gemeente
Goeree-Overflakkee

Risicomanagement

Uitvoeringsnota risicomanagement 2025-2028

Risicomanagement

Uitvoeringsnota risicomanagement 2025-2028

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

Deze uitvoeringsnota is het praktische vervolg op de kadernota risicomanagement. De uitvoeringsnota is gericht op het vertalen van beleid naar het bedrijfsproces. De organisatie streeft naar een zo optimaal mogelijke wijze van integraal risicomanagement Deze uitvoeringsnota beschrijft de wijze waarop kaders in de periode 2025 tot en met 2028 kunnen worden nageleefd en doelen kunnen worden gerealiseerd.

1.2 Doelstelling risicomanagement

Het doel van Risicomanagement is het inzichtelijk maken van de risico's die de gemeente loopt bij het realiseren van haar doelstellingen en kunnen nemen van beslissingen die gericht zijn op het voorkomen of minimaliseren van nadelige effecten die het optreden van risico's met zich mee kan brengen, zowel financieel als niet-financieel.

Voor de komende periode (2025-2028) willen we met Risicomanagement het volgende bereiken:

- **Continu inzicht in de risico's die de gemeente loopt;** Zowel risico's op het gebied van het behalen van beleidsdoelstellingen (strategisch/tactisch) als risico's die voortvloeien uit de dagelijkse werkzaamheden (operationeel).

- **Blijvende sturing en implementatie op beheersmaatregelen en hiermee het reduceren van risico's en de gevolgen van risico's;** Hiermee willen we waarborgen dat de gemeentelijke dienstverlening en essentiële processen kunnen blijven functioneren, zelfs of juist in het geval van onverwachte gebeurtenissen. Risico's kunnen het behalen van doelen belemmeren. Daarom is het van belang deze risico's te beheersen. Het beheersen van risico's is het implementeren van maatregelen om de kans van optreden van risico's te verlagen, ofwel schade veroorzaakt door risico's te beperken. Niet elk risico valt te beheersen of wil de organisatie beheersen. Het is van belang een goede afweging te maken tussen de kosten en de effectiviteit van de beheersmaatregel.

- **Risicobewustzijn/Risico-intelligentie van bestuur en organisatie blijven stimuleren;** Het bewustzijn is zowel van belang op het niveau van het bestuur als ook op organisatieniveau. Voor het bestuur geldt dit vooral bij het stellen van kaders en het nemen van belangrijke besluiten. Het bieden van inzicht in mogelijke risico's en kansen zorgt ervoor dat het bestuur onderbouwde en strategische beslissingen kan nemen.
  Het management zorgt voor een goede informatieverstrekking over risico's richting het bestuur ten behoeve van de besluitvorming. Het maken van verantwoorde keuzes in het al dan niet aanvaarden van risico's is hierbij een belangrijk punt. Daarnaast is het management verantwoordelijk voor het beheersen van de risico's.

- **Periodieke actualisatie van het weerstandsvermogen en de risico's;** De gemeentebrede risico-actualisatie dient tenminste twee keer per jaar plaats te vinden (als input voor de begroting en als input voor de jaarrekening). Er wordt beoordeeld of de genoemde risico's nog actueel zijn, of er risico's zijn bijgekomen of juist zijn afgenomen en wat de reden hiervan is. Daarnaast worden de beheersmaatregelen besproken en geactualiseerd.

- **Een gezonde weerstandsratio, in ieder geval een ratio in categorie C (1.0-1.4), zie tabel in paragraaf 3.2. van de Kadernota Risicomanagement;** Het weerstandsvermogen bestaat uit de beschikbare weerstandscapaciteit gedeeld door de benodigde weerstandscapaciteit. Wanneer het bedrag aan risico's even hoog is als het beschikbare vermogen dan is de weerstandsratio 1.0. Indien de gemeente een ratio van 1.0 of hoger heeft, betekent dit dat de gemeente de genoemde risico's voldoende tot uitstekend kan opvangen.

- **Het voldoen aan wettelijke vereisten omtrent het uitvoeren van risicomanagement:** De gemeente moet op basis van wet- en regelgeving (BBV, Gemeentewet, Financiële verordening) een inventarisatie

van risico's en het weerstandvermogen maken. Dit geldt ook voor het opstellen van beleid omtrent de weerstandcapaciteit en de risico's. Door het vaststellen van deze nota wordt het beleid van risicomanagement en weerstandvermogen geactualiseerd en voldoet de gemeente aan haar wettelijke verplichtingen. Hiermee worden bijvoorbeeld ook risico's met betrekking tot juridische en financiële consequenties gereduceerd.

- **Verhoging van doelmatigheid en effectiviteit:** Door het beter benutten van beschikbare middelen door risico's te beheersen en kansen te identificeren die bijdragen aan de gemeentelijke doelstellingen, wordt de doelmatigheid en doeltreffendheid verhoogd.

2 Het risicobeheersingsproces in de praktijk

2.1 Kaderstelling

De raad heeft een verordenende bevoegdheid, een kaderstellende, controlerende functie en budgetrecht. Het is aan de raad om in een nota de beleidskaders vast te stellen ten aanzien van risicomanagement en het weerstandsvermogen. De uitvoering van het risicomanagement is voorbehouden aan het college.

Een belangrijk onderdeel is het waarborgen van continuïteit van het beleid. Ook als zich onverhoopt een calamiteit voordoet, die een aanslag doet op het financieel vermogen van de gemeente, moet deze continuïteit worden gewaarborgd. Om die reden wordt via de algemene reserve een financiële buffer van € 2 miljoen (ondergrens algemene reserve) in stand gehouden om een eventuele ingrijpende financiële tegenslag op te kunnen vangen.

