Gemeente Amsterdam

Raadsinformatiebrief

Aan:	De leden van de gemeenteraad van Amsterdam
Datum	22 oktober 2024
Portefeuille(s)	ICT en Digitale Stad
Portefeuillehouder(s):	Wethouder Scholtes
Behandeld door	Cluster Digitalisering, Innovatie en Informatie, Sigrid Winkel, Bestuurszaken.DII@Amsterdam.nl
Onderwerp	Voortgangsbrief aanbevelingen I-domein

Geachte leden van de gemeenteraad,

Periodiek wordt in de commissie FKD de voortgang van de aanbevelingen voor het i-domein van de ACAM, de Rekeningencommissie en de Rekenkamer behandeld aan de hand van een ‘voortgangsbrief’. Dat is de brief die nu voorligt. Het betreft de aanbevelingen voor het informatie domein met betrekking tot de portefeuille ICT en Digitale Stad. De raad wordt separaat geïnformeerd over de aanbeveling van de Rekenkamer over het ‘Openbaar maken van overheidsinformatie in Amsterdam’ door de portefeuillehouder Algemene Zaken en over de aanbeveling van de Rekenkamer over de ‘Participatieparagraaf’ door de portefeuillehouder Democratisering.

Groepering naar onderwerpen
De afgelopen jaren zijn er over zes onderwerpen aanbevelingen gedaan door de ACAM, de Rekeningencommissie en/of de Rekenkamer. De voortgang wordt gemonitord in het gemeentelijk risicomanagementsysteem *Fully in Control*. Ten behoeve van de overzichtelijkheid zijn de aanbevelingen hier gegroepeerd naar onderwerp, te weten:

1 Algoritmen
2 Autorisatiebeheer
3 Business Continuity Management
4 Datacenter
5 SaaS-applicaties
6 Wet- en regelgeving, compliancy.

Hieronder treft u per onderwerp de diverse aanbevelingen, en daaronder de duiding en de stand van zaken.

1. Algoritmen

Aanbeveling
Dit betreft een aanbeveling van de Rekenkamer uit 2023:
1 Bevorder toepassing van het beheerskader in de praktijk
2 Verbeter de omgang met bias
3 Wees opener en transparanter over het gebruik van algoritmen
4 Blijf het beheerskader ontwikkelen met inachtneming van nieuwe kennis
5 Breng de privacybescherming van burgers bij algoritmen op orde

Stand van zaken
De aanbevelingen zijn verwerkt in het Plan van aanpak Algoritmen. Dit plan is goedgekeurd in het College en in mei 2024 besproken in de commissie FKD. De uitvoering vindt plaats tot en met 2026 (één actiepunt loopt tot begin 2027). Er zal jaarlijks in het eerste kwartaal worden gerapporteerd over de voortgang van het plan van aanpak. Ik zal de commissie hierover informeren.

Afhandeling
Het plan van aanpak – en daarmee de aanbevelingen – wordt grotendeels in 2026 afgerond.

2. Autorisatiebeheer

Aanbeveling
ACAM en Rekeningencommissie hebben diverse aanbevelingen gedaan over autorisatiebeheer. Actueel zijn de aanbevelingen van ACAM bij de jaarrekening 2023:

Autorisatiebeheer van applicaties in scope jaarrekeningcontrole: Wij vragen er aandacht voor dat:
1 De periodieke controle in 2024 in lijn met de BIO wordt uitgevoerd, dat is (minimaal) twee keer per jaar.
2 De periodieke controle van uitgegeven speciale rechten, eveneens in lijn met de BIO, per kwartaal wordt uitgevoerd.
3 De monitoring op ongewenste functievermenging in lijn met de BIO wordt uitgevoerd.

Toelichting
Autorisatiebeheer is het ervoor zorgen dat medewerkers gebruik kunnen maken van de applicaties die zij voor hun werk nodig hebben, en dat die toegang gestopt wordt als het (door uit- of doorstroom) niet meer nodig is. Dat vereist nauwe samenwerking tussen de lijn (die bepaalt welke medewerkers welke toegang tot welke applicaties moeten hebben) en het I-domein (dat de toegangsrechten per gebruiker technisch inregelt).

