

Zelfscan Risicomanagement

Inleiding

Welkom bij de Zelfscan Risicomanagement. Met dit document geeft het Commissariaat voor de Media een handreiking voor invulling van risicomanagement bij media-instellingen.

Kansen en onzekerheden

Het medialandschap staat voor tal van uitdagingen, zoals gedrag- en cultuur vraagstukken, digitalisering en opkomende AI en toenemende (internationale) concurrentie en veranderende wet- en regelgeving. Deze en andere ontwikkelingen brengen zowel kansen als onzekerheden met zich mee voor media-instellingen. Ze beïnvloeden de strategische doelen, het beleid en processen van de instellingen. Effectief risicomanagement stelt media-instellingen in staat tijdig actie te ondernemen om risico's die een bedreiging vormen voor de uitvoering van de publieke media opdracht te mitigeren of te verminderen. Daarnaast is het de basis voor het risico gebaseerd invulling geven aan de naleving van wet- en regelgeving (meer waar het moet, minder waar het kan).

Waarom een Zelfscan?

Media-instellingen zijn zelf verantwoordelijk hun organisatie zo in te richten dat risico's effectief worden beheerst. Kern van de interne risicobeheersing is risicomanagement. Met de Zelfscan kunnen media-instellingen hun eigen risicomanagement beoordelen aan de hand van een vragenlijst. De Zelfscan geeft ook inzicht in de onderdelen die het Commissariaat voor de Media (hierna: het Commissariaat) in zijn toezicht op de interne risicobeheersing belangrijk acht. De Zelfscan draagt bij aan de dialoog over risicomanagement tussen media-instellingen en het Commissariaat.

Wat is de rol van het Commissariaat voor de Media?

Het Commissariaat heeft een toezichthoudende rol als het gaat om de interne risicobeheersing door media-instellingen en de wijze waarop zij invulling geven aan hun risicomanagementsysteem. In dit toezicht richt het Commissariaat zich op diverse aspecten, waaronder de uitvoering en kwaliteit van het risicomanagement(proces), risico governance, gedrag & cultuur en kwaliteitsborging van het systeem.

Systeemtoezicht

De focus van het toezicht ligt op de kwaliteit en uitvoering van het interne risicomanagementsysteem van de media-instellingen, inclusief de periodieke toetsing van de effectiviteit van dit systeem. Bij incidenten, zoals overtredingen van wet- en regelgeving, richt het toezicht zich niet alleen op het incident zelf, maar vooral ook op de onderliggende oorzaken in de interne risicobeheersing van de media-instelling. Dit Systeemtoezicht begint met het vaststellen of het risicomanagementsysteem voldoende is. De verwachting is dat met het verder professionaliseren van risicomanagement binnen organisaties, er minder toezicht aandacht van het Commissariaat nodig zal zijn .



Wat is de Zelfscan?

De Zelfscan is een vragenlijst die is opgebouwd volgens de verschillende stappen van risicomanagement, de risicomanagementcyclus. De vragenlijst is samengesteld op basis van bestaande modellen en praktijkvoorbeelden. Media-instellingen kunnen de Zelfscan gebruiken voor de beoordeling van de opzet van hun risicomanagementsysteem.

Elke stap in de risicomanagementcyclus wordt geïntroduceerd met een korte toelichting op het betreffende onderdeel, gevolgd door een set relevante vragen. Deze vragen zijn richtinggevend en dienen als voorbeeld voor de vragen die het Commissariaat mogelijk kan stellen bij de uitvoering van toezicht op de interne risicobeheersing. Het Commissariaat kan bepaalde vragen meer nadruk geven dan andere, afhankelijk van de specifieke situatie van de individuele media-instelling. Daarnaast zijn de vragen in de Zelfscan niet allesomvattend. Dat betekent dat het Commissariaat ook andere vragen kan stellen aan de media-instelling.

Aan het einde van de Zelfscan vind je een overzicht van de belangrijkste begrippen. De Zelfscan is ook beschikbaar in een printbare versie, waarbij je bij elke vraag aantekeningen kunt maken. Deze aantekeningen zijn voor eigen gebruik. Het Commissariaat zal de ingevulde Zelfscans niet opvragen. Het invullen van de Zelfscan is niet verplicht.

Wat is de status van de Zelfscan?

Deze Zelfscan geeft weer hoe het Commissariaat de invulling en toepassing van de wettelijke normen beoordeelt. Er zijn verschillende manieren waarop media-instellingen kunnen voldoen aan de wet- en regelgeving. Het Commissariaat verwacht dat een media-instelling gemotiveerd kan aantonen dat ze aan de wet- en regelgeving voldoet.

Relevante wet- en regelgeving

- Mediawet, in het bijzonder artikel 2.3 lid 5, artikel 2.178 lid 1
- Beleidsregel Governance en Interne Beheersing 2017, in het bijzonder artikel 3, 4 en 5
- Gedragscode Integriteit Publieke Omroep 2021, in het bijzonder Principe 6



Begrip risicomanagement

Voor een goede dialoog over risicomanagement is het van belang dat iedereen dezelfde taal spreekt.

