzonderde interne controle, omdat beide disciplines een eigen planning en informatiebehoefte kennen. De IAF rapporteert voortaan halfjaarlijks; het college, de raad en de auditcommissie ontvangen daarbij de bestuurlijke samenvatting.

Wij verwachten u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
burgemeester en wethouders van de gemeente Haarlemmermeer,
de secretaris, de burgemeester,

Hermineke van Bockxmeer Marianne Schuurmans-Wijdeven



Voortgangsrapportage IAF
Eerste en tweede kwartaal 2026

Versie: Definitief (Bestuurlijke samenvatting)
02-09-2026

Cluster Concerncontrol

Interne Auditfunctie (IAF)

gemeente Haarlemmermeer

Managementsamenvatting

Conclusies beheersing audits en onderzoeken

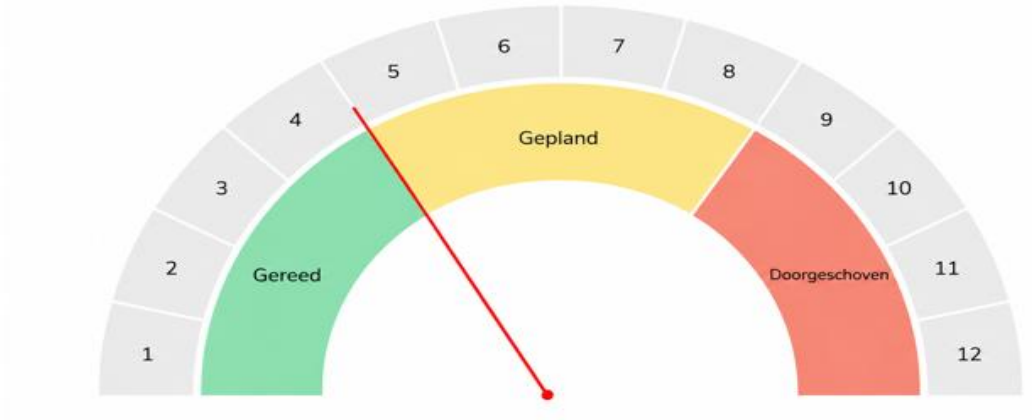
Onderwerp	Verantwoordelijkheid	Risicobeheersing
*Wpg-audit 2024 *Doorloopaudit 2025*	*Bestuurlijke; wettelijk verplichte audit*	
*BIO-audit 2025 *Doorloopaudit 2025*	*Bestuurlijk; wettelijk verplichte audit*	
213a-onderzoek - *Prestatielevering in de zorg (AJP 2026 - 1)*	*Bestuurlijk; verordening gebonden (213a)*	
Bestellen t/m Betalen - *Verlagen inkooporder grens (AJP 2026 - 10)*	*Organisatorisch; raakt aan interne bedrijfsvoering*	*Adviesopdracht*
** **Maatschappelijke Pas -** *Prepaid dienstverlening BNG Bank*	*Organisatorisch; raakt aan interne bedrijfsvoering*	
** **Telefonische dienstverlening -** *Pilot soft controls*	*Organisatorisch; raakt aan interne bedrijfsvoering*	*Adviesopdracht*

* *WPG staat voor De Wet politiegegevens en BIO staat voor Baseline Informatiebeveiliging Overheid*

** *Deze audits of onderzoeken betreffen overige werkzaamheden. Zij vallen buiten de scope van het Auditjaarplan (AJP) 2026 en zijn daarom niet opgenomen in de voortgangsmeter hiernaast.*

Legenda: Risicobeheersing is goed | Risicobeheersing kent aandachtspunten | Risicobeheersing is onvoldoende | Geen conclusie over risicobeheersing

Voortgang audits en onderzoeken Q1 en Q2 (AJP 2026)



Tot en met Q2 2026 zijn 4 audits en onderzoeken afgerond, 4 zijn gepland en 4 zijn doorgeschoven.



Lichtpunten

- ✓ Auditjaarplan 2026 is conform plan opgesteld (risk-based) en op 3 februari 2026 vastgesteld door het college van B&W.
- ✓ Auditbesluit 2026 is opgesteld voor de inrichting van de interne auditfunctie en op 1 september vastgesteld door het college van B&W.
- ✓ Per 1 juni 2026 zijn twee nieuwe auditors gestart binnen cluster CC, waarmee de benodigde capaciteit is versterkt.

