

Handreiking Risicomanagement op strategisch niveau

Datum	10 juni 2025
Status	DEFINITIEF

Colofon

Projectnaam	Handreiking Risicomanagement op strategisch niveau
Auteur(s)	Interdepartementale Werkgroep Risicomanagement

Inhoud

1	Inleiding—4
2	Strategisch niveau—5
3	Risicodialoog—6
4	Aanpak—7
5	Stappenplan voor de strategische risicoanalyse—8
6	Bijlage: Begrippen—10

1 Inleiding

Toepassing van de handreiking

Deze handreiking biedt een gestructureerde aanpak voor strategisch risicomanagement binnen ministeries. Het is een richtinggevend instrument dat departementen ondersteunt bij het versterken van hun strategisch risicobewustzijn en -sturing. De handreiking kan worden toegepast in verschillende organisatiecontexten: zowel bij het opstellen van één centrale strategische risicoanalyse als bij een meer thematische of directiegerichte aanpak. De uitgangspunten zijn generiek geformuleerd, met ruimte voor maatwerk in de toepassing, afhankelijk van de inrichting van het risicomanagement binnen het betreffende ministerie.

Uit verschillende initiatieven – zoals de interdepartementale werkgroep risicomanagement – komt naar voren dat het volwassenheidsniveau en de aanpak van risicomanagement verschilt per departement. Ook is niet altijd helder wat onder departementale risicoanalyses moet worden verstaan. De manier waarop de ambtelijke top invulling geeft aan dit onderwerp is per departement verschillend. Het toezicht op de uitvoering van de departementale risicoanalyse en advisering over deze analyse door directie FEZ is verankerd in het Besluit FEZ van het Rijk ¹.

Artikel 4, eerste lid, d, onder 3, van het Besluit FEZ van het Rijk:

*Het houden van toezicht op de uitvoering van **departementale risicoanalyses**;*

Artikel 4, eerste lid, f, onder 2:

*Op verzoek en uit eigen beweging in elk geval adviseren over de onderzoeken, voorstellen, voornemens, toezeggingen en **risicoanalyses***

Verantwoordelijkheden en governance

Risicomanagement is een integraal onderdeel van goed bestuur en de verantwoordelijkheid van alle lagen binnen een ministerie. De minister is op grond van artikel 3.3 van de Comptabiliteitswet 2016 eindverantwoordelijk voor het financieel en materieel beheer. Tegelijkertijd geldt dat strategische risico's vaak verder reiken dan het financiële domein en raken aan meerdere PIOFACH-processen, zoals personeel, informatievoorziening, uitvoering, toezicht en beleid. Risicomanagement helpt om samenhang aan te brengen in deze domeinen en draagt zo bij aan het realiseren van de strategische doelstellingen van het ministerie. Daarin wordt expliciet gesteld dat het toepassen van risicobeheer onderdeel is van een adequaat stelsel van intern beheer.

Binnen de rijksoverheid wordt het **Three Lines Model** gehanteerd. In dit model hebben beleidsdirecties (eerste lijn) en de financiële functie, zoals Directie FEZ (tweede lijn), ieder een eigen rol. De eerste lijn is verantwoordelijk voor het signaleren, analyseren en beheersen van risico's binnen hun beleidsdomein. De tweede lijn faciliteert, adviseert en houdt toezicht, zodat het MT of de bestuursraad beschikt over tijdige en betrouwbare informatie voor strategische besluitvorming. De onafhankelijke toetsing vindt plaats in de derde lijn, die wordt ingevuld door de interne auditfunctie.

Directie FEZ kan invulling geven aan deze rol door onder andere te rapporteren over het risicoproces, het begeleiden van risicodialogen en het opstellen van departementale kaders en handreikingen. Investeren in risicomanagementexpertise en heldere rolverdeling voor besluitvorming, communicatie en coördinatie draagt bij

¹ [Besluit FEZ met toelichting - Staatsblad 2019, 54 - OH.nl](#)
N.B.: Directie FEZ voert geen regie op risicomanagement.

aan de kwaliteit van risicomanagement. Ook audit committees kunnen hier sturend in zijn.

