Gemeente Amsterdam

Auditrapport

Risicomanagement

De inrichting en uitvoering van risicomanagement binnen de gemeente

Referentie: AOJP23/audit#33

Opdrachtgever: Concerncontroller

Auteur: IA&BO

Proceseigenaar: Directie Middelen en Control - afdeling Besturing en Begrotingszaken

11 december 2023 (definitieve versie 1.0)

1 Inleiding

Aanleiding

Interne audit- en beleidsonderzoek (IA&BO) evalueert vanuit haar verantwoordelijkheid de effectiviteit van de risicomanagementprocessen en draagt bij aan de verbetering daarvan (standaard 2120 – risicomanagement; standaarden voor de beroepsuitoefening van internal auditing). Hier geven we invulling aan door periodiek audits uit te voeren naar risicomanagement binnen de gemeente. Jaarlijks agenderen wij het onderwerp, zo ook in het audit- en onderzoeksprogramma 2023. Om inzicht te bieden in de effectiviteit van risicomanagement, gaan wij uit van ISO-31000. De norm biedt principes, een kader en een proces voor effectief risicomanagement binnen een organisatie. In de beleidsnota Risicomanagement 2022-2026 heeft het college en de raad vastgesteld dat ISO 31000 de standaard is bij de inrichting van het integrale risicomanagement.

Doelstelling en centrale vraag

De doelstelling van de audit is het bieden van inzicht in hoe gemeentebreed invulling wordt gegeven aan risicomanagement. De centrale vraag van de audit luidt: “Is de inrichting en uitvoering van risicomanagement binnen de gemeente volgens de richtlijnen van ISO 31000?”

Onze centrale vraag valt uiteen in de volgende drie deelvragen:

1. Zijn de richtlijnen van ISO 31000 opgenomen en uitgewerkt in de stedelijke kaders en richtlijnen over risicomanagement?
2. Hoe wordt uitvoering gegeven aan risicomanagement in de 1e en 2e lijn?
3. Zijn er menselijke en culturele factoren die van invloed zijn op de uitvoering van risicomanagement? (Soft controls)

Scope

De audit richt zich op de uitvoering van risicomanagement binnen vier eerstelijnsdirecties en de aan deze directies verbonden (proces) controllers vanuit DMC. Daarnaast nemen we vanuit de tweede lijn de stelselverantwoordelijkheid van de afdeling Besturing en Begrotingszaken mee. Op basis van onze observaties formuleren we gemeentebrede bevindingen en aanbevelingen.

De vier geselecteerde eerstelijnsdirecties zijn: Verkeer en Openbare Ruimte (V&OR), Data, Onderwijs, Jeugd, Zorg en Diversiteit (OJZD), Stadswerken.

Voor een nadere uitwerking van de scope verwijzen we naar bijlage 1.

Leeswijzer

In hoofdstuk 2 zijn de samenvatting en conclusies opgenomen. Hoofdstuk 3 richt zich op de beantwoording van de eerste deelvraag, met betrekking tot het inrichten en uitwerken van ISO 31000 in de stedelijke kaders en richtlijnen voor risicomanagement. In hoofdstuk 4 behandelen we de tweede deelvraag, die betrekking heeft op de uitvoering van risicomanagement in zowel de eerste als de tweede lijn. De beantwoording van deelvraag drie is geïntegreerd in de beantwoording van de eerste twee deelvragen in de respectievelijke hoofdstukken. Ten slotte zijn onze onafhankelijkheid, werkzaamheden, scope en gemaakte afspraken over deze audit beschreven in bijlage 1. In bijlage 2 is de managementreactie per bevinding opgenomen.

Dankwoord

Wij bedanken de medewerkers die bij dit onderzoek betrokken zijn geweest voor hun tijd en uitleg over hoe zij inrichting en uitvoering geven aan risicomanagement binnen hun functie. Tot het verstrekken van nadere toelichting zijn wij uiteraard bereid.

2 Samenvatting en conclusies

Dit auditrapport geeft inzicht in de inrichting en uitvoering van het stelsel van risicomanagement binnen de gemeente en of dit overeenkomt met de richtlijnen van ISO 31000. ISO 31000 is een raamwerk voor effectief risicomanagement. In 2012 heeft de gemeente gekozen het risicomanagement in te richten volgens deze internationale standaard.

Conclusie 

De conclusie van deze audit is dat de inrichting en uitvoering van risicomanagement binnen de gemeente deels voldoet aan de richtlijnen van ISO 31000. De risicomanagementkaders voldoen grotendeels aan de richtlijnen van ISO 31000. Betreffende het risicomanagementproces zien wij nog ruimte om deze tot een hoger volwassenheidsniveau te brengen voordat uitgegaan kan worden van een zekere mate van vertrouwen in elkaars vakmanschap. Bijvoorbeeld door het nader invullen van een aantal randvoorwaarden zoals beschreven in de onderstaande bevindingen. De bevindingen raken aan de soft controls helderheid, uitvoerbaarheid, voorbeeldgedrag en betrokkenheid. Voor nadere toelichting zie figuur 1.

