

Toelichting BZK Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Aanleiding

De Nederlandse overheid wordt in toenemende mate geconfronteerd met ondermijnende activiteiten. Er is een toenemend risico op corruptie en ondermijning, waarbij criminelen, statelijke actoren en andere kwaadwillenden op zoek gaan naar ambtenaren die hen kunnen voorzien van informatie of andere diensten. Daarom hebben alle Rijksorganisaties via de Interdepartementale Commissie Bedrijfsvoering Rijk (ICBR) **de weerbaarheid tegen ondermijning als prioriteit** aangemerkt. Rijksorganisaties, -medewerkers en hun bedrijfsvoeringprocessen moeten weerbaar zijn tegen corruptie en ondermijning. Ook vanuit de zorgplicht voor een veilige en gezonde werkomgeving voor medewerkers. Dit draagt bij aan een betrouwbare, integere en effectieve overheid.

Corruptie en ondermijning

Bij corruptie wordt in eerste instantie vaak gedacht aan omkoping en steekpenningen. Omkoping is één van de bekendste vormen van corruptie, maar corruptie is meer dan omkoping alleen. Bij corruptie kan het ook gaan om het lekken van informatie en vervalsen van documenten. Ook verduistering en afpersing zou je onder corruptie kunnen scharen. Bij verduisteren gaat het om het stelen van goederen van de organisatie. Bij afpersing komt intimidatie, bedreiging of geweld kijken om iets gedaan te krijgen. We hanteren daarom de brede definitie waarbij corruptie wordt gedefinieerd als “het misbruik maken van toevertrouwde macht voor persoonlijk gewin”. Met toevertrouwde macht bedoelen we in dit geval de bijzondere positie van de overheid en het vertrouwen van de burger dat hier integer en veilig mee wordt omgegaan. Bij ondermijning ligt de nadruk op misbruik van toevertrouwde macht door een externe partij. Bij ondermijning maken criminelen gebruik van de diensten van burgers, ambtenaren, bestuurders en private bedrijven voor illegale activiteiten.

Corruptie en ondermijning onderscheiden zich van andere typen risico's doordat zij direct raken aan de integriteit van de overheid en het vertrouwen van burgers en bedrijven. Het gaat niet alleen om financiële schade, maar om het ondermijnen van democratische processen en het misbruiken van publieke functies voor kwaadwillende belangen. Het is noodzakelijk om deze risico's in beeld te brengen en te begrijpen, zodat organisaties kunnen anticiperen op pogingen tot beïnvloeding en misbruik van publieke functies, kunnen voorkomen dat risico's zich daadwerkelijke voordoen en voorbereid zijn om te handelen wanneer risico's zich toch materialiseren.

Open over kwetsbaarheden = Weerbaar tegen corruptie en ondermijning

Corruptie en ondermijning kunnen in verschillende vormen voorkomen, en kunnen overal plaatsvinden. De oorzaak van corruptie en ondermijningsrisico's kan liggen op het niveau van het individu en de organisatie. Kwetsbaarheden ontstaan door een combinatie van naïviteit, hoge werkdruk, onduidelijke regels, systemen die onvoldoende zijn ingericht op toezicht, financiële prikkels, en een gebrek aan bescherming of begeleiding van medewerkers. Het begint bijvoorbeeld bij een kleine vriendendienst waarbij de medewerker misschien niet eens doorheeft dat het geven van bepaalde informatie niet juist is. Of er is onvoldoende toezicht op autorisaties. De aanpak van corruptie en ondermijning vraagt om organisatiecultuur waarin het normaal is om met elkaar, open te spreken over risico's en kwetsbaarheden op het niveau van het individu en de organisatie zelf.

Doel toolkit

De toolkit stelt rijksorganisaties in staat om risico's te identificeren en mitigeren. Het tegengaan van corruptie en ondermijning is een gezamenlijke opdracht voor alle organisatieonderdelen. Het gaat uit van een **integrale aanpak** waar mens, cultuur, proces en (digitale) systemen samenkomen en zorgen voor een omgeving waar maatregelen worden genomen om corruptie en ondermijning te voorkomen, te detecteren en te melden en bestraffen. De verschillende expertises komen samen in de toolkit. KPMG heeft ondersteund in de totstandkoming van de toolkit.

De toolkit maakt onderdeel uit van de bredere aanpak om de weerbaarheid van de Rijksoverheid tegen ondermijning te vergroten. Deze aanpak heeft als doel om rijksambtenaren weerbaar te maken, en rijksorganisaties in te richten zodat zij rijksambtenaren en het overheidswerk voldoende kunnen beschermen. Deze toolkit is slechts één van de maatregelen die rijksorganisaties helpt om de weerbaarheid te vergroten en staat niet op zichzelf. Aan de hand van de resultaten van de risicoanalyse kunnen nieuwe maatregelen worden getroffen. Ook helpt de toolkit om rijksbreed het gesprek te voeren over bestaande risico's en hierop te acteren. Daarbij geldt dat de toolkit een kader biedt, waarbij individuele organisaties in de verschillende stappen eigen keuzes kunnen maken, afhankelijk van de organisatiecontext.



Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties

Toolkit risicoanalyse voor preventie corruptie en ondermijning

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
18-03-2026

Inhoudsopgave (1/2)

	Pagina	Relevante bijlage
1. Introductie	5	
1.1. Aanleiding	6	
1.2. Wat is het doel?	6	
1.3. Waarom een risicoanalyse voor de preventie van corruptie en ondermijning?	6	
1.4. Voor wie?	6	
1.5. Leeswijzer	6	
1.6. Belangrijke opmerkingen vooraf	7	
2. Risicomanagementcyclus	8	
3. Scope en contextbepaling	11	B,C,D,E
Inleiding	12	
Stap 1. Inzichtelijk maken organisatie en scope	12	
Stap 2. Vastleggen rollen en verantwoordelijkheden	13	
4. Risicobeoordeling	15	F,G,H,I,J,K,L,M,N
Inleiding	16	
Stap 3. Identificatie van risico's, oorzaken, gevolgen en huidige beheersmaatregelen (Risico-identificatie)	17	

	Pagina	Relevante bijlage
Stap 4. Analyse maken van kans en impact van de risico's (Risicoanalyse)	18	
Stap 5. Opstellen risicobeeld (Risicoanalyse)	19	
Stap 6. Evaluatie van risico's (Risico-evaluatie)	19	
Stap 7. Vaststellen risicobereidheid (Risico-evaluatie)	20	
Stap 8. Bepalen risicorespons (Risico-evaluatie)	21	
5. Risicobehandeling	22	N
Inleiding	23	
Stap 9. Beschrijven beheersmaatregelen en acties	23	
Stap 10. Zorgen voor implementatie en borging	23	
6. Rapporteren	24	F,M,O
Inleiding	25	
Stap 11. Rapporteren van toprisico's, vastgestelde beheersmaatregelen, ontwikkelingen en actieplannen	25	
7. Monitoren en communiceren	26	P
Inleiding	27	
Stap 12. Voortgang actieplannen monitoren	27	
Stap 13. Communiceren over het belang, de voortgang, feedback en acties	28	

Inhoudsopgave (2/2)

	Pagina	Relevant hoofdstuk
Bijlagen	29	
A. Begrippenlijst	30	Allen
B. Template context organisatie	33	3
C. Voorbeeld rollen en verantwoordelijkheden	34	3
D. RASCI-model	38	3
E. Voorbeeld ingevuld RASCI-model	39	3
F. Template risicoregister	40	4,6
G. Bow-Tie methodiek	42	4
H. Voorbeeldrisico's corruptie en ondermijning	43	4
I. Integriteitscultuurmodel	45	4
J. Voorbeeldvragen ten behoeve van de grondoorzakenanalyse	46	4
K. Voorbeeldoorzaken lage meldingsbereidheid	49	4
L. Impactschalen	50	4
M. Template kans- en impactmatrix en heatmap	51	4,6
N. Voorbeelden beheersmaatregelen	52	4,5
O. Rapportage opzet	55	6
P. Voorbeelden communicatiemateriaal	57	7
Q. Verdere relevante Rijksbrede documenten	59	Allen

	Pagina	Relevant hoofdstuk
Losse bijlagen		
R. Vragen t.b.v. het risicobeeld (Word document)		3,4
X. Templates in Excel (Excel document)		3,4

01. Introductie

01. Introductie

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

1.1. Aanleiding

De rijksoverheid is kwetsbaar voor corruptie en ondermijning. Criminelen en andere kwaadwillenden proberen toegang te krijgen tot gevoelige informatie of producten. Dit bedreigt niet alleen de medewerkers en bedrijfsprocessen, maar ook het vertrouwen van burgers in de overheid. Door bewustwording van risico's en gerichte maatregelen **gericht op mens, cultuur, proces en systemen** versterken we het vertrouwen in een eerlijke en rechtvaardige overheid.

1.2. Wat is het doel?

Deze toolkit biedt praktische handvatten voor het uitvoeren van een risicoanalyse met als doel het risico op corruptie en ondermijning te herkennen, voorkomen en zo goed als mogelijk te beheersen.

1.3 Waarom een risicoanalyse voor de preventie van corruptie en ondermijning?

Risicomanagement helpt organisaties om beter om te gaan met onvoorziene gebeurtenissen en risico's. Je identificeert, analyseert, evalueert en pakt risico's aan die de dienstverlening en het goede functioneren van jouw organisatie kunnen belemmeren. Risico's klinken vaak negatief, maar het gebruik van risicomanagement biedt juist een kans. Het houdt de organisatie een spiegel voor en bereidt de organisatie voor op veranderingen en dreigingen als deze zich daadwerkelijk voordoen. De voorliggende toolkit helpt organisaties om corruptie en ondermijningsrisico's tijdig in kaart te brengen en zo goed als mogelijk te voorkomen dat deze risico's zich daadwerkelijk voordoen. Daarmee verandert een incident gedreven cultuur in een proactieve, weerbare cultuur.

De toolkit sluit aan op bestaande risicomanagementmethoden binnen de rijksoverheid en kan worden aangevuld met andere type risico's. Voor vragen of opmerkingen over de toolkit, kan contact worden opgenomen met PostbusPIM@minbzk.nl en weerbaarheidbvrijk@minbzk.nl.

1.4. Voor wie?

De toolkit is met name bedoeld voor rijksambtenaren verantwoordelijk voor het uitvoeren en/of begeleiden van risicoanalyses op corruptie en ondermijning voor hun organisatie. Belangrijke stakeholders hierbij zijn de BVA/BVC, CISO, integriteitscoördinator en HR-directeur.

Daarnaast dragen alle rijksambtenaren (inclusief leidinggevend en medewerkers) verantwoordelijkheid voor integriteit en veiligheid in hun taakuitoefening.

1.5. Leeswijzer

De toolkit is als volgt opgebouwd:

- Dit hoofdstuk beschrijft de aanleiding, het doel en de doelgroep van de toolkit;
- Hoofdstuk 2 licht de risicomanagementcyclus toe, inclusief een roadmap;
- Hoofdstuk 3 beschrijft de scope en contextbepaling;
- Hoofdstuk 4 introduceert de sub-fasen van risicobeoordeling en het risicoregister;
- Hoofdstuk 5 gaat in op de beheersmaatregelen en beoordeling daarvan;
- Hoofdstuk 6 beschrijft de risicorapportage;
- Hoofdstuk 7 zet de monitoring van risico's en beheersmaatregelen uiteen.

In de bijlagen zijn begrippen, diverse templates, modellen, voorbeelden en communicatiemateriaal te vinden.

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

01. Introductie

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

1.6. Belangrijke opmerkingen vooraf

- In deze pilot wordt **corruptie** gezien als het misbruik van toevertrouwde macht voor persoonlijk gewin. Vormen van ambtelijke corruptie zijn bijvoorbeeld omkoping, schending van ambtsgeheim, oplichting, valsheid in geschrifte of fraude. Een voorbeeld: toekennen van een subsidie aan een bevriende partij.
- Daarnaast wordt **ondermijning** gezien als het gebruik van legale structuren, diensten of voorzieningen om illegale activiteiten uit te voeren, waardoor het maatschappelijk systeem wordt aangetast. Het is een containerbegrip dat ook corruptie, fraude en andere vormen van criminaliteit omvat. Ondermijning speelt zich niet alleen af tussen een 'boven-' en 'onderwereld', maar kent ook een grijs gebied en betrokkenen handelen niet altijd met slechte intenties.
- Corruptie en ondermijning zijn een multidisciplinair probleem en vragen om een **integrale aanpak**. Om alle corruptie en ondermijningsrisico's op te halen, is het belangrijk dat een multidisciplinair team wordt betrokken bij de risicoanalyse. Dit betreft zowel experts op het gebied van risicomanagement, integriteit, corruptie en ondermijning als medewerkers binnen de afdelingen waar de risicoanalyse wordt uitgevoerd om een holistisch beeld te krijgen van de huidige risico's. De risicoanalyse brengt kennis over mens, cultuur, veiligheid en informatiebeveiliging samen. Alleen dan is de risicoanalyse compleet.
- Risicomanagement is **een continu proces**. Dit betekent dat het proces en de stappen omschreven in de toolkit periodiek terugkomen. Het is geen eenmalige exercitie. Dit is belangrijk, omdat de wereld snel verandert en daarmee de risico's die op ons afkomen ook. Het wordt aangeraden om de toolkit te verbinden aan de Planning en control of PCDA-cyclus. Ook helpt het om de uitvoering van de risicoanalyse terug te laten komen in jaarplannen van de betrokken teams, zodat er voldoende tijd en capaciteit kan worden gereserveerd om de stappen te doorlopen.
- Risicomanagement is effectief als het **geén papieren werkelijkheid** is. Hiermee wordt bedoeld dat risicomanagement doorleefd moet worden en onderdeel moet zijn van het continue proces. **Bestuurlijke commitment** is essentieel voor de uitvoering van risicomanagement.
- De toolkit biedt een methode om een risicoanalyse gericht op corruptie en ondermijningsrisico's uit te voeren, en biedt **praktische handvatten**. Het is aan individuele organisaties om hiermee aan de slag te gaan. Individuele organisaties kunnen aan de hand van de toolkit en hun ervaringen bepaalde eigen keuzes maken in het proces. Bijvoorbeeld over de manier waarop zij kans maal impact scoren, of de vormgeving van de workshops. Ook helpt de toolkit organisaties die nog helemaal niet bekend zijn met risicomanagement of de identificatie van corruptie- en ondermijningsrisico's. Deze organisaties worden aangemoedigd om vooral 'gewoon te doen' en te starten.
- De toolkit is een **levend document**. Dit betekent dat aan de hand van ervaringen bij organisaties de toolkit kan worden aangescherpt en aangevuld met veelvoorkomende risico's en verdere passende maatregelen.

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

02. Risicomanagementcyclus

02. Risicomanagementcyclus (1/2)

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Dit hoofdstuk behandelt de risicomanagementcyclus, alsmede de meest relevante concepten. Het risicomanagementproces is gebaseerd op de vier fasen van de risicomanagementcyclus, zoals hieronder geïllustreerd. De cyclus is gebaseerd op wetenschappelijke risicomanagementmodellen en sluit aan op bestaande risicomanagementmethoden binnen de rijksoverheid. De cyclus komt overeen met de P&C en/of PCDA-cyclus en moet herhaald worden. In de tabel aan de rechterkant zijn de fasen nader beschreven. De overige hoofdstukken geven een toelichting over deze fasen. Relevante begrippen die worden gebruikt in dit document zijn opgenomen in ‘*Bijlage A. Begrippenlijst*’.



Figuur 1. De risicomanagementcyclus

1. Scope en contextbepaling (Hoofdstuk 3)

De eerste fase betreft een verkenning van de organisatie, haar missie en de relevante rollen en verantwoordelijkheden in de risicomanagementcyclus. Dit is de basis voor de volgende fasen.

A. Identificatie (Hoofdstuk 4.3)

In de identificatiefase worden de ongewenste gebeurtenissen in kaart gebracht, de risico's gedefinieerd, de oorzaken en gevolgen vastgesteld en de bestaande beheersmaatregelen verzameld.

B. Analyse (Hoofdstuk 4.4)

Na de analyse van risico's en huidige beheersmaatregelen, volgt een analyse naar de kans en impact van de geïdentificeerde risico's. De risicoscore (kans maal impact) wordt getoetst tegen de risicobereidheid van de organisatie.

C. Evaluatie (Hoofdstuk 4.5)

Op basis van de risicoanalyse wordt de risicoscore bepaald (i.e., accepteren, monitoren, mitigeren of overdragen). Mitigeren bestaat doorgaans uit het nemen van additionele beheersmaatregelen.

2. Risicobeoordeling (Hoofdstuk 4)

Wanneer er is besloten om additionele beheersmaatregelen te nemen, moet er een risicomanagement actieplan worden opgesteld. Hierbij wordt er ook gekeken naar hoe succes wordt gemeten en hoe deze maatregelen geborgd en gemonitord moet worden.

3. Risicobehandeling (Hoofdstuk 5)

In deze fase wordt gerapporteerd op de toprisico's, vastgestelde beheersmaatregelen en actieplannen. De resultaten worden vastgelegd en gerapporteerd aan de relevante (interne en externe) stakeholders.

4. Rapporteren (Hoofdstuk 6)

De risico's en beheersmaatregelen worden continu of periodiek gemonitord. Dit omvat het monitoren van (wijzigingen in) de risico's, het toetsen van de effectiviteit van beheersmaatregelen en het bijhouden van de voortgang van de actieplannen. Op basis hiervan wordt bepaald of aanvullende acties nodig zijn. De bevindingen worden periodiek gecommuniceerd naar de relevante stakeholders.

Tabel 1. Overzicht risicomanagementcyclus-fasen

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

02. Risicomanagementcyclus (2/2)

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

Fase	Doel	Stappen	Rollen	Output
1. Scope en contextbepaling (Hoofdstuk 3)	Het startpunt bepalen	1. Inzichtelijk maken organisatie en scope 2. Vastleggen rollen en verantwoordelijkheden	- Risicomanager - Lijnmanagement	Contextdocument (zie ' Bijlage B. Template context organisatie ').
2. Risicobeoordeling (Hoofdstuk 4)	A. Identificatie (Hoofdstuk 4.3)	3. Identificatie van risico's, oorzaken, gevolgen en huidige beheersmaatregelen	- Lijnmanagement - Medewerkers	Risicoregister (zie ' Bijlage F. Template risicoregister ').
	B. Analyse (Hoofdstuk 4.4)	4. Analyse maken van kans en impact van de risico's 5. Opstellen risicobeeld	- Lijnmanagement - Medewerkers	Risicobeeld (zie ' Bijlage M. Template kans- en impactmatrix en heatmap ').
	C. Evaluatie (Hoofdstuk 4.5)	6. Evaluatie van risico's 7. Vaststellen risicobereidheid 8. Bepalen risicorespons	- Lijnmanagement - Medewerkers - Directie (onder Directoraten-generaal)	Risicorespons
3. Risicobehandeling (Hoofdstuk 5)	De beheersmaatregelen bedenken en actieplannen uitwerken	9. Beschrijven beheersmaatregelen en acties 10. Zorgen voor implementatie en borging	- Lijnmanagement - Afdeling(en) in scope	Actieplan (zie ' Bijlage N. Voorbeelden beheersmaatregelen ').
4. Rapporteren (Hoofdstuk 6)	De resultaten en ontwikkelingen vastleggen	11. Rapporteren van toprisico's, vastgestelde beheersmaatregelen, ontwikkelingen en actieplannen	- Risicomanager - Lijnmanagement	Rapportage en dashboard (zie ' Bijlage O. Rapportage opzet ').
Monitoren en communiceren (Hoofdstuk 7)	Monitoren van voortgang en hierover communiceren	12. Voortgang van actieplannen monitoren 13. Communiceren over het belang, de voortgang, feedback en acties	- Risicomanager - Lijnmanagement - Directie (onder Directoraten-generaal) (Plaatsvervangend) Secretaris-generaal	Plan voor monitoren en communicatie (zie ' P. Voorbeelden communicatiemateriaal ').