Belangrijkste bevindingen

Wpg-audit 2024 *Doorloopaudit 2025*	Afkeurend oordeel en verhoogde risico's rond datalekken, autorisaties en rechtmatige verwerking.
BIO-audit 2025 *Doorloopaudit 2025*	Positieve ontwikkeling zichtbaar, maar nog kwetsbaarheden in leveranciersbeheersing, uniforme werkwijzen en eigenaarschap.
213a-onderzoek - *Prestatielevering in de zorg (AJP 2026 - 1)*	Toezicht is grotendeels doelmatig ingericht, maar borging Wmo en structurele kwaliteitsmonitoring kennen verbeterpunten.
Bestellen t/m Betalen - *Verlagen inkooporder grens (AJP 2026 - 10)*	Aandachtspunten rondom naleving, procesdiscipline, uitvoerbaarheid en eigenaarschap (soft controls) én het vooraf concretiseren van beoogde effecten (meetbaar maken) voor een zorgvuldig proces.
* **Maatschappelijke Pas -** *Prepaid dienstverlening BNG Bank*	Bij de identificatie van één maatschappelijke pas is gebruik gemaakt van een verlopen identiteitsdocument.
* **Telefonische dienstverlening -** *Pilot soft controls*	De pilot bevestigt de meerwaarde van de softcontrolmethodiek; de directie heeft besloten deze breder in te zetten.

Het management onderschrijft bovenstaande bevindingen en zet in op opvolging van verbeterpunten.

1. Voortgang Auditjaarplan 2026 (I)

1.1 Voortgang Auditjaarplan 2026

Deze voortgangsrapportage (verkorte versie) geeft inzicht in de resultaten en voortgang van de interne audits en onderzoeken conform het Auditjaarplan 2026. Daarnaast rapporteren wij over de resultaten van afgeronde audits- en onderzoeken vanuit bestuurlijke verantwoordelijkheid, én de ontwikkeling van de interne auditfunctie. Hiermee ondersteunen wij de directie en het college bij het versterken van governance, risicomanagement en interne beheersing.

1.2 Resultaten afgeronde interne audits- en onderzoeken *(vanuit bestuurlijke verantwoordelijkheid)*

De belangrijkste resultaten hebben betrekking op:

- **Audit Wet Politiegegevens - (2024 - Extern)** *(Doorloopaudit 2025)*
  De Wet politiegegevens (Wpg) is van toepassing op de verwerking van politiegegevens door buitengewoon opsporingsambtenaren (boa's) en schrijft voor dat gemeenten eenmaal per vier jaar een externe privacy audit uitvoeren. Hiermee wordt vastgesteld in hoeverre wordt voldaan aan de wettelijke eisen voor de rechtmatige en veilige verwerking van politiegegevens. Deze audit heeft geresulteerd in een afkeurend oordeel. Hoewel ten opzichte van eerdere interne audits vooruitgang zichtbaar is binnen verschillende domeinen, onderstreept de huidige uitkomst dat verdere verbetering noodzakelijk blijft. Als gemeente lopen wij door de geconstateerde tekortkomingen een aantoonbaar verhoogd risico op incidenten rondom politiegegevens. Dit uit zich op meerdere niveaus: datalekken en informatiebeveiliging, misbruik en onrechtmatige inzage, verwerking en verstrekking. Het afkeurend oordeel vraagt om bestuurlijke prioritering en actieve sturing op een tijdgebonden verbeterplan, zodat tekortkomingen voortvarend worden hersteld en naleving van de Wpg aantoonbaar wordt geborgd. In november 2026 vindt onder coördinatie van cluster Concerncontrol een hercontrole plaats om vast te stellen in hoeverre de tekortkomingen zijn opgevolgd. De resultaten worden gerapporteerd aan directie, college en de Autoriteit Persoonsgegevens (AP).