De BIO bepaalt dat de autorisaties periodiek gecontroleerd moeten worden: minstens twee keer per jaar voor alle gebruikers, en per kwartaal voor de speciale rechten, zoals die voor systeembeheerders. Daarnaast wordt autorisatiebeheer ingezet om functievermenging te voorkomen.

Stand van zaken
- Alle aanbevelingen zijn opgepakt.
- De periodieke controles autorisatiebeheer zijn in het eerste half jaar voor 80% uitgevoerd. Gestuurd wordt op afronding van de bij de jaarrekening betrokken applicaties per eind dit jaar. Voor alle applicaties duurt dit langer en wordt afronding verwacht in het tweede kwartaal van 2025.
- Vanuit het i-domein wordt actief gemonitord op de realisatie van de toegangscontrole.
- Het uitvoeren van periodieke controles, in lijn met de BIO, is nu geborgd in de beheerprocessen.
- Een dashboard is gemaakt om voortgang te bewaken en hierover periodiek te rapporteren vanuit de taskforce aan de stuurgroep aanbevelingen.
- De doelstelling is dat in ieder geval alle door de ACAM aangedragen applicaties die het financiële beheersingsproces raken eind dit jaar 100% scoren. Voor de overige applicaties wordt dit in 2025 gerealiseerd.
- Voor het behalen van deze doelstelling is een taskforce ingericht.

Afhandeling
Naar verwachting kan de aanbeveling in het tweede kwartaal van 2025 worden afgerond. Dit vindt altijd in overleg met ACAM plaats zodat de maatregelen in lijn zijn met de ACAM-aanbevelingen.

3. Business Continuity Management

Aanbeveling
ACAM en Rekeningencommissie hebben sinds 2020 diverse aanbevelingen gedaan over BCM. Actueel is de aanbeveling van de Rekeningencommissie bij de jaarrekening van 2023:
1 Beleid ten aanzien van BCM in 2024 verder te concretiseren
2 De verantwoordelijkheid voor BCM breder te beleggen in het managementteam vanuit de coördinatie bedrijfsvoering
3 De impact van potentiële risico's te bepalen (business impact analyses) en vanuit de vastgestelde kernprocessen BCM in te richten voor de organisatie

Toelichting
Bedrijfscontinuïteitsmanagement (BCM) is de voorbereiding die de organisatie in staat stelt om, in geval van een verstoring, haar kritische diensten te blijven leveren.

De aanbeveling ad. 2 heeft het college niet overgenomen. Er is voor gekozen de stelselcoördinatie van BCM te beleggen bij de stedelijk directeur Digitalisering, Innovatie en Informatie, in samenwerking met de Concerncontroller. Daarnaast wordt BCM regelmatig besproken in het GMT, waardoor de verantwoordelijkheid breed is belegd.

Stand van zaken

- Op basis van de startnotitie van vorig jaar is het beleid verder geconcretiseerd in een beleidskader, dat naar verwachting in het vierde kwartaal van 2024 wordt vastgesteld.
- De prioriteit van de aanpak ligt op de stedelijke kernprocessen met de meeste impact op bewoners, ondernemers en bezoekers van Amsterdam.
- De aanpak houdt in dat er per directie een bedrijfscontinuïteitsplan wordt opgesteld. Daarin zijn een business impact analyse en de implementatie van mitigerende maatregelen opgenomen. Jaarlijks wordt een continuïteitsoefening georganiseerd, waarbij het plan, de noodoplossingen en de taakverdeling worden getest.
- Bij de impactanalyse wordt ook bekeken wat de impact is van het uitvallen van ketenpartners/leveranciers en welke afspraken daar dan dus mee gemaakt moeten worden in het kader van continuïteit.
- Een eerste uitwerking van BCM is gedaan met drie organisatieonderdelen: de GGD, Verkeer en Openbare Ruimte en Afval en Grondstoffen.
- Inmiddels zijn bij een zevental directies continuïteitsoefeningen gehouden. Bij nog eens 13 directies zijn de voorbereidingen hiervoor gestart. Dat maakt dat er in het derde kwartaal van 2024 bij de voor de continuïteit belangrijkste kernprocessen van de organisatie actief gewerkt wordt om de weerbaarheid te verhogen.