Tabel 2. Overzicht risicomanagementcyclus-fasen en stappen



Tip: Toelichting per stap

De stappen 1 t/m 13 worden toegelicht in de hoofdstukken die hierna volgen. Klik op de stappen om direct naar de toelichting te gaan.

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

03. Scope en contextbepaling

03. Scope en contextbepaling (1/3)

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

Inleiding

Als onderdeel van de risicomanagementcyclus is het van belang om eerst een goed begrip te krijgen van de organisatie waarvoor de risicoanalyse wordt uitgevoerd, namelijk de scope en contextbepaling. Dit omvat onder andere inzicht in de doelstellingen, missie, visie en de belangrijkste bedrijfsprocessen. Daarnaast is het cruciaal om duidelijke rollen en verantwoordelijkheden vast te stellen. Het bepalen van deze elementen zorgt ervoor dat de risicomanagementcyclus effectief en efficiënt kan worden uitgevoerd, doordat iedereen zich richt op de risico's en beheersmaatregelen die binnen zijn of haar domein vallen.

Stap 1. Inzichtelijk maken organisatie en scope

Voordat je risico's kunt analyseren, moet je begrijpen hoe de organisatie werkt. Denk aan doelstellingen, missie, visie en de belangrijkste processen. Ook is het belangrijk om rollen en verantwoordelijkheden duidelijk vast te leggen. Stel hierbij de volgende vragen:

- Wat is het doel, de missie en visie van de organisatie?
- Wat is de scope van de risicoanalyse? Gaat het om de hele organisatie, een afdeling of proces?
- Wat zijn de belangrijkste klanten, producten, diensten en partners?
- Zijn er recente veranderingen in klanten, producten of organisatie?
- Zijn er binnen de scope kwetsbare functies die extra gevoelig zijn voor integriteitsrisico's? Zijn er processen en diensten die extra relevant zijn voor kwaadwillenden of gevoelig zijn voor corruptie en ondermijning? Gebruik hiervoor bijvoorbeeld de TBB's van jouw organisatie.
- Welke externe en interne ontwikkelingen (bijv. geopolitiek, technologie, incidenten) spelen een rol?
- Welke wet- en regelgeving en interne gedragsregels zijn van toepassing?

De informatie wordt opgenomen in het daarvoor bedoelde template (zie '[Bijlage B. Template context organisatie](#)').

Verzamelen van informatie voor de scope en contextbepaling

Je verzamelt informatie door de volgende stappen te doorlopen:

- Documentanalyse: analyseren van interne beleidsdocumenten, compliance- en auditrapporten, (geanonimiseerde) meldingen en incidenten, plus externe bronnen zoals risicoanalyses en nieuws.
- Het afnemen van oriënterende gesprekken: In deze stap worden belangrijke sleutelfiguren uitgenodigd voor oriënterende gesprekken om inzicht te krijgen in de scope en context van de risicoanalyse. Deze gesprekken gaan onder andere in op de vragen die in stap 1 zijn uiteengezet en creëren een gezamenlijk begrip van de huidige situatie, belangen en verwachtingen. Deze gesprekken stemmen ook de rollen en verantwoordelijkheden met betrekking tot risicomanagement op elkaar af (zie stap 2). De stakeholders voor de oriënterende gesprekken zijn leidinggevend in de scope en experts op het gebied van risicomanagement, integriteit, corruptie en ondermijning, zoals de CISO, BVA/BVC, integriteitscoördinator en HR-adviseur. Een paar tips voor het afnemen van interviews:
 - Maak het doel van de oriënterende gesprekken (een duidelijke scope en relevante context) helder aan het begin van het gesprek.
 - Stel open vragen die niet leidend zijn. Bied ruimte aan de sleutelpersonen om zelf informatie aan te dragen.
 - Laat het een gesprek zijn in plaats van een vragenlijst. Ondanks dat het wordt gestimuleerd om de in stap 1 opgenomen vragen te behandelen, krijg je meer informatie door verder te vragen naar antwoorden die worden gegeven. Een voorbeeld: wanneer er gesproken wordt over relevante ontwikkelingen, vraag je dan af waar deze vandaan komen en of hier ook rekening mee moet worden gehouden.

Inhoudsopgave

- [01. Introductie](#)
- [02. Risicomanagementcyclus](#)
- [03. Scope en contextbepaling](#)
- [04. Risicobeoordeling](#)
- [05. Risicobehandeling](#)
- [06. Rapporteren](#)
- [07. Monitoren en communiceren](#)

Bijlagen

Relevante bijlagen

- [Bijlage A. Begrippenlijst](#)
- [Bijlage B. Template context organisatie](#)
- [Bijlage C. Voorbeeld rollen en verantwoordelijkheden](#)
- [Bijlage D. RASCI-model](#)
- [Bijlage E. Voorbeeld ingevuld RASCI-model](#)

03. Scope en contextbepaling (2/3)

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.



Het bepalen van de scope

De scope van een risicoanalyse kan op verschillende manieren worden vastgesteld. Soms kies je voor de hele organisatie, waarbij alle afdelingen of processen periodiek aan bod komen. In andere gevallen richt je je op een specifieke afdeling of proces, bijvoorbeeld na een incident.

- **Organisatie als scope.** Door de hele organisatie als scope te nemen, ontstaat een integraal beeld van risico's over afdelingen, functies en processen heen. Dit maakt het mogelijk om organisatiebrede kwetsbaarheden te identificeren, zoals onduidelijke governance of inconsistent toegepaste beheersmaatregelen. Het voordeel van deze scope is dat je samenhang en herhaling van risico's herkent en prioriteiten kunt stellen die effect hebben op de organisatie als geheel, in plaats van één onderdeel. Dit is vooral waardevol voor strategische besluitvorming en het versterken van het overall risicobeheersingsniveau.
- **Proces als scope.** Bij een proces krijg je een volledig beeld van kwetsbaarheden van begin tot eind. Door het hele proces in scope te nemen, zie je waar overdrachtsmomenten zijn, wie alleen kan handelen, welke systemen toegankelijk zijn en welke partijen betrokken zijn. Dit helpt om risico's in het proces goed te begrijpen.
- **Afdeling als scope.** Bij een afdeling analyseer je een deel van een organisatie die samenwerkt aan een gemeenschappelijk doel. Je kijkt naar werkwijzen en mogelijke kwetsbaarheden. Het voordeel is dat je de hele afdeling kunt versterken en risicobewust kunt maken. Dit biedt ook kansen om vervolgacties samen met de afdeling op te pakken.

Stap 2. Vastleggen rollen en verantwoordelijkheden

In '[Bijlage C. Voorbeeld rollen en verantwoordelijkheden](#)', 'Figuur 2. Schematisch overzicht van rollen en verantwoordelijkheden' zijn (indicatieve) rollen en verantwoordelijkheden in het risicomanagementproces weergegeven. De opgenomen rollen en verantwoordelijkheden vormen een voorstel en dienen per organisatie te worden gespecificeerd op basis van de eigen structuur en processen. De figuur is gebaseerd op de mogelijke organisatie binnen een departement. Zie de opvolgende tabellen (Tabel 7) in '[Bijlage C. Voorbeeld rollen en verantwoordelijkheden](#)' voor nadere toelichting van de in figuur opgenomen rollen.

Per organisatie, afdeling en/of proces in scope dient te worden bepaald wie waarvoor verantwoordelijk is en wie moet worden betrokken in het proces. Hiervoor kan bijvoorbeeld een RASCI-model gebruikt worden. Hierin wordt onderscheid gemaakt tussen Responsible (verantwoordelijk), Accountable (eindverantwoordelijk), Supporting (ondersteunend), Consulted (geraadpleegd) en Informed (geïnformeerd). Zie '[Bijlage A. Begrippenlijst](#)', '[Bijlage D. RASCI-model](#)' en '[Bijlage E. Voorbeeld ingevuld RASCI-model](#)' voor nadere toelichting van het RASCI-model.

Binnen het risicomanagementproces vervult elke organisatie een eigen rol en kent een eigen verantwoordelijkheid. BZK vervult een coördinerende verantwoordelijkheid en de inhoudelijke verantwoordelijkheid voor het implementeren van risicomanagement ligt bij de departementen en uitvoeringsorganisaties.¹ De ambtelijke leiding van departementen en uitvoeringsorganisaties draagt de eindverantwoordelijkheid voor risicomanagement binnen de eigen organisatie.

¹ De rollen en verantwoordelijkheden van de ambtelijke leiding, BZK en de uitvoeringsorganisaties zijn vastgelegd in het Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst, Ambtenarenwet 2017, Besluit BVA-stelsel rijksdienst 2021 (wordt momenteel herzien) en Besluit CIO-stelsel rijksdienst 2026.

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

[Bijlage B. Template context organisatie](#)

[Bijlage C. Voorbeeld rollen en verantwoordelijkheden](#)

[Bijlage D. RASCI-model](#)

[Bijlage E. Voorbeeld ingevuld RASCI-model](#)

03. Scope en contextbepaling (3/3)

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

BZK is verantwoordelijk voor:

- Stellen van kaders, monitoren en signaleren op het terrein van bedrijfsvoering.
- Het faciliteren van kennisdeling en best practices tussen departementen en uitvoeringsorganisatie;
- Het zorgdragen dat de op Rijksniveau bepaalde normen en regels worden nageleefd.

De ambtelijke leiding van departementen en uitvoeringsorganisaties is verantwoordelijk voor:

- Het implementeren van de rijksbrede kaders en richtlijnen in het kader van risicomanagement;
- Het coördineren van het risicomanagementproces binnen de eigen organisatie;
- Eindverantwoordelijk voor het decentrale risicobeeld en de opvolging van de nieuwe maatregelen.

Departementen en uitvoeringsorganisaties zijn verantwoordelijk voor:

- Het opstellen van risicoprofielen binnen hun eigen organisatie;
- Het identificeren, analyseren en evalueren van risico's en het implementeren en monitoren van beheersmaatregelen;
- Het cydisch toepassen van de toolkit in de organisatie.



Tip: Organiseer een startbijeenkomst voor de risicoanalyse

Bestuurlijke commitment is essentieel voor een effectieve risicoanalyse waarbij opvolging wordt gegeven aan de uitkomsten. Organiseer een startbijeenkomst op managementniveau (afhankelijk van bepaalde scope) zodat alle betrokken organisatiedelen vanaf het begin betrokken zijn bij het traject.

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

[Bijlage B. Template context organisatie](#)

[Bijlage C. Voorbeeld rollen en verantwoordelijkheden](#)

[Bijlage D. RASCI-model](#)

[Bijlage E. Voorbeeld ingevuld RASCI-model](#)

04. Risicobeoordeling

04. Risicobeoordeling (1/6)

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

Inleiding

In deze fase bepaal je welke risico's belangrijk zijn, hoe groot hun kans en impact is, en of ze acceptabel zijn. Dit vormt de basis voor het nemen van maatregelen. De risicobeoordeling bestaat uit drie stappen:

- A. **Risico-identificatie:** Welke corruptie en ondermijningsrisico's zijn er? Wat zijn de oorzaken, gevolgen en bestaande maatregelen? (Stap 3)
- B. **Risicoanalyse:** Hoe groot is de kans dat het risico zich voordoet? En, hoe groot is de impact van het risico als deze zich voordoet? (Stappen 4 en 5)
- C. **Risico-evaluatie:** Welke risicoscore is passend op basis van het risicoprofiel en de risicobereidheid van de organisatie en de geldende wet- en regelgeving en interne normenkaders? (Stappen 6, 7 en 8)

Meer uitleg over deze stappen vind je in de volgende paragrafen.

Verzamelen van informatie voor de gehele risicobeoordeling

In de risicobeoordeling worden risico's, oorzaken, gevolgen en huidige beheersmaatregelen geïdentificeerd aan de hand van interviews en workshops met relevante stakeholders. Stakeholders zijn medewerkers en leidinggevend in de scope en experts op het gebied van risicomanagement, integriteit, corruptie en ondermijning, zoals de CISO, BVA/BVC, integriteitscoördinator en HR-adviseur.

- **Verdiepende interviews:** Tijdens een beperkt aantal interviews met verschillende stakeholders worden relevante risicoscenario's (bestaande uit de ongewenste gebeurtenissen of risico's, oorzaken en gevolgen) en huidige beheersmaatregelen besproken. Hiermee wordt de basis gelegd voor het risicoregister (zie Stap 3. Risico-identificatie) die verder zal worden aangescherpt tijdens de workshops. De verdiepende interviews zijn onderdeel van Stap 3. Een paar tips voor het afnemen van interviews:

- Stel open vragen. Bied ruimte aan de stakeholders om zelf informatie aan te dragen zonder dat zij hierin te veel gestuurd worden. Gebruik hiervoor bijvoorbeeld de vragen die zijn opgenomen in de losse bijlage '**Bijlage R. Vragen t.b.v. het risicobeeld**'.
- Maak duidelijk dat het interview gaat om risico's en niet om bestaande kwetsbaarheden. Daag stakeholders uit om out-of-the-box te denken en hun beeld niet teveel te laten beïnvloeden door bestaande kwetsbaarheden en beheersmaatregelen.
- Gebruik het inzicht in de organisatie om gesprekspartners kritisch te bevragen. Aan elk kwetsbaar proces of kwetsbare dienstverlening kleven corruptie en ondermijningsrisico's.

- **Workshop 1:** Tijdens deze workshop worden de risicoscenario's en beheersmaatregelen getoetst in een bredere groep. Het doel van de workshop is het valideren, aanvullen en/of aanscherpen van de risicoscenario's, de grondoorzaken en de beheersmaatregelen (onderdeel van Stap 3). Tijdens of na afloop van de workshop worden risicoscenario's door de deelnemers – onafhankelijk van elkaar – gescoord op kans en impact (zie op de volgende pagina's de opties; onderdeel van Stap 4).
- **Workshop 2:** Tijdens deze workshop reflecteren de deelnemers op het risicobeeld c.q. de risicoscores (onderdeel van Stap 5). Het doel is om te komen tot een gedragen risicobeeld, zodat passende maatregelen – met de juiste prioriteit – kunnen worden genomen (ter voorbereiding op Stap 6 en 7).

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

[Bijlage F. Template Risicoregister](#)

[Bijlage G. Bow-Tie methodiek](#)

[Bijlage H. Voorbeeldrisico's corruptie en ondermijning](#)

[Bijlage I. Integriteitscultuurmodel](#)

[Bijlage J. Voorbeeldvragen ten behoeve van de grondoorzakenanalyse](#)

[Bijlage K. Voorbeeldoorzaken lage meldingsbereidheid](#)

[Bijlage L. Impactschalen](#)

[Bijlage M. Template kans- en impactmatrix en heatmap](#)

[Bijlage N. Voorbeelden beheersmaatregelen](#)

04. Risicobeoordeling (2/6)

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning



Mogelijke werkwijze workshop 1: scoring

- **Scoring gedurende workshop 1.** Deelnemers geven tijdens de workshop een score aan elk risicoscenario op kans en impact om te komen tot een gedeeld beeld. Daarna wordt besproken welke risicoscenario's het hoogst scoren en waarom, en waar de scores van elkaar verschillen. Deze discussie laat vaak zien dat risicoscenario's verschillend worden geïnterpreteerd, wat helpt om ze verder aan te scherpen. Na de workshop maakt de facilitator een risicobeeld op basis van de scores en gesprekken. Dit risicobeeld wordt besproken in workshop 2.
- **Scoring na afloop van workshop 1.** De facilitator scherpt c.q. vult risicoscenario's aan op basis van de discussies tijdens de workshop. Iedere deelnemer krijgt twee weken de tijd om de aangepaste risicoscenario's op kans en impact te scoren. De facilitator analyseert de scores, kijkt naar de hoogste risico's en afwijkingen en bespreekt deze in workshop 2. Ook hier blijkt vaak dat risicoscenario's anders zijn begrepen, waarna ze verder worden aangescherpt en scores – waar nodig – worden aangepast. Na de workshop stelt de facilitator een risicobeeld op.

Stap 3. Identificatie van risico's, oorzaken, gevolgen en huidige beheersmaatregelen (Risiko-identificatie)

De eerste stap in de risicobeoordeling is het identificeren van corruptie en ondermijningsrisico's binnen de vastgestelde scope. Hierbij beschrijf je de risico's op corruptie en ondermijning, inclusief de mogelijke oorzaken, gevolgen en bestaande beheersmaatregelen. Dit kan worden gedaan aan de hand van de volgende stappen:

1. Inventariseer ongewenste resultaten c.q. uitkomsten. Maak hierbij inzichtelijk:
 - Welke – interne en externe – incidenten bekend zijn over corruptie en ondermijning (Gebruik hiervoor ook de voorbeeldrisico's uit '[Bijlage H. Voorbeeldrisico's corruptie en ondermijning](#)') en hoe die ook op de het proces c.q. de afdeling in scope van toepassing kunnen zijn?
 - Wat er fout kan gaan in het licht van het behalen van (bedrijfs)doelstellingen?

2. Bepaal oorzaken die kunnen leiden tot een ongewenste uitkomst. Hierbij kunnen de '5 maal waarom-methode' (zie volgende pagina) en de 'Signalenkaart Betrouwbare overheid' worden gebruikt en kan er onder andere gekeken worden naar cultuuraspecten aan de hand van het Integriteitscultuurmodel (nader toegelicht in '[Bijlage I. Integriteitscultuurmodel](#)' en '[Bijlage J. Voorbeeldvragen ten behoeve van de grondoorzakenanalyse](#)').
3. Bepaal de gevolgen wanneer het risico werkelijkheid wordt. Ter inspiratie kan gekeken worden naar de impactschalen zoals opgenomen in '[Bijlage L. Impactschalen](#)'.
4. Breng de huidige preventieve, detectieve en repressieve beheersmaatregelen in kaart. Door de '5W-1H methodiek' kunnen de huidige beheersmaatregelen overzichtelijk in kaart worden gebracht. Een toelichting op de typen beheersmaatregelen en de toepassing van de '5W-1H-methodiek' is opgenomen in hoofdstuk '5. Risicobehandeling' (zie ook '[Bijlage N. Voorbeelden beheersmaatregelen](#)').