De kadernota en uitvoeringsnota weerstandsvermogen & risicomanagement hebben als oogmerk het risicomanagement structureel in de organisatie en het bestuur te (blijven) verankeren en de risico's te monitoren. Er wordt hierbij aandacht geschonken aan de rol van het bestuur, de positie van risicomanagement binnen de gemeentelijke organisatie, verantwoordelijkheden en bevoegdheden, de relatie met de weerstandsparagraaf, de P&C-cyclus en de praktische uitvoering van het proces risicobeheersing.

Dit leidt samengevat tot de volgende kaders en richtlijnen.

1. De gemeente Goeree-Overflakkee voldoet aan de wettelijke verplichtingen op het gebied van risicomanagement (zoals een juiste invulling van de paragraaf Weerstandsvermogen bij de begroting en jaarrekening).
2. De gemeente Goeree-Overflakkee houdt vast aan een risico neutrale houding, wat inhoudt dat de gemeente geen onvoorzienbare risico's wil dragen, maar wel risico's accepteert, mits deze toelaatbaar zijn qua invloed op de weerstandscapaciteit.
3. De gemeente Goeree-Overflakkee stuurt op een ratio weerstandsvermogen in Categorie C, zie tabel in paragraaf 3.2. van de Kadernota Risicomanagement. Dit is een ratio van 1.0 - 1.4. In de paragraaf Weerstandsvermogen wordt uitgegaan van één ratio voor zowel de gemeentebrede risico's als de risico's met betrekking tot de grondexploitatie. Voor wat betreft de paragraaf Grondbeleid wordt verwezen naar de Nota Grondbeleid. Daarin wordt nader ingegaan op de methode om de risico's inzake het grondbeleid in beeld te brengen.
4. Het weerstandsvermogen is opgebouwd uit de algemene reserve, de vrije bestemmingsreserves en de post onvoorzien.
5. College- en raadsvoorstellen moeten, indien van toepassing, te zijn voorzien van een risicoparagraaf dan wel risico-analyse, waarbij eventuele beheersmaatregelen moeten worden uitgewerkt.
6. De gemeente beschikt over inzicht in haar weerstandscapaciteit en actualiseert dit periodiek.
7. In de programmabegroting en het jaarverslag doet het college via de paragraaf Weerstandsvermogen en risicobeheersing verslag over de tien hoogste risico's voor de gemeente.
8. Nieuwe risico's en bestaande risico's vanaf € 50.000 worden in de risicorapportage per team opgenomen en toegelicht.

2.2 Kwaliteitsontwikkeling

Het risicomanagement draagt bij aan de kwaliteitsontwikkeling van de organisatie. Het geeft inzicht in de kwaliteit van processen, producten en diensten. Simpel gesteld kan worden: hoe hoger de geleverde kwaliteit, des te lager zijn de bijkomende risico's. Door dit instrument juist in te zetten en de samenhang aan te tonen en toe te passen is het mogelijk om de komende jaren stappen te blijven zetten op het gebied van risicobeheersing en het gericht toepassen van maatregelen. Deze maatregelen kunnen aanpassingen zijn in het proces waardoor risico's worden vermeden of beperkt.
De streefratio van 1.0 – 1.4 biedt onze gemeente een weerbaarheid om een aantal financiële tegenvallers te verwerken en toch voldoende weerstandsvermogen te houden.

2.3 Uitgangspunten

Ten aanzien van het risicomanagement hanteren we de volgende uitgangspunten:

1. Risico's moeten worden vermeden, gereduceerd en/of beheerst;
2. Risicomanagement is een systematisch en cyclisch proces om risico's te identificeren en te beoordelen, op basis hiervan maatregelen te nemen en te evalueren;
3. Risicomanagement is primair een bestuurlijke activiteit. Het college is immers verantwoordelijk voor het realiseren van de beoogde programmatische doelstellingen;
4. Risicomanagement is eveneens een activiteit van de ambtelijke organisatie: de teamleider is verantwoordelijk voor de beheersing van de risico's op zijn/haar verantwoordelijkheidsgebied;
5. Risico-inventarisaties worden periodiek geactualiseerd en vormen de basis van ons risicoprofiel. Tevens maken zij geïntegreerd onderdeel uit van de paragraaf weerstandsvermogen en risicobeheersing.
6. Adequate maatregelen kunnen de financiële gevolgen van risico's reduceren en dienen dan ook structureel onderdeel uit te maken van het risicomanagement.
7. Bij college-/raadsvoorstellen moet er aandacht zijn voor de risico's, die bijvoorbeeld nieuw beleid of projecten met zich meebrengen.

Om het risicoproces te beheersen wordt aan de volgende voorwaarden voldaan:
1. De rapportage over risico's en maatregelen is gekoppeld aan de Planning & Control-cyclus binnen de organisatie. Daarmee wordt zij onderdeel van een groter geheel waardoor rapportage automatisch moet volgen. De adviseur AO/IC belast met risicomanagement dient zoveel als mogelijk ondersteuning te bieden aan de (inhoudelijk) verantwoordelijken voor de risicogebieden (teamleiders en projectleiders).
2. De verantwoordelijke voor een risicogebied moet binnen het team regelmatig de risico's behandelen. Dit moet waarborgen dat wijzigingen of nieuwe risico's worden gesignaleerd en geregistreerd.
3. Het onderdeel "kanttekeningen" in adviezen moet ingevuld worden waarin meteen ingegaan wordt op het al dan niet treffen van beheersmaatregelen en welke dit dan eventueel moeten zijn.

Door het risicobeheersingsproces op een continue basis in de organisatie te borgen wordt de cyclus telkens weer doorlopen.

2.4 Risico overleggen

De basis voor risicomanagement ligt in het goede gesprek dat periodiek over risico's wordt gevoerd op verschillende niveaus in de organisatie. Van belang is dat daarbij het brede pallet aan risico's (financieel en niet-financieel) aan bod komt. Risicobewustzijn is een onderdeel van de cultuur van een organisatie. Het is daarom belangrijk dat er bereidheid en ruimte is om open over risico's (en fouten) te communiceren. Daarnaast is het van belang dat risicomanagement onderdeel is van de dagelijkse gang van zaken zodat alert wordt gereageerd op kansen en risico's.

