Vervoerregio Amsterdam

Risicomanagementbeleid Vervoerregio Amsterdam

COLOFON

Datum	November 2024
Kenmerk	BBV/2025/14581
Opgesteld door	Albert Scheven en Ronald de Bruijn
Vastgesteld door	……
Versie	03 (concept)

Vervoerregio Amsterdam
Postbus 626
1000 AP Amsterdam

T 020- 527 37 00
E info@vervoerregio.nl
W www.vervoerregio.nl

INHOUDSOPGAVE

AFKORTINGEN

AVG	Algemene Verordening Gegevensbescherming
BIO	Baseline Informatiebeveiliging Overheid
CISO	Beveiligingsfunctionaris (Chief Information Security Officer)
CSB	Cyber Security Board
FG	Functionaris Gegevensbescherming
IBD	InformatieBeveiligingsDienst
ISMS	Information Security Management System
ISO	Information Security Officer
MCS	Management Control Systeem
NIS2	Network and Information Security Directive
P&C	Planning en Control
PDCA	Plan - Do - Check – Act

1 INLEIDING

Dit document geeft sturing aan de wijze waarop de Vervoerregio met risicomanagement moet omgaan. Een gedocumenteerd beleid zorgt dat iedereen dezelfde informatie heeft en zodoende op dezelfde wijze handelt. Achter een beleid gaan eisen schuil. Eisen die voortkomen uit afspraken en verplichtingen (al dan niet voortvloeiend uit de verschillende normenkaders). Dit document helpt om de uitvoering daarvan te borgen en te verbeteren.

De directie onderschrijft in haar beleidsplan het belang van interne beheersing en risicomanagement en stelt zich ten doel aantoonbaar in control te zijn en daarvoor te willen groeien naar sturing vanuit een lerende organisatie.

Dit document gaat over risicomanagement, de betekenis en de toepassing daarvan. Het heeft betrekking op alle soorten risico's binnen de Vervoerregio. Het is belangrijk om met risico's rekening te houden want ze helpen ons als organisatie om schadelijke onzekerheden te ontdekken, te borgen en te verbeteren ten dienste van onszelf en onze betrokkenen. De kwaliteit van de interne beheersing gaat omhoog. We hebben er dus voordeel bij.
Een risico is een effect van onzekerheid op de realisatie van doelstellingen en kan positief of negatief zijn. Risicomanagement helpt interne beheersing naar een hoger volwassenheidsniveau en zorgt ervoor dat de (bedrijfs)doelstellingen behaald kunnen worden. Interne beheersing heeft betrekking op verschillende dimensies binnen de organisatie: wet- en regelgeving, efficiency & effectiviteit van processen, integriteit, betrouwbare rapportages, informatiebeveiliging en dergelijke.

Dit beleid beschrijft op hoofdlijnen het zogenaamde risicomanagementproces. De gevolgde methode is die van de ISO31000, een generieke risiomanagementmethodiek volgens internationale standaarden.

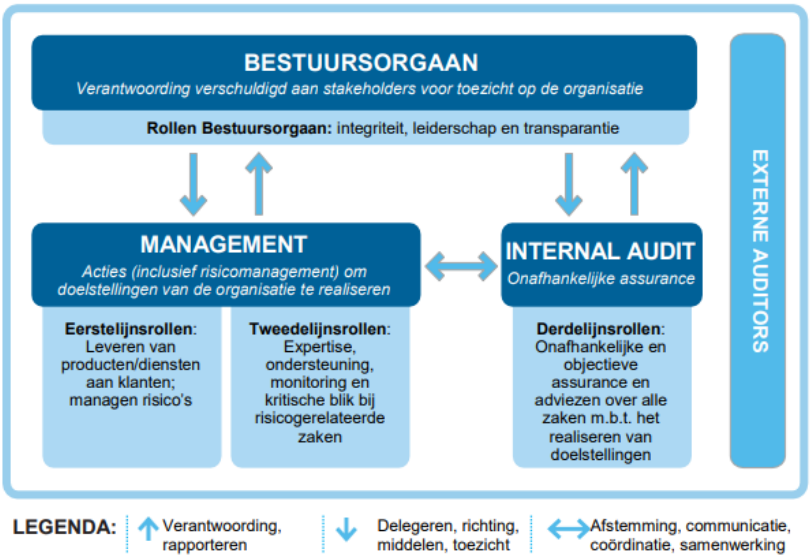
Risico's worden beheerd in het Management Control Systeem (MCS) waarvoor gebruik gemaakt wordt van Key2Control. Dit geldt ook voor de normenkaders en beheersmaatregelen (key controls).