De informatie wordt verzameld via documentanalyse, interviews en workshops met verschillende stakeholders. Dit geeft een breed beeld van risico's en bestaande beheersing. Voor een overzichtelijke vastlegging gebruik je '[Bijlage F. Template Risicoregister](#)'.

De Bow-Tie methodiek ('[Bijlage G. Bow-Tie methodiek](#)') kan helpen om het proces inzichtelijk te maken, maar hoeft niet voor elk risico volledig uitgewerkt te worden. Voorbeelden van beheersmaatregelen staan in '[Bijlage N. Voorbeelden beheersmaatregelen](#)'. Daarnaast bevat '[Bijlage H. Voorbeeldrisico's corruptie en ondermijning](#)' een overzicht van corruptie- en ondermijningsrisico's op basis van input van experts op het gebied van corruptie en ondermijning.



Tip: Oorzaken achterhalen met behulp van de signalenkaart

De Rijksrecherche heeft eind 2024 de '[Signalenkaart Betrouwbare overheid](#)' uitgebracht. Dit is een "overzicht van kritische vragen over mogelijke kenmerken van ambtelijke corruptie en mogelijke aanwijzingen voor het ontstaan ervan". De vragen die zijn opgenomen in de Signalenkaart kunnen helpen met het achterhalen van de oorzaken achterliggend kunnen zijn aan corruptie en ondermijning.

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

[Bijlage F. Template Risicoregister](#)

[Bijlage G. Bow-Tie methodiek](#)

[Bijlage H. Voorbeeldrisico's corruptie en ondermijning](#)

[Bijlage I. Integriteitscultuurmodel](#)

[Bijlage J. Voorbeeldvragen ten behoeve van de grondoorzakenanalyse](#)

[Bijlage K. Voorbeeldoorzaken lage meldingsbereidheid](#)

[Bijlage L. Impactschalen](#)

[Bijlage M. Template kans- en impactmatrix en heatmap](#)

[Bijlage N. Voorbeelden beheersmaatregelen](#)

04. Risicobeoordeling (3/6)

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning



De '5 maal waarom-methode' voor oorzaken

Het is belangrijk om de dieperliggende oorzaken van de geïdentificeerde risico's in kaart te brengen, zodat beter kan worden bepaald welke maatregelen nodig zijn om het risico te voorkomen dan wel te beheersen. Hiervoor blijf je je afvragen wat onderliggend is aan het risico; de waarom-vragen.

Voorbeeld 'Infiltratie door criminelen via het reguliere werving en selectieproces'

De eerste geïdentificeerde oorzaak van de ongewenste uitkomst 'infiltratie door criminelen via het reguliere werving en selectieproces' is het ontbreken van gestandaardiseerde processen voor een achtergrondcheck, zoals opvragen van referenten.

De onderliggende oorzaken kunnen worden verkend door gerichte waarom-vragen te stellen, zoals:

- *Vraag 1. Waarom ontbreken gestandaardiseerde processen voor een achtergrondcheck?* Antwoord 1. Omdat er geen duidelijke organisatiebrede richtlijnen of beleid zijn vastgesteld voor hoe achtergrondchecks moeten worden uitgevoerd.
 - *Vraag 2. Waarom zijn er geen duidelijke richtlijnen of beleid vastgesteld?* Antwoord 2. Omdat eigenaarschap voor screening en integriteitscontroles niet expliciet is belegd binnen de organisatie.
 - *Vraag 3. Waarom is eigenaarschap voor screening en integriteitscontroles niet expliciet is belegd?* Antwoord 3. Omdat integriteitsrisico's in het werving- en selectieproces onvoldoende zijn onderkend en geprioriteerd op strategisch niveau.
 - [Etc.]
- Om verschillende kwetsbaarheden binnen de organisatie naar boven te halen, kan gebruik gemaakt worden van het integriteitscultuurmodel van professor Muel Kaptein (zie 'Bijlage I. Integriteitscultuurmodel').

Stap 4. Analyse maken van kans en impact van de risico's (Risicoanalyse)

Tijdens stap 3 heb je verschillende risico's en bestaande beheersmaatregelen in kaart gebracht. Om te helpen bij prioriteren, breng je in stap 4 de kans en impact van de risico's in kaart. Dit noem je de risicoscore. Om de risicoscore in kaart te brengen is het nodig om de waarschijnlijkheid dat een risico optreedt (*kans*) af te wegen tegen het resultaat en gevolgen als een risico zich materialiseert (*impact*). De **kansscore** krijgt een cijfer van 1 tot en met 5, duidende op zeer kleine tot zeer grote kans op het voordoen van een risico. De inschatting van de kans is gebaseerd op het aantal keer per jaar dat het in het verleden is voorgekomen en hoe vaak het in de toekomst zal gaan voorkomen. Het inschatten van de kans is belangrijk om onjuiste acceptatie van een risico of onjuiste prioritering te voorkomen. Zie de tabel 3 op de volgende pagina voor uitleg van de scores.

De **impactscore** krijgt ook een cijfer van 1 tot en met 5, waarbij een score van 1 betekent dat er minimale tot geen gevolgen zijn en een score van 5 dat er desastreuze gevolgen zijn na het voordoen van het risico. Zie de tabel 2 op de volgende pagina voor uitleg van de scores en voorbeelden van wat de impact kan zijn. De impact wordt ingeschat op basis van impactschalen. Het hanteren van meerdere impactcategorieën en -schalen maakt het mogelijk om de effecten van een risico gedifferentieerd te beoordelen, aangezien een incident op één gebied een grote impact kan hebben, terwijl de gevolgen op andere gebieden beperkt blijven. De impactschalen zijn uitgewerkt in 'Bijlage L. Impactschalen'.

De kans- en impactscore worden vermenigvuldigd; dit is de **risicoscore**. De risicoscores van alle geïdentificeerde risico's worden weergegeven in een kans- en impactmatrix. Tevens wordt er op basis van de kans- en impactmatrix een **heatmap** gemaakt, wat kan helpen met het inzichtelijk maken welke risico's als eerste aandacht behoeven. Zie 'Bijlage M Template kans- en impactmatrix en heatmap' voor nadere toelichting en een voorbeeld van de kans- en impactmatrix en heatmap.

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

[Bijlage F. Template Risicoregister](#)

[Bijlage G. Bow-Tie methodiek](#)

[Bijlage H. Voorbeeldrisico's corruptie en ondermijning](#)

[Bijlage I. Integriteitscultuurmodel](#)

[Bijlage J. Voorbeeldvragen ten behoeve van de grondoorzakenanalyse](#)

[Bijlage K. Voorbeeldoorzaken lage meldingsbereidheid](#)

[Bijlage L. Impactschalen](#)

[Bijlage M. Template kans- en impactmatrix en heatmap](#)

[Bijlage N. Voorbeelden beheersmaatregelen](#)

04. Risicobeoordeling (4/6)

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

Stap 5. Opstellen risicobeeld (Risicoanalyse)

Na het inschatten van de kans en impact van de geïdentificeerde risico's wordt een **risicobeeld** opgesteld. Dit risicobeeld bevat een overzicht van de toprisico's. Het biedt een helder inzicht in de grootste risico's van de organisatie en ondersteunt een gestructureerde prioritering en besluitvorming.

Impactscore			
Impact	Score	Beschrijving	Voorbeeldimpact
Minimaal	1	Minimale tot geen gevolgen	Klein incident met beperkte financiële consequenties en publiek vertrouwen in de overheid is niet of nauwelijks aangetast c.q. kan snel worden hersteld
Klein	2	Beperkte gevolgen, lokaal effect	Klein incident dat leidt tot een lichtelijke verstoring van de realisatie van de organisatiedoelen en schriftelijke vragen vanuit de Tweede Kamer
Gemiddeld	3	Merkbare gevolgen	Matig incident dat verschijnt in het regionale nieuws en leidt tot een toename van schendingen en afname in meldingsbereidheid binnen de organisatie
Groot	4	Grote gevolgen	Groot incident met financiële consequenties die buiten de begroting van de organisatie vallen en waardoor er een onderzoek vanuit de Algemene Rekenkamer wordt geïnitieerd
Desastreus	5	Zeer ernstige gevolgen	Ernstig incident of structurele ondermijning wat leidt tot het niet behalen van doelstellingen, juridische gevolgen en ernstige aantasting in het vertrouwen in de overheid

Tabel 3. Uitleg van de impactscore op een schaal van 1 (minimaal) tot 5 (desastreus)

Kansscore		
Kans	Score	Beschrijving
Zeër klein	1	Minder dan 1 keer per 10 jaar
Klein	2	Eén keer per 5-10 jaar
Gemiddeld	3	Eén keer per 2-5 jaar
Groot	4	Eén keer per jaar
Zeër groot	5	Meerdere keren per jaar

Tabel 4. Uitleg van de kansscore op een schaal van 1 (zeer klein) tot 5 (zeer groot)

Stap 6. Evaluatie van risico's (Risico-evaluatie)

De risicoscores geven richting aan het risicobeeld en de prioritering, maar vormen slechts één van de invalshoeken in het gesprek en zijn daarmee vooral een leidraad, niet doorslaggevend. In paragraaf '6.2 Rapporteren van relevante resultaten' wordt nader ingegaan op de wijze waarop het risicobeeld en de relevante resultaten worden gerapporteerd.



Effectiviteit huidige beheersmaatregelen achterhalen

Om de effectiviteit van huidige beheersmaatregelen te meten wordt er gekeken naar of de beheersmaatregel het doel behaalt waarvoor deze is opgesteld.

Dit wordt gedaan aan de hand van de volgende vragen:

- Wat houdt de beheersmaatregel in? Wat is de beoogde werking en het doel van de beheersmaatregel?
- Is de maatregel logisch en volledig ontworpen om het risico te mitigeren?
- Zijn de maatregelen werkbaar en begrijpelijk voor medewerkers?

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

[Bijlage F. Template Risicoregister](#)

[Bijlage G. Bow-Tie methodiek](#)

[Bijlage H. Voorbeeldrisico's corruptie en ondermijning](#)

[Bijlage I. Integriteitscultuurmodel](#)

[Bijlage J. Voorbeeldvragen ten behoeve van de grondoorzakenanalyse](#)

[Bijlage K. Voorbeeldoorzaken lage meldingsbereidheid](#)

[Bijlage L. Impactschalen](#)

[Bijlage M. Template kans- en impactmatrix en heatmap](#)

[Bijlage N. Voorbeelden beheersmaatregelen](#)

04. Risicobeoordeling (5/6)

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

Effectiviteit huidige beheersmaatregelen achterhalen (vervolg)

- Is de maatregel voldoende geïmplementeerd en wordt deze correct en consistent toegepast?
- Wordt de kans en/of de impact beperkt?
- Draagt het bij aan het behalen van de missie, visie en doelen van de organisatie of team?
- Zijn er meetpunten waaraan de effectiviteit van de maatregel kan worden gemeten (dashboards, KPI's, etc.)? Zo ja, laten de metingen een positief effect zien?
- Zijn er tekortkomingen of inefficiënties in de beheersmaatregel? Zijn er herhaalde incidenten ondanks bestaande maatregelen?
- Zijn er aanpassingen nodig in de beheersmaatregel om het risico te mitigeren?
- Is het risico veranderd ten opzichte van de laatste risicoanalyse waardoor de beheersmaatregel niet meer aansluit bij het originele doel?

De evaluatie helpt bij het opstellen van de actieplannen voor nieuwe beheersmaatregelen (zie hoofdstuk '5. Risicobehandeling').

Stap 7. Vaststellen risicobereidheid (Risico-evaluatie)

Het vaststellen van de **risicobereidheid** is een essentiële stap binnen het risicomanagementproces. De risicobereidheid geeft aan welke mate van risico de uitvoeringsorganisatie bereid is te accepteren bij het realiseren van haar doelstellingen. Hiermee wordt expliciet gemaakt waar de grens ligt tussen aanvaardbare en onaanvaardbare risico's.

De bestuursraad / ambtelijke top is verantwoordelijk voor het vaststellen of bekrachtigen van de organisatiebrede risicobereidheid. Hiermee wordt richting gegeven aan het omgaan met risico's op strategisch niveau en wordt geborgd dat de risicobereidheid aansluit bij de maatschappelijke opdracht, wet- en regelgeving en publieke waarden van de uitvoeringsorganisatie.

Door de risicobereidheid vooraf (of expliciet tijdens de risico evaluatie) te bepalen, ontstaat een gemeenschappelijk referentiekader voor het beoordelen en prioriteren van risico's. Dit voorkomt dat risico's uitsluitend op basis van gevoel, incidentgedrevenheid of individuele opvattingen worden beoordeeld. In plaats daarvan ondersteunt de risicobereidheid een consistent en uitlegbaar besluitvormingsproces.

In de context van corruptie en ondermijning is de risicobereidheid vaak laag tot zeer laag, met name waar het gaat om integriteit, publieke betrouwbaarheid, veiligheid van medewerkers en het vertrouwen van burgers. Tegelijkertijd kan de risicobereidheid per risicotype verschillen; zo kan een organisatie bijvoorbeeld minder ruimte hebben voor integriteitsrisico's dan voor operationele of financiële risico's. De eindverantwoordelijke voor een specifieke afdeling, proces of taak (bijvoorbeeld DG, directeur of afdelingshoofd) is verantwoordelijk voor het toepassen en – waar nodig – aanscherpen van de risicobereidheid binnen het eigen domein, binnen de kaders van de organisatiebrede risicobereidheid.

Het expliciteren van deze verschillen helpt om gericht te bepalen welke risico's actief gemitigeerd moeten worden en welke gemonitord of – onder voorwaarden – geaccepteerd kunnen worden.

De risicobereidheid vormt daarmee een belangrijk ijkpunt bij:

- het toetsen van de risicoscore (kans × impact);
- het bepalen van de risicorespons (accepteren, mitigeren, overdragen of vermijden);
- het prioriteren van maatregelen en de inzet van schaarse middelen;
- het voeren van het bestuurlijke gesprek over risico's en verantwoord risicogedrag.

Het expliciet bespreken en vastleggen van de risicobereidheid draagt bij aan transparantie, voorspelbaarheid en draagvlak in het risicomanagementproces en versterkt het risicobewustzijn binnen de uitvoeringsorganisatie.

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

[Bijlage F. Template Risicoregister](#)

[Bijlage G. Bow-Tie methodiek](#)

[Bijlage H. Voorbeeldrisico's corruptie en ondermijning](#)

[Bijlage I. Integriteitscultuurmodel](#)

[Bijlage J. Voorbeeldvragen ten behoeve van de grondoorzakenanalyse](#)

[Bijlage K. Voorbeeldoorzaken lage meldingsbereidheid](#)

[Bijlage L. Impactschalen](#)

[Bijlage M. Template kans- en impactmatrix en heatmap](#)

[Bijlage N. Voorbeelden beheersmaatregelen](#)

04. Risicobeoordeling (6/6)

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

Stap 8. Bepalen risicorespons (Risico-evaluatie)

Op basis van de kans- en impactmatrix en risicobereidheid ontstaat het **risicoprofiel**: het risicobeeld op basis van de vastgestelde scope, waarin de geïdentificeerde risico's en de reeds geïmplementeerde beheersmaatregelen zijn samengebracht. Hierop gebaseerd wordt de **risicorespons** bepaald. Hierbij wordt overwogen of de kans en impact van de geïdentificeerde risico's binnen of buiten de **risicobereidheid** van de organisatie valt. Daarnaast moet er ook rekening worden gehouden met geldende wet- en regelgeving en interne normenkaders.

De risicorespons betreft één van de volgende opties:

- **Accepteren:** besluiten om door te gaan met de activiteit die het risico veroorzaakt (bijv. geen behandeling beschikbaar, niet economisch haalbaar, biedt ook mooie kansen);
- **Mitigeren/beheersen:** beheersmaatregelen invoeren om de kans en/of impact te verkleinen (bijv. nog geen of onvoldoende effectieve maatregelen);
- **Overdragen:** uitbesteden aan een andere partij (bijv. belangrijk risico, maar geen mandaat);
- **Vermijden:** stoppen met de activiteit die het risico veroorzaakt (bijv. mogelijk om een andere keuze te maken).

De risico's die (verdere) mitigatie behoeven worden geprioriteerd op basis van:

- de actualiteit van de risico's,
- de verwachte effectiviteit en haalbaarheid van de behandeling,
- de kosten ten opzichte van de potentiële baten,

- de potentiële impact van de behandeling op andere risico's, en
- de effectiviteit van de huidige beheersmaatregelen.

Deze prioritering is van belang om beschikbare middelen doelgericht in te zetten en te verzekeren dat de meest urgente en impactvolle risico's als eerste worden behandeld.

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

[Bijlage F. Template Risicoregister](#)

[Bijlage G. Bow-Tie methodiek](#)

[Bijlage H. Voorbeeldrisico's corruptie en ondermijning](#)

[Bijlage I. Integriteitscultuurmodel](#)

[Bijlage J. Voorbeeldvragen ten behoeve van de grondoorzakenanalyse](#)

[Bijlage K. Voorbeeldoorzaken lage meldingsbereidheid](#)

[Bijlage L. Impactschalen](#)

[Bijlage M. Template kans- en impactmatrix en heatmap](#)

[Bijlage N. Voorbeelden beheersmaatregelen](#)

05. Risicobehandeling

05. Risicobehandeling

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

Inleiding

In fase 3, risicobehandeling, wordt uiteengezet hoe (additionele) beheersmaatregelen en bijbehorende actieplannen worden opgesteld, en wordt het belang van een effectieve implementatie en borging toegelicht.

Stap 9. Beschrijven beheersmaatregelen en acties

Beheersmaatregelen kunnen worden gecategoriseerd als preventieve, detectieve of repressieve beheersmaatregelen.

- **Preventieve beheersmaatregelen** zijn gericht op het voorkomen van het ontstaan van ongewenste gebeurtenissen, oftewel het verminderen van de kans (waarschijnlijkheid) dat een risico zich daadwerkelijk materialiseert.
- **Detectieve beheersmaatregelen** zijn gericht op het opsporen van afwijkingen of fouten, oftewel tijdig detecteren van signalen van ongewenste gebeurtenissen.
- **Repressieve beheersmaatregelen** zijn gericht op het beperken van de gevolgen als de ongewenste gebeurtenis zich heeft voorgedaan oftewel, het minimaliseren van de impact nadat een ongewenste gebeurtenis (risico) tot uiting is gekomen.

De beheersmaatregelen moeten aansluiten bij de scope van de risicoanalyse en bijdragen aan het behalen van de organisatie- of teamdoelen. Bij het beschrijven van de (nieuwe) preventieve, detectieve en repressieve beheersmaatregelen voor corruptie- en ondermijningsrisico's wordt rekening gehouden met zowel relevante wet- en regelgeving en interne richtlijnen.