Zowel in de praktijk als in de literatuur bestaan verschillende interpretaties en definities van risicomanagement. Zelfs in alledaagse gesprekken worden vaak (onbewust) diverse betekenissen gebruikt. Het is belangrijk om hiervoor een heldere definitie te hanteren.

Twee kernbegrippen vormen het uitgangspunt van de Zelfscan, namelijk "risico" en "risicomanagement". Het Commissariaat hanteert voor het begrip risico de definitie zoals gebruikt in de NEN-ISO 31000 richtlijn voor risicomanagement. Volgens deze richtlijn is een risico een onzekere gebeurtenis die invloed heeft op het behalen van doelstellingen.

Voor het begrip risicomanagement gebruiken we in deze Zelfscan de definitie het systematische proces om risico's zodanig te beheersen dat meer zekerheid bestaat dat de organisatie haar doelstellingen zal realiseren. Dit betekent dat risicomanagement een doelgericht, expliciet, gestructureerd, integraal en continu proces is.

De belangrijkste begrippen uit de Zelfscan worden achter in dit document beknopt toegelicht. De toegelichte begrippen zijn in dit document dikgedrukt.

Doelgericht	Risicomanagement levert een bijdrage aan het realiseren van doelen met inachtneming van onzekerheden.
Expliciet	De risico's en de bijbehorende onzekerheden worden volledig en eenduidig beschreven.
Gestructureerd	Risicomanagement vindt plaats volgens een vooraf bepaalde methodiek.
Integraal	De risico's worden opgehaald bij, en besproken met alle voor het risico relevante betrokkenen.
Continu	Risicomanagement is een continu (leer)proces.



Risicomanagementcyclus

De kern van interne beheersing is risicomanagement. Het Commissariaat kijkt naar de wijze waarop een media-instelling risicomanagement heeft vormgegeven én toepast en hanteert hierin de risicomanagementcyclus.

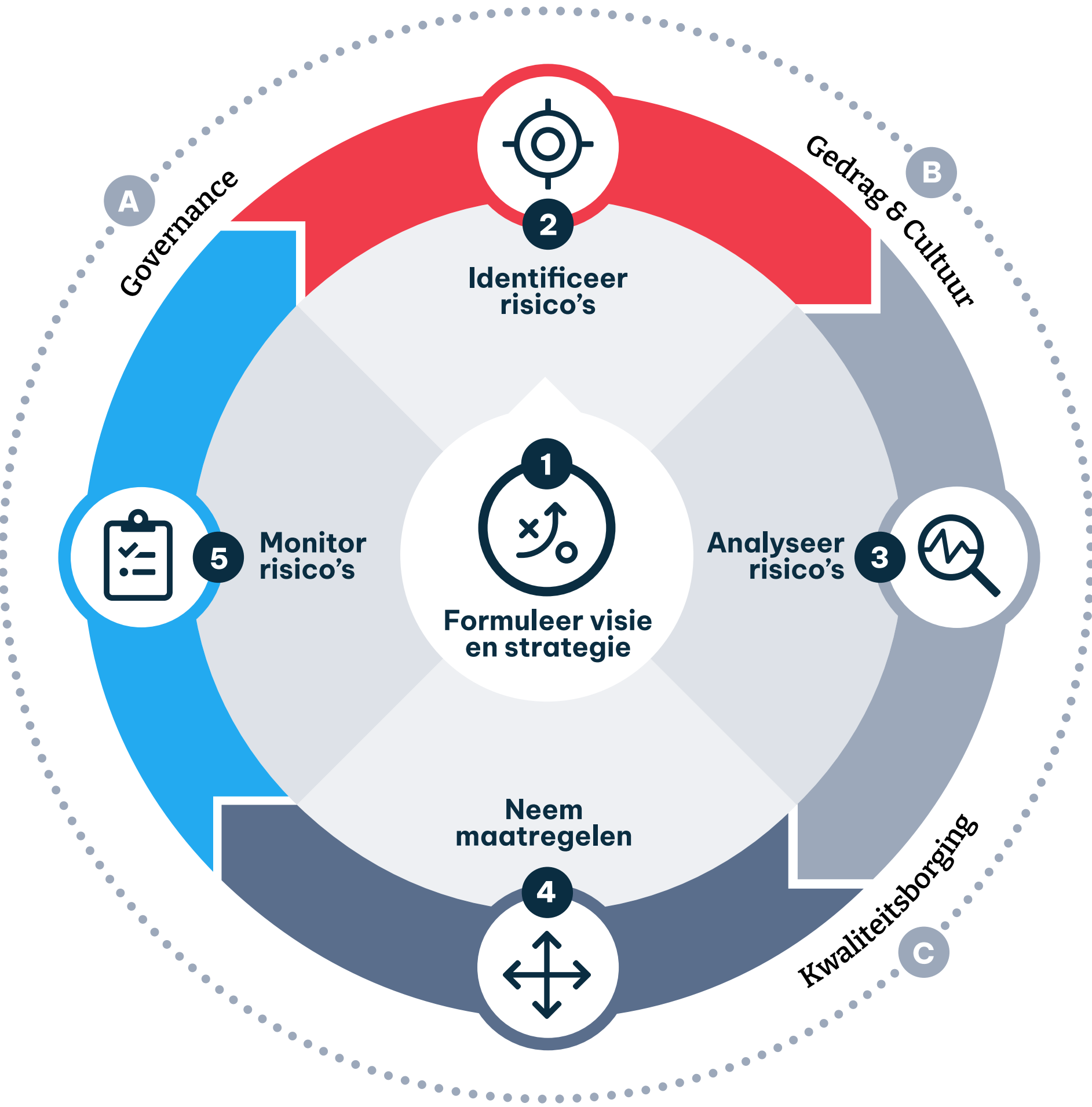
Om risico's effectief te beheren, verwacht het Commissariaat dat media-instellingen een goed georganiseerde **risicomanagementcyclus** hanteren. Deze cyclus is van vitaal belang voor het uitvoeren van doeltreffend risicomanagement. Door alle stappen van deze cyclus voortdurend te doorlopen, kunnen media-instellingen zichzelf continu verbeteren in het bewust omgaan met risico's.