Voor de inrichting en uitvoering van risicomanagement signaleren we de volgende bevindingen:

- Risicomanagementkaders bieden goede aanknopingspunten voor effectief risicomanagement maar zijn niet volledig;
- Verantwoordelijkheden van DMC-Risicomanagement en de risicomanagementkaders zijn niet bij alle betrokkenen bekend;
- Het risicomanagementproces bij de directies vindt veelal niet structureel en gestructureerd plaats;
- Niet alle directeuren beschikken over volledige informatie om te kunnen sturen op risico's;
- Verwachtingen van directeuren en afdelingsmanagers over de rol van control matchen niet altijd met de werkelijkheid.

Een niet optimaal ingericht en uitgevoerd risicomanagementproces kan ertoe leiden dat niet alle risico's worden beheerst en kansen worden benut. Het gevolg hiervan kan zijn dat (programma)doelen niet (tijdig) worden gerealiseerd.

Aanbevelingen

- Neem een uitwerking van het generieke risicomanagementproces zoals beschreven in ISO 31000 op in de risicomanagementkaders. Geef hierin ook aan wat DMC-Risicomanagement verwacht van de directies over de implementatie van een risicomanagementproces.
- Communiceer alle stedelijke kaders inclusief bovenstaande uitwerking (opnieuw) met de organisatie en plaats deze op een toegankelijke plek. Besteed hierbij ook aandacht aan de effectiviteit van de communicatie.
- Specificeer in de Leidraad Risicomanagement wat de ambtelijke verantwoordelijkheden van DMC-Risicomanagement behelzen, zoals de regierol en het toetsen van de consistentie van afgeleide kaders.
- Voer periodiek het gesprek met control om inzicht te krijgen in de beheersing van risico's door directeuren.
- Communiceer de 'Werkwijze Advisering' vanuit control met de eerste lijn via een effectief communicatiekanaal. Voer daarnaast ook gesprekken met betrokkenen uit de eerste lijn over de rol van control en hun verwachtingen hierbij.

Vertrouwen

Vertrouwen op andermans vakmanschap is een principe waar de gemeente naar streeft. Volgens ISO 31000 beïnvloeden menselijk gedrag en cultuur (soft controls) alle aspecten van risicomanagement op elk niveau en in elke fase. Dit zijn cruciale elementen voor het opbouwen en behouden van vertrouwen binnen de organisatie. Het implementeren van effectieve soft controls kan een positieve invloed hebben op het vertrouwen op andermans vakmanschap. Zie figuur 1. Overzicht van bevindingen soft controls m.b.t. risicomanagement voor onze belangrijkste constateringen inzake soft controls.



Figuur 1. Overzicht van bevindingen soft controls m.b.t. risicomanagement

In de rapportage geven we aan welke prioriteit we aan de bevindingen toekennen. Bevindingen met prioriteit 1 worden in de voortgangsrapportages aan het GMT opgenomen. Prioriteit 2 bevindingen worden alleen aan het GMT gemeld als er geen opvolging aan wordt gegeven en prioriteit 3 bevindingen (opvolging niet noodzakelijk) worden enkel aan de directie en het management gerapporteerd. Standaardrisico`s, beheersmaatregelen, bevindingen en aanbevelingen worden opgenomen in het gemeentebrede risicomanagementsysteem FullyInControl (FIC).

Bevindingen	Prioriteit 3 Laag	Prioriteit 2 Midden	Prioriteit 1 Hoog
1. Risicomanagementkaders bieden goede aanknopingspunten voor effectief risicomanagement maar zijn niet volledig.			X
2. Verantwoordelijkheden van DMC-risicomanagement en de risicomanagementkaders zijn niet bij alle betrokkenen bekend.		X	
3. Het risicomanagementproces bij directies vindt veelal niet structureel en gestructureerd plaats.		X	
4. Niet alle directeuren beschikken over volledige informatie om te kunnen sturen op risico's.		X	
5. Verwachtingen van directeuren en afdelingsmanagers over de rol van de controller matchen niet altijd met de werkelijkheid.	X		

Tabel 1. Prioriteit 1: Zeer belangrijk, grote impact, urgent, opvolging direct vereist; Prioriteit 2: Belangrijk, gemiddelde impact, minder urgent, opvolging nodig; Prioriteit 3: Aandacht nodig, beperkte impact, niet urgent, opvolging niet noodzakelijk.

Managementreactie afdeling Besturing en Begrotingszaken

Afdeling Besturing en Begrotingszaken heeft op 6 december een managementreactie per bevinding gegeven op dit rapport. Deze reactie is opgenomen in bijlage 2.

3 ISO 31000 in de stedelijke kaders en richtlijnen over risicomanagement.

In dit hoofdstuk geven wij antwoord op deelvraag 1: Zijn de richtlijnen van ISO 31000 opgenomen en uitgewerkt in de stedelijke kaders en richtlijnen over risicomanagement? In de beantwoording nemen wij ook de menselijke en culturele factoren mee die van invloed zijn op de uitvoering van risicomanagement (deelvraag 3).