Tot slot moeten ook de Frauderisico's worden benoemd en besproken. Hiervoor wordt verwezen naar de vastgestelde Nota Fraude Misbruik & Oneigenlijk gebruik Goeree-Overflakkee 2025. Ook wordt er elk jaar in het intern controleplan inzake de rechtmatigheid aandacht aan dit onderwerp besteed.

2.5 Cyberbeveiligingswet (Cbw) en informatiebeveiligingsrisico's

De Cyberbeveiligingswet (Cbw) is een Nederlandse wet die voortvloeit uit de Europese richtlijn NIS2 (Network and Information Security Directive 2). Deze wet verplicht gemeenten (en andere organisaties) om hun digitale weerbaarheid structureel te versterken door middel van een management control cyclus. Deze cyclus bestaat op hoofdlijnen uit de volgende onderdelen: risicomanagement als basis van technische en organisatorische maatregelen. De effectiviteit van deze maatregelen wordt gemonitord. Het doel is om de continuïteit van publieke diensten te waarborgen/verhogen en de impact van cyberincidenten te minimaliseren. Hiervoor zijn bestuurders expliciet verantwoordelijk.

In deze uitvoeringsnota willen we daarom ook specifiek stilstaan bij informatiebeveiligingsrisico's. Op 28 mei 2025 is door de VNG/IBD de handleiding "Risicomanagement voor gemeenten op basis van de BIO2" gepubliceerd.

De belangrijkste inhoud is als volgt:
De handreiking biedt een gestructureerde aanpak voor het uitvoeren van risicoanalyses op gemeentelijke processen, gericht op het verhogen van de cyberveiligheid en informatiebeveiliging. Dit gebeurt in lijn met de BIO2 en ISO 27005-normen, en met behulp van erkende methodieken zoals het Business Model Canvas (BMC) en MAPGOOD (dit een hulpmiddel wat gemeenten helpt om de digitale veiligheid beter in kaart te brengen en te verbeteren). De aanpak is ontwikkeld om gemeenten te helpen voldoen aan de NIS2-richtlijn en de Cyberbeveiligingswet (Cbw).

De kern van de aanpak ligt in het systematisch identificeren, analyseren en beheren van risico's binnen gemeentelijke processen. Dit wordt gedaan door:

- Het uitvoeren van een Business Impact Analyse (BIA) om kritieke processen te identificeren.
- Het invullen van het Business Model Canvas (BMC) om procesafhankelijkheden te begrijpen.
- Het identificeren en waarderen van risico's op basis van kans en impact.
- Het behandelen van risico's volgens de strategieën: vermijden, verminderen, overdragen of accepteren.
- Het uitvoeren van een GAP-analyse op basis van de BIO2-maatregelen.
- Het integreren van risicomanagement in het Informatiebeveiligingsmanagementsysteem (ISMS) en de gemeentelijke planning- en controlcyclus.

In de praktijk kunnen risico's worden geïdentificeerd op verschillende manieren. Voorbeelden zijn: het gesprek aan gaan met betrokkenen, het houden van brainstormsessies, scenario denken en het bestuderen van historisch incidentenmateriaal. Op deze manier wordt een goed beeld verkregen van de aanwezige risico's en hoe deze eventueel te beheersen zijn.

De handreiking benadrukt de rol van verschillende actoren, waaronder bestuurders, gemeentesecretarissen, lijnmanagers, proceseigenaren, CISO en Privacy Officer (PO). Samenwerking tussen deze rollen is essentieel om een effectief en toekomstbestendig risicomanagementsysteem op te zetten. De totale handreiking is hier te vinden: Z-24-164442 Handleiding: Risicomanagement voor gemeenten op basis van de BIO2.

De belangrijkste acties zijn:
1. Strategische Acties:
Bestuurders: Bepalen van risicobereidheid, vaststellen van kaders en zorgen voor bestuurlijke betrokkenheid.
Gemeentesecretaris: Verankeren van risicomanagement in strategie en organisatiecultuur; zorgen voor integrale sturing.
Concerncontroller: Toezicht houden op financiële haalbaarheid en integratie van risicomanagement in de P&C cyclus.

2. Praktische Stappen voor Risicoanalyse:

- **Context vaststellen:** Begrijp de scope van processen en risicobereidheid.
- **BIA uitvoeren:** Identificeer welke processen kritiek zijn op basis van impactaspecten (zoals beschikbaarheid, integriteit, vertrouwelijkheid, privacy, etc.).
- **Groepssessies organiseren:** Betrek proceseigenaren, de CISO, PO, en andere relevante partijen. Zorg voor een verplichte training voor bestuurders.
- **BMC invullen:** Breng procesafhankelijkheden in kaart.
- **Risico's identificeren:** Benoem risico's per procesblok en categoriseer ze (BIV en MAPGOOD).
- **Risico's waarderen**: Gebruik een 5-puntsschaal om kans en impact te beoordelen.
- **Risico's behandelen:** Kies een strategie (vermijden, verminderen, overdragen, accepteren) en stel maatregelen vast.
- **GAP-analyse uitvoeren:** Controleer de implementatie van BIO2-maatregelen en stel een actieplan op.
- **Resultaten vastleggen:** Documenteer risico's, maatregelen, en acties in een risicoregister en ISMS-documentatie. De risico actualisatie vervolgens periodiek mee laten lopen in de gemeentebrede risico actualisatie.