Afhandeling

Zoals aangegeven wordt eind 2024 BCM toegepast bij de directies die verantwoordelijk zijn voor de geselecteerde kernprocessen. Dit wordt in 2025 afgerond. Dan wordt ook bezien hoe BCM bij de overige directies kan worden ingezet. Er zal jaarlijks over de voortgang van BCM worden gerapporteerd via het jaarverslag van de Chief Information Security Officer (CISO).

4. Datacenter

Aanbeveling

Dit betreft een aanbeveling van ACAM van 2021:
Afbouw Datacenter 1 (DC1) loopt en kan nog niet volledig worden afgerond

1 Afbouw Datacenter-1 nog niet volledig afgerond (Erfpacht)
2 Uitwijkvoorzieningen voor resterende applicaties Datacenter-1
3 Aandacht voor lifecycle management

Stand van zaken

De afbouw van Datacenter 1 heeft geruime tijd geduurd, met name door complicaties met de erfpachtapplicatie en met de Amsterdamse Digitale Werkplek (ADW). Bij Erfpacht liep een nieuwbouwproject en zolang dat liep kon de oude erfpachtapplicatie niet aangepast worden. Bij ADW speelde de migratie van het oude naar het nieuwe ADW een rol.

Het derde punt van de aanbeveling met betrekking tot DC1 betrof lifecycle management. Dit is het up-to-date houden van je applicaties door alleen de laatste versies ervan te gebruiken en de applicaties ook tijdig uit te faseren en te vervangen.

Dit is afgehandeld doordat aandacht is/wordt geschonken aan lifecycle management vanuit een drietal programma's:

- Programma DC1 Leeg – Alle applicaties (m.u.v. de Erfpachtsuite) zijn gemigreerd naar Datacenters van KPN. Hierbij zijn oude applicaties uitgezet, vernieuwd of vervangen.
- Programma ADW-nieuw – Alle applicaties zijn waar nodig technisch aangepast (vernieuwd) om ze gereed te maken voor ADW-nieuw. Om dit te realiseren zijn verouderde applicaties eerst geüpdatet om ze 'ADW-klaar' te maken. Voor applicaties waarvoor dit niet meer mogelijk was geldt dat deze zijn uitgezet en een alternatief is aangeboden.
- Programma Toekomstvast en Beheersbaar Applicatielandschap (TBA) – Applicaties die niet in beheer zijn binnen het i-domein worden onder beheer/regie gebracht van Functioneel Beheer. Hierbij wordt gekeken naar de staat van de applicaties in kwestie en worden afspraken gemaakt met de lijnorganisatie over het upgraden van applicaties met een versie N -2 of ouder naar versie N -1, en over het uitfaseren van applicaties.

Afhandeling
De aanpak van lifecycle management voor de applicaties van DC1 is afgehandeld. De afbouw van Datacenter 1 (DC1) nadert nu zijn voltooiing. Er wordt gestuurd op het uitzetten van alle functionaliteit in DC1 in het vierde kwartaal van 2024, en daarbij worden geen complicaties meer verwacht. Het eerste kwartaal van 2025 zal worden gebruikt om het datacenter te ontmantelen.

5. SaaS-applicaties

Aanbeveling
ACAM en Rekeningencommissie hebben sinds 2021 diverse aanbevelingen gedaan over de inzet van Software-as-a-Service (SaaS)-applicaties. Recent zijn de aanbevelingen bij de jaarrekening 2023.

Aanbeveling ACAM:
Assurance-rapportages uitbestede diensten (SaaS-applicaties): Maak gemeentebreed (centraal) inzichtelijk bij welke applicaties de assurance-rapportages er niet zijn en bij welke applicaties deze er wel zijn. De rapportages die er wel zijn dienen jaarlijks te worden beoordeeld door de gemeente, voor rapportages die er niet zijn dienen deze alsnog te worden verkregen.