3.1 Risicomanagementkaders bieden goede aanknopingspunten voor effectief risicomanagement maar zijn niet volledig

DMC-Risicomanagement is onder andere verantwoordelijk voor het opstellen van de stedelijke kaders over risicomanagement (de Beleidsnota Risicomanagement 2022-2026 en de Leidraad Risicomanagement). Wij hebben geconstateerd dat deze stukken veel aanknopingspunten bieden ter ondersteuning van effectief risicomanagement. In de stukken zijn onder andere de rollen en verantwoordelijkheden met betrekking tot risicomanagement beschreven, wordt het proces voor financieel risicomanagement geschetst, wordt duiding gegeven aan risicomanagementbegrippen (Amsterdamse risicotaal) en wordt verwezen naar de pagina waarin toelichting gegeven wordt op het gebruik van FIC.

Bevinding:

- DMC-Risicomanagement biedt in de risicomanagementkaders belangrijke uitgangspunten voor een effectieve inrichting en uitvoering van risicomanagement. Zo is er in de leidraad aandacht voor hoe risico's te kwantificeren met kans en impact en worden verschillende vormen van risicobeheersing benoemd. De kaders zijn echter niet volledig. Het ontbreekt aan een gedetailleerde omschrijving van het risicomanagementproces. Denk hierbij aan processtappen als: risicobeoordeling, risicobehandeling, monitoring, registratie en rapportage.

Risico

Zonder de juiste middelen en structuren, zoals een gedetailleerde beschrijving van risicomanagementprocesstappen, kan de organisatie moeite hebben om risico's volledig te identificeren, juist te beoordelen, te beheersen en te monitoren. Dit heeft invloed op de kwaliteit van de risicoinformatie in de organisatie. Het gevolg kan zijn dat besluitvorming plaatsvindt op basis van onvolledige informatie. Dit kan leiden tot beslissingen die niet (volledig) in lijn zijn met het realiseren van de (programma)doelstellingen.

(Mogelijke) oorzaak

- De risicomanagementprocesstappen zijn niet uitgewerkt, omdat DMC-Risicomanagement verwacht dat directies zelf de ISO 31000 norm weten te vinden en hier een vertaling van maken naar hun eigen beleid. De norm is echter niet kosteloos toegankelijk.
- Elke directie zit anders in elkaar. Volgens DMC-Risicomanagement zou uitwerken van ISO 31000 naar directie, gezien haar beschikbare capaciteit, te veel tijd kosten.

Aanbeveling

- Wij raden aan het generieke risicomanagementproces uit te werken zoals beschreven in ISO 31000. Betrek hierbij DMC-Procescontrol vanwege de link met het Kader Procesbeheersing. Geef hierin ook aan wat DMC-Risicomanagement verwacht van de directies over de implementatie van een risicomanagementproces.
- Communiceer alle stedelijke kaders incl. bovenstaande uitwerking (opnieuw) met de organisatie en plaats deze op een toegankelijke plek.

3.2 Verantwoordelijkheden van DMC-risicomanagement en de risicomanagementkaders zijn niet bij alle betrokkenen bekend

In de Leidraad Risicomanagement staan de verantwoordelijkheden van DMC-Risicomanagement beschreven. Zo zijn zij onder andere verantwoordelijk voor de concernbrede regie op risicomanagement, het toetsen van afgeleide kaders om consistentie te bewaken, het maken van (gemeentebrede) analyses op basis van (de best beschikbare) risicoinformatie en het bevorderen van een uniforme en integrale wijze van risicomanagement via communicatie en risicosessies.

Wij hebben geconstateerd dat DMC-risicomanagement werkzaamheden uitvoert om invulling te geven aan de benoemde verantwoordelijkheden. Zo verzamelt DMC-Risicomanagement signalen vanuit de 1e lijn, vanuit control en audits. Analyses op risicoinformatie worden gemaakt op basis van de risicoinformatie in FIC. Daarnaast wordt een uniforme en integrale wijze van risicomanagement bevorderd door de risicomanagementkaders te delen via de directeurenmail en op aanvraag selectief risicosessies te faciliteren. DMC-Risicomanagement faciliteert vooral sessies in voorbereiding op de invoering van nieuwe initiatieven of doorvoering van stelselwijzigingen (strategisch en extern risico context).