3. Continue Verbetering:

- **Monitoring:** Zorg voor periodieke evaluatie van risico's, bijvoorbeeld jaarlijks of bij significante wijzigingen.
- **Audits en reviews:** Voer interne audits uit en bespreek resultaten in een management review.
- **Integratie:** Koppel risicomanagement aan de gemeentelijke P&C-cyclus en aan andere processen zoals incidentmanagement en leveranciersbeheer.

4. Governance en Rollen:

- **CISO:** Coördineert het ISMS, ondersteunt proceseigenaren en rapporteert over risico's.
- **Proceseigenaren:** Voeren risicoanalyses uit en implementeren maatregelen.
- **Privacy Officer:** Adviseert over privacyrisico's en AVG-compliance.
- **Bestuurders en gemeentesecretaris:** Stellen beleid vast en zorgen voor bestuurlijke besluitvorming.

Deze aanpak moet de volgende resultaten opleveren:

- ✓ Een volledig ingevuld BMC: Overzicht van processen en afhankelijkheden.
- ✓ Risicoregister: Documentatie van risico's, kans, impact, maatregelen en eigenaren.
- ✓ GAP-analyse en actieplan: Status van maatregelen en benodigde acties.
- ✓ ISMS-documentatie: Input voor informatiebeveiligingsplannen en audits.
- ✓ Continu verbeterproces: Ingevoerd via de PDCA-cyclus.

Deze werkwijze wordt zoveel mogelijk geïntegreerd in de bestaande management- en controlcyclus.

2.6 Advisering over risico's

Het onderkennen van risico's bij de besluitvorming draagt bij aan een zorgvuldig afwegingsproces. Door de risico's en beheersmaatregelen inzichtelijk te maken, is vooraf duidelijk waaraan het bestuur goedkeuring verleend en worden onaangename verrassingen achteraf voorkomen. Om dit afwegingsproces en dit risicobewustzijn te stimuleren is in het adviessjabloon het onderdeel: "kanttekeningen" opgenomen. Hiermee wordt de steller van het voorstel uitgedaagd om na te denken over onder andere de risico's en hier op transparante wijze over te communiceren. De betrokken financieel adviseur toetst, eventueel in overleg met concerncontrol, of de risico's in de voorstellen juist en volledig zijn beschreven en voert hierover het gesprek met de steller van het voorstel.

Voor het opstarten van projecten wordt gebruikgemaakt van een startnotitie met bijbehorende formats. Hierin wordt aandacht geschonken aan risico's. De projectleider is verantwoordelijk voor het opstellen van het risicoprofiel van het project en het beheersen van de risico's.

2.7 Rollen, taken en verantwoordelijkheden

Om de effecten van risico's te minimaliseren en de continuïteit te waarborgen is het van belang inzicht te hebben in de risico's die de organisatie loopt. Dit vereist een **integrale aanpak** binnen de gehele organisatie waarbij niet alleen financiële risico's worden onderkend, maar ook die op het terrein van bijvoorbeeld milieu, letsel/veiligheid, imago en juridische zaken.

Inzicht in de risico's die de gemeente Goeree-Overflakkee loopt, begint bij het risicobewustzijn van de medewerkers in de organisatie. Als zij risicobewust zijn in hun dagelijkse werkzaamheden, neemt het inzicht in de risico's toe. Om de risico's in beeld te krijgen en te houden is voor de rapportage aangesloten op de bestaande producten van de planning- en controlcyclus.

Duidelijkheid over de rolverdeling is belangrijk in de uitvoering van het risicomanagement. Daarom geven wij hieronder een verdeling van de rollen binnen het risicomanagement.

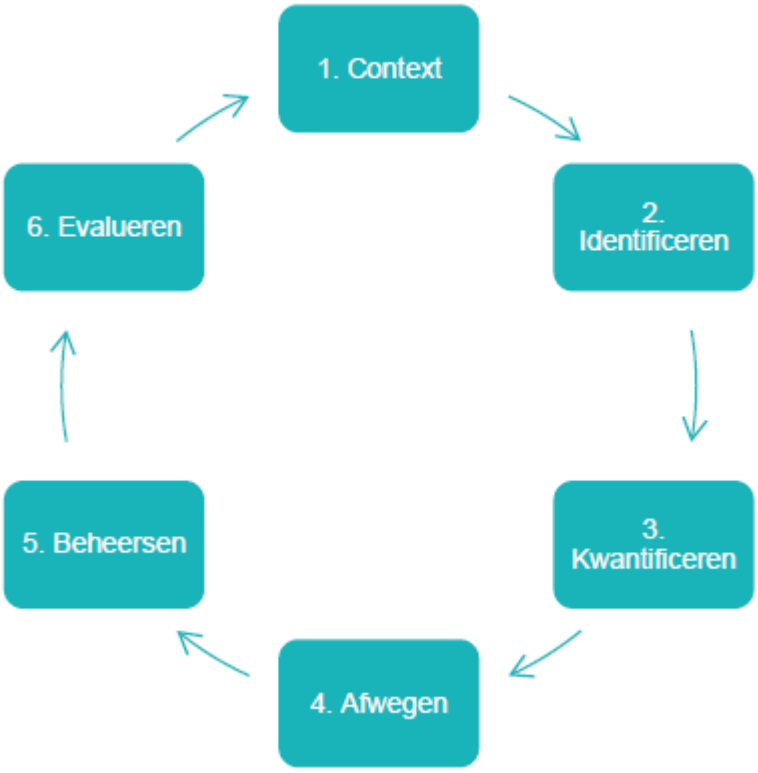
Actoren	Rollen	Acties en besluiten
Raad	Kaderstellend sturen en toezicht houden	• Kadernota Risicomanagement vaststellen; • Gewenste hoogte weerstandsvermogen vaststellen (ratio); • Paragraaf weerstandvermogen en risicobeheersing in jaarrekening en begroting vaststellen; • Toezicht houden op de uitvoering van risicomanagement door het college van burgemeester en wethouders.
College	Sturen en toezicht	• Vastellen van de Uitvoeringsnota Risicomanagement; • Toezien op implementatie van het risicomanagement; • Verantwoordelijkheid dragen voor het weerstandsvermogen; • Besluiten nemen over risicobeheersingsmaatregelen; • Sturen op verantwoording van risico's; • Rapporteren aan de gemeenteraad over risico's en beheersmaatregelen.
Directie	Sturen en verantwoorden	• Hanteren risicomanagement als rapportage-instrument; • Opdracht geven tot inventarisatie en kwantificering risico's; • Aanspreken op gedrag.
Teamleiders/ Projectleiders/ Domeinstrategen	Beheersen	• Kwantificeren van de risico's i.s.m. de Adviseur AO/IC belast met risicomanagement; • Implementatie en sturing op beheersmaatregelen; • Maatregelen nemen t.b.v. risicobeheersing binnen team of project (verhogen risicobewustzijn); • Verantwoordelijkheid nemen voor het behalen van doelen met inachtneming van risico's.
Concerncontroller	Adviseur	• Versterken risicobewustzijn binnen de organisatie; • Adviseren over risicobeheersingsmaatregelen;