- **Audit Baseline Informatiebeveiliging Overheid (BIO)** *(Doorloopaudit 2025)*
  De gemeente legt via ENSIA (Eenduidige Normatiek Single Information Audit) jaarlijks verantwoording af over informatiebeveiliging en privacy van specifieke aansluitingen. De BIO-audit beoordeelt in hoeverre de onderliggende informatiebeveiliging van de gemeente op orde is en vormt daarmee een belangrijke basis voor een betrouwbare ENSIA-verantwoording. Binnen de audit is tevens aandacht besteed aan Verhogen Digitale Weerbaarheid (VDW), waarbij de bevindingen zijn vertaald naar de bredere vraag in hoeverre de gemeente weerbaar is tegen digitale dreigingen. De BIO 1.04 volwassenheidsscore laat een positieve ontwikkeling zien: van 1,3 (2023) naar 1,7 (2024) en 2,0–2,44 in 2025, richting het gemeentelijke streefniveau van 3,0. De audit constateert positieve ontwikkelingen in de borging en aantoonbaarheid van beheersmaatregelen en in de continue monitoring op digitale incidenten. Tegelijkertijd signaleert de audit kwetsbaarheden met betrekking tot: onvoldoende grip op externe leveranciers (keten) en verschillen in werkwijzen tussen clusters waardoor beveiliging niet overal uniform wordt toegepast en organisatie breed niet altijd aantoonbaar in control wordt gewerkt. De CISO signaleert daarnaast dat verantwoordelijkheden voor informatiebeveiliging en de vertaling van BIO-normen naar de praktijk niet overal voldoende duidelijk zijn en de verdeling van de normen (en bijbehorende maatregelen) niet overal aansluiten op de feitelijke verantwoordelijkheden. Dit vraagt bestuurlijk om verduidelijking en mogelijk ook herziening van rollen en verwachtingen, mede in het licht van de overgang naar BIO 2.0 (uitwerking van de zorgplicht uit de Cyberbeveiligingswet (Cbw).

- **213a-onderzoek - Toezicht op prestatielevering in de zorg** *(AJP 2026 – 1)*
  Het onderzoek richtte zich op de doelmatigheid en doeltreffendheid van het huidige toezicht, mede in vergelijking met andere gemeenten. Belangrijkste conclusie is dat de organisatie het toezicht over het algemeen doelmatig is ingericht en op onderdelen efficiënter opereert dan vergelijkbare gemeenten. Verbeterpunten liggen bij het toezicht op prestaties binnen de Wmo en de structurele monitoring en vastlegging van zorgkwaliteit.

1. Voortgang Auditjaarplan 2026 (II)

1.3 Herijking Auditjaarplan 2026

De interne audit- en onderzoeksonderwerpen uit het Auditjaarplan 2026 zijn, in overleg met de lijnorganisatie, herijkt en opnieuw beoordeeld op urgentie en haalbaarheid in relatie tot de beschikbare audit capaciteit. Op basis van de herijking worden de volgende interne audits- en onderzoeken *doorgeschoven* naar Auditjaarplan 2027:

- **Audit Leveranciersmanagement** *(AJP 2026 – 2)*
  De BIO-audit 2025 heeft dit onderwerp reeds geraakt. Daarbij zijn bevindingen geconstateerd op het gebied van leveranciersmanagement, die nog opvolging vragen. Gelet op de beperkte aanvullende meerwaarde in 2026 is besloten deze audit door te schuiven naar het Auditjaarplan 2027.

- **Audit Beheer van Logische Toegangsbeveiliging** *(AJP 2026 – 3)*
  Op dit onderdeel is recent beleid vastgesteld en de implementatie is momenteel gaande. Gelet op deze ontwikkeling wordt een interne audit in 2026 als te vroeg beschouwd en is besloten deze audit door te schuiven naar het Auditjaarplan 2027.

- **Audit Databeheer** *(AJP 2026 – 4)*
  De clusters werken momenteel aan de actualisatie van informatiebeheerplannen, naar aanleiding van bevindingen van de archiefinspectie en provincie in het kader van interbestuurlijke toezicht. Een audit in 2026 wordt qua timing niet passend geacht. In 2027 kan de audit meer inzicht geven in de mate waarin een actueel en volledig totaaloverzicht van decentraal beheerde informatie beschikbaar is.

- **Audit Beheer Basisregistratie Personen** *(AJP 2026 – 9)*
  De belangrijkste risico-invalshoek ligt bij de organisatie brede toegang tot BRP-gegevens via andere organisatieonderdelen en applicaties. De auditee wenst eerst zelf na te gaan welke koppelingen gebaseerd zijn op een zorgvuldige afweging. Gelet op deze behoefte is besloten deze audit door te schuiven naar het Auditjaarplan 2027.