Een meer gedetailleerde uitwerking is opgenomen in de risicoprocedure van het betreffende domein waarin de verschillende stappen onder verantwoordelijkheid van de risico eigenaar worden doorlopen.

2 ALGEMEEN

2.1 CONTEXT

Dit beleid beschrijft het integrale risicomanagement voor de gehele Vervoerregio. Hierbij wordt gebruik gemaakt van de internationale standaard ISO 31000 en het 3 Lines Model. Het eerste beschrijft een volledig model van risicomanagement; de tweede zoomt meer in op het ontwerp van de governance en de focus op de interne organisatie (taken, bevoegdheden & verantwoordelijkheden).



De eerstelijnsrollen worden vervuld door de managers die in hun hoedanigheid verantwoordelijk zijn voor het normenkader, risicomanagement en de implementatie van beheersmaatregelen. De tweedelijnsrollen worden vervuld door de controllers (hele organisatie, financieel), de CISO (Informatiebeveiliging), FG (Privacy), juristen, inkopers en anderen die hiervoor binnen het domein zijn aangesteld. Zij richten zich op de checks & balances. De derde lijn vervult een onafhankelijke rol en toetst de effectiviteit van de werkzaamheden door de eerste en tweede lijn. Het is belangrijk op te merken dat risicomanagement een integraal onderdeel dient te zijn van de bedrijfsvoering binnen de Vervoerregio en geborgd moet zijn in de cultuur en werkwijze van de organisatie.

2.2 DEFINITIE

De internationale Standaard ISO 31000 definieert een risico als 'het effect van onzekerheid op doelstellingen'. Een effect is een afwijking van het verwachte en kan (dus) negatief of positief zijn. In een negatieve situatie is dit een bedreiging (bijv. de kans op diefstal), in een positieve situatie een kans (bijv. de kans op winnen van een loterij).
In een formule wordt het risico gezien als het product van kans en impact.

Omdat de kans van optreden van een risico vaak nogal abstract is wordt ook wel gebruik gemaakt van inzicht in een dreiging waardoor de definitie uitgebreid kan worden: een risico is de kans dat een dreiging een kwetsbaarheid uitbuit waardoor er (negatieve of positieve) gevolgen zijn.

2.3 RISICOCRITERIA

Binnen de procedure wordt gebruikt gemaakt van zogenaamde risicocriteria. Deze zijn opgenomen in tabellen die voor alle domeinen binnen de Vervoerregio gebruikt worden. Ze zijn opgebouwd uit 5-puntsschalen en zijn als bijlage A opgenomen. Hierin is tevens de legenda opgenomen. Met deze tabellen kan de risicoscore voor een bepaald risico vastgesteld worden. Hierbij gelden de volgende uitgangspunten:

- Het niveau waarop een risico acceptabel is, is de zogenaamde risicobereidheid en wordt vastgesteld op alle score beneden de 40[1] punten.
- Er kunnen risico's gedefinieerd worden die ondanks hun lage risicoscore toch behandeld dienen te worden. Risico's met een brutorisicoscore lager dan de risicobereidheid maar die te maken hebben met het overtreden van een wet of regelgeving moeten worden voorgelegd aan de directie. Deze zal besluiten om deze risico's wel dan niet te accepteren.
- Voor risico's die behandeld worden maar waarvoor de kosten voor de maatregel(en) erg hoog uitvallen, kan in voorkomende gevallen besloten worden het (rest)risico te accepteren. De risico's waarvan de kosten van de te nemen maatregel(en) hoger of gelijk zijn aan de kosten van de impact bij optreden van het risico, zullen voorgelegd worden aan de directie.
- Kosten van maatregelen die het bedrag van € 25.000[2] te boven gaan dienen voorgelegd te worden aan de directie.