Actoren	Rollen	Acties en besluiten
		• Toezicht houden op de uitvoering van risicomanagement binnen de organisatie.
Adviseur AO/IC belast met risicomanagement	Regisseur/ Adviseur	• Initiëren van het proces van Inventarisatie en herijking risico's (i.s.m. de teams); • Identificeren en analyseren van risico's; • Adviseren over risicobeheersingsmaatregelen; • Versterken risicobewustzijn binnen de organisatie; • Opstellen van risicorapportages en het weerstandsvermogen.
Financieel adviseurs	Adviseur	• Identificeren en analyseren van risico's; • Adviseren over risicobeheersingsmaatregelen; • Versterken risicobewustzijn binnen de organisatie; • Deelnemen aan inventarisatie/actualisatie van de risico's samen met de teams.
Medewerkers	Signaleren en aanpakken van risico's	• Signaleren van risico's en deze melden aan leidinggevende of risicomanager; • Uitvoeren van risicobeheersingsmaatregelen binnen hun takenpakket; • Bewust omgaan met risico's in de dagelijkse werkzaamheden.

N.B. deze rollen kunnen nog nader worden uitgewerkt als dit in de praktijk nodig blijkt te zijn.

2.8 Het proces

Het proces van risicomanagement bestaat uit een aantal stappen dat uitgevoerd wordt op basis van het vastgestelde beleid. De eerste stap in het proces van risicomanagement is de context (waarover gaat het?), daarna volgt het (continu) benoemen (identificeren) van risico's (wat kan ons allemaal overkomen). Vervolgens wordt voor de benoemde risico's de kans op optreden en de mogelijke gevolgen ingeschat. Daarbij is ook aandacht voor samenhang tussen risico's. Afhankelijk van deze inschattingen is het vervolgens mogelijk op verschillende dimensies (bijvoorbeeld geld of tijd) een prioritering in de lijst met risico's aan te brengen. Op basis van deze prioritering is het mogelijk om beheersmaatregelen te benoemen en implementeren. Tot slot worden in de laatste stap de resultaten van het proces geëvalueerd en gerapporteerd.



1. Context: waarover gaat het en wat willen we bereiken?
In deze stap wordt gekeken naar interne en externe factoren die van belang zijn voor de risicoanalyse. De omgeving waarin de gemeente opereert verandert en de organisatie verandert mee. Deze context is van invloed op de risico's die de organisatie loopt. Het gaat om vragen als: welke doelstellingen wil de organisatie behalen? Waar staat de organisatie nu? Wat is de maatschappelijke en economische omgeving? Hoeveel risico zijn we bereid te nemen? Het inzichtelijk maken van deze context maakt het eenvoudiger om in de volgende stap de risico's te identificeren en te kwantificeren.

2. Identificeren: wat kan ons overkomen?
Deze stap heeft tot doel een beeld te krijgen van de gebeurtenissen die het behalen van doelen kunnen belemmeren of vertragen. Het gaat erom inzicht te krijgen in een zo breed mogelijk spectrum aan risico's. De doelstellingen en processen moeten daarom vanuit meerdere invalshoeken worden bekeken. Hiertoe wordt een risico-overleg georganiseerd.
In de fase van risico analyse worden potentiële risico's binnen de organisatie geïnventariseerd en/of herijkt. Deze inventarisatie vindt plaats door de directie, teamleiders en de diverse medewerkers binnen de teams die op hun beleidsterrein met de risico's in aanraking komen. Concerncontrol ondersteunt dit hele proces.

De volgende risico's worden geïdentificeerd:

1. Juridisch: Risico's die de vermogenspositie van de organisatie aantasten door juridische procedures;
2. Organisatorisch: Risico's die verband houden met de wijze waarop de organisatie is ingericht en als zodanig handelt (bijvoorbeeld organisatiestructuur, richtlijnen, regelgeving, administratieve organisatie, protocollen, interne gedragsregels, interne controle);
3. Imago/politiek: Risico's die verband houden met de lokale politiek en het lokale bestuur en het gekozen beleid. Hierbij kan worden gedacht aan besluitvorming in strijd met de wet- en regelgeving, onbehoorlijk bestuur, onbevoegde besluitvorming en onbevoegde toezegging. Dit kan leiden tot negatieve publiciteit;
4. Materieel: Risico's van beschadiging of verlies van een materieel bezit;
5. Milieu: Risico's van aantasting van bodem, water, lucht en leefomgeving;

6. Relaties met derden: Risico's met betrekking tot diensten en producten die worden uitgevoerd in samenwerking met andere partijen/organisaties. Dit betreft bijvoorbeeld de samenwerking met gesubsidieerde instellingen en verbonden partijen.
7. Schadeclaims: Risico's die de vermogenspositie van de organisatie aantasten door (schade)claims;
8. Fraude-gerelateerd: Deze risico's omvatten verschillende vormen van opzettelijk misleidend gedrag met als doel financieel voordeel of andere voordelen te behalen.