De risicomanagementcyclus in de Zelfscan is gebaseerd op bestaande methoden en bestaat uit vijf processtappen, namelijk:

- 1 Formuleer een visie en strategie
- 2 Identificeer risico's
- 3 Analyseer risico's
- 4 Neem maatregelen
- 5 Monitor en rapporteer risico's

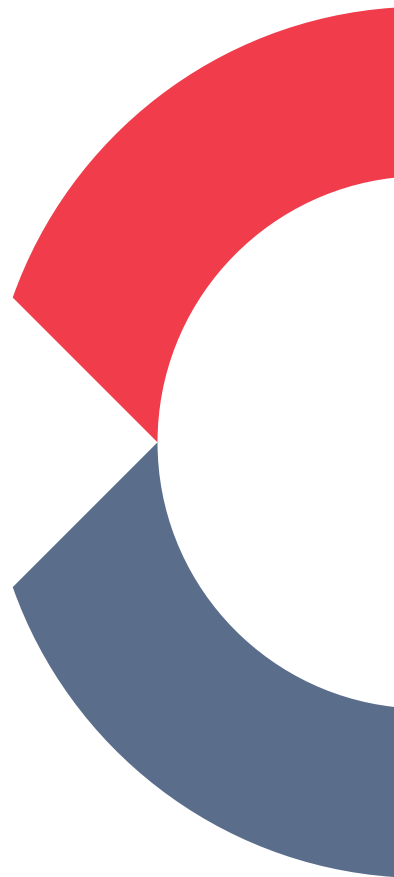
De genoemde stappen dienen te worden beoordeeld tegen de achtergrond van de volgende randvoorwaarden: **A** adequate **governance**, **B** een gebalanceerde **risicocultuur** en gedrag, en **C** professionele **kwaliteitsborging** die passend is voor de aard, omvang en relevantie van de risico's binnen de media-instelling.

Op de volgende pagina begint de Zelfscan, waar de processtappen en randvoorwaarden van de risicomanagementcyclus, inclusief bijbehorende vragen, verder worden toegelicht.



1 • Visie & Strategie

Het startpunt van de risicomanagementcyclus is een **risicostrategie** en **risicobeleid** die aansluiten op de missie, visie en strategie van de organisatie en de daaruit voortvloeiende doelstellingen en processen.



Ruimte voor aantekeningen

- 1

Heeft de organisatie een missie, visie en strategie uitgewerkt?
- 2

Heeft de organisatie strategische, operationele, financiële en compliance doelstellingen bepaald en vastgelegd die aansluiten bij de missie, visie en strategie?
- 3

Heeft de organisatie een uitgewerkte **risicostrategie** die aansluit op de strategische, operationele, financiële en compliance doelstellingen van de organisatie?
- 4

Is de visie en risicostrategie uitgewerkt in een risicobeleid?
- 5

Is het risicobeleid per **risicocategorie** beschreven?
- 6

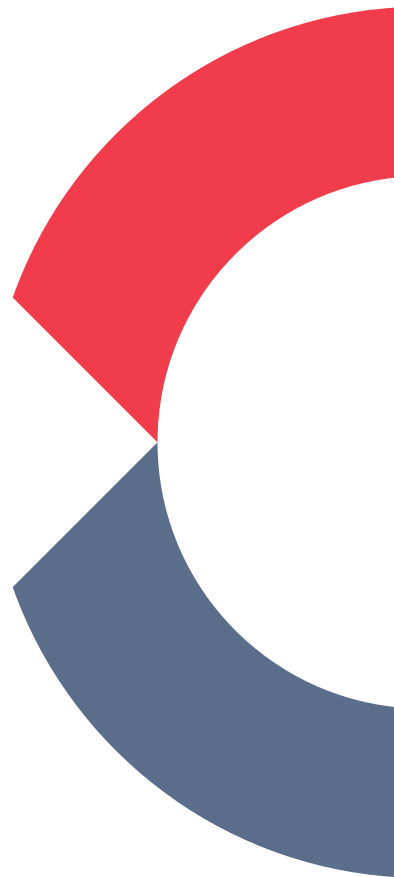
Is het **risicobeleid** vastgesteld door het Bestuur en formeel bekrachtigd door de Raad van Toezicht?
- 7

Heeft de organisatie een **risicobereidheid** gedefinieerd?
- 8

In hoeverre sluit deze **risicobereidheid** aan bij de strategische, operationele, financiële en compliance doelstellingen van de organisatie?