Aanbevelingen Rekeningencommissie:
Nog onvoldoende voortgang in het inzicht in de risico's met betrekking tot (beheer) SaaS toepassingen:

1 Alle uitbestede diensten in beeld te krijgen en na te gaan of afspraken rondom assurance rapporten zijn gemaakt.
2 De inhoud van de verkregen assurance rapportages jaarlijks te beoordelen en de risico's voor continuïteit, informatiebeveiliging en privacy te identificeren en benodigde acties te formuleren en uit te voeren.
3 Organisatorisch te zorgen voor centraal inzicht op de risico's rondom continuïteit, informatiebeveiliging en privacy ten aanzien van uitbestede diensten, waaronder SaaS-oplossingen.

4 Het college een concreet plan te laten opstellen waarin het tijdspad opvolging aanbevelingen en tussentijdse rapportage over de voortgang worden vastgelegd.

Toelichting
Zowel ACAM als Rekeningencommissie hebben aanbevelingen gedaan over de Software as a Service (Saas) applicaties. SaaS-applicaties draaien bij een leverancier en worden door die leverancier beheerd. Daarbij dient de gemeente te bewaken dat dat beheer conform de gemeentelijke normen en eisen is. Dat gebeurt met ‘assurance-rapportages’, waarmee de leverancier aantoont dat de beheersing van de bedrijfsprocessen op orde is.

Assurance-rapportages worden in opdracht van de leverancier door onafhankelijke auditors opgesteld. Met de leveranciers wordt contractueel vastgelegd dat zij één keer per jaar een assurance-rapportage leveren, dat gebeurt meestal aan het einde van het jaar.

Dit wordt in eerste instantie opgepakt voor alle applicaties die de kritische processen en de financiële beheersprocessen ondersteunen. Dit betreft in Amsterdam nu 89 leveranciers. De assurance-rapportages worden intern beoordeeld en zo nodig worden aanvullende maatregelen getroffen. Dit vindt altijd in overleg met ACAM plaats zodat de maatregelen in lijn zijn met de ACAM-aanbevelingen.

Stand van zaken
Alle aanbevelingen zijn opgepakt. Voor alle SaaS-applicaties die ter ondersteuning van de kritische processen worden gebruikt zijn nu assurance-rapportages opgevraagd bij de leveranciers, de reacties worden vanaf oktober beoordeeld.

Voor de overige applicaties wordt gewerkt aan een meerjarenplan om het opvragen, beoordelen, de risicoregistratie en opvolging op basis van de assurance-rapportages te borgen in het reguliere proces. Dit plan wordt in maart 2025 opgeleverd.

Afhandeling
De beoordeling en het treffen van aanvullende maatregelen naar aanleiding van de assurance-rapportages van de genoemde 89 leveranciers, wordt naar verwachting in het tweede kwartaal van 2025 afgerond. Vervolgens wordt dit een jaarlijkse exercitie.

6. Wet- en regelgeving (compliancy)

Aanbeveling
Over de naleving van wet- en regelgeving i.c. de compliancy hebben ACAM en Rekeningencommissie sinds 2018 een aantal aanbevelingen gedaan. Actueel zijn de aanbevelingen naar aanleiding van het jaarverslag 2023:

ACAM:
- Wij adviseren u de voortgang de BIO, AVG, Wpg, Woo in 2024 te blijven volgen

Rekeningencommissie:

1 De overweging van het bewust niet voldoen aan onderdelen van de geldende wet- en regelgeving systematisch vast te leggen, zodat deze inzichtelijk en uitlegbaar zijn.
2 Over te gaan tot daadwerkelijke implementatie van ontbrekende beheersmaatregelen en de periodieke toetsing op opzet, bestaan en werking van relevante beheersmaatregelen te borgen (BIO).
3 In kaart te brengen welke toekomstige wet- en regelgeving wordt doorgevoerd en processen in te richten om de toekomstige wet- en regelgeving te implementeren.