Deze handreiking biedt de mogelijkheid om risicomanagement tot een hoger volwassenheidsniveau te brengen en duidelijkheid te bieden over wat van een departementale risicoanalyse op strategisch niveau mag worden verwacht. Daarbij wordt zoveel mogelijk gebruik gemaakt van bestaande theoretische modellen en best practices bij de departementen. Verder kan de handreiking tot op zekere hoogte meer uniformiteit en eenduidigheid creëren betreffende de risicomanagementaanpak bij de departementen en ook door eenduidige definities voor de diverse begrippen te hanteren. Eenduidig risicomanagement (tot op zekere hoogte) zorgt ervoor dat risico's op een gestandaardiseerde en gestructureerde manier worden aangepakt en bevordert tevens de interdepartementale samenwerking voor het oppakken van departement overstijgende risico's. Een uniforme aanpak tot op zekere hoogte moedigt samenwerking aan. Als departementen – waar mogelijk en passend binnen geldende informatiebeveiliging en rubricering – openlijk en bewust risico's delen, kunnen zij elkaars risico's aanvullen of beheersmaatregelen versterken. Dit leidt tot het ontdekken van risico's die optreden op het snijvlak van departementen of die door de gehele overheid lopen.

Het is ook van belang om aan te geven dat er diverse gremia zijn waar er middels praktijkvoorbeelden worden aangetoond welke werkwijzen in de praktijk tot succesvol risicomanagement kunnen leiden. Het leerwerkatelier van de Rijksacademie is daar een voorbeeld van.

2 Strategisch niveau

De werkgroep erkent de veelzijdigheid van risicomanagement op verschillende vlakken. Risicomanagement op zowel strategisch niveau als op tactisch- en operationeel niveau speelt een belangrijke rol voor het dagelijks functioneren van een ministerie. Deze handreiking risicomanagement is bedoeld voor het geven van handvaten voor risicomanagement op strategisch niveau, maar kan ook helpen bij andere niveaus/thema's.

Een handreiking risicomanagement op strategisch niveau heeft verschillende voordelen, namelijk:

- Focus op lange termijn versus korte termijn
Strategische risicoanalyses richten zich vaak op de lange termijnrisico's die de strategische doelstellingen en de toekomstige prestaties van het departement kunnen beïnvloeden. Deze doelstellingen kunnen zowel beleidsmatig van aard zijn (zoals maatschappelijke transities, wetgeving of publieke dienstverlening) als bedrijfsvoering gericht (zoals personeelscapaciteit, informatieveiligheid of financiële continuïteit). Strategische risico's hebben doorgaans impact op de koers, reputatie, slagkracht of legitimiteit van het ministerie en verdienen daarom structurele aandacht, ongeacht of ze binnen het beleidsdomein of de ondersteunende processen liggen. Tactische en operationele risicoanalyses daarentegen richten zich vaak op de korte termijnrisico's die o.a. de financiële stabiliteit en de operationele prestaties van het departement kunnen beïnvloeden, omdat een minister jaarlijks beoordeeld wordt op het begrotingsbeheer en financieel beheer, etc.

- **Onzekerheden: Bedreigingen en kansen**
Strategische risicoanalyses kunnen zich proactief richten op het identificeren van bedreigingen maar ook op kansen die het bereiken van de strategische doelstellingen van het departement kunnen bevorderen. Het gaat hier bijvoorbeeld om nieuw beleid, technologische ontwikkelingen of veranderende regelgeving.
- **Verantwoordelijkheid en betrokkenheid**
Strategische risicoanalyses vereisen de betrokkenheid en samenwerking van de eerste lijn topmanagers in de bestuursraad en strategisch adviseurs. Dit draagt bij aan een gestructureerde aanpak van risicomanagement die het eigenaarschap en risicoleiderschap bij de top bevordert. Ook blijft risicomanagement op deze wijze niet los behandeld in de eerste en tweede lijn, maar wordt dit integraal in het departement onder de aandacht gebracht. Deze integrale aanpak is gunstig voor groei van risicovolwassenheid.