2 • Identificeer risico's

Een risico is een onzekere gebeurtenis die ertoe kan leiden dat een doelstelling niet wordt gerealiseerd. Voor het identificeren van risico's is het van belang te redeneren vanuit doelstellingen en de processen die hieraan ten grondslag liggen. Dit gebeurt idealiter vanuit meerdere invalshoeken, vanuit een vast format en met oog voor oorzaak en gevolg van het risico.



Ruimte voor aantekeningen

- 1

Worden voor alle afdelingen van de organisatie de relevante risico's geïdentificeerd?
- 2

Worden de risico's op gestructureerde (systematische) wijze geïdentificeerd?
- 3

Worden risico's aantoonbaar gekoppeld aan (afdelings)doelstellingen, processen, (IT) systemen en projecten?
- 4

In hoeverre vindt de identificatie van risico's plaats vanuit **risicocategorieën**?
- 5

Is er oog voor bestaande/bekende risico's én nieuwe risico's?
- 6

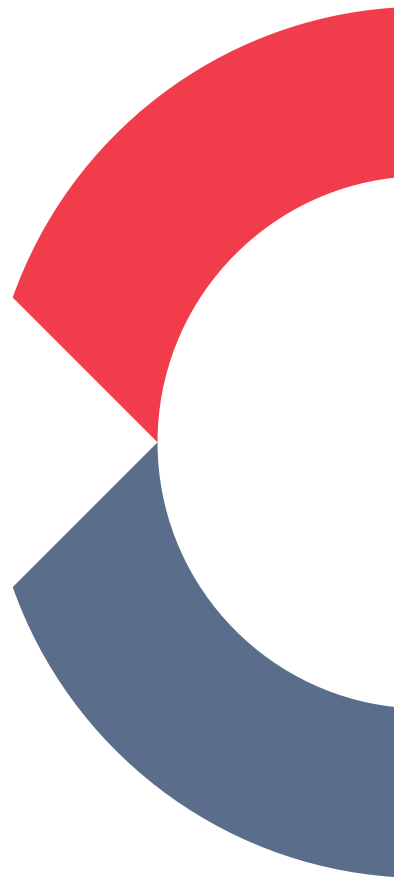
Is er een "signaalfunctie" ingericht? Hoe verloopt de identificatie van bestaande en toekomstige risico's en relevante trends/ontwikkelingen?
- 7

Worden (signalen op) mogelijke nieuwe relevante risico's centraal vastgelegd?
- 8

Heeft de organisatie een totaaloverzicht van alle relevante risico's?

3 • Analyseer risico's

Het analyseren van een risico betreft het bepalen van de omvang van het risico ten opzichte van de gekozen **risicobereidheid**. Alle in kaart gebrachte risico's worden geclassificeerd. Dit wil zeggen dat de kans van optreden wordt berekend of ingeschat, evenals de effecten op bijvoorbeeld tijd, geld, veiligheid, kwaliteit en reputatie van de betrokken partijen. Tevens wordt gekeken naar de **beheersmaatregelen** die voor het risico zijn genomen.

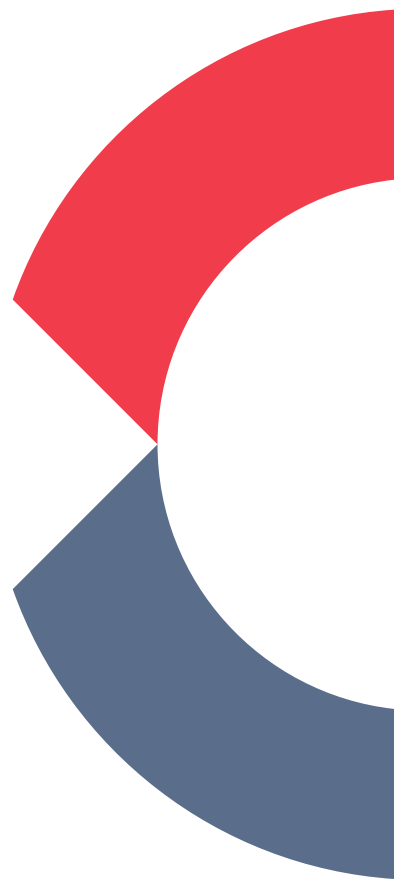


Ruimte voor aantekeningen

- | | |
|---|---|
| 1 | Is voldoende duidelijk wat mogelijke oorzaken en gevolgen zijn van de geïdentificeerde risico's? |
| 2 | Zijn alle risico's beschreven in een heldere oorzaak-gevolgrelatie ? |
| 3 | Worden alle geïdentificeerde risico's op basis van een op voorhand bepaalde methode geclassificeerd, bijvoorbeeld op kans van optreden en impact? |
| 4 | Is er inzicht in onderlinge verbanden en afhankelijkheden van de risico's? |
| 5 | Maakt de organisatie de koppeling tussen het risico en de risicobereidheid ? |
| 6 | Worden risicoanalyses en de uitkomsten hiervan vastgelegd? |

4 • Neem maatregelen

In deze stap maak je de reactie op het risico expliciet. Hierbij wordt een prioritering aangebracht. Op basis hiervan bepaal je welke maatregelen nodig zijn om de kans van optreden van een risico te verkleinen of weg te nemen, of om de gevolgen te beperken of te compenseren. Dit zijn de **beheersmaatregelen**.