Voorbeelden van beheersmaatregelen tegen corruptie en ondermijning zijn opgenomen in '[Bijlage N. Voorbeelden beheersmaatregelen](#)'.

Stap 10. Zorgen voor implementatie en borging

Om te zorgen dat beheersmaatregelen effectief worden geïmplementeerd behoren actieplannen te worden opgesteld. Hierin worden de beheersmaatregelen voor corruptie- en ondermijningsrisico's opgenomen volgens de 5W-1H methodiek.



De 5W-1H methode voor nieuwe beheersmaatregelen

Het opstellen van nieuwe beheersmaatregelen gebeurt aan de hand van zes vragen:

1. **Waarom** wordt een beheersmaatregel ingevoerd en welk specifiek effect moet zij realiseren om het risico te mitigeren? (Het doel)
2. **Wie** voert de maatregel uit? (De verantwoordelijken)
3. **Wat** is de maatregel die wordt uitgevoerd en welk bewijs bestaat er? (De inhoud)
4. **Wanneer** wordt de maatregel uitgevoerd en hoe vaak? (De frequentie)
5. **Hoe** wordt de maatregel uitgevoerd en zijn er specifieke rapporten vereist? (De stappen)
6. **Waar** wordt de maatregel uitgevoerd? (De partij/het proces waar het invloed op heeft)

Belangrijk: Om effectiviteit van de beheersmaatregelen te waarborgen, dienen deze periodiek geëvalueerd te worden. Deze informatie geeft inzichten over de effectiviteit en kansen om tijdig bij te sturen wanneer nodig. Gezien de beheersmaatregelen uiteenlopend kunnen zijn, is er niet één evaluatiemethode, maar bekijk je per maatregel hoe je de effectiviteit kan toetsen. Denk hierbij bijvoorbeeld aan het gebruik van personeel enquêtes. Bij de periodieke herhaling van de risicoanalyse komt de evaluatie van je nieuw getroffen maatregelen terug in Fase 2. Risicobeoordeling.

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

[Bijlage N. Voorbeelden beheersmaatregelen](#)

06. Rapporteren

06. Rapporteren

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

Inleiding

De laatste fase van de risicomanagementcyclus is het rapporteren van de bevindingen, observaties en actieplannen. In de rapportage staan de toprisico's, concrete beheersmaatregelen en openstaande acties opgenomen. De rapportage wordt voorgelegd aan de relevante stakeholders. Dit zijn bijvoorbeeld de bestuursraad en betrokken risico-eigenaren (BVA/BVC, CISO, integriteitscoördinator en HR-directeur). Met de rapportage biedt je inzicht in het doorlopen traject en leg je verantwoording af over de keuzes die hierin zijn gemaakt. Ook zorgt de rapportage voor draagvlak binnen de eigen organisatie, en stimuleert de rapportage risicobewustzijn binnen de organisatie.

Stap 11. Rapporteren van toprisico's, vastgestelde beheersmaatregelen, ontwikkelingen en actieplannen

In de rapportage neem je in ieder geval de volgende punten mee:

- Uitleg over het document en leeswijzer. Afhankelijk van het volwassenheidsniveau van de organisatie kan je algemene informatie opnemen over corruptie en ondermijningsrisico's en informatie over het doorlopen traject. Gebruik de informatie uit de toolkit hiervoor als inspiratiebron of neem de toolkit op als bijlage.
- Tabel 1 – Dashboard: overzicht van de toprisico's met de huidige risicoscore, de trend ten opzichte van de vorige rapportage en gewenste risicoscore ofwel de risicobereidheid.
- Figuur 1 – Heatmap: de heatmap van de toprisico's zoals beschreven in paragraaf '4.3. Risicoanalyse' en geïllustreerd in '[Bijlage M. Template kans- en impactmatrix en heatmap](#)'.
- Tabel 2 – Relevante ontwikkelingen ten opzichte van de toprisico's: relevante ontwikkelingen en reeds genomen en toekomstige acties/beheersmaatregelen.
- Tabel 3 – Lessons learned ten opzichte van de toprisico's : incidenten of bijna-incidenten en reeds genomen en toekomstige acties/beheersmaatregelen.

- In de appendix zullen de impact-, kans- en risicoscores nader zijn toegelicht.

De bovenstaande elementen zorgen voor een **risicobeeld** op basis van de scope, een samenhangend overzicht van de belangrijkste risico's binnen een organisatie, inclusief hun huidige status, impact en beheersing. Deze dient als basis voor besluitvorming, prioritering en communicatie richting stakeholders.

In '[Bijlage O. Voorbeeld rapportage opzet](#)' zijn voorbeelden van de diverse tabellen opgenomen. De risico's die ter illustratie staan opgenomen in de tabellen zijn verder uitgewerkt in '[Bijlage F. Template Risicoregister](#)'.



Tip: Verplaats je in de ontvanger van de rapportage

Een rapportage met hierin alle corruptie en ondermijningsrisico's kan bij de ontvanger best overweldigend overkomen. Neem de lezer mee in het verschil tussen risico's en daadwerkelijke kwetsbaarheden en hoe de rapportage is opgesteld. Het is niet de bedoeling dat een rapportage verlamd of een overreactie ontlokt. De risicoanalyse is juist bedoeld om zo goed als mogelijk incidenten te voorkomen.

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

[Bijlage F. Template Risicoregister](#)

[Bijlage M. Template kans- en impactmatrix en heatmap](#)

[Bijlage O. Rapportage opzet](#)

07. Monitoren en communiceren

07. Monitoren en communiceren

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

Inleiding

Een continu proces in de risicomanagementcyclus is het monitoren van de voortgang van de risicoanalyse en daarop gebaseerde actieplannen. Dit doorlopende proces en de periodieke communicatie zijn in dit hoofdstuk opgenomen.

Stap 12. Voortgang actieplannen monitoren

De aangewezen risicomanager is verantwoordelijk voor het goede verloop van de verschillende fasen. De risicomanager controleert of alle fasen correct doorlopen worden, alle analyses, interviews en workshops plaatsvinden en of iedereen zijn of haar verantwoordelijkheid neemt. De voortgang van de actieplannen wordt meegenomen in de periodieke rapportage zoals beschreven in hoofdstuk '6. Rapporteren'.

De risicomanager kan de toetsing uitvoeren op verschillende manieren, afhankelijk van de type beheersmaatregelen en persoonlijke voorkeuren. Dit kan bijvoorbeeld aan de hand van voortgangsgesprekken met actiehouders, statusrapportages en KPI-monitoring, steekproeven of audits op de uitvoering, digitale dashboards voor real-time inzicht of checklists voor leidinggevendenden om naleving te beoordelen. Daarnaast zijn er bij de monitoring van risico's en beheersmaatregelen een aantal onderdelen die in ieder geval moet worden uitgevoerd. Deze vormen de basis voor een gestructureerde en consistente toetsing.



Vereisten van monitoring en periodieke review

Zie onderstaande punten voor de belangrijkste vereisten van monitoring en periodieke review:

1. Controleer of de afgesproken risicobeheersingsmaatregelen daadwerkelijk worden uitgevoerd zoals gepland.

Vereisten voor monitoring en periodieke review (vervolg)

2. Beoordeel of de getroffen maatregelen effectief blijven werken en het beoogde risicoreducerende effect behouden.
3. Monitor relevante wijzigingen in wetgeving, technologie, organisatie of systemen die invloed kunnen hebben op het risicolandschap.
4. Analyseer of dergelijke wijzigingen impact hebben op bestaande risico's of aanleiding geven tot nieuwe risico's.
5. Herzie periodiek het volledige risicoprofiel om te beoordelen of het nog actueel en volledig is.
6. Actualiseer risicobeoordelingen, risicoregisters en beheersmaatregelen op basis van nieuwe inzichten en ontwikkelingen.



Monitoring van de beheersmaatregelen met de 5W-1H methodiek

Het monitoren van nieuwe beheersmaatregelen gebeurt aan de hand van de volgende vragen:

- **Waarom:** Is het doel van de beheersmaatregelen duidelijk bij de actiehouders en begrijpen zij hoe dit bijdraagt aan de missie, visie en risicobeheersing?
- **Wie:** Zijn de actiehouders zich bewust van hun verantwoordelijkheid voor het actieplan en is dit expliciet vastgelegd?
- **Wat:** Worden de afgesproken acties en verantwoordelijkheden nageleefd zoals vastgelegd in het plan?
- **Wanneer:** Worden de beheersmaatregelen toegepast op de afgesproken momenten en vindt evaluatie tijdig plaats?
- **Hoe:** Worden de maatregelen correct en volgens de afgesproken werkwijze geïmplementeerd?
- **Waar:** Worden de maatregelen toegepast binnen de juiste doelgroep, afdeling of processen?
- **Randvoorwaarden:** Beschikken actiehouders over de benodigde middelen, kennis en randvoorwaarden om hun taken uit te voeren?

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

[Bijlage P. Voorbeelden
communicatiemateriaal](#)

07. Monitoren en communiceren

Toolkit risicoanalyse voor de preventie van corruptie en ondermijning

Voor verdieping verwijzen wij naar de bijlagen. Klik op onderstaande items voor meer informatie over de onderwerpen gepresenteerd op deze dia.

Stap 13. Communiceren over het belang, de voortgang, feedback en acties

Voorafgaand aan de risicomanagementcyclus

Nog voordat je begint aan stap 1 (inzichtelijk maken van organisatie en scope) is het van belang dat je de hele organisatie meeneemt in de uitvoering van de risicoanalyse. Dit kan bijvoorbeeld door een artikel te publiceren op het intranet van jouw organisatie, of door een artikel te schrijven voor een nieuwsbrief. Door alle medewerkers (ook medewerkers eventueel werkzaam buiten de scope) te informeren over de werkzaamheden, ontstaat er meer risicobewustzijn. Bij interne communicatie kan het handig zijn om continu toe te lichten waar het om gaat: wat bedoelen we met corruptie en ondermijning en waarom is het belangrijk dat we deze risico's in beeld brengen? Daarbij is de risicoanalyse vooral een preventief instrument. Door de uitvoering van een risicoanalyse is de kans kleiner dat een risico zich materialiseert, en zijn organisaties beter in staat om adequaat te handelen wanneer de risico's zich toch voordoen. We kunnen onze organisatie en onze medewerkers dus beter beschermen!

Tijdens de risicomanagementcyclus

Tijdens de risicomanagementcyclus zijn er verschillende belanghebbenden, waarvan sommige personen of groepen nauw betrokken zijn en andere slechts geïnformeerd worden. Naast informeren en kennisdeling wordt ook actief input opgehaald via gesprekken, interviews en workshops. Deze input is essentieel om risico's actueel te houden en vormt de basis voor effectieve monitoring en periodieke herbeoordeling. In de tabel in paragraaf '3.4. Rollen en verantwoordelijkheden' zijn de verschillende doelgroepen opgenomen evenals de mate waarin zij betrokken moeten worden bij de risicomanagementcyclus volgens het RASCI-model. Voorbeelden van uitnodigingen naar deelnemers zijn opgenomen in '[Bijlage P. Voorbeelden communicatiemateriaal](#)'.

Naast interne communicatie, wordt ook samenwerking en kennisdeling tussen verschillende rijksorganisaties gestimuleerd om de effectiviteit van beheersmaatregelen verder te vergroten. Ervaringen, 'good practices' en knelpunten kunnen worden gedeeld via worden gezamenlijke evaluatiesessies, werkgroepen en/of periodieke rapportages.

Door deze uitwisselingen van informatie ontstaat een lerend netwerk waarin organisaties elkaar versterken, waardoor beheersmaatregelen niet alleen beter worden geïmplementeerd, maar ook continu worden geoptimaliseerd.

Inhoudsopgave

[01. Introductie](#)

[02. Risicomanagementcyclus](#)

[03. Scope en contextbepaling](#)

[04. Risicobeoordeling](#)

[05. Risicobehandeling](#)

[06. Rapporteren](#)

[07. Monitoren en communiceren](#)

[Bijlagen](#)

Relevante bijlagen

[Bijlage A. Begrippenlijst](#)

[Bijlage P. Voorbeelden communicatiemateriaal](#)

Bijlagen

Bijlage A. Begrippenlijst (1/3)

Deze bijlage betreft een begrippenlijst van de relevante begrippen uit dit document en bijbehorende definitie.

Begrippenlijst	
Begrip	Definitie
Analyse	Het beoordelen van geïdentificeerde risico's door kans en impact te analyseren. De uitkomst is een risicoscore (kans × impact), die wordt getoetst aan de risicobereidheid van de organisatie.
Beheersmaatregel	Een actie of procedure die gericht is om de kans en/of impact van een risico te verminderen. Er wordt onderscheid gemaakt tussen preventieve, detectieve en repressieve maatregelen.
Bow-Tie methodiek	Een visuele risicomanagementmethodiek die oorzaken, gevolgen en beheersmaatregelen rondom een centrale ongewenste gebeurtenis overzichtelijk in kaart brengt. Door relevante elementen gebalanceerd te selecteren, voorkomt men overmatige detaillering die de effectiviteit van het model schaadt. Binnen uitvoeringsorganisaties helpt de Bow-Tie methodiek bij het identificeren van risico's en het formuleren van passende beheersmaatregelen.
Bruto risico	Een bruto risico is de inschatting van een risico zonder rekening te houden met bestaande beheersmaatregelen.
Corruptie	Het misbruik van toevertrouwde macht voor persoonlijk gewin. Vormen van ambtelijke corruptie zijn bijvoorbeeld omkoping, schending van ambtsgeheim, oplichting, valsheid in geschrifte of fraude.
Detectieve beheersmaatregelen	Beheersmaatregelen gericht op het opsporen van afwijkingen of fouten, oftewel tijdig detecteren van signalen van ongewenste gebeurtenissen.
Evaluatie	Het vergelijken van geanalyseerde risico's met vastgestelde criteria en risicobereidheid om te bepalen welke risico's acceptabel zijn en waar aanvullende maatregelen of respons nodig is.
Heatmap	Een visuele weergave van risico's op basis van hun kans en impact.
Identificatie	Het in kaart brengen van ongewenste gebeurtenissen, het definiëren van risico's, het vaststellen van oorzaken en gevolgen en het verzamelen van bestaande beheersmaatregelen.
Impact	Het potentiële effect of gevolg van het risico als deze zich materialiseert. De impact kan variëren van minimaal tot desastreus.
Impactschalen	Gebied waar risico's en kansen effect op kunnen hebben (bijv. op het gebied van financiën, reputatie, politiek/bestuurlijk en integriteit).

Tabel 5. Begrippenlijst (deel 1/3)

Bijlage A. Begrippenlijst (2/3)

Begrippenlijst	
Begrip	Definitie
Kans	De waarschijnlijkheid dat een specifiek risico zich daadwerkelijk materialiseert en een gevolg heeft dat een (gunstig/ongunstig) effect heeft op het behalen van de doelstellingen. De kans kan variëren van zeer klein tot zeer groot.
Kans- en impactmatrix	Een matrix waarmee risico's worden beoordeeld en gevisualiseerd op basis van de kans dat een risico materialiseert en de mogelijke impact als het risico zich voordoet. De matrix draagt bij aan het maken van een beslissing op het gebied van risicorespons.
Monitoren en communiceren	Een continue feedbackloop waarin risico's, beheersmaatregelen en actieplannen worden gemonitord en gecommuniceerd naar de relevante stakeholders.
Netto risico	Een netto (rest) risico is het risico waarbij de huidige aanwezige beheersmaatregelen in beschouwing worden genomen.
Ondermijning	Het gebruik van legale structuren, diensten of voorzieningen om illegale activiteiten uit te voeren, waardoor het maatschappelijk systeem wordt aangetast. Het is een containerbegrip dat ook corruptie, fraude en andere vormen van criminaliteit omvat. Ondermijning speelt zich niet alleen af tussen een 'boven-' en 'onderwereld', maar kent ook een grijs gebied en betrokkenen handelen niet altijd met slechte intenties.
Preventieve beheersmaatregelen	Beheersmaatregelen gericht op het voorkomen van het ontstaan van ongewenste gebeurtenissen, oftewel het verminderen van de kans (waarschijnlijkheid) dat een risico zich daadwerkelijk materialiseert.
RASCI-model	Een hulpmiddel voor het vastleggen van de verantwoordelijkheden van de verschillende rollen in de risicomanagementcyclus. De afkorting RASCI staat voor Responsible (Verantwoordelijk), Accountable (Eindverantwoordelijk), Supporting (Ondersteunend), Consulted (Geraadpleegd) en Informed (Geïnformeerd). Zie Bijlage D voor nadere duiding.
Repressieve beheersmaatregelen	Beheersmaatregelen gericht op het beperken van de gevolgen als de ongewenste gebeurtenis zich heeft voorgedaan oftewel, het minimaliseren van de impact nadat een ongewenste gebeurtenis (risico) tot uiting is gekomen.
Risico	Een onzekere toekomstige gebeurtenis (of reeks gebeurtenissen) die, indien deze zich materialiseert, invloed heeft op het uitvoeren van taken en verantwoordelijkheden en/of het bereiken van doelstellingen. Belangrijk om je bewust van te zijn: Zodra de gebeurtenis zich voordoet, is het geen risico meer maar een probleem voor de organisatie om mee om te gaan.
Risicobeeld	Een samenhangend overzicht van de belangrijkste risico's binnen een organisatie, inclusief hun huidige status, impact en beheersing.
Risicobereidheid	Het niveau per type risico dat een organisatie bereid is te accepteren bij het nastreven van haar doelstellingen, Het is een keuze die aangeeft welke mate van onzekerheid de organisatie tolereert.

Tabel 5. Begrippenlijst (deel 2/3)

Bijlage A. Begrippenlijst (3/3)

Begrippenlijst	
Begrip	Definitie
Risico-eigenaar	De persoon verantwoordelijk voor het beheersen van een risico tot een acceptabel niveau in lijn met de vastgestelde risicobereidheid.
Risicomanagement	Het gestructureerde proces van gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot risico's (ISO 31000). Het doel is risico's en kansen te identificeren, beoordelen en beheersen binnen de vastgestelde risicobereidheid, zodat doelstellingen worden bereikt.
Risicomanagementcyclus	Een systematische en continue aanpak om risico's binnen de organisatie context en scope te identificeren, analyseren, evalueren en behandelen evenals het rapporteren van bevindingen en monitoren van en communiceren over de verschillende fasen.
Risicoprofiel	Het risicobeeld op basis van de vastgestelde scope, waarin de geïdentificeerde risico's en de reeds geïmplementeerde beheersmaatregelen zijn samengebracht.
Risicorespons	Risicorespons is het geheel van maatregelen of acties die worden genomen op basis van de kans en impact van geïdentificeerde risico's, in relatie tot de risicobereidheid van de organisatie. De risicorespons betreft één van de volgende opties: • Accepteren: besluiten om door te gaan met de activiteit die het risico veroorzaakt; • Mitigeren/beheersen: beheersmaatregelen invoeren om de kans en/of impact te verkleinen; • Overdragen: uitbesteden aan een andere partij; • Vermijden: stoppen met de activiteit die het risico veroorzaakt.
Risicoscore	De kans vermenigvuldigd met de impact van een risico.