Toelichting

Bij de digitalisering moet de gemeente voldoen aan een reeks van Europese en landelijke wet- en regelgeving. De belangrijkste zijn:

- De Baseline Informatiebeveiliging Overheid (BIO)
- De Algemene Verordening Gegevensbescherming (AVG)
- De Wet politie gegevens (Wpg)
- De Wet open overheid (Woo).

Stand van zaken

Het college wil de voortgang van de toepassing van deze wetten inderdaad blijven volgen, ook als het om geactualiseerde wet- en regelgeving gaat (zoals BIO-2). Daartoe is het risicomanagementsysteem Fully in Control ingericht. We beschouwen deze ACAM-aanbeveling daarom als gerealiseerd.

De vulling van Fully in Control per directie loopt nu, dat is naar verwachting eind 2024 (informatiebeveiliging) resp. medi0 2025 (privacy) gereed. Voor informatiebeveiliging betreft dit de risico's voortkomend uit de BIO op basis van de verbeterplannen per directie, alsmede de risico's die gesignaleerd worden bij testen en audits. In het laatste kwartaal van 2024 wordt een audit op de BIO uitgevoerd in opdracht van het GMT. Ook de eventuele risico's die hierbij worden gesignaleerd worden in bovenstaande aanpak verwerkt. Bij privacy betreft het de risico's per directie op basis van de Baseline Privacy Amsterdam (BPA), onder andere eisen van de Algemene Verordening Gegevensbescherming (AVG), en de risico's op basis van audits, de Autoriteit Persoonsgegevens en de Functionaris Gegevensbescherming.

Het mitigeren van de risico's is de verantwoordelijkheid van de risico-eigenaar (meestal de eigenaar van het betreffende proces of informatiesysteem). De security officer en de privacy officer ondersteunen en houden de vinger aan de pols.

De risico's per directie worden geaggregeerd tot een stedelijk risicobeeld. Op grond hiervan zullen in het tweede kwartaal van 2025 (informatiebeveiliging) en het eerste kwartaal van 2026 (privacy) nieuwe stedelijke maatregelen voor de mitigatie van de risico's worden voorgesteld. Tevens wordt een aanpak voorgesteld om het stedelijk risicomanagement te concretiseren voor de directies, zodat hun rol duidelijk wordt.

Toekomstige wet- en regelgeving: met de raadsinformatiebrief van 2 november 2023 is de raad geïnformeerd over nieuwe digitaliseringswetgeving. De directie Juridische Zaken heeft een

aanpak uitgewerkt om alle nieuwe en gewijzigde wetgeving in kaart te brengen en de implementatie toe te wijzen aan een directie. Deze werkwijze is recent door het GMT vastgesteld en wordt vanaf nu toegepast. Binnen het I-domein is een team actief om de consequenties van deze ontwikkelingen op de digitalisering te volgen.
We beschouwen dit deel van de aanbeveling daarmee als afgedaan.

Afhandeling

- Het blijvend volgen van de voortgang van BIO, AVG, Wpg en Woo is ingericht. Deze aanbeveling is afgedaan.
- Het opnemen van de risico's per directie in Fully in Control zal naar verwachting eind 2024 gereed zijn voor Informatiebeveiliging en Informatiebeheer. Voor Privacy is dat medio 2025 het geval.
- De toekomstige wet- en regelgeving is in kaart gebracht en er zijn processen ingericht voor de implementatie. Dit deel van de aanbeveling is dus afgedaan.

Conclusie
De afhandeling van de aanbevelingen op deze zes onderwerpen loopt. De meest recente aanbevelingen van ACAM en Rekeningencommissie zijn kortgeleden gedaan naar aanleiding van het jaarverslag 2023, met uitzondering van nummer 4 (Datacenter) die uit 2021 dateert en die zich qua realisatie in een afrondende fase bevindt. Ik zal u in het vierde kwartaal van 2025 wederom informeren over de voortgang.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd over de voortgang van de aanbevelingen.

Met vriendelijke groet,
Namens het college van burgemeester en wethouders van de gemeente Amsterdam,

Alexander Scholtes
Wethouder ICT en digitale stad