Ruimte voor aantekeningen

- 1

Wordt voor alle relevante risico's bepaald of **beheersmaatregelen** mogelijk, passend én noodzakelijk zijn?
En worden de uitkomsten hiervan vastgelegd?
- 2

Zijn de gekozen **beheersmaatregelen** in lijn met de vastgestelde **risicobereidheid** (zie vraag 1.8)?
- 3

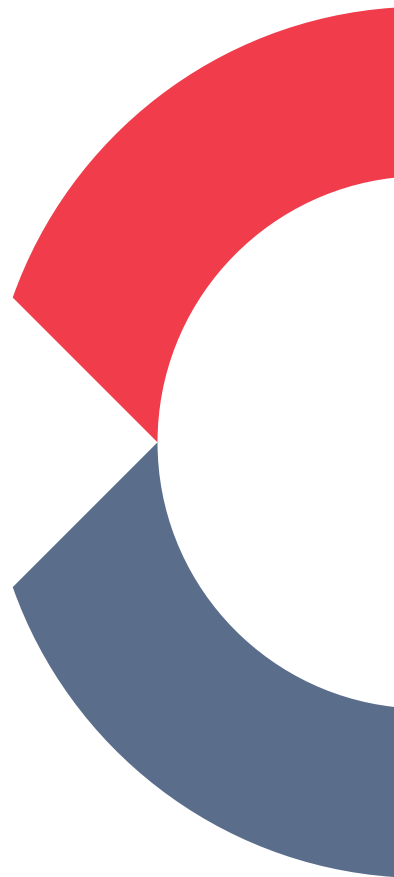
Zijn de **beheersmaatregelen** duidelijk omschreven (dat wil zeggen: wie is verantwoordelijk voor de uitvoering, hoe vaak en wanneer wordt deze maatregel toegepast, wat wordt er precies gedaan en wordt duidelijk welk risico hiermee wordt afgedekt)?
- 4

Worden risico's die resteren na het nemen van **beheersmaatregelen (restrisico's)** besproken door het Bestuur met de Raad van Toezicht en worden de uitkomsten hiervan vastgelegd?
- 5

Is er voldoende aandacht voor de beheersing van risico's in geval van uitbestede activiteiten?

5 • Monitoren en rapporteren

Bij deze stap kijk je hoe de risico's zich ontwikkelen en of de gekozen **beheersmaatregelen** voldoende werken. Dit doe je op vaste momenten en bij bijzondere aanleidingen. Hoe en hoe vaak je dit bekijkt, verschilt per risico. Na de monitoring van de opzet, bestaan en werking van de **beheersmaatregelen** wordt de bevindingen over de risico's (en eventuele incidenten) periodiek en consistent gerapporteerd.

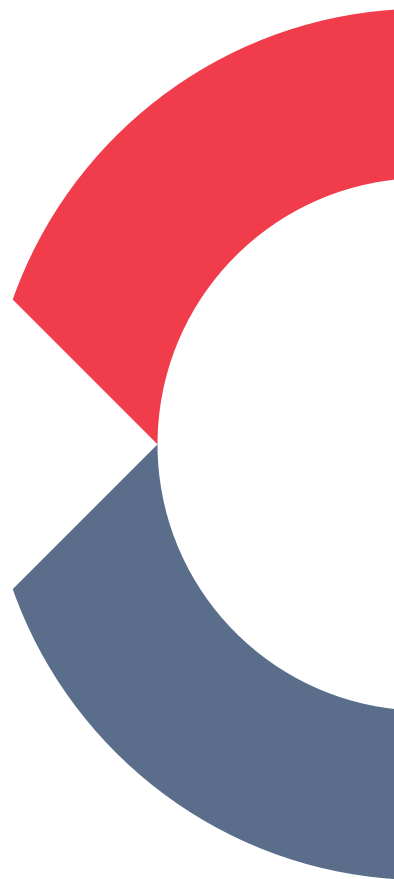


Ruimte voor aantekeningen

- | | |
|---|--|
| 1 | Wordt de werking van de beheersmaatregelen (aantoonbaar) vastgesteld? |
| 2 | Is er beschikking over tijdige, actuele, accurate en toegankelijke risicomanagementinformatie ? |
| 3 | Is de verantwoordelijkheid voor de monitoring en rapportage van de risico's duidelijk belegd? |
| 4 | Worden risicorapportages structureel gedeeld en besproken in bestuursvergaderingen en worden de uitkomsten hiervan vastgelegd? |
| 5 | Worden risicorapportages structureel gedeeld en besproken door het Bestuur met de Raad van Toezicht (en andere stakeholders) en worden de uitkomsten van deze gesprekken vastgelegd? |
| 6 | Het doel van monitoren is dat de maatregelen op tijd bijgesteld kunnen worden. In hoeverre leiden risicorapportages tot nieuw onderzoek en/of aanvullende (beheers)maatregelen ? |
| 7 | Wordt periodiek getoetst of de risicobeheersing in lijn is met de risicobereidheid ? |