3 Risicodialoog

In een steeds dynamischer en complexe wereld is een geïntegreerde aanpak van risico's nodig. Het aanpakken van risicomanagement met bijvoorbeeld ingewikkelde modellen of meer regels en protocollen zal in zo een complexe omgeving niet tot voldoende resultaat leiden. Om risicomanagement niet tot een 'afvinklijst' te maken wordt daarom steeds meer nadruk gelegd op de risicodialoog. Martin van Staveren² omschrijft de risicodialoog als een gesprek over expliciet, realistisch en gestructureerd omgaan met onzekerheden, risico's en kansen, waarbij alle deelnemers aan het gesprek vrijmoedig spreken en openhartig luisteren. Een veel gebruikte methode voor de risicodialoog is het 'Doel-Onzeker-Doen' (DOD) aanpak. Het DOD-model zorgt voor een gerichte en eenvoudige aanpak om juist complexe vraagstukken terug tot de essentie te brengen. De drie belangrijke vragen bij deze aanpak zijn:

- 1) Wat is het Doel?
- 2) Wat is daarbij Onzeker?
- 3) Wat staat ons te Doen?

Het beantwoorden van deze vragen helpen om de doelen van de organisatie scherper te maken en geven daarnaast ook ruimte om de handelingsperspectieven te verkennen.

In de volgende paragraaf is een stappenplan weergegeven aan de hand waarvan de benadering van risicoanalyses kan worden aangepakt. Bij deze aanpak blijft het essentieel om de risicodialoog in alle aspecten als uitgangspunt mee te nemen.

² [Martin van Staveren, *Risicodialoog: Gericht aan de slag met de Doel-Onzeker-Doen-aanpak*, Boom, 2023](#)

4 Aanpak

Rol van Beleidsdirecties en Directies FEZ in de voorbereiding

Het risicomanagementproces op strategisch niveau is een gedeelde verantwoordelijkheid van beleidsdirecties en de FEZ-afdeling. De bestuursraad (BR) speelt een centrale rol in de besluitvorming, maar wordt daarbij ondersteund door medewerkers uit de eerste en tweede lijn.

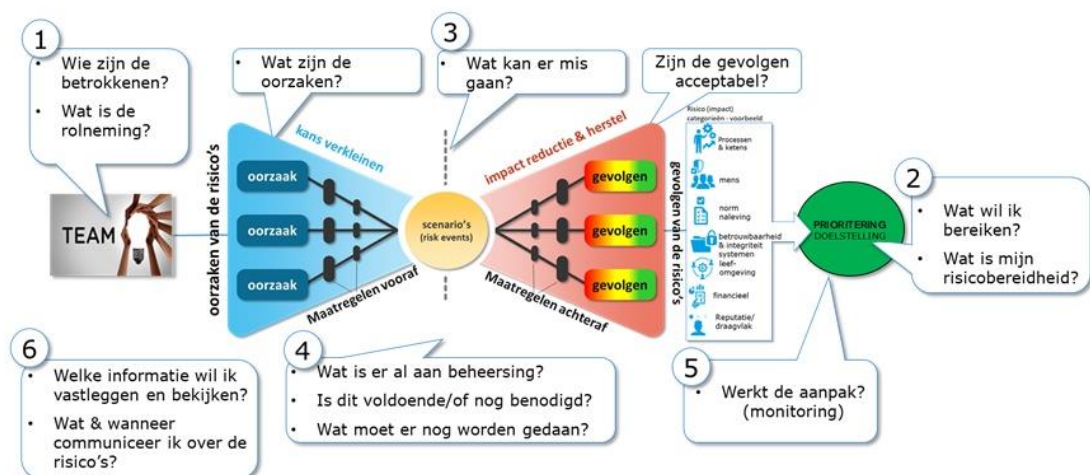
De beleidsdirecties leveren input over risico's binnen hun domein, signalen uit beleid en uitvoering, en relevante externe ontwikkelingen. Directie FEZ coördineert en faciliteert het proces, draagt zorg voor de methodologische ondersteuning, bewaakt de kwaliteit en samenhang van de risicoanalyse en kan optreden als procesbegeleider of risk facilitator.

Gezamenlijk bereiden zij de risicoanalyse voor, structureren de dialoog en zorgen ervoor dat de BR tijdig over de juiste informatie beschikt om strategische keuzes te maken.

Op basis van bestaande gerenommeerde modellen (waaronder COSO, ISO 31000) en praktijkervaringen/ best practices bij de departementen is onderstaand stappenplan ontwikkeld.