Tabel 5. Begrippenlijst (deel 3/3)

Bijlage B. Template context organisatie

In de tabellen hieronder zijn de elementen opgenomen die voortkomen uit de verkenning van de organisatie en de scope (Fase 1 – Scope en contextbepaling).

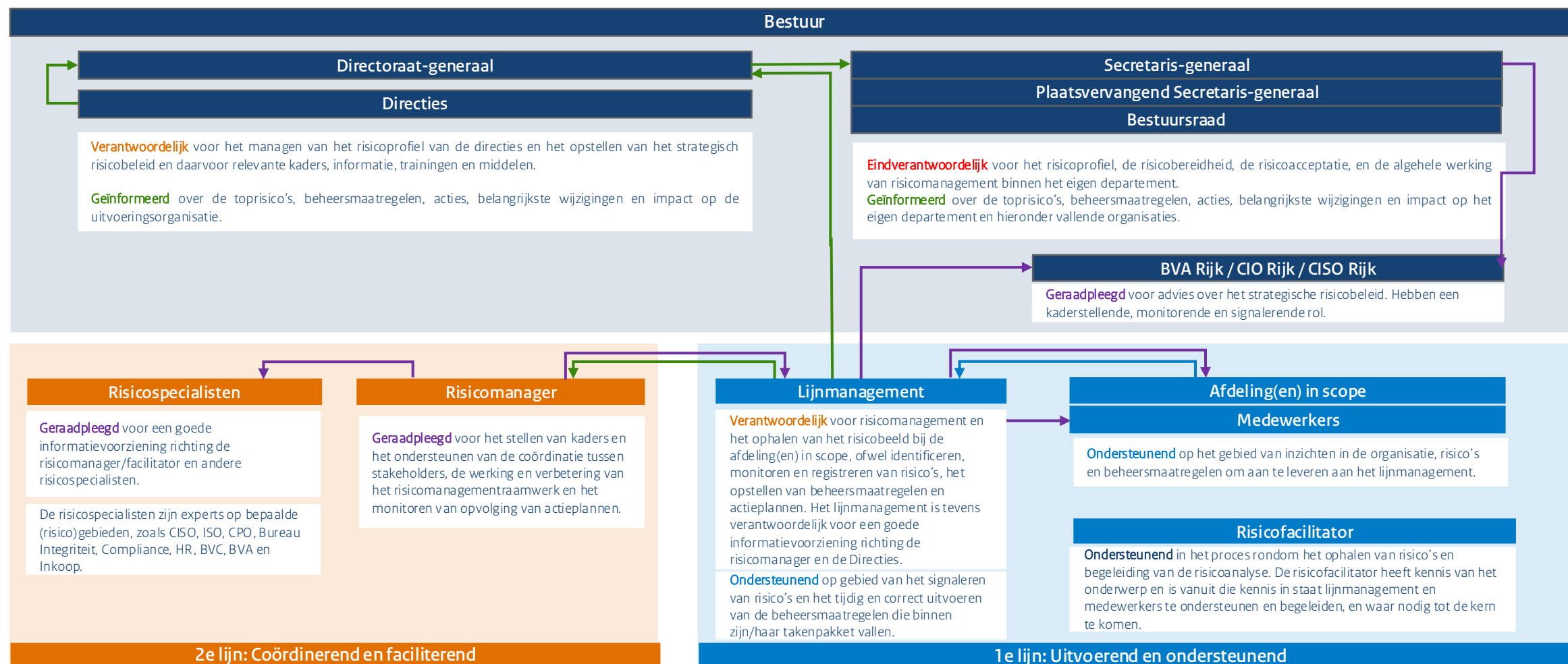
Organisatie	Afdeling(en)	Scope	Missie afdeling(en)	Visie afdeling(en)	Hoofd doelen afdeling(en)	Risicobereidheid
<i>Naam organisatie</i>	<i>Naam afdeling(en) in scope</i>	<i>Bepaal welke afdeling, proces en/of taak centraal staat in dit risicoanalyse</i>	<i>Beschrijf de missie van de afdeling(en) in scope</i>	<i>Beschrijf de visie van de afdeling(en) in scope</i>	<i>Beschrijf de belangrijkste doelen van de afdeling(en) in scope</i>	<i>Beschrijf welke mate van risico de organisatie bereid is te accepteren bij het behalen van de doelstellingen</i>
[Voorbeeld]	Afdeling Autorisatie- en Toegangsbeheer.	Proces autorisatiebeheer.	Zorgen dat medewerkers alleen toegang hebben tot de informatie die zij noodzakelijk nodig hebben voor hun functie (need-to-know), zodat veiligheid, integriteit en vertrouwelijkheid van informatie gewaarborgd blijft.	Een digitaal veilige organisatie waarin (gevoelige) informatie optimaal wordt beschermd en misbruik of ongeoorloofde toegang structureel wordt voorkomen.	- Zorgdragen voor correcte toekenning van autorisaties. - Voorkomen van ongeautoriseerde toegang tot gevoelige systemen en gegevens. - Logging en monitoring op toegang.	Mitigeren/Beheersen

Tabel 6. Template context organisatie (deel 1/2)

Bedrijfs-/werkprocessen	Relevante producten/diensten	Relevante derde partijen	Relevante ontwikkelingen	Relevante wet- en regelgeving	Relevante overige afspraken	Relevante rollen, incl. verantwoordelijkheden
<i>Bepaal de belangrijkste bedrijfs-/werkprocessen in scope.</i>	<i>Bepaal welke producten en/of diensten mogelijk invloed hebben op de risicoanalyse</i>	<i>Bepaal welke derde partijen mogelijk invloed hebben op de risicoanalyse</i>	<i>Bepaal welke ontwikkelingen mogelijk invloed hebben op de risicoanalyse</i>	<i>Bepaal welke wet- en regelgeving mogelijk invloed hebben op de risicoanalyse</i>	<i>Bepaal welke gedragsregels, beleid of andere afspraken mogelijk invloed hebben op de risicoanalyse</i>	<i>Bepaal welke rollen er zijn in de risicomanagementcyclus en welke verantwoordelijkheden zijn belegd bij deze personen</i>
- Toekennen en aanpassen van autorisaties. - Periodieke controle, opschoning en intrekking van ongebruikte en onterechte autorisaties. - Signaleren van incorrect aangevraagde of toegewezen autorisaties.	- HR-data van medewerkers. - Toegangsrechten tot systemen. - Rollen- en autorisatiematrices.	- Softwareleveranciers. - IT-dienstverleners van het Rijk. - Shared service organisaties (SSC-ICT).	- Toenemende dreiging insider threats en ondermijning. - Nieuwe wetgeving voor digitale overheid. - Strengere eisen rond logging en monitoring (BIO 3.0).	- Baseline Informatiebeveiliging Overheid (BIO). - Wet digitale overheid (WDO). - Archiefwet (voor toegangslogs).	- Integriteitscode van de organisatie en het Rijk. - Gedragscode ambtenaren. - Interne compliance-afspraken.	Zie paragraaf '3.3. Rollen en verantwoordelijkheden'

Tabel 6. Template context organisatie (deel 2/2)

Bijlage C. Voorbeeld rollen en verantwoordelijkheden (1/4)



Figuur 2. Schematisch overzicht van rollen en verantwoordelijkheden

*De rollen en verantwoordelijkheden zijn gebaseerd op de interne organisatie binnen een departement en kunnen verschillen per organisatie.

→ Geïnformeerd → Geraadpleegd → Ondersteunend

Bijlage C. Voorbeeld rollen en verantwoordelijkheden (2/4)

Rollen en verantwoordelijkheden		
Funcietitel	Belangrijkste verantwoordelijkheden	RASCI
Secretaris-generaal en Plaatsvervangend Secretaris-generaal	- De Secretaris-generaal (SG) draagt ambtelijke eindverantwoordelijk voor het risicoprofiel, risicobereidheid, risicoacceptatie en de werking van het risicomanagementtraamwerk binnen de eigen organisatie. Echter zijn zij niet nauw betrokken bij risicomanagement binnen uitvoeringsorganisaties en geen eindverantwoordelijke voor risicomanagement op directieniveau. - Om een organisatiebrede afweging te borgen, laat de (p)SG zich hierbij informeren door de Directoraten-generaal en Directies.	Eindverantwoordelijk De SG draagt ambtelijke eindverantwoordelijkheid voor het risicoprofiel, risicobereidheid, risicoacceptatie en de werking van het risicomanagementtraamwerk binnen de eigen organisatie. Geïnformeerd De SG en pSG worden door de Directoraten-generaal en Directies hoogover geïnformeerd over de toprisco's, beheersmaatregelen, acties, belangrijkste wijzigingen en impact op de uitvoeringsorganisatie en het Rijk.
Directoraten-generaal en Directies	- De Directoraten-generaal (DG) en Directies zijn verantwoordelijk voor het opstellen van het risicomanagementtraamwerk en risicoprofiel op directieniveau. - Daarnaast laten zij de benodigde beheersmaatregelen naar aanleiding van het gestelde beleid en bevindingen ten aanzien van geïdentificeerde risico's uitvoeren. - Tevens zijn de Directies verantwoordelijk voor het voorzien van de medewerkers van de juiste informatie, trainingen en middelen om bij te dragen aan veilig werken, risico-identificatie en het uitvoeren van beheersmaatregelen. Hierin worden zij ondersteund door managers, de CISO en andere bij risicomanagement betrokken personen.	Verantwoordelijk De DG's en Directies zijn verantwoordelijk voor het managen van het risicoprofiel van de Directies en het opstellen van strategisch risicobeleid en daarvoor relevante kaders, informatie, trainingen en middelen. Geïnformeerd De Directies worden door de het lijnmanagement, de risicomanager en de risicospecialisten geïnformeerd over de toprisco's, beheersmaatregelen, acties, belangrijkste wijzigingen en impact op de organisatie.
BVA-Rijk, CIO-Rijk en CISO-Rijk	- De BVA-Rijk heeft een kaderstellende, adviserende en toezichhoudende rol over de integrale beveiliging van het departement. Per departement is een BVA aangewezen die de BVA-Rijk inlicht. - De CIO Rijk is belast met de ontwikkeling en coördinatie van het rijksbrede informatievoorziening - en digitaliseringsbeleid en draagt zorg voor de ontwikkeling en het beheer van de ICT-voorzieningen en informatiesystemen, bedoeld in artikel 2, eerste lid onder b, van het Coördinatiebesluit. - De CISO Rijk is belast met de coördinatie van de maatregelen en het beleid voor de informatiebeveiliging voor zover deze betrekking hebben op de rijksdienst en ressorteert onder de CIO Rijk.	Geraadpleegd - De BVA Rijk wordt geraadpleegd door de ambtelijke leiding en het lijnmanagement over de integrale beveiliging, te realiseren verbeteringen en beveiligingsmaatregelen. - De CIO Rijk wordt geraadpleegd door de ambtelijke leiding en het lijnmanagement over de gevolgen voor het rijksbrede digitaliserings- en informatievoorzieningsbeleid. - De CISO Rijk wordt geraadpleegd door de ambtelijke leiding en het lijnmanagement over de informatiebeveiliging en de risico's daarvoor van (voorgenomen) wet- en regelgeving, investeringen, beleid, uitvoeringstrajecten, informatieprocessen en informatiesystemen voor zover deze betrekking hebben op de rijksdienst

Tabel 7. Rollen en verantwoordelijkheden (deel 1/3)
 *De rollen en verantwoordelijkheden zijn gebaseerd op de interne organisatie binnen een departement en kunnen verschillen per organisatie.

Bijlage C. Voorbeeld rollen en verantwoordelijkheden (3/4)

Rollen en verantwoordelijkheden		
Functietitel	Belangrijkste verantwoordelijkheden	RASCI
Lijnmanagement	- Het lijnmanagement is verantwoordelijk voor het risicomanagement en ophalen van een risicobeeld bij de afdeling(en) in scope, ofwel identificeren, monitoren en registreren van risico's, opstellen van beheersmaatregelen een actieplannen en goede informatievoorziening richting de risicomanager. - Het lijnmanagement is verantwoordelijk voor de goede informatievoorziening richting de risicomanager en de Directies. - Het lijnmanagement wordt door de Directies op de hoogte gehouden van de ontwikkelingen in het risicoprofiel en veranderingen.	Verantwoordelijk Het Lijnmanagement is verantwoordelijk voor de risico's en daarmee het ophalen van het risicobeeld bij de afdeling(en) in scope, ofwel identificeren, monitoren en registreren van risico's, het opstellen van beheersmaatregelen en actieplannen. Het lijnmanagement is tevens verantwoordelijk voor een goede informatievoorziening richting de risicomanager en de Directies.
Risicomanager	- De pSG stelt een risicomanager aan. - De risicomanager is verantwoordelijk voor (de werking en continue verbetering van) het risicomanagementraamwerk binnen de organisatie. - Dit betekent dat hij/zij het risicomanagementproces coördineert, een effectieve informatievoorziening daarbinnen borgt, eventuele knelpunten signaleert en input levert ten behoeve van de bestuurlijke verantwoording. - Indien gewenst kan ervoor worden gekozen om één risicomanager verantwoordelijk te maken voor meerdere afdelingen of programma's, mits dit de effectieve uitvoering van de rol van risicomanager niet belemmert.	Geraadpleegd De risicomanager wordt geraadpleegd voor het stellen van kaders en het ondersteunen van de coördinatie tussen stakeholders, de werking en verbetering van het risicomanagementraamwerk en het monitoren van opvolging van actieplannen. De risicomanager is het centrale punt voor het beantwoorden van vragen en uitzetten van verzoeken.
Risicofacilitator	De risicofacilitator ondersteunt de organisatie zowel centraal als decentraal met het begeleiden van risicodialogen. De risicofacilitator is geen risico-expert maar zorgt ervoor dat de verschillende stappen uit de toolkit wordt opgevolgd en uitgevoerd.	Verantwoordelijk De risicofacilitator is verantwoordelijk voor de begeleiding van de uitvoering van de risicoanalyse. Deze functionaris zorgt voor de goede uitvoering van de stappen en betrokkenheid van de verschillende experts.
Risicospecialisten	- De risicospecialisten zijn experts op bepaalde (risico)gebieden, zoals de Chief Information Security Officer (CISO), Chief Privacy Officer (CPO), Chief Technology Officer (CTO), Bureau Integriteit en/of integriteitscoördinator, Compliance officer, de Beveiligingscoördinator (BVC) en de Beveiligingsambtenaar (BVA). - Risicospecialisten zijn tevens verantwoordelijk voor een goede informatievoorziening richting de risicomanager en andere risicospecialisten. - De expertise is decentraal belegd, aangezien de risicospecialisten op verschillende domeinen opereren.	Geraadpleegd De risicospecialisten zijn bekend met alle risicomanagementactiviteiten en verantwoordelijk voor informatiedeling tussen de verschillende risicospecialisten. De risicospecialisten worden geraadpleegd door de risicomanager en geven hun input vanuit hun expertise.

Tabel 7. Rollen en verantwoordelijkheden (deel 2/3)

*De rollen en verantwoordelijkheden zijn gebaseerd op de interne organisatie binnen een departement en kunnen verschillen per organisatie.

Bijlage C. Voorbeeld rollen en verantwoordelijkheden (4/4)

Rollen en verantwoordelijkheden		
Functietitel	Belangrijkste verantwoordelijkheden	RASCI
Medewerkers	- Van medewerkers wordt verwacht dat zij bewust zijn van mogelijke risico's op het gebied van corruptie en ondermijning, hoe zij moeten omgaan met vertrouwelijke informatie en welke wetten, regelgeving en richtlijnen gelden. - Elke medewerker is verantwoordelijk voor het signaleren en melden van risico's ten behoeve van het tijdig acteren op de risico's alsmede het verrijken van de risicoanalyse. Daarnaast wordt er van medewerkers verwacht dat zij de beheersmaatregelen die binnen zijn/haar takenpakket vallen correct en zorgvuldig uitvoeren.	Ondersteunend Medewerkers ondersteunen hun leidinggevende(n) van de afdeling(en) in scope voor het leveren van input aan het lijnmanagement. Medewerkers binnen de uitvoeringsorganisatie worden ook geïnformeerd over veranderingen, zodat zij hun verantwoordelijkheid kunnen nemen in het signaleren van risico's en het correct uitvoeren van beheersmaatregelen, maar worden niet betrokken bij het nemen van beslissingen.
Afdeling(en) in scope en bijbehorende leidinggevenden	- De afdeling in scope is verantwoordelijk voor het leveren van input op het gebied van inzichten in de organisatie, risico's en beheersmaatregelen. - De input wordt verzameld en gedeeld door de leidinggevende(n) van de afdeling(en) ofwel het MT (zie ook vorige pagina).	Ondersteunend De afdeling in scope wordt gevraagd om input te leveren tijdens interviews en workshops ten behoeve van de risicoanalyse en beheersmaatregelen.

Tabel 7. Rollen en verantwoordelijkheden (deel 3/3)
 *De rollen en verantwoordelijkheden zijn gebaseerd op de interne organisatie binnen een departement en kunnen verschillen per organisatie.

Bijlage D. RASCI-model

Het RASCI-model is een hulpmiddel dat gebruikt wordt om rollen en verantwoordelijkheden bij onder andere de risicomanagementcyclus helder vast te leggen. Door deze matrix toe te passen, is het voor iedereen duidelijk wie welke rol vervult en wie de uiteindelijke verantwoordelijkheid draagt. Hiermee wordt onduidelijkheid voorkomen en communicatie versneld. De RASCI kan ook nog verder uitgediept worden door het model toe te passen op de individuele fasen of taken binnen de risicomanagementcyclus.

De afkorting RASCI staat voor:



- **Responsible (Verantwoordelijk):** Dit is de persoon of het team dat het project (of fase) daadwerkelijk uitvoert. Zij zorgen ervoor dat het werk wordt gedaan volgens de afgesproken kwaliteit en binnen de gestelde termijn. Er kunnen meerdere personen verantwoordelijk zijn voor één project (of fase), maar er moet altijd duidelijk zijn wie het uitvoert;



- **Accountable (Eindverantwoordelijk):** Dit is degene die de uiteindelijke verantwoordelijkheid draagt voor het resultaat. Deze persoon keurt het werk goed en is degene die aangesproken wordt als iets niet volgens plan verloopt. Voor elk project (of fase) mag er maar één eindverantwoordelijke zijn om verwarring te voorkomen;



- **Supporting (Ondersteunend):** Dit zijn personen die actief bijdragen aan het uitvoeren van het project (of fase), maar niet de verantwoordelijkheid dragen. Zij bieden hulp, middelen of expertise om het werk te realiseren en ondersteunen hiermee de Verantwoordelijke (Responsible).