A • Risico governance

Risico **governance** vormt de basis voor goed functionerend risicomanagement. Het omvat de wijze waarop een organisatie zijn risicomanagement heeft ingericht, zoals met beleid, processen, procedures, verantwoordelijkheden en onafhankelijke toetsing. Hoe zien de taken, rollen en bevoegdheden voor risicomanagement eruit? En hoe vindt er weloverwogen besluitvorming plaats?



Ruimte voor aantekeningen

- 1 Zijn risicomanagement en compliance een terugkerend agendapunt tijdens bestuurs- en managementvergaderingen?
- 2 Wordt ieder besluit vooraf getoetst aan de **risicobereidheid** en het **risicomanagementbeleid**?
- 3 Worden de gesignaleerde risico's grondig en aantoonbaar betrokken in de afwegingen bij de besluitvorming?
- 4 Wordt de **risicomanagement- en/of de compliancefunctie** (eventueel aangevuld met andere relevante expertises) betrokken bij besluitvorming? Indien afgeweken wordt van het advies van de risicomanagement- en/of compliancefunctie wordt dit dan gemotiveerd vastgelegd?

Bewaakt het Bestuur de onafhankelijkheid en deskundigheid van de risicomanagementfunctie?

- 1 Heeft de organisatie een deskundige risicomanagementfunctie toegewezen?
- 2 Zijn de taken, verantwoordelijkheden en bevoegdheden van de risicomanagementfunctie ingericht en schriftelijk vastgelegd?

Ruimte voor aantekeningen

- 3

Zijn er maatregelen getroffen om de onafhankelijkheid van de risicomanagementfunctie te garanderen?
(bijvoorbeeld: escalatiemogelijkheden, toegang tot informatie, voldoende middelen, etc.)
- 4

Is de rol van de risicomanagementfunctie voor de organisatie helder en eenduidig?
- 5

Is de risicomanagementfunctie betrokken in het bijstaan, ondersteunen en adviseren van het Bestuur en het management van de organisatie in het uitvoeren van hun risicomanagementverantwoordelijkheden?
- 6

Is de risicomanagementfunctie betrokken in het bevorderen en ontwikkelen van voldoende **risicobewustzijn** bij de medewerkers?
- 7

Heeft de risicomanagementfunctie een actieve en onafhankelijke inbreng bij het bespreken van de **risicorapportages**?

Bewaakt het Bestuur de onafhankelijkheid en deskundigheid van de compliancefunctie?

- 1

Heeft de organisatie een deskundige compliancefunctie toegewezen?
- 2

Zijn de taken, verantwoordelijkheden en bevoegdheden van de compliancefunctie ingericht en schriftelijk vastgelegd?
- 3

Zijn er maatregelen getroffen om de onafhankelijkheid van de compliancefunctie te garanderen?
(bijvoorbeeld: escalatiemogelijkheden, toegang tot informatie, voldoende middelen, etc.)
- 4

Is de rol van compliancefunctie voor de organisatie helder en eenduidig?
- 5

Is de compliancefunctie vanuit haar expertiserol betrokken bij het vaststellen, beoordelen, monitoren en rapporteren van alle relevante compliancerisico's?
- 6

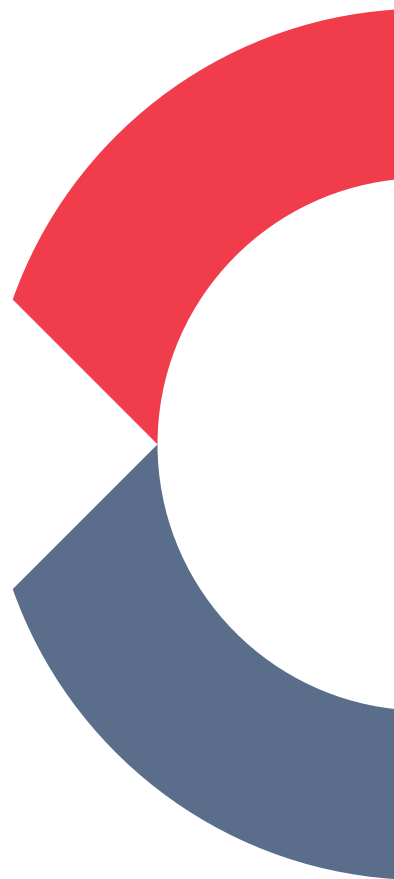
Is de compliancefunctie betrokken in het bijstaan, ondersteunen en adviseren van het Bestuur en het management van de organisatie in het uitvoeren van hun complianceverantwoordelijkheden?
- 7

Is de compliancefunctie betrokken in het bevorderen en ontwikkelen van voldoende compliancebewustzijn bij de medewerkers?
- 8

Heeft de compliancefunctie een actieve en onafhankelijke inbreng bij het bespreken van de **compliancerapportages**?