2.4 UITVOERINGSCRITERIA

Het proces van risicomanagement is niet een proces dat eenmalig doorlopen kan worden. Er zijn verschillende criteria die de uitvoering van risico assessment en -behandeling noodzakelijk maken. Deze criteria kunnen tijd- of gebeurtenis gebonden zijn en zijn in dit beleid als volgt vastgesteld:[3]

- In het jaarverslag en de begroting moet over risico's worden gerapporteerd in de paragraaf risicobeheersing & weerstandsvermogen.
- Minstens eenmaal per jaar dienen alle risico's opnieuw beoordeeld te worden.
- Wanneer een incident is voorgevallen dat vermoedelijk opnieuw kan gebeuren.

[1] In de tabel is dit weergegeven als een risicoscore beneden de 40 punten maar dit is nog ter besluitvorming
[2] Hoogte van het bedrag is ter besluitvorming
[3] Dit betekent dat risicomanagement geïntegreerd moet worden in de verschillende bedrijfsprocessen, zoals incidentmanagementproces, inkoopproces e.d.

- Een (significante) verandering in de externe en interne invloedsfactoren[4].
- Een verandering in de interne of externe stakeholders en hun vereisten, zoals
    - Een verandering in de organisatiestructuur met inbegrip van processen, verantwoordelijkheden en informatiesystemen
    - Een verandering in leveranciers- of klantrelatie met contractuele overeenkomsten
    - Elke andere verandering die als belangrijk wordt gezien om risico assessment op te starten.

2.5 TAKEN EN VERANTWOORDELIJKHEDEN

Binnen de Vervoerregio zijn de managers aangesteld als risico eigenaren indien het risico binnen de processen vallen waarvoor zij verantwoordelijk zijn. Indien het risico betrekking heeft op meerdere processen / teams wordt een eigenaar door de directie aangewezen. De risico eigenaren zullen voor hun verantwoordingsgebied de risico's in kaart (laten) brengen en zorgdragen dat de juiste maatregel(en) hiervoor gedefinieerd én uitgevoerd worden.

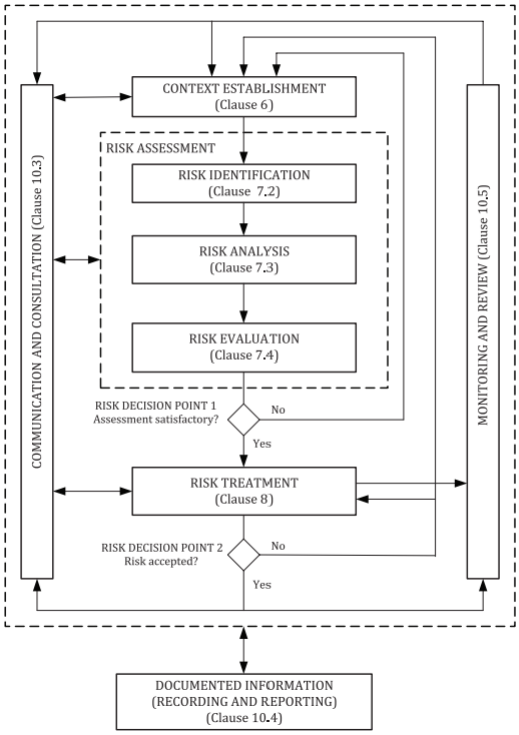
2.6 HERBEOORDELEN EN GOEDKEUREN VAN DIT BELEID

Elk jaar zal dit beleid herbeoordeeld moeten worden door de Concerncontroller en eventueel worden geactualiseerd en vastgesteld door het Dagelijks Bestuur. Eventuele aanpassingen zullen worden opgenomen met betrokkenen zoals het CSB, managers, CISO e.d.
Aanpassingen in de risicotabellen zullen eveneens moeten worden vastgesteld door het DB.