<u>Bevindingen</u>

1 De verantwoordelijkheid voor concernbrede regie op risicomanagement en het toetsen van afgeleide kaders om de consistentie te bewaken, wordt in de leidraad risicomanagement niet gespecificeerd. Het is onduidelijk wat deze verantwoordelijkheden behelzen.
2 Communicatie over de uniforme en integrale wijze van risicomanagement bereikt niet altijd alle betrokkenen: directies, evenals een aantal actoren uit de tweede lijn, zijn niet op de hoogte van het bestaan van de risicomanagementkaders. Of ze geven aan wel op de hoogte te zijn van het bestaan ervan, maar geen kennis te hebben van de inhoud.
3 De verantwoordelijkheden van DMC-risicomanagement zijn niet altijd bekend bij de directies. De directies geven bijvoorbeeld aan niet te weten waarbij DMC-Risicomanagement hen kan ondersteunen.
4 Risicoinformatie is niet compleet: niet alle (operationele) risico's zijn opgenomen in FIC. DMC-Risicomanagement heeft hierdoor geen volledig risicobeeld om rode draden uit te halen. De standaardisering van operationele risico's in FIC is een stap in de goede richting voor het verkrijgen van een completer risicobeeld.

<u>Risico</u>

Het risico is dat DMC-Risicomanagement in onvoldoende mate in staat is om invulling te geven aan hun ambtelijke verantwoordelijkheid voor het risicomanagementstelsel. Dit kan ertoe leiden dat bekendheid met risicomanagementkaders en nut en noodzaak van risicomanagementtools (zoals FIC) niet landen in de organisatie. Het gevolg is dat risicomanagement niet effectief, uniform en integraal plaatsvindt waardoor risico's mogelijk in onvoldoende mate beheerst zullen worden en analyses op risicoinformatie berusten op onjuiste of onvolledige informatie.

<u>(Mogelijke) oorzaken</u>

- Vanwege de beperkte capaciteit van DMC-Risicomanagement moeten zij een prioritering aanbrengen in hun werkzaamheden. Momenteel ervaren zij bijvoorbeeld drukte vanwege FIC en compliance vraagstukken. Dit gaat ten koste van het aantal risicomanagementsessies dat zij kunnen faciliteren.
- Vanwege de beperkte capaciteit wordt onvoldoende ingezet op bewustwording van risicomanagement, het uitdragen van de rol en verantwoordelijkheden van DMC-Risicomanagement en het bekend maken van de risicomanagementkaders.

- DMC-Risicomanagement verwacht dat directies zelf risicomanagement op hebben genomen in hun beleid en dit toetsen aan ISO 31000. Directies zijn veelal niet op de hoogte van de verwachtingen die DMC-Risicomanagement hierover heeft.

FIC wordt niet (volledig) gebruikt omdat:

- FIC alleen een risicotolerantiegrens voor de financiële impact van risico's biedt. Niet alle type risico's lenen zich voor een dergelijke indeling. Denk aan bedrijfswaarden zoals (informatie)veiligheid en duurzaamheid.
- Het invullen van FIC wordt vanuit de directies voornamelijk ervaren als een verplichting. De toegevoegde waarde van een risicomanagementsysteem voor risicobeheersing wordt door de meeste directies onvoldoende ervaren.

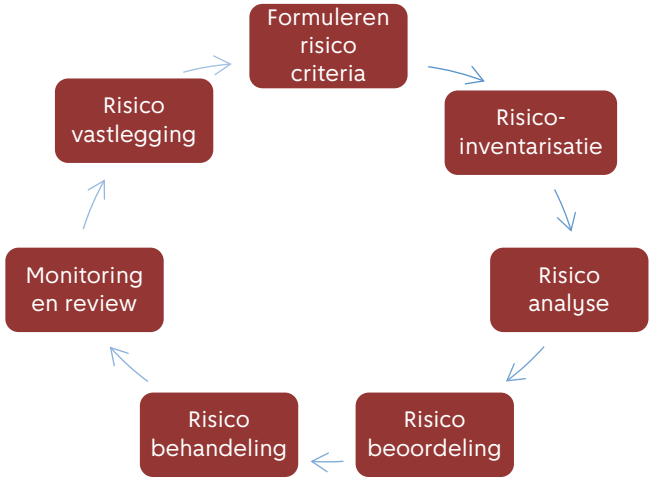
Aanbeveling

- Specificeer in de Leidraad Risicomanagement wat de ambtelijke verantwoordelijkheden van DMC-risicomanagement behelzen, zoals de regierol en het toetsen van de consistentie van afgeleide kaders.
- Besteed aandacht aan de effectiviteit van de communicatie van DMC-Risicomanagement naar de organisatie.

4 Het risicomanagementproces in de 1e en 2e lijn

In dit hoofdstuk beantwoorden wij deelvraag 2: “Hoe wordt uitvoering gegeven aan risicomanagement in de 1e en 2e lijn?”. De verantwoordelijkheden van de 1e en de 2e lijn met betrekking tot sturen en beheersen zijn opgenomen in het stelsel van uitgangspunten “Amsterdam Doelgericht”. Daarin staat dat de 1e lijn verantwoordelijk is voor het beheersen van risico’s en het benutten van kansen. De 2e lijn observeert en adviseert hierover. In de beantwoording van deelvraag 3, nemen wij ook de menselijke en culturele factoren mee die van invloed zijn op de uitvoering van risicomanagement.