B • Gedrag & cultuur

De wijze waarop Bestuur, management en medewerkers binnen de organisatie omgaan met werk – gedrag, attitude, normen en waarden – en de mate waarin dit bijdraagt aan de effectiviteit van risicomanagement.



Ruimte voor aantekeningen

- 1

Hoe is de ‘toon aan de top/voorbeeldgedrag’ door het Bestuur als het gaat om risicomanagement en compliance?
- 2

Stimuleert het Bestuur dat medewerkers zich over risico’s durven uit te spreken?
- 3

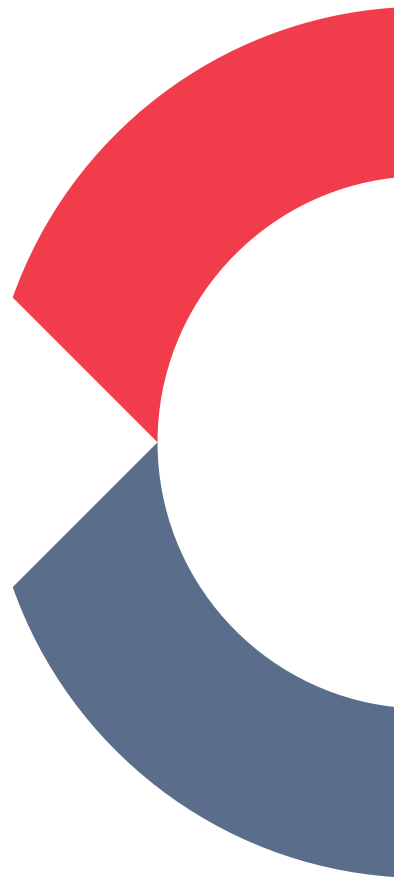
Zorgt het Bestuur ervoor dat risicomanagement en compliance organisatiebreed geïntegreerd wordt in de (dagelijkse) werkzaamheden?
- 4

Wordt het bewustzijn, begrip en eigenaarschap van risicomanagement en compliance bevorderd en actief ontwikkeld binnen de organisatie?
- 5

Wordt er adequate opvolging gegeven aan de gesignaleerde risico’s en/of problemen?

C • Kwaliteitsborging van het systeem

Kwaliteitsborging van risicomanagement richt zich op de kwaliteit en beschikbaarheid van mensen en middelen die worden ingezet voor de uitvoering van risicomanagement en de periodieke evaluatie van het risicomanagementsysteem. Per saldo gaat dit over het vermogen om (continu) te verbeteren in risicomanagement.



Ruimte voor aantekeningen

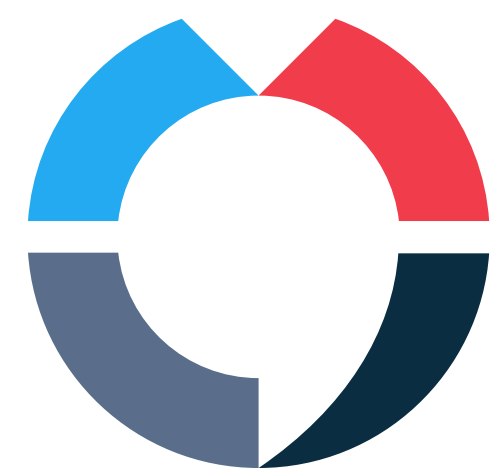
- 1 Is het **intern beheerssysteem** helder beschreven en duidelijk voor de betrokkenen?
- 2 Wordt de kwaliteit en de onafhankelijkheid van de **risicomanagement- en compliancefunctie** geëvalueerd?
- 3 Zorgt het Bestuur dat de organisatie haar kennis voldoende op peil houdt met betrekking tot risicomanagement en compliance?
- 4 Is voor de belangrijkste bestuurlijke, primaire en ondersteunende processen eigenaarschap bepaald?
- 5 Worden de risicomanagement- en compliance processen afdoende ondersteund door technologie (IT)?
- 6 Wordt het **intern beheerssysteem** periodiek (extern) onafhankelijk geëvalueerd en zo nodig herzien?
- 7 Leidt evaluatie tot aanpassing van het **interne beheerssysteem**?

Begrippenlijst

De belangrijkste begrippen uit de Zelfscan zijn hieronder in alfabetische volgorde weergegeven.