Dit stappenplan richt zich op risicoanalyses op strategisch niveau en dient met de bestuursraad te worden doorlopen. Daarbij is vanuit o.a. het oogpunt van risicoleiderschap gekozen voor een top-down benadering. Uiteraard kunnen hiernaast de belangrijkste operationele risico's bottom-up in de bestuursraad worden ingebracht. Bij het doorlopen van dit stappenplan is het essentieel om de risicodialoog in acht te nemen.

Onderstaande afbeelding geeft een weergave van de stappen.



5 Stappenplan voor de strategische risicoanalyse

STAP 1 Bepaal de uitgangspunten t.a.v. de organisatie (door de BR); wie zijn de actoren

- a. Organiseer de strategische risicoanalyse in een cyclisch proces van jaarlijkse actualisatie van de strategische risico's en de beheersing hiervan.
- b. Richt de analyse van risico's op de strategische doelen van het departement.

STAP 2 Bepaal de scope ³van de risicoanalyse (door de BR)

- a. Breng de strategische doelstellingen van het ministerie in beeld.
- b. Maak een onderbouwde selectie van doelstellingen die het meest in aanmerking komen voor verdere risicoanalyse, bijvoorbeeld op basis van hun strategische relevantie, onzekerheid of potentiële impact.
- c. Houd daarbij oog voor het totaalbeeld: een risicoanalyse hoeft niet alle doelen te omvatten, maar moet wel representatief zijn voor de belangrijkste aandachtsgebieden van het ministerie.
- d. Stem per geselecteerd doel de risicobereidheid af: welke risico's worden als acceptabel beschouwd, en waar liggen de grenzen?

STAP 3 Inventariseer en beoordeel de risico's (door BR)

- a. Breng relevante interne en externe ontwikkelingen systematisch in kaart en identificeer op basis daarvan de risico's die de realisatie van strategische doelstellingen kunnen beïnvloeden. Gebruik hierbij signalen uit zowel de organisatie als haar omgeving.
- b. Waardeer elk risico door de kans van optreden en de mogelijke impact op de doelstelling te bepalen. Dit kan kwalitatief (laag/midden/hoog) of kwantitatief, afhankelijk van wat binnen het ministerie gangbaar is.
- c. Prioriteer de risico's door ze te plotten in een risicomatrix of volgens een andere gehanteerde beoordelingsmethodiek.
- d. Focus op die risico's die boven de risicobereidheid uitkomen of die een disproportioneel effect kunnen hebben.

STAP 4 Behandel de (top) risico's (DG en BR)

- a. Bespreek de risicoanalyse met de directeuren-generaal (DG's). Toets of zij zich herkennen in de benoemde risico's en prioriteiten, en of zij aanvullingen of kanttekeningen hebben.
- b. Verzamel zo nodig input vooraf, maar zorg ook achteraf voor expliciete terugkoppeling of validatie. Dit bevordert zowel de kwaliteit van de analyse als het bestuurlijk draagvlak binnen het ministerie.
- c. Geef opdracht mee op het niveau van DG om de risico's op te pakken en hiervoor een uitvoerbaar beleidsadvies op te leveren over nieuwe en of aan te passen (beleids)maatregelen (houden/schrappen/aanvullen).
- d. BR neemt besluit op basis van bovenbedoelde beleidsadviezen welke risico's, wanneer kunnen worden geaccepteerd in relatie tot risicobereidheid en effectiviteit van de (beleids)maatregelen.

³ Ter voorbereiding is het van belang om een systematische analyse te maken van relevante externe en interne ontwikkelingen die invloed kunnen hebben op deze doelen. Denk hierbij aan wetswijzigingen, maatschappelijke of politieke trends, planbureaus, inspecties of ADR-rapportages (extern), en interne signalen zoals personele krapte, IT-veranderingen of indicatoren uit operationele risicoanalyses.

STAP 5 Monitor de (top) risico's en de werking van de maatregelen

- a. Leg vast hoe en door wie de BR tijdige en betrouwbare informatie ontvangt over de ontwikkelingen in de risico's en de effectiviteit van de getroffen beheersmaatregelen.
- b. Koppel de monitoring en evaluatie expliciet aan de PDCA-cyclus: Plan – Do – Check – Act.
- c. Richt als BR een proces in voor verantwoording en besluitvorming over risicobeheersing, inclusief het bijstellen van risico-inschattingen en maatregelen.
- d. Bespreek de risico's periodiek in de BR- en AC-overleggen, en eventueel in andere gremia.
- e. Sta expliciet stil bij de vraag of maatregelen hebben gewerkt, of aanvullende acties nodig zijn, en koppel de uitkomsten terug aan de DG's.