4.1 Het risicomanagementproces bij directies vindt veelal niet structureel en gestructureerd plaats



Figuur 2: het risicomanagementproces conform ISO 31000.

De Leidraad Risicomanagement benoemt dat risicomanagement niet iets is wat af en toe of alleen op gezette tijden gedaan zou moeten worden, zoals bij de begroting en de jaarrekening. Het is een doorlopend proces en zou integraal onderdeel uit moeten maken van onze bedrijfsvoering. Zoals weergegeven in figuur 2: het risicomanagementproces conform ISO 31000.

Bevindingen

1 Hoewel er op verschillende momenten aandacht is voor risicomanagement, hebben wij geconstateerd dat de meeste directies risico’s buiten de P&C-momenten om niet gestructureerd en structureel inventariseren.
2 Risico-inventarisatie en –actualisatie betreffen veelal een samenspel tussen een select aantal stakeholders. Vaak betreffen dit de afdelingsmanager, controller en financieel adviseur. Bij sommige directies is ook een risicomanager, teamleider of strategisch adviseur betrokken. De brede control functie wordt echter onvoldoende aangehaakt.
3 Wij hebben geconstateerd dat niet alle directies expliciet de waarschijnlijkheid van het optreden en de impact van risico’s identificeren op het moment dat risico’s geïnventariseerd worden. Als kwantificering van risico’s al plaatsvindt, dan gebeurt dit pas op het moment dat risico’s opgenomen worden in FIC. Het systeem dwingt namelijk het kwantificeren van risico’s af. Het heeft de voorkeur dat risico’s eerder gekwantificeerd worden, omdat:
    - De input gebruikt kan worden voor het prioriteren van risico’s in een vroeg stadium;
    - Er meer stakeholders betrokken zijn wat ten goede komt aan de kwaliteit van de risicoinformatie;
    - Niet alle risico’s door directies opgenomen worden in FIC waardoor kwantificering van risico’s niet afgedwongen wordt.
4. De meeste directies stellen hun risicocriteria niet vooraf vast. Daarnaast maken zij veelal ook geen structurele en gestructureerde afweging of

beheersmaatregelen noodzakelijk zijn dan wel of de voordelen hiervan opwegen tegen de nadelen.

5. Risicomanagement wordt in veel gevallen nog eenzijdig benaderd. De nadruk ligt bijna uitsluitend op het beheersen van risico's en nagenoeg niet op het benutten van kansen. Risicobereidheid wordt veelal niet bewust meegenomen als criterium bij de bepaling hoe om te gaan met risico's.

Risico-inventarisaties bij directies

Wij hebben een aantal positieve voorbeelden van aandacht voor het inventariseren van risico's bij de directies opgehaald. Zo is er bij de afdeling Contractmanagement Jeugd en Zorg een waardevolle risicosessie onder begeleiding van DMC-Risicomanagement gefaciliteerd, worden bij directie Stadswerken bedrijfsplannen en afdelingsplannen inclusief risico's en beheersmaatregelen periodiek besproken en organiseren de assetteams binnen afdeling Stedelijk Beheer (V&OR) periodiek risicosessies.

Risico

Wanneer er geen structureel en gestructureerd risicomanagementproces is ingericht, loopt de directie het risico dat niet alle risico's in beeld zijn, dat risico's niet juist ingeschat worden door het ontbreken van een kwantificeringssystematiek en risicocriteria en dat er geen goede vervolgacties dan wel beheersmaatregelen gekoppeld worden aan geïdentificeerde risico's. Het gevolg kan zijn dat risico's niet tijdig worden geïdentificeerd, dat risico's onterecht onvoldoende beheerst worden of dat kansen niet benut worden of onvoldoende worden overwogen. Dit zou kunnen leiden tot het niet (tijdig) realiseren van (programma)doelen.

(Mogelijke) oorzaken

- Een groot deel van de directies is niet bekend met de risicomanagementkaders (de Beleidsnota Risicomanagement 2022-2026 en de Leidraad Risicomanagement). Ook wanneer directies wel bekend zijn met deze kaders, bieden de kaders te weinig houvast voor de inrichting van integraal risicomanagement en het risicomanagementproces. Zo is het risicomanagementproces volgens ISO 31000 niet uitgewerkt terwijl we als gemeente wel uitspreken ons hieraan te committeren.
- Bekendheid met en het bewustzijn van de baten van een gedegen risicomanagementproces ontbreekt bij een groot deel van de directies.
- Risicomanagement wordt door het overgrote deel van de directies gezien als het beheersen van risico's. Het besef dat risicomanagement ook gaat over het benutten van kansen is minder bekend.

Aanbeveling

- Zie de aanbeveling bij paragraaf 3.1. Wij raden aan hierin ook voorbeelden van de te betrekken stakeholders op te nemen.
- Zie de aanbeveling bij paragraaf 3.2. Besteed in de communicatie ook aandacht aan het belang van een structureel en gestructureerd risicomanagementproces.