Beheersmaatregel	Een maatregel die is ontworpen om de kans op gebeurtenissen te verkleinen en/of de impact ervan te beperken.
Compliancerapportage	Periodieke rapportage over aan compliance gerelateerde risico's door de compliancefunctie aan het Bestuur en/of de Raad van Toezicht.
Governance (risk)	Het geheel van afspraken, rollen, taken, bevoegdheden en verantwoordelijkheden rondom de omgang met risico's.
Intern beheerssysteem	Het geheel aan beheersingsmaatregelen om te bewerkstelligen dat de gestelde organisatiedoelen gehaald worden.
Kwaliteitsborging	Het proces dat is ingericht om ervoor te zorgen dat het risicomanagementproces voldoet aan de gestelde kwaliteitseisen.
Oorzaak-gevolgrelatie	Het verband tussen de oorzaak van de onverwachte gebeurtenis, de gebeurtenis zelf, en het mogelijke (schadelijke) gevolg ervan.
Restrisico	Het resterende niveau van een risico dat blijft bestaan na het implementeren van risicobeperkende maatregelen. Het vertegenwoordigt het overgebleven risico dat niet volledig kan worden geëlimineerd of verminderd, en waarvoor de organisatie bereid moet zijn om het te accepteren en te beheren binnen aanvaardbare grenzen.
Risicoanalyse	Het analyseren van een risico door het uiteenrafelen van een onzekere gebeurtenis in oorzaken en gevolgen. Voor de oorzaken en gevolgen worden de onzekerheden in kaart gebracht. Voor het optreden van het risico worden kansen ingeschat.
Risicobeleid	Het formele kader en de richtlijnen die worden vastgesteld om de benadering van risicobeheer binnen de organisatie te sturen. Het omvat de doelstellingen, principes, verantwoordelijkheden en procedures die nodig zijn om risico's effectief te identificeren, beoordelen, beheren en monitoren in lijn met de strategische doelstellingen van de organisatie.
Risicobereidheid (ook wel risk appetite genoemd)	Verwijst naar de mate waarin de organisatie bereid is om risico's te nemen of blootgesteld te worden aan onzekerheid in het streven naar het behalen van doelstellingen.

Risicobewustzijn	Het hebben van voldoende besef van risico's die in een omgeving van de organisatie spelen. Het is hierbij belangrijk dat medewerkers, overal in de organisatie, zich realiseren dat risico's zich op verschillende plaatsen en manieren kunnen voordoen. Ook is het bij risicobewustzijn belangrijk dat er op een neutrale manier naar risico's kan worden gekeken en dat daarover op een open wijze een dialoog kan worden gevoerd.
Risicocategorieën	Geven een beeld van de risico's die een organisatie kan lopen. Risicocategorieën worden ook wel risicogebieden genoemd en hebben betrekking op die organisatieaspecten waarvan de organisatie denkt dat ze daar risico kan lopen. Risicocategorieën fungeren als het ware als een checklist zodat geen risico's vergeten worden. Het Commissariaat is in bijzonder gefocust op risicocategorieën die de wet beoogt te beschermen, zoals bijvoorbeeld: redactionele onafhankelijkheid, doelmatigheid en rechtmatigheid, integriteit of gedrag en cultuur.
Risicocultuur	De manier waarop risico's deel uitmaken van de organisatiecultuur en hoe de organisatie reageert op interne en externe uitdagingen. De risicocultuur betreft een (on)zichtbaar patroon van waarden, doeleinden, normen, verwachtingen e.d. die voor het functioneren van de risicobeheersing binnen de organisatie van belang zijn.
Risicomanagement- en compliancefunctie	Zijn personen die zijn belast met het identificeren, evalueren en beheersen van risico's om de strategische doelen van de organisatie te ondersteunen. Binnen deze functie kunnen personen specifiek belast zijn met het waarborgen van naleving van wet- en regelgeving, interne beleidslijnen en ethische normen om te voldoen aan wettelijke vereisten en het minimaliseren van juridische en reputatierisico's (het compliance risico). Dat noemen we de compliancefunctie.
Risicomanagementinformatie	Informatie en relevante indicatoren die ondersteunen bij het realiseren van doelstellingen op het gebied van risicomanagement.
Risicomanagementproces	Betreft het gehele proces om risico's systematisch te identificeren, te analyseren, een beheerstrategie te bepalen (vermijden, accepteren, mitigeren of overdragen) en vervolgens de risico's te monitoren en erover te rapporteren.
Risicoprofiel	Een overzichtelijke beschrijving en evaluatie van de risico's waaraan de organisatie wordt blootgesteld, inclusief de aard, omvang en mogelijke impact van deze risico's.
Risicorapportage	Periodieke rapportage over de risico's door de risicomanagementfunctie aan het Bestuur en/of de Raad van Toezicht.
Risicostrategie	De geplande aanpak en richting die de organisatie neemt om met de geïdentificeerde risico's om te gaan. Het omvat de keuzes en beslissingen met betrekking tot het accepteren, verminderen, overdragen of vermijden van risico's, evenals de implementatie van passende beheersmaatregelen om de doelstellingen van het bedrijf te beschermen.
Toon aan de top/voorbeeldgedrag	In het kader van risicocultuur een van de belangrijke factoren. Het Bestuur moet in woord en daad het belang van risicomanagement uitdragen. Vervolgens moet dit op alle niveaus geïntegreerd worden in de (dagelijkse) werkzaamheden.



Commissariaat
voor de Media

cvdm.nl

Colofon

Deze zelfscan is een uitgave van
het Commissariaat voor de Media
April 2024

Commissariaat voor de Media

Hoge Naarderweg 78, 1217 AH Hilversum
Postbus 1426, 1200 BK Hilversum
T 035 773 77 00

cvdm@cvdm.nl
www.cvdm.nl