De volgende audits zijn *gepland* ter uitvoering in 2026:

- **Audit Wet politiegegevens - (2025 intern + hercontrole)** *(AJP 2026 – 5)*
  In 2026 vindt de hercontrole plaats in het kader van afkeurend oordeel Wpg-audit 2024. Daarnaast vindt een interne audit plaats m.b.t. controlejaar 2025.

- **Audit - Beveiliging van informatie en informatiesystemen** *(AJP 2026 – 6)*
  In 2026 voert de IAF een pré-audit uit op de DigiD en SuwiNet aansluitingen, waarbij de externe IT-auditor (RE) verantwoordelijk blijft voor het assurance-oordeel.

- **Audit - Beheer van het verwerkingsregister (AVG)** *(AJP 2026 – 7)*
  Deze audit is verschoven naar Q4 2026 op verzoek van de auditee.

- **Audit - Conflicterende belangen in projecten** *(AJP 2026 – 8)*
  Deze audit is verschoven naar Q4 2026 vanwege beschikbare capaciteit IAF.

1.4 Vooruitblik

Soft controls in interne audits
Soft controls worden nadrukkelijker meegenomen in audits, naast hard controls. Hiermee wordt gekeken naar gedrags- en cultuurfactoren die risicobeheersing beïnvloeden. Dit helpt om beter te begrijpen waarom processen in de praktijk wel of niet goed werken.

Monitor opvolging audit aanbevelingen
Cluster Concerncontrol verkent momenteel de mogelijkheden voor een integraal GRC-tool. In Q3/Q4 wordt onderzocht of statusinformatie (over eerder uitgevoerde interne audits) bij proceseigenaren kan worden opgehaald. Follow-up audits worden naar verwachting vanaf 2027 uitgevoerd.

Missie – Interne Auditfunctie
Ons missie: *“Wij zijn de sportarts die de fitheid van processen beoordeelt en stimuleert in continue verbeteren”*. Wij zullen verkennen hoe we het auditlandschap binnen de gemeente inzichtelijker kunnen maken.

2. Kwaliteit van de Interne Auditfunctie

2.1 Onafhankelijkheid en naleving van de GIAS
De onafhankelijke positionering van de interne auditfunctie (IAF) is geborgd en er zijn geen incidenten bekend die deze hebben aangetast. De IAF sluit zoveel mogelijk aan bij de Global Internal Audit Standards (GIAS); volledige conformiteit is vanwege de ontwikkelfase nog niet gegarandeerd.

2.2 Programma voor kwaliteitsboring- en verbetering
Het programma voor kwaliteitsborging en -verbetering is in ontwikkeling. Auditwerkzaamheden worden intern gereviewd en zichtbaar vastgelegd. Externe peer reviews en kwaliteitstoetsingen hebben nog niet plaatsgevonden.

2.3 Stappen in verdere professionalisering
Het Auditbesluit 2026 (ook wel Auditcharter genoemd) vormt het strategisch fundament voor de positionering, taken en bevoegdheden van de IAF. Feedback op uitgevoerde audits wordt gebruikt om de werkwijze, het audithandboek en de kwaliteitsborging verder te verbeteren. Met de komst van twee auditors is de IAF verder versterkt. Capaciteit blijft vanwege de ontwikkelfase een aandachtspunt en wordt daarom risicogericht ingezet.

2.4 Randvoorwaarden effectieve interne auditfunctie
De effectiviteit van de interne auditfunctie hangt samen met deskundigheid, onafhankelijkheid, onbelemmerde toegang tot informatie, voldoende capaciteit, een risicogericht auditjaarplan en transparante rapportage. Via het Auditbesluit, het Auditjaarplan en de verdere professionalisering wordt stapsgewijs invulling gegeven aan de randvoorwaarden voor een effectieve IAF.

2.5 Externe ontwikkelingen en impact op de IAF
Cybersecurity, digitalisering en AI beïnvloeden het risicolandschap en de auditprioriteiten. Deze ontwikkelingen zijn onderdeel van het auditjaarplan-traject en de herijking van het AJP. Ook zoeken wij afstemming met stakeholders binnen en buiten de organisatie om beter te duiden wat dit betekent voor onze rol, prioriteiten en werkwijze.