4.2 Niet alle directeuren beschikken over volledige informatie om te kunnen sturen op risico's

In Amsterdam Doelgericht staat beschreven dat (stedelijk) directeuren verantwoordelijk zijn voor het beheersen van risico's en het benutten van kansen. Om op een goede manier invulling te kunnen geven aan deze verantwoordelijkheid is het belangrijk dat directeuren over juiste en volledige risicoinformatie beschikken met betrekking tot diens risico's. Een volledig risicobeeld bij directeuren is een randvoorwaarde om het gesprek over risico's te kunnen voeren op cluster- of programmaniveau. Alleen wanneer alle directeuren binnen een cluster of programma een juist en volledig beeld

hebben van de risico's binnen hun directie, kan het gesprek over risico's gelijkwaardig worden gevoerd binnen cluster MT's en kunnen gedegen beslissingen worden gemaakt over te ondernemen acties.

Bevindingen

1. De meeste directies consolideren de afdelingsrisico's (nog) niet tot een totaaloverzicht van directiebrede risico's. Daarbij wordt de actualisatie van deze risico's bij de begroting en jaarrekening niet altijd even grondig uitgevoerd. Bij de actualisatie leveren afdelingsmanagers hun risico-inventarisaties aan, echter, in de praktijk betekent dit vaak een actualisatie van de al eerder geïnventariseerde risico's op afdelingsniveau. We zien dat vaak geldt dat de optelsom van de afzonderlijk van elkaar opgestelde overzichten binnen de directie uiteindelijk de directielijst van risico's vormt. In deze structuur worden risico's die de afdeling overstijgen onvoldoende gesignaleerd.
2. De risico-inventarisatie heeft veelal betrekking op het weerstandsvermogen en niet zozeer op operationele risico's. Dit maakt de risicoinformatie incompleet, waardoor het overkoepelende beeld van risico's en de mate van beheersing van risico's bij sommige directeuren ontbreekt.
3. Ook risico-inventarisaties buiten de P&C-cyclus om vinden vooral plaats op afdelingsniveau. Deze inventarisaties worden niet altijd gedeeld met de directeur. Directeuren beschikken zodoende niet altijd over een totaalbeeld van risico's op directieniveau.
4. Het totaalbeeld van risico's op directieniveau is niet uit FIC te halen, want niet alle directierisico's zijn hierin opgenomen.

Risico's

Het risico van een onvolledige rapportagestructuur en beperkte centrale vastlegging is dat risicoinformatie niet bij de juiste stakeholders terechtkomt. Risico's op cluster of programmaniveau zijn onvoldoende of niet in beeld. Zo kan een onvolledig risicobeeld bij directeuren leiden tot een onvolledig risicobeeld op clusterniveau. Het gevolg kan zijn dat besluitvorming plaatsvindt op basis van onvolledige informatie. Dit kan leiden tot beslissingen die niet volledig in lijn zijn met het realiseren van de (programma)doelstellingen.

(Mogelijke) oorzaak

- Hoewel directeuren eindverantwoordelijk zijn voor de risico's die een directie loopt, hebben wij vernomen dat directeuren met betrekking tot risicomanagement veelal vertrouwen op de professionaliteit van hun afdelingsmanagers. Vanwege dit vertrouwen komen de risicorapportages niet altijd terecht bij de directeuren.
- Zie voor de oorzaken van het beperkte gebruikt van FIC in paragraaf 3.2.

4.3 Verwachtingen van directeuren en afdelingsmanagers over de rol van de controller matchen niet altijd met de werkelijkheid

Aanbeveling

Voer periodiek het gesprek met control om inzicht te krijgen in de beheersing van risico's door directeuren. Control kan hierin een belangrijke signaalfunctie vervullen. Doordat zij vanuit hun verantwoordelijkheid periodiek gesprekken voeren met directeuren over de beheersing van risico's en de kwaliteit van risicoinformatie (Leidraad Risicomanagement), zouden zij de onvolledigheid van risicoinformatie bij directeuren moeten signaleren. Dit geldt ook voor managers control op clusterniveau.

In de Leidraad Risicomanagement zijn de verantwoordelijkheden van control opgenomen. Enkele van deze verantwoordelijkheden zijn:

- Het analyseren, adviseren en signaleren over risico's conform de stedelijke criteria;
- Coördineren van de brede control;

- Periodiek de risicobeheersing bespreken met de directeur en adviseren over de kwaliteit van risicoinformatie;
- Het wijzen op risico's en kansen met betrekking tot doelrealisatie.

In de 'Werkwijze Advisering' wordt nader ingegaan op de rollen en verantwoordelijkheden van de controlorganisatie met betrekking tot het advieswerk dat de controller verricht.

Bevindingen

Verwachtingen die directeuren hebben over de rol van control matchen niet altijd met de werkelijkheid. Zo geven sommige directeuren aan dat controllers veelal fungeren als financiële controllers en geen bredere blik op risico's hanteren. Daarnaast zouden controllers nog groeiende zijn in hun rol en geven sommige directeuren aan dat de procescontroller onvoldoende zichtbaar is.

Risico's

Controllers kunnen niet aan de verwachtingen van de directeuren of afdelingsmanagers voldoen en/of verwachtingen van directeuren en afdelingsmanagers zijn niet bekend bij controllers. Mogelijke onrealistische verwachtingspatronen kunnen tot gevolg hebben dat onvoldoende aandacht besteed wordt aan (specifieke) risico's. Daarnaast kan dit ook leiden tot het niet of te laat aanhaken van control bij specifieke vraagstukken of opgaven. Onvoldoende beheersing van risico's kan op zijn beurt leiden tot dat (programma)doelen niet gerealiseerd worden.

(Mogelijke) oorzaken

Directeuren en afdelingsmanagers noemen verschillende redenen waardoor control niet altijd aan de verwachtingen van de directies voldoet:

- De rol van control is in de afgelopen jaren veranderd. Sommige controllers zijn nog zoekende naar de juiste invulling van hun rol;
- Er zijn veel wisselingen geweest in portefeuilleverdeling van controllers. Niet alle controllers beschikken (nog) over voldoende directie-specifieke inhoudelijke kennis om goede adviezen uit te kunnen brengen;
- Sommige controllers hebben nog te weinig ervaring als controller om te kunnen fungeren als volwaardige sparringpartner;
- De controllers van afdeling Control-DMC adviseren de directies onder andere over risicomanagement. Sommige van deze controllers hebben als specifiek aandachtsgebied procescontrol. Zij zijn niet aan een specifieke directie verbonden en daarmee niet altijd zichtbaar. Indien procescontrol niet expliciet betrokken is bij een directie, vervullen de controllers deze rol en taak. Zij kunnen (indien nodig) een beroep doen op de expertise van de procescontroller.

Aanbeveling

- In de 'Werkwijze Advisering' staan de verantwoordelijkheden van control beschreven met betrekking tot risicomanagement. Het handboek fungeert als naslagwerk voor controllers maar informeert collega's van de eerste lijn ook over de Werkwijze van Control. Ons advies zou zijn om dit handboek via een effectief communicatiekanaal te delen met de eerste lijn.
- Geef opvolging aan het delen van de 'werkwijze advisering' door het gesprek met betrokkenen uit de eerste lijn aan te gaan over de rol van control en de verwachtingen hierbij vanuit de directie. Maak duidelijk wat vanuit de rol van control haalbaar en realistisch is en wat niet.

Bijlage 1: Werkzaamheden, scope, afspraken en onafhankelijkheid

Werkzaamheden

Op basis van de doelstelling van de audit heeft het auditteam de volgende werkzaamheden uitgevoerd.

Verantwoording werkzaamheden

Wij hebben deze audit uitgevoerd conform het Audit Charter 2023, welke is ondertekend door onze opdrachtgever, de Gemeentesecretaris. Hierin staat de reikwijdte van onze werkzaamheden en bevoegdheden beschreven. Het Audit Charter 2023 is te vinden op de intranetpagina van IA&BO. Onze werkzaamheden worden uitgevoerd in overeenstemming met de normen van de beroepsgroep voor interne auditors. Dit is het Instituut voor Interne Auditors (IIA). Sinds september 2022 is IA&BO gecertificeerd.

Scope

De audit heeft betrekking op de inrichting en de uitvoering van risicomanagement door 1e en 2e lijn. Onze audit richt zich op de 4 directies V&OR, Data, OJZD en Stadswerken.

De volgende aspecten zijn geen onderdeel van ons onderzoek:

- De general IT-controls (GITC) en application controls;
- Risicomanagement binnen projecten;
- Het weerstandsvermogen;
- Analyse op gebruik FIC;
- De overige modules vanuit FIC;
- De juistheid en volledigheid van de gegevens in de risicomodule in FIC.

Afspraken

Voor de audit gelden onderstaande afspraken:

Verspreidingskring

Het definitieve rapport wordt gedeeld met de afdeling Besturing en Begrotingszaken, de directeuren en controllers van de geselecteerde organisatieonderdelen en zal daarnaast worden aangeboden aan de concerncontroller en de gemeentesecretaris als onze (gedelegeerde) opdrachtgever. De uitkomsten van de audit worden in hoofdlijnen opgenomen in de kwartaalrapportage die aan het GMT wordt toegestuurd. Ook delen wij onze definitieve rapporten met ACAM. Indien ACAM daarom verzoekt, wordt aan hen inzage gegeven in ons dossier.

FIC

Zoals aangegeven in de Auditbrief worden de bevindingen door IA&BO overgenomen in het Governance, Risk en Compliance Tool van Gemeente Amsterdam genaamd FullyInControl. Vervolgens dient de auditee de nadere opvolging in dit systeem vast te leggen.