STAP 6 Registratie, Rapportage en Communicatie van risico's

- a. Bepaal welke gegevens voor het risicomanagement worden vastgelegd.
- b. Bepaal welke informatie en in welke vorm benut wordt voor besluitvorming.
- c. Bepaal welke risicomanagement informatie voor wie en wanneer beschikbaar is.
- d. Communiceer de risico-informatie zodanig dat deze is afgestemd op de belevingswereld van de verschillende doelgroepen en/of stakeholders voor de bijdrage aan het risicobewustzijn en het handelingsperspectief (bijv. voor het stimuleren van de zelfredzaamheid van burgers).

6 Bijlage: Begrippen

Risico: een onzekere toekomstige gebeurtenis of reeks gebeurtenissen die, als die zou plaatsvinden, een negatief dan wel gunstig effect zou hebben op het bereiken van doelstellingen.

Risicomanagement: alle processen met betrekking tot het expliciet identificeren, bepalen en beoordelen van risico's en kansen in lijn met de risicobereidheid, het aanwijzen van risico-eigenaren, het nemen van actie (maatregelen) om de risico's te mitigeren of hierop te anticiperen en het monitoren en reviewen van de voortgang.

Bruto en netto risico's: een bruto risico is de inschatting van een risico zonder daarbij eventueel aanwezige beheersmaatregelen in ogenschouw te nemen. Een netto (rest) risico is het risico waarbij de huidige aanwezige beheersmaatregelen wel in beschouwing worden genomen.

Risicobereidheid: verwijst naar het niveau van risico dat een ministerie bereid is te accepteren om zijn doelstellingen te bereiken. Het is een strategische keuze die aangeeft welke mate van onzekerheid het ministerie tolereert.

Risico-acceptatie: is het operationele proces waarin specifieke risico's, binnen de vastgestelde risicobereidheid, daadwerkelijk worden geaccepteerd door het ministerie. Dit betekent dat, ondanks de risico's, wordt besloten om geen verdere maatregelen te nemen omdat de risico's als beheersbaar en acceptabel worden beschouwd.

Risicobereidheid vs. risicoacceptatie

Risico-acceptatie is het praktische, operationele aspect van risicomanagement, terwijl risicobereidheid het strategische kader biedt waarbinnen deze beslissingen worden genomen. Ze zijn complementair: risicobereidheid bepaalt de grenzen en normen, terwijl risico-acceptatie de daadwerkelijke implementatie is binnen die grenzen. Voor een effectief risicomanagement binnen een ministerie moeten beide zorgvuldig op elkaar zijn afgestemd en regelmatig worden geëvalueerd en aangepast.

Kans (Waarschijnlijkheid): De kans of waarschijnlijkheid dat een specifiek risico zich voordoet. Dit kan variëren van zeer laag (bijna onmogelijk) tot zeer hoog (bijna zeker).

Impact (Gevolg): De potentiële gevolgen of effecten van het risico als het zich daadwerkelijk voordoet. De impact kan variëren van gering (weinig tot geen gevolgen) tot catastrofaal (zeer ernstige gevolgen voor het ministerie en zijn doelstellingen).

Risicomatrix: Een veelgebruikte methode om de relatie tussen kans en impact te visualiseren is de risicomatrix. In deze matrix worden de kans en de impact op een grafiek geplaatst, wat helpt bij het prioriteren van risico's.

Risk facilitator: Een risk facilitator is een professional die gespecialiseerd is in het begeleiden van risicomanagementprocessen binnen een organisatie of project. Deze persoon speelt een centrale rol in het identificeren, evalueren en beheren van

risico's die een impact kunnen hebben op het succes van een project of de werking van een organisatie.

Een risk facilitator bevordert een open communicatiecultuur rondom risico's, waardoor alle betrokken partijen beter op de hoogte zijn en beter voorbereid zijn om met risico's om te gaan. In essentie helpt een risk facilitator organisaties om veiliger en efficiënter te werken door risico's effectief te beheren en te minimaliseren.