3. Kwantificeren: hoe groot zijn de risico's?

Nadat bij de inventarisatie/herijking een beeld is ontstaan van welke risico's zich kunnen voordoen, worden de risico's geanalyseerd en beoordeeld. De acties die nu volgen worden allemaal doorlopen bij nieuwe risico's. Bij bestaande risico's die aan wijzigingen onderhevig zijn wordt dit proces eveneens doorlopen maar dan wel gezien vanuit het opnieuw waarderen/kwantificeren. Hiervoor worden de volgende stappen gezet:

- Omschrijven soort risico/ onderwerp
- Kort omschrijven risico
- Beoordelen kans dat een risico zich voordoet

Voor de beoordeling van de kans worden de volgende vijf klassen met referentiebeelden gehanteerd.

Klasse	Referentiebeelden	Kans
1 verwaarloosbaar	< 0 of 1 keer per 10 jaar	0%
2 aanwezig	1 keer per 5-10 jaar	25%
3 waarschijnlijk	1 keer per 2-5 jaar	50%
4 zeer waarschijnlijk	1 keer per 1-2 jaar	75%
5 zeker	1 keer per jaar of >	100%

Toelichting kansklasse:
Klasse 1: Deze klasse wordt gehanteerd voor risico's waarvan het onwaarschijnlijk is dat deze zich in de komende jaren voordoen.
Klasse 2: Deze klasse hanteren we voor risico's waarvan het niet waarschijnlijk is dat ze zich voordoen.
Klasse 3: Deze klasse hanteren we voor risico's die zich in het komende jaar wel, maar ook niet kunnen voordoen.
Klasse 4: Deze klasse wordt gehanteerd voor risico's waarvan het waarschijnlijk is dat ze zich in het komende jaar zullen voordoen.

De risico's die binnen de klassen 1-4 vallen worden afgedekt door het weerstandsvermogen.

Klasse 5 wordt gehanteerd voor risico's waarvan het zeer waarschijnlijk is dat ze zich in het komende jaar gaan voordoen. Voor risico's in klasse 5 wordt zo nodig een afzonderlijke beheersmaatregel getroffen. Zie hierna onder stap 8 voor voorbeelden.

- Beoordelen van het gevolg (financiële impact) van het risico

Voor de beoordeling van het gevolg hanteren we vijf klassen met de volgende klassenindeling

Klasse	Referentiebeelden/bandbreedte = gevolg
1 zeer klein	< € 10.000
2 klein	€ 10.000 - € 100.000
3 gemiddeld	€ 100.000 - € 250.000
4 groot	€ 250.000 - € 500.000
5 zeer groot	> € 500.000

- Berekenen risicoscore

De risicoscore wordt berekend door de kansscore te vermenigvuldigen met de gevolgscore. Hoe hoger de uitkomst, hoe groter het risico. De berekening is als volgt: Risico = Kans x Gevolg (max. score 5 x 5 = 25).
Hiermee wordt het bruto risico (risicobedrag vóór beheersmaatregel) omgezet naar een netto risico (risicobedrag ná beheersmaatregel).

Vervolgens is het mogelijk dat een restrisico overblijft. Dit is een risico dat overblijft na het nemen van maatregelen om een bepaald risico te verminderen of te beheersen. Met andere woorden, het is het deel van het risico dat niet volledig kan worden geëlimineerd, zelfs nadat passende technische, organisatorische, of andere maatregelen zijn getroffen.

Een restrisico wordt geaccepteerd als:
- ✓ Aanvullende maatregelen niet proportioneel of haalbaar zijn;
- ✓ Het accepteren van een restrisico een bewuste keuze is die moet bijdragen aan een balans tussen risico's, kosten, en de continuïteit van diensten.

- Berekenen financieel effect/kwantificeren

De financiële risico's van het voordoen van elk risico worden in beeld gebracht, tenzij dit niet mogelijk is. Voor de meeste risico's kan het financiële gevolg berekend worden aan de hand van historische cijfers of ervaringsgegevens.

4. Afwegen: hoe kunnen we onze risico's beheersen?

Beheersing vraagt om een heldere verantwoordelijkheidsverdeling en bewuste keuzes ten aanzien van beheersingsmaatregelen. In onderstaande tabel is opgenomen hoe diverse risico's kunnen worden beheerst:

Te voorkomen Risico's	Strategische Risico's	Externe risico's
Voorbeeld • onrechtmatig handelen, **fouten** in (geautomatiseerde) processen en **ongeautoriseerde** toegang tot informatiesystemen	• **investeringen**, samenwerkingen, subsidies, **decentralisaties**, fusies, nieuwe activiteiten	• **economische en demografische verschuivingen**, politieke onstabiliteit, nieuwe wet en regelgeving, verbonden partijen, natuurrampen
Kenmerken • **Intern & beheersbaar** en betrekking op menselijk gedrag • Doordat ze te voorkomen zijn emotie en media aandacht • Vaak niet acceptabel en gevaar voor risicoregelreflex	• Inherent aan het uitvoeren van beleid • Afweging **kans/bedreiging** rondom maatschappelijk/financieel rendement • Gedeelde verantwoordelijkheid	• **Buiten de invloedsfeer** van een organisatie • Meestal lange termijn, kan legitimiteit organisatie uithollen • Raakt de hele organisatie als het mis gaat.
Beheersing • Kans verkleinen door actieve preventie • Systemen **monitoren**, interne **controles** uitvoeren, **gedragsregels** vast te stellen	• Integrale aanpak besluitvorming • Kans en impact verkleinen • Zorgen dat niet de hele organisatie in gevaar komt • **Scenario's en tegenspraak**	• **Monitoring signalen** • Flexibiliteit organisatie vergroten • Voldoende reservemiddelen • **Scenario's en dialoog**

Nederlands adviesbureau risicomanagement

Hier wordt in paragraaf 2.10 verder op ingegaan.