[4] Externe invloedsfactoren zijn de factoren uit bijvoorbeeld de DESTEP: demografische, economische, sociaal/culturele, technologische, ecologische en politiek/juridische factoren
Interne invloedsfactoren kunnen de factoren zijn uit het 7S-model van McKinsey: structuur, strategie, systemen, staf/personeel, (kern)vaardigheden, stijl en gedeelde waarden/cultuur

3 RISICOMANAGEMENT PROCES

Het risicoproces ziet er schematisch als volgt uit:



De te nemen stappen worden toegelicht in de risicoprocedure. In het kort zijn ze:

1. *Vaststellen van de scope*: om welk domein gaat het? Welke processen en/of informatiesystemen?
2. Risico assessment met daarin de volgende substappen:
    a. *Risico identificatie.*
    Welke risico's kunnen bepaald worden?
    b. *Risicoanalyse.*
    In deze stap worden de risico's geanalyseerd zodat de risico's gekwantificeerd kunnen worden.
    c. *Risico evaluatie.*
    Wanneer bekend is wat het bruto risico is kan bepaald worden of een risico behandeld moet worden en wat de meest geschikte behandeling is.
3. *Risicobehandeling.*
    In deze substap wordt de netto risico bepaald aan de hand van de gekozen behandeling. Mogelijk zit hier een iteratie in net zolang totdat het netto risico onder de vastgestelde risicobereidheid valt van de Vervoerregio.
4. *Beoordeling en bewaking.*
    Deze stap kan periodiek gepland worden of ad-hoc uitgevoerd worden. Risico's

dienen namelijk opnieuw beoordeeld te worden of periodiek of bij significante veranderingen (zie par. 2.4).

5. *Rapportage.*
   Risico's en hun mitigerende maatregelen worden bijgehouden in Key2Control. De eerste lijn bepaalt op basis van haar risicoanalyse welke mitigerende maatregelen nodig zijn en ziet toe op implementatie daarvan. De tweelijnsverantwoordelijke houdt toezicht op deze risico's en bewaakt dat deze volgens plan worden gemitigeerd. Rapportage en verantwoording afleggen hierover, monitoring en evaluatie van het risicomanagementproces geven vorm aan de PDCA-cyclus en een lerende organisatie.

BIJLAGE A: RISICOTABELLEN

		Gevolgen				
		Verwaarloosbaar	Beperkt	Serieus	Kritiek	Catastrofaal
Waarschijnlijkheid		2	4	6	8	10
Zeer waarschijnlijk	10	20	40	60	80	100
Waarschijnlijk	8	16	32	48	64	80
Mogelijk	6	12	24	36	48	60
Onwaarschijnlijk	4	8	16	24	32	40
Zeer onwaarschijnlijk	2	4	8	12	16	20

	Risiconiveaus				
Score	Zeer laag	Laag	Gemiddeld	Hoog	Zeer hoog
Bereik (van)	4	20	40	60	80
Bereik (tot en met)	19	39	59	79	100

Legenda - Waarschijnlijkheid				
Categorie	Score	Beschrijving	Percentage	Frequentie
Zeer onwaarschijnlijk	2	Dit zal waarschijnlijk nooit plaatsvinden	<1%	<1:100
Onwaarschijnlijk	4	De verwachting is dat dit niet zal optreden, maar het is wel mogelijk	1-5%	1:100 - 1:20
Mogelijk	6	Kan mogelijk optreden	5-25%	1:20 - 1:4
Waarschijnlijk	8	Zal waarschijnlijk gebeuren	25-50%	1:4 - 1:2
Zeer waarschijnlijk	10	De kans dat dit optreedt is bijna zeker. Wanneer is wellicht niet duidelijk, maar dat het zal gebeuren wel	>50%	>1:2

Legenda - Gevolgen			
Categorie	Score	Beschrijving	Geldwaarde
Verwaarloosbaar	2	Gevolgen die hinderlijk zijn, maar in 1ste instantie te verwaarlozen. Géén prioriteit	<€ 100
Beperkt	4	Gevolgen die aandacht vereisen	€ 100 - € 1.000
Serieus	6	Gevolgen waar serieus rekening gehouden dient te worden en maatregelen vereisen	€ 1.000 - € 10.000
Kritiek	8	Gevolgen die slechts met heel veel moeite en kosten te beheersen zijn. Directe verbetering is noodzakelijk	€ 10.000 - € 100.000
Catastrofaal	10	Gevolgen die niet of nauwelijks te beheersen zijn en het einde van de organisatie kunnen betekenen. Werkzaamheden dienen gestopt te worden.	>€ 100.000