Openbaar maken van rapporten

Het rapport mag door de afdeling Besturing en Begrotingszaken worden gedeeld aan interne stakeholders van de Gemeente Amsterdam. Het auditrapport wordt 6 maanden na bespreking in het Risk en Audit Comité (RAC) openbaar gemaakt op het internet (open.amsterdam) in het kader van de Wet Open Overheid (WOO). Hierna mag het auditrapport door u ook gedeeld worden met externe stakeholders.

Onafhankelijkheid

IA&BO voert in opdracht van de ambtelijke opdrachtgever onafhankelijk onderzoek uit binnen de gemeente. Onze ambtelijk opdrachtgever, de gemeentesecretaris heeft het opdrachtgeverschap van IA&BO gemandateerd aan de Concerncontroller (DMC). Aangezien de concerncontroller tevens de eindverantwoordelijke directeur is voor het proces risicomanagement van afd. Besturing en Begrotingszaken en daarmee in die hoedanigheid invloed zou kunnen uitoefenen op het controleobject hebben wij aanvullende maatregelen getroffen. Een maatregel is dat de bevindingen direct aan de gemeentesecretaris worden gerapporteerd. Overigens hebben wij bij de uitvoering van de werkzaamheden geen enkele belemmering op dit vlak ervaren.

Bijlage 2: Managementreactie per bevinding

Bevinding 1: Risicomanagementkaders bieden goede aanknopingspunten voor effectief risicomanagement maar zijn niet volledig.

Managementreactie	Wordt herkend en overgenomen. ISO 31000 is de internationaal meest gebruikte richtlijn voor risicomanagement en voldoende volledig. Wij herkennen de noodzaak om een uitwerking van de richtlijn op te stellen in de vorm van een aantal duidelijke spelregels en deze op te nemen in de leidraad Risicomanagement. Voorts zullen wij de hernieuwde leidraad opnieuw communiceren met de organisatie	[Binnen welk tijdsbestek] **Half jaar** [Einddatum gereed] **Q2-2024** Follow-up audit: ja

Bevinding 2: Verantwoordelijkheden van DMC-risicomanagement en de risicomanagementkaders zijn niet bij alle betrokkenen bekend.

Managementreactie	Wordt herkend en overgenomen. De beschrijving in de leidraad Risicomanagement van rollen en verantwoordelijkheden van DMC-Risicomanagement vullen we aan met een specificatie van de regierol in het risicomanagementproces. Ook deze aanvulling zullen wij via de hernieuwde leidraad opnieuw communiceren met de organisatie	[Binnen welk tijdsbestek] **Half jaar** [Einddatum gereed] Q2-2024 Follow-up audit: ja

Bevinding 3: Het risicomanagementproces bij directies vindt veelal niet structureel en gestructureerd plaats.

Managementreactie	We nemen kennis van de bevinding. Met het stellen van “spelregels’ voor risicomanagement - die met een GMT besluit zijn bekrachtigd - stelt DMC-Risicomanagement duidelijke verwachtingen aan het risicomanagementproces in de directies. De directies hebben daarmee een concreet houvast voor het benoemen en beheersen van risico’s en de sturing daarop. We beschouwen bevinding 3 daarom als een bevinding voor de ge-audite directies. We zijn beschikbaar om die directies te adviseren bij het structureren van hun risicomanagement proces. Een voorbeeld hiervan is de systematiek van standaardrisico’s, geïntroduceerd in 4e kwartaal 2023.	[n.v.t.] [n.v.t.] [Follow-up audit: ja/nee]

Bevinding 4: Niet alle directeuren beschikken over volledige informatie om te kunnen sturen op risico's.

Managementreactie	De bevinding geeft aan dat de ge-audite directies belangrijke principes van risicomanagement niet toepassen. De deelaanbevelingen geven concreet aan dat het gaat om principes van structurering, inclusiviteit, integraliteit, best beschikbare informatie en cultuur. De bevinding gaat daarmee over een afwijking van gemeentelijk beleid door een directie. Dat kan op grond van proportionaliteit gerechtvaardigd zijn of niet. Een gesprek in een andere verhouding dan tussen control en directie is dan nuttig. Dat kan bijvoorbeeld een prestatiedialoog zijn tussen directeur en stedelijk directeur, of een themabespreking in het Risicoauditcomité van het Gemeentelijk Managementteam of agendering in het Bedrijfsvoeringsberaad. Die gesprekken kunnen gaan over de wijze waarop een directie invulling geeft aan integraal risicomanagement. De directies waarop deze aanbeveling betrekking hebben bereiden dit dan voor.	[Binnen welk tijdsbestek] [Einddatum gereed] [Follow-up audit: ja/nee]

Bevinding 5: Verwachtingen van directeuren en afdelingsmanagers over de rol van de controller matchen niet altijd met de werkelijkheid.

Managementreactie	In afstemming met DMC IA&BO: deze bevinding heeft IA&BO reeds voorgelegd aan Control. Hier is verdere reactie vanuit 'risicomanagement' niet meer nodig.	[n.v.t.] [n.v.t.] [Follow-up audit: ja/nee]