5. Beheersen: hoe gaan we beheersmaatregelen implementeren?

Nadat de beheerstrategie is bepaald, moeten de beheersmaatregelen worden geïmplementeerd.

- In beeld brengen beheersingsmaatregelen

Het is niet voldoende om de geïdentificeerde risico's jaarlijks op te sommen. Het is belangrijk dat er iets met de risico's gebeurt. Voor elk risico wordt in de risicoregistratie aangegeven hoe hiermee wordt omgegaan. Beheersmaatregelen zijn gericht op het beheersbaar maken van een risico. Veelal gaat dit gepaard met het verlagen van de risicoscore (kans x gevolg). Zowel de verlaging van de kans als het verlagen van het gevolg dragen bij aan de beheersing van het risico. Er zijn verschillende soorten maatregelen. Kansverlagende maatregelen zijn altijd preventief (vooraf) van aard. Een voorbeeld hiervan is het uitvoeren van preventief onderhoud. Gevolgverlagende maatregelen kunnen zowel preventief (vooraf) als repressief (achteraf) van aard zijn. Een voorbeeld hiervan is het afsluiten van een verzekering of het treffen van een voorziening. Daarnaast wordt in beeld gebracht of het risico wel of niet beïnvloedbaar is en wanneer er sprake is van een restrisico.

- Benoemen risico eigenaar

Het is van groot belang aan te geven wie of welk team verantwoordelijk is voor het melden en beheersen van een risico. Daarom wordt voor elk risico een eigenaar benoemd.

- Berekenen van de benodigde weerstandscapaciteit en berekenen van de weerstandsratio

Wanneer de totale risico's in beeld zijn dan wordt bekeken welke financiële middelen de organisatie heeft om de risico's op te vangen. Het totaal aan risico's afgezet tegen de weerstandscapaciteit geeft de weerstandsratio.

- Rapporteren

Risico's die van grote invloed zijn op de benodigde weerstandcapaciteit noemen wij vanuit financieel oogpunt de hoogste risico's. In de weerstandsparagraaf komt dit terug in de vorm van een top tien met concernbreed de hoogste risico's. Er wordt tevens gerapporteerd over de invloed die het risico heeft op het weerstandsvermogen.

Zowel het college als de directie ontvangen twee keer per jaar een risicorapportage. In deze rapportages is het volgende opgenomen:

- De tien hoogste risico's;
- De risico's per team vanaf € 50.000;
- Verloop risico bedrag per team in vergelijking met de voorgaande rapportage;
- Noemenswaardige PM-risico's en noemenswaardige niet-financiële risico's;
- Conclusie en eventueel aanbevelingen.

6. Evalueren: wat hebben we geleerd?

In deze stap evalueren we het proces en de uitkomsten daarvan. Op basis van de evaluatie wordt er bijgestuurd en start het cyclisch proces van het risicomanagement opnieuw.

2.9 Procedure bij optredende risico's (van risico naar dekking)

Wanneer een situatie dreigt te ontstaan waarbij een risico in die hoedanigheid optreedt dat er mogelijk een beroep moet worden gedaan op het aanwezige weerstandsvermogen, dan zullen de hiernavolgende stappen worden genomen. De procedure start bij de risico-eigenaar. De risico-eigenaar is de aangewezen medewerk(st)er, het team en/of de teamleider. Het verantwoordelijke directielid voor het desbetreffende team is vanuit de gedachte van integraal management altijd eindverantwoordelijk voor de processen binnen zijn of haar team.

1 **Vaststellen:** De risico eigenaar stelt vast dat een risico binnen zijn of haar expertise- en verantwoordelijkheidsgebied optreedt of zal gaan optreden en dit (mogelijk) nadelige gevolgen heeft voor de gemeente.

2 **Kwantificeren:** De risico-eigenaar stelt in overleg met zijn teamleider of directeur vast dat dit aannemelijk is en tracht de (te verwachten) schade te kwantificeren. De ontstane situatie wordt gemeld bij de adviseur AO/IC belast met risicomanagement en de concerncontroller.

3 **Financiële dekking zoeken:** Primair zal de dekking voor een optredend financieel risico binnen de budgettaire mogelijkheden van het team worden gezocht. Optredende risico's met een financieel gevolg tot € 10.000 dienen altijd binnen de eigen exploitatie of budgetten te worden opgevangen.

4 **Soort risico analyseren:** Wanneer het imagotechnische schade betreft, stellen de teamleider of de directie en betrokken medewerker na constatering, de adviseur AO/IC belast met risicomanagement en de concerncontroller op de hoogte van de ontstane situatie.

5 **Ontoereikende dekking:** Wanneer blijkt dat de schade een aanzienlijk financieel gevolg heeft dat niet volledig is op te vangen binnen de budgettaire mogelijkheden van het team dan stelt de teamleider de directie en de betrokken portefeuillehouder middels een duidelijke uiteenzetting van de situatie en de onderzochte mogelijkheden op de hoogte. Tevens worden hierbij vanuit het team maatregelen aangedragen die ervoor zorgdragen dat dit risico niet langer kan optreden of tenminste tot een minimum wordt teruggebracht (voor zover de aard van het risico dit toelaat).

6 **Integraliteit:** De directie onderzoekt (of laat onderzoeken) in hoeverre de schade uit concernbrede middelen kan worden opgevangen.