- **Consulted (Geraadpleegd):** Dit zijn personen die inhoudelijke kennis of expertise hebben en daarom geraadpleegd worden. Zij geven advies, feedback of input voordat een project (of fase) wordt afgerond. Het is een tweerichtingscommunicatie en zij worden actief om hun mening gevraagd (bijvoorbeeld aan de hand van de interviews en/of workshops);



- **Informed (Geïnformeerd):** Dit zijn personen die op de hoogte moeten blijven van de voortgang of het resultaat, maar niet actief betrokken zijn bij de uitvoering of besluitvorming. Het gaat hier om eenrichtingscommunicatie waarbij zij updates ontvangen, maar geen input geven.



Tip: Leg je ingevulde RASCI-model voor aan het MT

Een risicoanalyse kan behoorlijk wat tijd vragen. Het is daarom belangrijk dat de rollen en verantwoordelijkheden van tevoren duidelijk zijn én dat iedereen zich hieraan houdt, ook als prioriteiten verschuiven. Het kan daarom helpen om het ingevulde RASCI-model voor akkoord voor te leggen aan het MT en/of betrokken leidinggevenden voorafgaand aan de risicoanalyse.

Bijlage E: Voorbeeld ingevuld RASCI-Model*

	SG, pSG, Bestuursraad	Risicomanager	Risico facilitator	BVA-Rijk, CIO-Rijk, CISO- Rijk, BZK Integriteit	Risico- specialisten (BVA/BVC, CIO, CISO, HR, Inkoop, etc.)	Afdeling(en) in scope, incl lijn- management	Medewerkers
1. Inzichtelijk maken organisatie en scope	A	S	S	-	C	R	S
2. Vastleggen rollen en verantwoordelijkheden	A	S	S	-	C	R	S
3. Identificatie van risico's, oorzaken, gevolgen en huidige beheersmaatregelen	I	C	S	-	C	A	S
4. Analyse maken van kans en impact van de risico's	I	C	S	-	S	A	S
5. Opstellen risicobeeld	I	C	S	-	S	A	S
6. Evaluatie van risico's	I	C	S	-	S	R	S
7. Vaststellen risicobereidheid	A	C	S	-	C	S	I
8. Bepalen risicorespons	I	C	S	-	S	R	S
9. Beschrijven beheersmaatregelen en acties	I	S	S	-	S	R	S
10. Zorgen voor implementatie en borging	I	S	S	-	S	R	S
11. Rapporteren van toprisico's, vastgestelde beheersmaatregelen, ontwikkelingen en actieplannen	I	A	R	I	C	R	I
12. Voortgang van actieplannen monitoren	I	A	R	I	C	R	I
13. Communiceren over voortgang, feedback en acties	I	A	R	I	C	R	I

Tabel 8. Voorbeeld van een ingevuld RASCI-model

*De rollen en verantwoordelijkheden zijn gebaseerd op een mogelijke organisatie binnen een departement en kunnen verschillen per organisatie.

-  R = Responsible (Verantwoordelijk)
-  A = Accountable (Eindverantwoordelijk)
-  S = Supporting (Ondersteunend)
-  C = Consulted (Geraadpleegd)
-  I = Informed (Geïnformeerd)

Bijlage F. Template Risicoregister (1/2)

In de tabellen hieronder zijn de elementen van het risicoregister opgenomen, evenals drie voorbeelden.

Risico-ID	Risico titel	Risico beschrijving	Oorzaken	Gevolgen	Kans	Impact	Risicoscore	Beheersmaatregel doel	Huidige Beheersmaatregel(en)
<i>Uniek risico nummer (RID)</i>	<i>Risico titel</i>	<i>Risicobeschrijving met focus op de ongewenste gebeurtenis</i>	<i>Overzicht van de mogelijke oorzaken (niet uitputtend), met focus op de belangrijkste oorzaken</i>	<i>Overzicht van de mogelijke gevolgen (niet uitputtend), met focus op de belangrijkste gevolgen</i>	<i>Bepaal de kans van optreden met behulp van de kans-schaal</i>	<i>Bepaal de impact van het risico met behulp van de impact-schaal</i>	<i>De risicoscore is kans maal impact</i>	<i>Formuleer de doelstelling (de waarom) van de beheersmaatregel</i>	<i>Gebruik de 4W – 1H methodiek om de beheersmaatregelen concreet mogelijk uit te schrijven.</i>
RID-01	Aannemen steekpenning voor informatie door persoonlijke kwetsbaarheid	De persoonlijke situatie van medewerkers leidt ertoe dat medewerkers steekpenningen aannemen in ruil voor vertrouwelijke informatie	- Onvoldoende binding met medewerkers, individualistisch werk - Vertrouwen beschadigd - Hoge werkdruk	- Consequenties omtrent integriteit - Financiële consequenties	Gemiddeld (3)	Gemiddeld (3)	9	Gesprekken om de verbinding op de werkvloer te verbeteren en de motivatie om over te gaan tot crimineel gedrag te verkleinen	Wie: Leidinggevende en plaatsvervanger Wat: Eén-op-één gesprekken tussen leidinggevend en medewerker waar professionele en persoonlijke zaken aan bod komen Wanneer: Maandelijks Hoe: Implementeren van een IT-tool om de systemen te monitoren en rapporteren van bevindingen voor de compliance-afdeling Waar: Medewerker en leidinggevende
RID-02	Makkelijk toegang tot systemen	Medewerkers die vanuit hun rol geen toegang zouden moeten hebben tot informatie, kunnen makkelijk gevoelige informatie van de burger opzoeken, downloaden, aanpassen en verspreiden	- Gebrek aan controles - Autorisaties worden niet toegepast. - Verouderde systemen	- Reputatieschade - Maatschappelijke impact - Veiligheid mensen	Groot (4)	Groot (4)	16	Autorisatiebeleid wordt vastgesteld en nageleefd om ervoor te zorgen dat toegang tot informatie alleen mogelijk is voor medewerkers die vanuit hun verantwoordelijkheid toegang zouden moeten hebben.	Wie: Compliance officer en CISO. Wat: Vaststellen autorisatiebeleid en inrichten systemen volgens dit beleid. Wanneer: Continu Hoe: Implementeren van een IT-tool om de systemen te monitoren en rapporteren van bevindingen voor de compliance-afdeling Waar: Compliance- en IT-afdeling

Tabel 9. Template risicoregister, inclusief voorbeelden (deel 1/2)

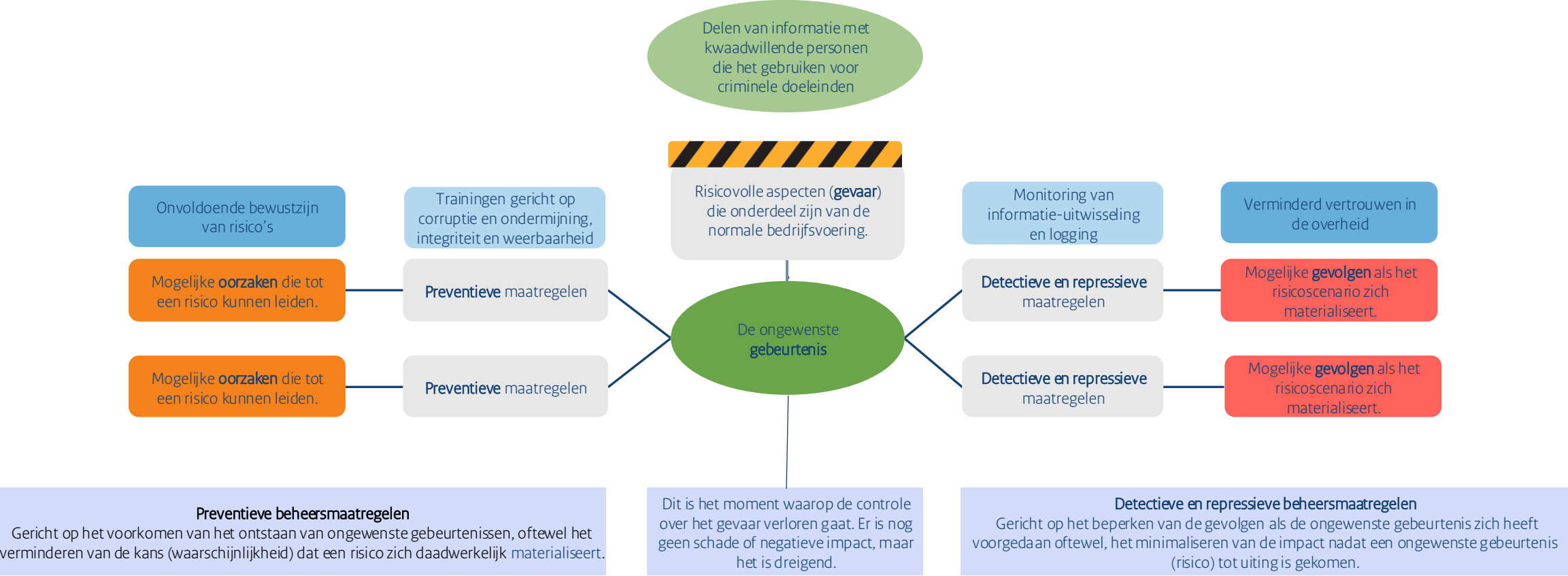
Bijlage F. Template Risicoregister (2/2)

Risico-ID	Risico titel	Risicobeschrijving	Oorzaken	Gevolgen	Kans	Impact	Risicoscore	Beheersmaatregel doel	Huidige Beheersmaatregel(en)
Uniek risico nummer (RID)	Risico titel	Risicobeschrijving met focus op de ongewenste gebeurtenis	Overzicht van de mogelijke oorzaken (niet uitputtend), met focus op de belangrijkste oorzaken	Overzicht van de mogelijke gevolgen (niet uitputtend), met focus op de belangrijkste gevolgen	Bepaal de kans van optreden met behulp van de kans-schaal	Bepaal de impact van het risico met behulp van de impact-schaal	De risicoscore is kans maal impact	Formuleer de doelstelling (de waarom) van de beheersmaatregel	Gebruik de 4W – 1H methodiek om de beheersmaatregelen concreet mogelijk uit te schrijven.
RID-03	Ondermijning binnen werving en selectie	Criminele netwerken proberen invloed uit te oefenen op besluitvorming bij werving en selectie door HR-adviseurs te beïnvloeden of zelf onderdeel te worden van het proces.	- Gebrek aan toezicht en objectieve procedures - Onvoldoende bewustzijn en kennis m.b.t. ondermijning	- Consequenties omtrent integriteit - Reputatieschade - Maatschappelijke gevolgen	Klein (2)	Desastreus (5)	10	Training gericht op objectieve werving en selectie, zodat selectiecommissieleden meer kennis en vaardigheden leren ten aanzien van integriteit en weerbaarheid tegen corruptie en ondermijning.	Wie: HR-manager en compliance officer Wat: Training objectief werven en selecteren geven aan selectiecommissieleden om bewustwording van en weerbaarheid tegen criminele beïnvloeding te stimuleren Wanneer: Jaarlijks Hoe: Organiseren van verplichte trainingssessies en informatie beschikbaar stellen Waar: HR-afdeling en compliance officer

Tabel 9. Template risicoregister, inclusief voorbeelden (deel 2/2)

Bijlage G. Bow-Tie methodiek

De Bow-Tie analyse brengt risico's overzichtelijk in kaart door oorzaken, gevolgen en beheersmaatregelen te visualiseren rond een centrale ongewenste gebeurtenis. Een gebalanceerde selectie van relevante elementen is essentieel;. Overmatige detaillering kan het model minder effectief maken. De methodiek kan gebruikt worden om risico's te identificeren, gevolgen en oorzaken te bepalen en passende preventieve, detectieve en repressieve maatregelen te formuleren, maar hoeft niet in zijn geheel te worden ingevuld voor alle risico's.



Figuur 3. Schematisch voorbeeld van de Bow-Tie methodiek

Bijlage H. Voorbeeldrisico's corruptie en ondermijning ^(1/2)

De onderstaande tabel bevat voorbeelden van ondermijning- en corruptierisico's op basis van input van experts op het gebied van corruptie en ondermijning.

Voorbeeldrisico	Beschrijving
Ongedetecteerde corruptie door onvoldoende zicht op persoonlijke situaties van medewerkers	Het risico dat door een gebrek aan verbinding en contact met medewerkers signalen van ongewenst gedrag, integriteitsproblemen of persoonlijke problemen niet op tijd worden herkend, waardoor incidenten (onopgemerkt) kunnen ontstaan of escaleren.
Ondermijning door verspreiding van informatie	Het risico dat onbevoegden door onvoldoende toegangsbeveiliging systemen binnenkomen en gegevens inzien en verspreiden, wat kan leiden tot datalekken, fraude of verstoring van processen.
Criminele beïnvloeding van werving en selectie	Het risico dat criminelen of andere ongewenste partijen het werving- en selectieproces beïnvloeden, waardoor personen worden aangenomen die voor eigen of criminele belangen handelen en de organisatie kwetsbaar maken.
Omkoping en belangenverstrengeling	Het risico dat medewerkers (bewust of onbewust) besluiten nemen op basis van persoonlijke, zakelijke of financiële belangen (omkoping of belangenverstrengeling), wat leidt tot onrechtmatige besluiten, benadeling van de organisatie en verlies van vertrouwen.
Misbruik van vertrouwelijke informatie	Het risico dat medewerkers gevoelige of vertrouwelijke informatie gebruiken voor eigen gewin of delen met onbevoegden, wat leidt tot privacyrisico's, chantage of reputatieschade.
Criminele beïnvloeding van besluitvorming	Het risico dat externe partijen druk uitoefenen of infiltreren in bestuurlijke of ambtelijke besluitvorming, waardoor besluiten worden genomen op basis van ongewenste invloed in plaats van objectieve criteria.
Misbruik van diensten en voorzieningen	Het risico dat publieke diensten en voorzieningen door medewerkers of derden worden misbruikt voor persoonlijke of criminele doeleinden, wat leidt tot financiële schade en verlies van integriteit.
Ondermijning door manipulatie van systemen en processen	Het risico dat systemen of administratieve processen worden gemanipuleerd (bijv. door informatie te wijzigen of verwijderen) om voordelen te behalen of fraude te plegen, wat leidt tot onjuiste registraties, financiële schade of verlies van data-integriteit.
Oneigenlijk gebruik van bevoegdheden	Het risico dat medewerkers hun autorisaties of invloed gebruiken voor persoonlijke belangen of om anderen te bevoordelen, wat kan leiden tot onrechtmatige of ongelijkwaardige besluitvorming.
Criminele infiltratie	Het risico dat criminele organisaties proberen invloed of toegang te krijgen binnen de organisatie, wat risico's oplevert voor veiligheid, integriteit en verstoring van publieke taken.

Tabel 10. Voorbeelden van ondermijning- en corruptierisico's (1/2)

Bijlage H. Voorbeeldrisico's corruptie en ondermijning (2/2)

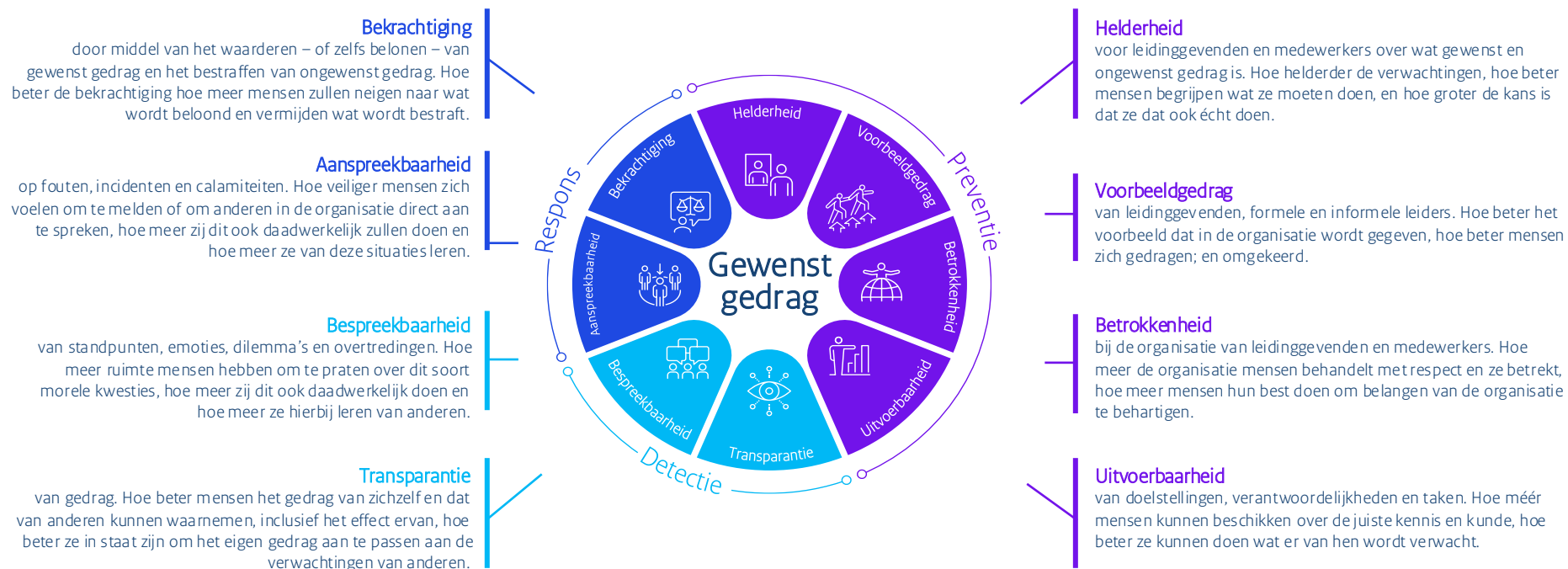
Voorbeeldrisico	Beschrijving
Onbehandelde corruptie en ondermijning door onvoldoende bewustzijn van integriteitsrisico's	Het risico dat als medewerkers onvoldoende kennis of bewustzijn hebben van integriteits- en corruptierisico's, signalen niet worden herkend of worden onderschat waardoor hier geen beheersmaatregelen op worden getroffen en er een verhoogde kans is op herhaaldelijke en onopgemerkte integriteitsschendingen.
Onopgemerkte ondermijning door lage meldingsbereidheid bij incidenten	Het risico dat incidenten of vermoedens van integriteitsproblemen worden niet gemeld uit angst, wantrouwen of onbekendheid, waardoor risico's blijven bestaan en niet worden aangepakt.
Ongedetecteerde incidenten door onvoldoende monitoring op systemen	Het risico dat gebrek aan automatische beveiligings- en controlesystemen zorgt ervoor dat ongeautoriseerde toegang, datalekken of frauduleuze handelingen niet tijdig worden gedetecteerd.
Onvoldoende naleving van veiligheidsregels door klantgericht gedrag	Het risico dat medewerkers, doordat klanttevredenheid belangrijker wordt gevonden dan naleving van veiligheidsregels, te veel of ongepaste informatie delen, wat leidt tot misbruik van gegevens, ongeautoriseerde toegang en criminele beïnvloeding.
Ongedetecteerde corruptie en ondermijning door gebrek aan prioriteit voor risicomanagement	Het risico dat door een gebrek aan prioriteit, tijd en eigenaarschap vanuit de ambtelijke of bestuurlijke leiding onderwerpen zoals risicomanagement, corruptie en onvoldoende worden onderkent en onder de aandacht wordt gebracht en dat er onvoldoende tijd wordt vrij gemaakt voor de beheersing van risico's, wat de organisatie kwetsbaarder maakt voor corruptie- en ondermijningsincidenten.
Onopgemerkte ondermijning verminderd toezicht en contact door plaats- en tijdonafhankelijk werken	Het risico dat de afname van contact met collega's en leidinggevend door plaats- en tijdonafhankelijk werken zorgt dat signalen van ondermijning, beïnvloeding of integriteitsproblemen onopgemerkt blijven, waardoor medewerkers kwetsbaarder worden voor criminele benadering.
Incidenten door versnelde besluitvorming en politieke urgentie	Het risico dat medewerkers door hoge politieke urgentie besluiten of processen versneld uitvoeren, waardoor noodzakelijke integriteits-, controle- en zorgvuldigheidsstappen worden overgeslagen.

Tabel 10. Voorbeelden van ondermijning- en corruptierisico's (2/2)

Bijlage I. Integriteitscultuurmodel

Het KPMG Integriteitscultuurmodel

Het door KPMG ontwikkelde integriteitscultuurmodel, zoals getoond in figuur 4, vormt de basis voor het doen van onderzoek naar grondoorzaken van risico's. Dit model is gebaseerd op wetenschappelijk onderzoek naar 150 integriteitsschendingen waarbij is aangetoond dat er acht cultuurdimensies zijn die van invloed zijn op het handelen van medewerkers en leidinggevend. De dimensies Helderheid, Voorbeeldgedrag, Betrokkenheid en Uitvoerbaarheid zijn preventief van aard; Transparantie en Bespreekbaarheid zijn detectief; en Aanspreekbaarheid en Bekrachting zijn repressief. Hoe sterker de cultuurdimensies zijn verankerd binnen een organisatie, hoe groter de kans op integer gedrag. Uit aanvullend wetenschappelijk onderzoek in 2008 en 2011 is gebleken dat bij organisaties waarbinnen de acht cultuurdimensies sterk zijn verankerd, een gemiddelde afname van integriteitsschendingen is geconstateerd van 30%. De meest serieuze integriteitsschendingen, waaronder corruptie en ondermijning, dalen gemiddeld met een nog groter percentage.



Figuur 4. Het KPMG Integriteitscultuurmodel, inclusief uitleg van de cultuurdimensies

Bijlage J. Voorbeeldvragen ten behoeve van de grondoorzakenanalyse (1/3)

De onderstaande tabel bevat voorbeeldvragen die bijdragen aan de analyse van de grondoorzaken van risico's. De vragen zijn opgesteld op basis van de cultuurdimensies uit het KPMG Integriteitscultuurmodel.

Voorbeeldvragen ten behoeve van de grondoorzakenanalyses		
Cultuurdimensie	Doel	Voorbeeldvraag
Helderheid <i>Helderheid voor leidinggevend en medewerkers over wat gewenst en ongewenst gedrag is. Hoe helder de verwachtingen, hoe beter mensen begrijpen wat ze moeten doen, en hoe groter de kans is dat ze dat ook écht doen.</i>	Begrip van gedragsnormen	Is de communicatie over gedragsnormen binnen de organisatie duidelijk en gemakkelijk te begrijpen?
	Bekendheid van risico's	Zijn medewerkers op de hoogte van de algemene waarden en principes die ethisch gedrag binnen de organisatie sturen?
	Bekendheid van beleid	Begrijpen medewerkers wat ondermijning en corruptie inhoudt en welke vormen dit kan aannemen binnen de organisatie?
	Bekendheid van meldpunten	Begrijpen medewerkers wat ondermijning en corruptie inhoudt en welke vormen dit kan aannemen binnen de organisatie? Zijn medewerkers bekend met het beleid en de gedragsnormen voor: • het aanbieden en accepteren van geschenken of uitnodigingen; • het beschermen van vertrouwelijke en persoonlijke informatie; • het gebruik van sociale media?
Voorbeeldgedrag <i>Voorbeeldgedrag van leidinggevend, formele en informele leiders. Hoe beter het voorbeeld dat in de organisatie wordt gegeven, hoe beter mensen zich gedragen; en omgekeerd.</i>	Voorbeeldgedrag directe leidinggevend	Geven directe leidinggevend een positief voorbeeld op het gebied van ethiek, integriteit en het tegengaan van ondermijning en corruptie?
		Hebben direct leidinggevend een duidelijke en juiste aanpak voor ethiek, integriteit en het voorkomen van ondermijning en corruptie?
		Stimuleren directe leidinggevend actief een cultuur binnen de afdeling waarin ethiek, integriteit en het tegengaan van ondermijning en corruptie centraal staan?
	Voorbeeldgedrag management	Geeft het management een positief voorbeeld op het gebied van ethiek, integriteit en het tegengaan van ondermijning en corruptie? Stimuleert het management actief een cultuur waarin ethiek, integriteit en het tegengaan van ondermijning en corruptie centraal staan?
Betrokkenheid <i>Betrokkenheid bij de organisatie van leidinggevend en medewerkers. [...]</i>	Toewijding	Zijn medewerkers en leidinggevend volledig toegewijd aan het naleven van de gedragsnormen van de organisatie?
		Voelen medewerkers zich comfortabel bij de waarden en normen van de organisatie?

Tabel 11. Voorbeeldvragen ten behoeve van de grondoorzakenanalyse op basis van de cultuurdimensies uit het KPMG Integriteitscultuurmodel (deel 1/3)

Bijlage J. Voorbeeldvragen ten behoeve van de grondoorzakenanalyse (2/3)

Voorbeeldvragen ten behoeve van de grondoorzakenanalyses		
Cultuurdimensie	Doel	Voorbeeldvraag
Betrokkenheid <i>[...] Hoe meer de organisatie mensen behandelt met respect en ze betreft, hoe meer mensen hun best doen om belangen van de organisatie te behartigen.</i>	Stimuleren verantwoord gedrag	Worden medewerkers actief gemotiveerd en aangemoedigd om verantwoordelijk en integer te handelen?
	Respectvolle werkomgeving	Zorgt de organisatie voor een werkomgeving waarin respectvol gedrag de norm is?
	Betrouwbare werkomgeving	Vertrouwen medewerkers de collega's en externe partners waarmee zij samenwerken?
Uitvoerbaarheid <i>Uitvoerbaarheid van doelstellingen, verantwoordelijkheden en taken. Hoe méér mensen kunnen beschikken over de juiste kennis en kunde, hoe beter ze kunnen doen wat er van hen wordt verwacht.</i>	Haalbare doelen	Stelt het management doelen die realistisch en haalbaar zijn, zonder dat deze in strijd komen met de waarden en normen van de organisatie?
		Biedt de organisatie voldoende tijd en middelen aan medewerkers om doelstellingen te behalen, zonder dat er druk ontstaat die kan leiden tot ongewenst gedrag?
		Voelen medewerkers geen disproportionele druk om kortetermijndoelstellingen te behalen?
	Prioritering van integer handelen	Wordt bij de besluitvorming binnen de organisatie ethiek, integriteit en het voorkomen van ondermijning en corruptie nadrukkelijk gewaardeerd boven het nastreven van kortetermijndoelstellingen?
Transparantie <i>Transparantie van gedrag. Hoe beter mensen het gedrag van zichzelf en dat van anderen kunnen waarmaken, in dusief het effect ervan, hoe beter ze in staat zijn om het eigen gedrag aan te passen aan de verwachtingen van anderen.</i>	Preventieve beheersing	Worden bij belangrijke zakelijke beslissingen de bijbehorende risico's tijdig en adequaat geïdentificeerd?
	Bewustzijn	Is de directe leidinggevende en het management op de hoogte van het ongewenste gedrag dat plaatsvindt binnen de afdeling / organisatie?
		Wordt ongewenst gedrag opgemerkt door collega's?
	Beperken overtredingskans	Is de gelegenheid om overtredingen te plegen minimaal?
	Beperken geheimhouding	Zijn er voldoende controles aanwezig om overtredingen tijdig aan het licht te brengen?
		Is de mogelijkheid om overtredingen geheim te houden minimaal?

Tabel 11. Voorbeeldvragen ten behoeve van de grondoorzakenanalyse op basis van de cultuurdimensies uit het KPMG Integriteitscultuurmodel (deel 2/3)

Bijlage J. Voorbeeldvragen ten behoeve van de grondoorzakenanalyse (3/3)

Voorbeeldvragen ten behoeve van de grondoorzakenanalyses		
Cultuurdimensie	Doel	Voorbeeldvraag
Bespreekbaarheid <i>Bespreekbaarheid van standpunten, emoties, dilemma's en overtredingen. Hoe meer ruimte mensen hebben om te praten over dit soort morele kwesties, hoe meer zij dit ook daadwerkelijk doen en hoe meer ze hierbij leren van anderen.</i>	Open communicatie	Voelen medewerkers zich vrij om hun meningen en ervaringen te delen binnen hun afdeling?
	Hoge meldingsbereidheid	Worden incidenten en risico's openlijk besproken binnen de organisatie?
	Adviserende en stimulerende rol leidinggevende	Voelen medewerkers zich veilig en comfortabel om ondermijning en corruptie te melden?
		Voelen medewerkers zich comfortabel om advies te vragen aan hun leidinggevende bij het nemen van ethische beslissingen?
Aanspreekbaarheid <i>Aanspreekbaarheid op fouten, incidenten en calamiteiten. Hoe veiliger mensen zich voelen om te melden of om anderen in de organisatie direct aan te spreken, hoe meer zij dit ook daadwerkelijk zullen doen en hoe meer ze van deze situaties leren.</i>	Feedbackcultuur	Kunnen medewerkers elkaar en hun leidinggevendens aanspreken op ongewenst gedrag?
	Hoge meldingsbereidheid	Staan medewerkers open voor feedback op hun gedrag?
		Is er bij medewerkers sprake van terughoudendheid uit angst voor negatieve consequenties bij het melden van ongewenst gedrag?
		Is er bij medewerkers sprake van terughoudendheid uit angst voor een gebrek aan vertrouwelijkheid bij het melden van ongewenst gedrag?
Bekrachtiging <i>Bekrachtiging door middel van het waarderen – of zelfs belonen – van gewenst gedrag en het bestraffen van ongewenst gedrag. Hoe beter de bekrachtiging, hoe meer mensen zullen neigen naar wat wordt beloond en vermijden wat wordt bestraft.</i>	Positief gedrag stimuleren	Is er bij medewerkers sprake van terughoudendheid omdat zij niet verwachten dat ze tevreden zullen zijn met het afronden van ongewenst gedrag?
	Negatief gedrag bestraffen	Worden medewerkers gewaardeerd voor het naleven van gedragsregels?
		Neemt de organisatie voldoende maatregelen naar aanleiding van een incident?
	Leren van incidenten	Worden de betrokken medewerkers gestraft, ongeacht van hun positie binnen het bedrijf?
		Leren de betrokken medewerkers van hun misdragingen en fouten?
		Wordt door de organisatie geleerd van de incidenten, en worden deze geleerde lessen ingezet om het proces te verbeteren?

Tabel 11. Voorbeeldvragen ten behoeve van de grondoorzakenanalyse op basis van de cultuurdimensies uit het KPMG Integriteitscultuurmodel (deel 3/3)

Bijlage K. Voorbeeldoorzaken lage meldingsbereidheid



Tip: Oorzaken lage meldingsbereidheid achterhalen

Het rapport 'Waarom melden mensen (niet) bij meldpunten' bevat een werkblad met als doel om te helpen bepalen of het oprichten van een meldpunt verstandig is en hoe meldpunten effectief kunnen worden ingericht. Door het invullen van dit werkblad kun je beslissen welke factoren specifiek voor jouw meldpunt en/of doelgroep relevant zijn zodat je daarop kunt inzetten.

Figuur 5. 18 factoren die meldgedrag kunnen beïnvloeden – CCV, *Waarom melden mensen (niet) bij meldpunten* (2025)

Bijlage L. Impactschalen

Impactschalen								
	Organisatiedoel	Financieel	Imago / reputatie	Juridisch	Maatschappelijk	Politiek	Veiligheid mensen	Integriteit
Desastreus	De realisatie van het organisatiedoel is blijvend verstoord. Het voortbestaan van de organisatie wordt bedreigd.	Financiële consequenties vallen buiten de begroting van de aangesloten partijen.	Het incident bereikt het nieuws wereldwijd.	Strafrechtelijke vervolging van de organisatie en/of bestuurders door het Openbaar Ministerie (Punitief).	Uitval of ernstige verstoring van vitale processen of basisvoorzieningen. De continuïteit wordt ernstig verstoord. Dit raakt meerdere steden of meer dan een miljoen mensen.	Het kabinet / de verantwoordelijke bewindspersoon treedt af.	Ongeval met één of meerdere doden.	Structurele ondermijning door leidinggevend en of grote delen van de organisatie. Schendingen worden systemisch en meldingen stoppen door angst en gebrek aan aanspreekbaarheid.
Groot	De realisatie van het organisatiedoel is ernstig verstoord. Het vertrouwen in de organisatie is beschadigd.	Financiële consequenties vallen buiten de begroting van de organisatie.	Het incident bereikt de landelijke pers.	Bestuurlijke sanctie opgelegd door een toezichthouder (last onder dwangsom, bestuursdwang en/of bestuurlijke boete) (Repressief).	Verstoring van essentiële processen die cruciaal zijn voor dienstverlening. Dit raakt honderdduizenden mensen.	Een incident leidt tot een plenair debat of een onderzoek vanuit de Algemene Rekenkamer.	Ongeval met één of meerdere personen met blijvend zwaar letsel.	Incident raakt meerdere organisatielagen, inclusief leidinggevend en. Schendingen nemen merkbaar toe en vertrouwen in meldingsproces verdwijnt.
Gemiddeld	De realisatie van het organisatiedoel is tijdelijk verstoord. Er worden vragen gesteld over de betrouwbaarheid van de organisatie.	Financiële consequenties vallen buiten de post onvoorzien, maar binnen de begroting van de organisatie.	Het incident bereikt het regionale nieuws.	Een (mogelijke publieke) waarschuwing door een toezichthouder en/of een bindende aanwijzing van een toezichthouder om aanbevelingen of een verbetertraject uit te voeren (Correctief).	Hinder in belangrijke processen voor een beperkte groep. Dit raakt tienduizenden mensen.	Een incident leidt tot meerdere Kamerbrieven en schriftelijke vragen en Kamerdebatten.	Ongeval met één of meerdere personen met herstelbaar zwaar letsel.	Incident veroorzaakt verwarring over normen. Schendingen komen vaker voor en meldingsbereidheid neemt af.
Klein	De realisatie van het organisatiedoel is lichtelijk verstoord, zonder serieuze gevolgen.	Financiële consequenties vallen binnen de post onvoorzien van begroting van de organisatie.	Het incident bereikt het lokale nieuws.	Aanbevelingen door een toezichthouder en/of het maken van afspraken met een toezichthouder over verbetertrajecten (Coöperatief).	Tijdelijke verstoring van niet-kritieke processen; beperkte gevolgen zoals vertraging. Dit raakt enkele honderden tot tienduizenden mensen.	Een incident leidt tot mondelinge vragen tijdens vragenruimte in Tweede Kamer.	Ongeval met één of meerdere personen met licht letsel.	Incident beperkt tot één team of individu. Schendingen blijven incidenteel en worden direct opgepakt.
Minimaal	De realisatie van het organisatiedoel is zeer tijdelijk en/of gedeeltelijk verstoord, zonder gevolgen.	Geringe financiële consequenties.	Het incident krijgt niet of nauwelijks media-aandacht.	Een gesprek met en/of voorlichting door een toezichthouder (Informatief).	Korte onderbreking van een ondersteunend proces. Dit raakt minder dan 500 mensen.	Aandacht is beperkt schriftelijke vragen in de Tweede Kamer.	Ongeval met één of meerdere personen met verwaarloosbaar letsel.	Geringe consequenties voor integriteitscultuur. Geen toename van schendingen en meldingsbereidheid blijft stabiel.

Tabel 12. Toelichting van de impactschalen, bestaande uit de mogelijke impact van een risico per impactcategorie

Bijlage M. Template kans- en impactmatrix en heatmap

In deze bijlage zijn een template van een kans- en impactmatrix en een heatmap, met geplote voorbeeldrisico's opgenomen. De voorbeeldrisico's zijn geplot op basis van een score voor kans en impact.

Kans- en impactmatrix						
Impact	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	1
		1	2	3	4	5
		Kans				

Figuur 6. Kans- en impactmatrix

Voorbeeld heatmap risicoanalyse							
Impact	5	Desastreus					
	4	Groot					
	3	Gemiddeld				RID-02	
	2	Klein		RID-03	RID-01		
	1	Minimaal					
			Zeer klein	Klein	Gemiddeld	Groot	Zeer groot
			1	2	3	4	5
			Kans				

Figuur 7. Heatmap, inclusief geplote voorbeeldrisico's

Bijlage N. Voorbeelden beheersmaatregelen (1/3)

De onderstaande tabel bevat voorbeelden van preventieve, detectieve en repressieve beheersmaatregelen ter beheersing van ondermijning- en corruptierisico's.

Beheersmaatregel	Doel (waarom)	Beschrijving (wie, wat, wanneer, hoe, waar)
Preventieve beheersmaatregelen		
Functiescheiding	Waarom: Om te voorkomen dat één persoon volledige controle heeft over een bepaald proces en daarmee mogelijkheid tot frauderingen van systemen en processen te verlagen	Wie: Manager en teamleider zorgen voor functiescheiding Wat: Scheiding in verantwoordelijkheden, bijvoorbeeld tussen uitvoeren en goedkeuren van een bepaalde taak Wanneer: Bij het verdelen van verantwoordelijkheden Hoe: Vastlegging in werkdocumentatie en/of richtlijnen en het mondeling communiceren tijdens de onboarding van medewerkers Waar: In het gehele team en bij alle processen
Aanbieden van Gedragscode Integriteit Rijk bij indiensttreding en afleggen ambtseed, periodiek bespreken van gedragscode en dilemma's in teamoverleg	Waarom: Om een cultuur van eerlijkheid en transparantie te waarborgen, waardoor de kans op omkoping, belangenverstrengelingen, misbruik van positie en te verkleinen	Wie: HR-manager en afdelingshoofd Wat: Medewerkers ontvangen gedragscode en leggen ambtseed af. Wanneer: Bij indiensttreding leggen medewerkers ambtseed af Hoe: Documenten worden opgesteld, ondertekend, verzameld en bijgehouden in een HR-tool Waar: HR-afdeling
Screening van medewerkers, leveranciers en partners	Waarom: Om te begrijpen met welke personen de organisatie te maken krijgt en daarmee de kans op criminele infiltratie te verkleinen	Wie: HR-manager en werving en selectie-afdeling Wat: Screening van medewerkers en externe partijen op mogelijke kwetsbaarheden in hun profiel Wanneer: Voorafgaand aan het inhuren van nieuwe medewerkers en externe partijen Hoe: De uitslag van de screening wordt uitgevoerd en in een screeningsrapport vastgelegd Waar: Werving en selectie-afdeling
Trainingen over integriteit en weerbaarheid	Waarom: Om medewerkers meer kennis en vaardigheden aan te leren ten aanzien van integriteit en weerbaarheid tegen corruptie en ondermijning, waarmee de alertheid op mogelijke incidenten versterkt wordt	Wie: HR-manager en compliance officer Wat: Training geven aan medewerkers om bewustwording van en weerbaarheid tegen criminele beïnvloeding te stimuleren Wanneer: Jaarlijks Hoe: Organiseren van verplichte trainingssessies en informatie beschikbaar stellen Waar: HR-afdeling of integriteitsfunctionaris in samenwerking met BVA/BVC

Tabel 13. Voorbeelden van uitgewerkte beheersmaatregelen (deel 1/3)

Bijlage N. Voorbeelden beheersmaatregelen (2/3)

Beheersmaatregel	Doel (waarom)	Beschrijving (wie, wat, wanneer, hoe, waar)
Detectieve maatregelen		
Periodieke analyse van toegangslogs en systeemgebruik	Waarom: Om ongebruikelijke toegang tot gevoelige informatie op te sporen en daarmee de kans op bijvoorbeeld datalekken en sabotage te onderscheppen.	Wie: Compliance officer en IT security officer Wat: Opsporen van ongebruikelijke toegang tot systemen en processen Wanneer: Maandelijks Hoe: Analyse van de toegangslogs in vergelijking met de lijst met autorisaties, bijgehouden in een IT-tool en gerapporteerd naar de compliance officer Waar: IT security- en compliance-afdelingen
Mystery audits bij risicovolle processen	Waarom: Om naleving van procedures te toetsen zonder dat personen tijd hebben om aanpassingen te maken en hiermee manipulatie van de processen te detecteren.	Wie: Auditdienst Rijk of interne auditor en afdelingshoofd Wat: Onaangekondigde controles op het gebruik en verloop van risicovolle processen Wanneer: Tweemaandelijks Hoe: Naar aanleiding van het verzoek vanuit de afdelingshoofd, zal de auditor de kwetsbare processen observeren en analyseren om mogelijke manipulatie hiervan te detecteren Waar: Auditafdeling en team dat gebruik maakt van de risicovolle processen
Protective monitoring	Waarom: Om ongebruikelijke handelingen, verzoeken en andere druk op medewerkers vroegtijdig te signaleren en hierdoor vroegtijdig te kunnen detecteren en acteren op (mogelijke) incidenten	Wie: Compliance officer en IT-afdeling Wat: Automatisch monitoren van systemen en het flaggen van afwijkingen Wanneer: Continu Hoe: Implementeren van de protective monitoring-tool om de systemen te monitoren en rapporteren van bevindingen voor de compliance-afdeling Waar: Compliance- en IT-afdeling

Tabel 13. Voorbeelden van uitgewerkte beheersmaatregelen (deel 2/3)

Bijlage N. Voorbeelden beheersmaatregelen (3/3)

Beheersmaatregel	Doel (waarom)	Beschrijving (wie, wat, wanneer, hoe, waar)
Repressieve maatregelen		
Escalatieprotocol bij vermoedens van ondermijning	Waarom: Om een snelle reactie op incidenten te bevorderen, waarmee de gevolgen beperkt kunnen worden	Wie: Compliance officer en juridisch adviseur Wat: Protocol waar in staat beschreven wat er gedaan moet worden in geval van een incident, zoals de ontzegging van toegang tot systemen en gebouwen, bevriezen van financiële stromen en opschorting van contracten Wanneer: Bij incidenten Hoe: Het protocol wordt opgesteld, gecommuniceerd in de organisatie en gehandhaafd door de compliance afdeling Waar: Compliance afdeling
Interne onderzoeksunit	Waarom: Om het onderzoeken van incidenten te bespoedigen, waarmee de gevolgen beperkt kunnen worden	Wie: Compliance officer, integriteitsonderzoekers Wat: Team dat zich bezig houdt met interne onderzoeken naar (mogelijke) integriteit, corruptie en ondermijning incidenten Wanneer: Bij incidenten Hoe: Het team wordt opgericht voorafgaand aan incidenten en wordt ingezet als er een incident geïdentificeerd is, waarna zij rapporteren aan de compliance en risk management afdelingen Waar: Compliance en integriteitsafdeling
Intern sanctiebeleid	Waarom: Om ongewenst gedrag, zoals corruptie en ondermijning, te kunnen handhaven op een transparante en legale manier, waarbij de betrokkenen doormiddel van consequenties leren het gedrag niet nogmaals te vertonen en afschrikking voor andere medewerkers te verhogen	Wie: HR-manager en juridisch adviseur Wat: Een beleid waarin de sancties (zoals ontslag of juridische gevolgen) in staan beschreven, zodat er transparante, legale gronden zijn om acties te nemen bij overtredingen Wanneer: Bij incidenten Hoe: Het beleid wordt opgesteld, gecommuniceerd in de organisatie en gehandhaafd door de HR-afdeling Waar: HR- en juridische afdelingen

Tabel 13. Voorbeelden van uitgewerkte beheersmaatregelen (deel 3/3)

Bijlage O. Voorbeeld rapportage opzet (1/2)

Rapportage tabel 1 – Dashboard							
#	Toprisico	Minimaal	Klein	Gemiddeld	Groot	Desastreus	Trend
1	Geen verbinding met medewerkers						
2	Makkelijk toegang tot systemen						
3	Ondermijning binnen werving en selectie						

Huidige risicoscore periode Q2

Risicoscore periode Q1

Gewenste risicoscore/Risicobereidheid

Huidige risicoscore periode Q2

Risicoscore periode Q1

Gewenste risicoscore/Risicobereidheid

Tabel 14. Voorbeeld van de in de rapportage opgenomen tabel 1 – Dashboard

Rapportage tabel 2 –Relevante ontwikkelingen en status actieplan				
#	Toprisico	Belangrijkste ontwikkelingen	Status actieplan	
			Genomen acties/beheersmaatregelen	Toekomstige acties/beheersmaatregelen
1	Geen verbinding met medewerkers	- Herindeling van afdelingen door nieuwe diensten - Toename van personeel	- Periodieke gesprekken ingesteld tussen leidinggevende en medewerkers voor betere verbinding - Additionele vacatures opengesteld om de werkdruk te verlagen	- Teambuilding activiteiten ten behoeve van de verbinding - Implementeer een meldpunt/vertrouwenspersoon om signalen vroegtijdig op te vangen
2	Makkelijk toegang tot systemen	Wisseling van IT-systeem die dagelijks gebruikt wordt binnen de organisatie	Verouderde IT-systeem vervangen voor een systeem met meer functionaliteiten	- Opstellen van een handleiding van het IT-systeem - Automatisch monitoring installeren om ongebruikelijke handeling te detecteren
3	Ondermijning binnen werving en selectie	- Additionele vacatures opengesteld die met enige druk moeten worden gevuld - Nieuwe begroting voor de organisatie is recent gepresenteerd	Training over ondermijning en weerbaarheid gefaciliteerd	- Vastleggen van additionele controles en screening voor nieuwe kandidaten - Online omgeving creëren met additionele informatie over ondermijning en weerbaarheid

Tabel 15. Voorbeeld van de in de rapportage opgenomen tabel 2 – Relevante ontwikkelingen en status actieplan

Bijlage O. Voorbeeld rapportage opzet (2/2)

Rapportage tabel 3 – Lessons learned			
#	Toprrisico	(Bijna-)incident	Lessons learned
1	Geen verbinding met medewerkers	Een medewerker voelde zich geïsoleerd door persoonlijke problemen (scheiding) en een negatieve ervaring met zijn leidinggevende. De medewerker is benaderd door een externe partij met een voorstel dat in strijd was met integriteitsregels, namelijk het delen van informatie over een aantal personen in ruil voor geld. Door gebrek aan interne communicatie en betrokkenheid werd dit niet tijdigesignaleerd.	• Zorg voor regelmatige communicatie en betrokkenheid van medewerkers, vooral bij gevoelige functies, want persoonlijke omstandigheden beïnvloeden het handelen en nalaten in werksferen • De aanwezigheid van een anoniem meldpunt of extern vertrouwenspersoon kan de kans op het tijdig melden van corruptie en ondermijning bevorderen
2	Makkelijk toegang tot systemen	Een medewerker kreeg bij de overgang naar het nieuwe IT-systeem toegangsrechten tot kritische systemen, waardoor er ongeautoriseerde wijzigingen konden worden aangebracht. De medewerker heeft deze fout gemeld bij zijn leidinggevende.	• Controles voorafgaand aan het implementeren van nieuwe processen en systemen evenals periodieke controles op toegangsrechten en log monitoring zijn cruciaal • Het least privilege-principe behoort gehanteerd te worden, waarbij medewerkers alleen toegang krijgen tot wat strikt noodzakelijk is
3	Ondermijning binnen werving en selectie	Een kandidaat met een relatie met een persoon die aangesloten is bij een criminele netwerk was aangenomen door gebrek aan grondige screening. De focus lag vooral op ervaring en competenties, terwijl integriteitsrisico's niet systematisch werden getoetst. Daarnaast voelde het werving en selectie team veel druk om spoedig nieuw personeel aan te nemen.	• Laat werkdruk nooit de reden zijn om een integriteitsscreening (bijv. VOG, referentiecheck, social media check) niet uit te voeren • Er is een behoefte aan duidelijke richtlijnen voor werving en selectie, inclusief escalatie bij twijfel over een kandidaat

Tabel 16. Voorbeeld van de in de rapportage opgenomen tabel 3 – Lessons learned

Bijlage P. Voorbeelden communicatiemateriaal (1/2)

In deze bijlage zijn voorbeelden opgenomen van communicatiemateriaal ten behoeve van de diverse interviews en workshops.

Eerste interview m.b.t. het ophalen van casuïstiek en beheersmaatregelen

Het eerste interview betreft een gesprek met één persoon met relevante kennis en ervaring met de risico's, casuïstiek en beheersmaatregelen op het gebied van corruptie en ondermijning, specifiek binnen de vastgestelde scope.

Beste [naam participant],

In opdracht van het bestuur en met prioriteit vanuit de ambtelijke leiding voeren wij een risicoanalyse uit met de focus op corruptie en ondermijning binnen [organisatie]. Deze analyse is bedoeld om de weerbaarheid van de organisatie te versterken.

Binnen deze analyse wordt *corruptie* gezien als het misbruik van toevertrouwde macht voor persoonlijk gewin en *ondermijning* als het gebruik van legale structuren, diensten of voorzieningen om illegale activiteiten uit te voeren, waardoor het maatschappelijk systeem wordt aangetast.

Om tot een realistisch en bruikbaar risicobeeld te komen, is inzicht nodig in de praktijk: concrete casuïstiek, risico's en bestaande beheersmaatregelen binnen de [scope]. Jouw ervaring, kennis en inzichten zijn daarbij van grote waarde.

Daarom nodigen wij je graag uit voor een gesprek van circa 1 uur. We realiseren ons dat dit tijd vraagt, maar jouw bijdrage is essentieel om de risicoanalyse goed te onderbouwen en daadwerkelijk te laten aansluiten bij de praktijk.

Graag vernemen wij op welk van de onderstaande momenten je beschikbaar bent:

[Data opties]

Mocht je voorafgaand aan het gesprek vragen hebben, vernemen wij deze graag.

Alvast bedankt voor de medewerking.

Met vriendelijke groet,
[naam afzender]

Interviews m.b.t. het evalueren risicoanalyse en grondoorzaken onderzoeken

Er worden drie interviews afgenomen met personen binnen de teams/afdelingen in scope die bij de relevante risicoanalyseprocessen betrokken (zullen) zijn. Tijdens de gesprekken wordt er ingegaan op het risicoanalyseproces over het algemeen en zullen de eerste inzichten worden opgehaald omtrent het risicobeeld en grondoorzaken.

Beste [naam participant],

Sinds [datum] wordt binnen de [scope], in opdracht van het bestuur en met nadrukkelijke prioriteit vanuit de ambtelijke leiding, gewerkt aan een risicoanalyse gericht op corruptie en ondermijning. Hierbij wordt *corruptie* gezien als het misbruik van toevertrouwde macht voor persoonlijk gewin en *ondermijning* als het gebruik van legale structuren, diensten of voorzieningen om illegale activiteiten uit te voeren, waardoor het maatschappelijk systeem wordt aangetast.

Vanwege jouw rol, expertise en ervaringen nodigen wij je graag uit voor een gesprek over het risicoanalyseproces en de eerste inzichten. Tijdens dit gesprek bespreken we de geïdentificeerde risico's en beheersmaatregelen en verdiepen we ons in de grondoorzaken en gevolgen.

Jouw inbreng helpt om de analyse scherper, realistischer en beter toepasbaar te maken. Daarmee lever je een directe bijdrage aan het versterken van de organisatie. Het gesprek duurt circa 1 uur.

Graag vernemen wij op welk van de onderstaande momenten je beschikbaar bent:

[Data opties]

Mocht je voorafgaand aan het gesprek vragen hebben, vernemen wij deze graag.

Alvast bedankt voor de medewerking.

Met vriendelijke groet,
[naam afzender]

Bijlage P. Voorbeelden communicatiemateriaal (2/2)

Workshop 1 m.b.t. het opstellen van een risicobeeld

De eerste interactieve workshop zal gericht zijn op het vaststellen van het risicobeeld binnen de scope op basis van de uitgevoerde risicoanalyse. De focuspunten staan verder uitgewerkt in de onderstaande mail.

Beste [naam participant],

Binnen de afdeling [afdeling] van [organisatie] wordt momenteel, in opdracht van het bestuur en met prioriteit vanuit de ambtelijke leiding, een risicoanalyse uitgevoerd met focus op corruptie en ondermijning. Hierbij wordt *corruptie* gezien als het misbruik van toevertrouwde macht voor persoonlijk gewin en *ondermijning* als het gebruik van legale structuren, diensten of voorzieningen om illegale activiteiten uit te voeren, waardoor het maatschappelijk systeem wordt aangetast.

Graag nodigen wij jullie uit voor een interactieve workshop waarin we de opgehaalde risico's bespreken en het risicobeeld gezamenlijk aanscherpen. Het doel is om te komen tot een gedeeld en goed onderbouwd beeld van de belangrijkste risico's. De verschillende perspectieven en ervaringen van de deelnemers zijn hierbij cruciaal.

De workshop zal zich richten op de volgende zaken:

- Versterken van het risicobewustzijn, incl. de rol van bias in risicobeoordeling;
- Valideren, verdiepen en aanscherpen van de risico's, grondoorzaken, gevolgen en beheersmaatregelen;
- Individueel scoren van de risico's op kans en impact, als basis voor het dialoog in workshop 2.

Graag vernemen wij of het voor jullie mogelijk is om aan te sluiten op [datum] van [tijd] tot [tijd] (3 uur). De workshop zal plaatsvinden op [locatie]. We realiseren ons dat dit een aanzienlijke tijdsinvestering is, maar deze gezamenlijke sessie vormt een belangrijke basis voor vervolgkeuzes en maatregelen ten behoeve van de weerbaarheid binnen [organisatie].

Mocht je voorafgaand aan het gesprek vragen hebben, vernemen wij deze graag.

Alvast bedankt voor de medewerking.

Met vriendelijke groet,
[naam afzender]

Workshop 2 m.b.t. het evalueren van de risicoscore

Naar aanleiding van de eerste workshop is het risicobeeld en een risicoscore vastgesteld. Tijdens de tweede workshop wordt er gereflecteerd op deze uitkomsten en kunnen het risicobeeld en -score worden aangescherpt waar nodig.

Beste [naam participant],

Op [datum] is in workshop 1 gezamenlijk het risicobeeld vastgesteld en zijn de risico's individueel gescoord op kans en impact. In vervolg hierop organiseren wij een tweede workshop om te reflecteren op de geaccumuleerde risicoscores en het gesprek aan te gaan over welke risico's als eerste aandacht behoeven.

Deze sessie is belangrijk om tot een zorgvuldig afgewogen en breed gedragen eindresultaat te komen. Het resultaat vormt een basis voor bestuurlijke en ambtelijke besluitvorming en biedt handvatten om aan de slag te gaan met beheersmaatregelen.

Graag vernemen wij of het voor jullie mogelijk is om aan te sluiten op [datum] van [tijd] tot [tijd] (1 uur). De workshop zal plaatsvinden op [locatie].

Mocht je voorafgaand aan het gesprek vragen hebben, vernemen wij deze graag.

Alvast dank voor jullie blijvende inzet en betrokkenheid.

Met vriendelijke groet,
[naam afzender]

Bijlage Q: Verdere relevante Rijksbrede documenten*

Document	Toelichting
Kaderboek Organisatie en Bedrijfsvoering 2025	Doel van het kaderboek is het bijeenbrengen en ontsluiten van Rijksbrede afspraken met betrekking tot organisatie en bedrijfsvoering.
Gedragscode Integriteit Rijk (GIR)	De Gedragscode Integriteit Rijk (GIR) geeft een overzicht van de belangrijkste rijksbrede afspraken op het gebied van integriteit. Daarnaast biedt de gedragscode een houvast bij het maken van afwegingen en het nemen van beslissingen. De code geldt voor iedereen die voor het Rijk werkt.
Gedragsregeling voor de digitale en fysieke werkomgeving, Rijksoverheid	Deze gedragsregeling gaat vooral over digitale informatie en informatiesystemen. Het gaat daarbij om het werken met informatie zodat die volledig, actueel en vindbaar is. En het gaat ook om een veilige en privacy verantwoorde manier van werken
Handreiking kwetsbaarhedenscan	Deze handreiking geeft praktische richtlijnen om proactief scans uit te voeren op bekende kwetsbaarheden zodat die opgelost kunnen worden.
Handreiking veilig op (dienst)reis naar het buitenland	Deze handreiking biedt adviezen en maatregelen voor rijksmedewerkers wanneer zij zowel voor werk als privé naar het buitenland reizen. Hierbij ligt de focus op eigen veiligheid, informatiebeveiliging en beveiliging van apparatuur.
Handreiking identificeren kwetsbare functies	Doelstelling van de handreiking is het aanleveren van een kader op basis waarvan de individuele departementen en/of onderdelen van departementen kwetsbare functies (in relatie tot ondermijning) kunnen gaan identificeren.

Tabel 17. Verdere relevante bijlagen vanuit het Rijk
 *De lijst met documenten is niet limitatief, maar biedt inzicht in een aantal relevante documenten t.a.v. corruptie en ondermijning.



Bedankt!