7 **College-/Raadsvoorstel:** De risico-eigenaar zal vanuit de verkregen onderbouwing (punt 5 en 6) in samenspraak met zijn leidinggevende, de directie en de Portefeuillehouder, een collegevoorstel (en zo nodig raadsvoorstel) indienen inzake het aanspreken van het weerstandsvermogen teneinde de ongedekte schade incidenteel op te vangen.

Van risico naar dekking
Bij de dekking van incidentele risico's wordt de volgende volgorde gehanteerd:
1e Opvangen binnen bestaande budgetten/bestaande verzekeringen/incidentele baten (binnen hetzelfde product);
2e Post onvoorzien;
3e Opvangen binnen de begroting middels een mutatie in de tussentijdse rapportages mits de totale tussentijdse rapportage positief sluit (begrotingsruimte); indien het saldo niet positief is, zie dan 4.;
4e (Vrije) bestemmingsreserves of voorzieningen, op basis van het betreffende risico de meest relevante;
5e Algemene reserve.

Voor structurele risico's dient dekking gevonden te worden in de meerjarenraming.

2.10 Risicobeheersing

Afhankelijk van kans, impact, aard van het risico, urgentie, organisatie (cultuur), draagvlak en de beschikbare middelen wordt afgewogen welke beheersmaatregelen per risico genomen moeten worden. De risico-eigenaar heeft bij het treffen van maatregelen die genomen moeten worden om risico's te beperken of weg te nemen keuze uit een aantal basisstrategieën:

- **Accepteren**. Bij acceptatie zal de eventuele financiële schade door de weerstandscapaciteit moeten worden afgedekt.
- **Reduceren.** Omgaan met een risico vereist aanpassing van bijvoorbeeld de organisatie, procedures, systemen en organisatiecultuur.
- **Elimineren/vermijden.** Dit houdt in dat het beleid waardoor een risico ontstaat, wordt beëindigd, op een andere manier wordt vorm gegeven of geen beleid gestart wordt dat een risico met zich meebrengt. Dit kan voorkomen als een risico bijvoorbeeld onacceptabel* is.
- **Overdragen/verzekeren.** Dit kan door het beleid dat een risico met zich meebrengt, uit te laten voeren door een andere betrokken partij, die daarbij ook de financiële risico's overneemt (inkopen of uitbesteden) of door het afsluiten van een verzekering. Voor het onderwerp verzekeringen wordt verwezen naar de notitie "Uitgangspunten bij het verzekeren van risico's" . Dit beleidsstuk gaat over het verzekeringsbeleid van de gemeente.

*Per onacceptabel risico kunnen op de volgende manieren beheersmaatregelen worden bepaald:
- Reductieve maatregelen (deze zijn gericht op het reduceren van bedreigingen);
- Preventieve maatregelen (deze zijn gericht op het voorkomen van incidenten);
- Detectieve maatregelen (deze zijn bedoeld om incidenten te detecteren);
- Repressieve maatregelen (deze zijn bedoeld om de gevolgen te stoppen);
- Correctieve maatregelen (deze richten zich op het herstellen van de ontstane schade).

Vervolgens kan een behandelplan worden opgesteld waarin in ieder geval het volgende wordt beschreven:
- Wat er gedaan moet worden;
- Welke middelen er nodig zijn;
- Wie er verantwoordelijk is;
- Wanneer de beheersmaatregelen geïmplementeerd moeten zijn;
- Hoe de resultaten geëvalueerd moeten worden.

Een behandelplan biedt een gestructureerde en doelgerichte aanpak om een risico effectief te beheersen. Het maakt duidelijk welke acties nodig zijn en het helpt om prioriteiten te stellen. Een behandelplan zorgt er daarnaast voor dat risicobeheersing niet ad hoc gebeurt, maar systematisch en duurzaam wordt ingebed in de organisatie. Bij het in beeld brengen van risico's wordt bepaald of het risico van dien aard is dat het opstellen van een behandelplan nodig is.

2.11 Rapportage

De volgende rapportagemomenten komen voor bij het proces van risicomanagement

Document	Gericht aan	Door	Frequentie
Programmabegroting, paragraaf Weerstands-vermogen (top 10. Risico's)	Gemeenteraad	College	Jaarlijks
Jaarrekening, paragraaf Weerstandsvermogen (top 10. Risico's)	Gemeenteraad	College	Jaarlijks
Risicorapportage per team (risico's vanaf € 50.000)	Directie en college	Adviseur AO/IC belast met risicomanagement	1 x per half jaar
Raadsvoorstellen, onderdeel kanttekeningen	Gemeenteraad	College	Continu
Collegevoorstellen, onderdeel kanttekeningen	College	Medewerkers	Continu

3 Borging

3.1 Borging

Om te bevorderen dat risicomanagement een goede inbedding in de organisatie krijgt, zijn de volgende maatregelen getroffen:

- toekennen bevoegdheden en verantwoordelijkheden;
- beschrijving van het proces;
- het benoemen van verslagleggingsmomenten gekoppeld aan de P&C-cyclus;
- risico's maken deel uit van college- en raadsvoorstellen;
- risico's worden periodiek geactualiseerd;
- risico's zijn opgevoerd in Trustbound, zie uitleg hieronder.*
- deze uitvoeringsnota gelijktijdig met de kadernota, periodiek herzien.

***Trustbound**
Binnen de gemeente werken we met een GRC-tool (Governance, Risk, Compliance) genaamd: Trustbound. In deze tool zijn alle gemeentebrede risico's opgenomen (behalve de risico's op de grondexploitaties, deze worden separaat bijgehouden). De risico's zijn geclassificeerd zoals beschreven in paragraaf 2.8 en middels een risicomatrix in beeld gebracht. Door het werken met deze tool ontstaat structuur waardoor de risico's makkelijk te actualiseren zijn en makkelijk en snel te raadplegen. Hieronder is een afbeelding opgenomen van de risicomatrix van de financiële risico's: