# Integraal Risicomanagement in de Zorgsector

## Onze aanpak

Baarn 2019 - Marc Breij & Frank van Egeraat

**Disclaimer**
Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand en/of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier zonder voorafgaande schriftelijke toestemming van Accent Organisatie Advies.

Accent
Organisatie Advies

# Inhoudsopgave


**1 Inleiding** . . . 5

1.1 Risicomanagement: de theorie. . . . 5

1.2 Risicomanagement: onze werkwijze . . . 6

**2 Integraal risicomanagement** . . . 9

2.1 Strategisch risicomanagement . . . 10

2.1.1 Strategische risico's bepalen . . . 10

2.1.2 Risicobereidheid bepalen . . . 12

2.2 Tactisch risicomanagement . . . 13

2.2.1 Sturingskader voor risicobeheersing op tactisch niveau . . . 13

2.2.2 Tactische besluitvorming . . . 13

2.3 Operationeel risicomanagement . . . 14

2.3.1 Risico's identificeren . . . 14

2.3.2 Beheersmaatregelen treffen, key controls definiëren en periodiek toetsen . . . 15

2.3.3 Risico's bewaken en rapporteren . . . 16

2.3.4 Risicomanagement evalueren en herijken. . . . 18

**3 Risicocultuur** . . . 21

3.1 Risicocultuur en soft controls . . . 21

3.2 Risico en gedrag . . . 23

3.3 Risicocultuur in relatie tot besluitvorming . . . 24

**4 Governance** . . . 27

4.1 Governance vanuit RvT . . . 27

4.2 Governance vanuit bestuur . . . 28

**5 Organisatie inrichting** . . . 29

5.1 Three Lines of Defence . . . 29

5.2 Controlfunctie in de driehoek. . . . 30

5.3 Personele invulling. . . . 30

**Over Accent** . . . 32

# 1 Inleiding

Voor u ligt de brochure 'Integraal Risicomanagement in de Zorgsector'. Met deze publicatie geven wij u onze visie op de opzet, inhoud en werking van een integraal risicomanagement. Wij bieden u de laatste inzichten vanuit de theorie en onze praktijk. In deze brochure zetten we uiteen wat de stappen zijn die, afhankelijk van uw ambitieniveau, gezet moeten worden om integraal risicomanagement bij een zorginstelling in te voeren. We beschrijven ons risicomanagement model, de Risico8Baan, en geven daarbij de instrumenten die nodig zijn voor de invoering van de stappen. We kijken vervolgens naar de governance en inrichting van risicomanagement in de organisatie, waarbij we wat langer stilstaan bij de 'zachte kant' van het risicomanagement, de risicocultuur en soft controls. De risicocultuur is immers mede bepalend voor de wijze waarop en de mate waarin een organisatie risico's neemt.

## 1.1 Risicomanagement: de theorie

Voordat wij het begrip risicomanagement definiëren, is het goed om stil te staan bij het begrip risico. Intuïtief hebben we allemaal een beeld bij wat risico is. Bij het begrip "risico" komen termen als "onzekerheid", "negatieve ontwikkelingen" en "ongewenste uitkomsten" in ons op. Over het algemeen kunnen we legio voorbeelden geven van wat risico's zijn. Denk bijvoorbeeld aan patiëntveiligheid, zorgvastgoed risico's, onvoldoende beschikbaar gekwalificeerd personeel, onvoldoende schaalgrootte, fraude, fouten, of ongunstige ontwikkeling van de rente. Tegelijk weet ook iedereen dat het lopen van risico onlosmakelijk verbonden is met het ondernemen van activiteiten. Zonder het nemen van risico's zal een organisatie haar doelstellingen niet kunnen realiseren.

Een definitie van het begrip risico kunnen wij ontlenen aan een tweetal internationaal breed gedragen standaarden voor risicomanagement: de ISO 31000 standaard en het COSO Enterprise Risk Management Framework. In lijn met deze standaarden definiëren wij risico als:

> "Het effect van onzekere gebeurtenissen op het behalen van doelstellingen".

Zorginstellingen hebben te maken met een veelheid aan onzekere gebeurtenissen (zowel intern als extern van oorsprong - zie afbeelding hieronder) die van invloed zijn op het al dan niet realiseren van hun doelstellingen. Doelstellingen kunnen worden gekenmerkt door verschillende aspecten (met name toegankelijkheid, betaalbaarheid en kwaliteit van de zorg, maar ook financiële doelen) en kunnen betrekking hebben op verschillende niveaus (zoals strategisch, tactisch of operationeel).

| Externe ontwikkelingen | | | Interne organisatie | | |
|---|---|---|---|---|---|
| **Politiek / Sociaal-maatschappelijk** | **Economisch / Technologisch** | **Demografisch / Ecologisch** | **Strategische / Tactische sturing** | **Operationele processen** | **Organisatie / Compliance** |
| Wet- en regelgeving | Bekostiging zorgstelsel | Cliënten, patiënten verwanten en doelgroepen | Zorgportfolio | Zorgprocessen en systemen | Naleving wet- en regelgeving |
| Toezichthouders & zorgverzekeraars | Financiering en middelenbeheer | (Keten)partners en belanghebbenden | Planning & control cyclus | HRM / Medewerkers | Governance en organisatie-structuur |
| Samenleving (legitimatie en reputatie) | Technologische innovaties en digitalisering | Milieu en klimaat | Vastgoedbeheer | Zorgkwaliteit en veiligheid | Organisatiecultuur en integere bedrijfsvoering |

Een risico wordt vaak gekarakteriseerd door verwijzing naar de mogelijke gebeurtenissen, de oorzaken en gevolgen daarvan of een combinatie van deze drie. Een voorbeeld ter illustratie. Een zorginstelling loopt het risico dat als gevolg van besluiten in het politieke speelveld er een onverwachte wijziging komt in de bekostiging van de zorg waardoor de financiering en het bestaansrecht van de instelling wordt geraakt.

Alle activiteiten die een zorginstelling uitvoert hebben een bepaalde mate van risico in zich. Het beheersen van die risico's is wat risicomanagement behelst. Risicomanagement omschrijven wij, wederom in lijn met internationaal erkende kaders, als:

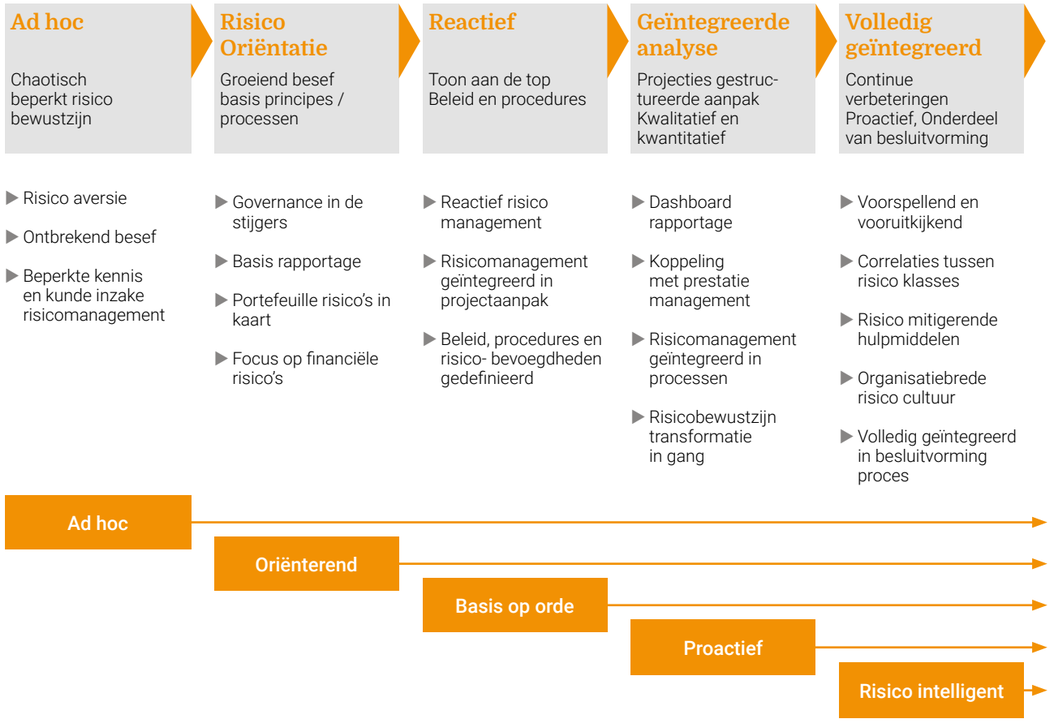
> "Een proces gericht op het identificeren en beoordelen van potentiële gebeurtenissen die invloed kunnen hebben op de zorginstelling, en deze risico's zodanig te beheersen dat deze binnen de risicobereidheid van de zorginstelling vallen, zodat een redelijke zekerheid bestaat ten aanzien van het behalen van de doelstellingen van de zorginstelling".

Er bestaat een grote hoeveelheid methoden, technieken en instrumenten om risicomanagement vorm te geven. Daar ontbreekt het niet aan. De kunst is de juiste selectie daaruit te maken en de toepassing ervan te borgen in de reguliere beleidscyclus, zodat risicomanagement daadwerkelijk effectief bijdraagt aan het realiseren van de doelstellingen zonder als een "overhead" ervaren te worden. In de volgende paragraaf beschrijven wij onze werkwijze om risicomanagement vorm te geven.

### 1.2 Risicomanagement: onze werkwijze

Allereerst zal moeten worden vastgesteld waar de zorginstelling op dit moment staat op het gebied van risicomanagement. Veelal wordt er al bewust en onbewust omgegaan met risico's al zijn dit vaak de risico's op het operationele vlak. Men zal dus moeten beginnen met het vaststellen welke activiteiten reeds worden ontplooid. Op basis van deze analyse kan worden vastgesteld waar de zorginstelling staat op de risicomanagement volwassenheidsladder (zie afbeelding volgende pagina). De volwassenheidsladder geeft aan wat de (toenemende) waarde is die risicomanagement toevoegt in relatie tot een steeds hoger volwassenheidsniveau.

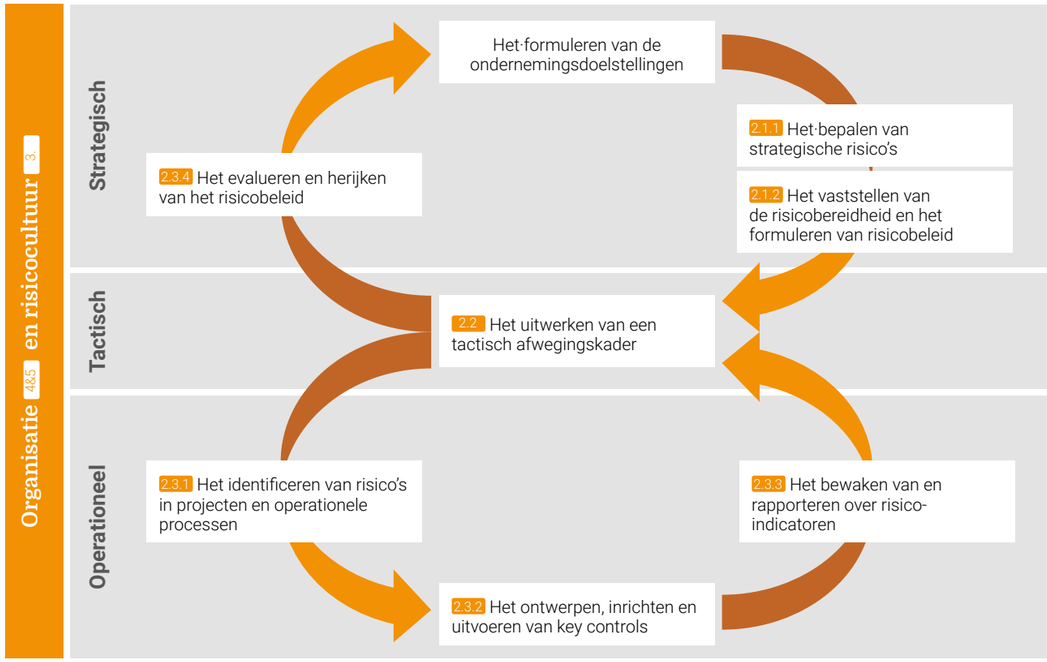
Daarnaast zal de zorginstelling moeten bepalen welk volwassenheidsniveau realiseerbaar is binnen de eigen organisatie. Hierbij moet naast het ambitieniveau gekeken worden naar de kosten van het realiseren van deze ambitie. Het mag duidelijk zijn dat risicomanagement bij een kleine lokale zorginstelling pragmatischer ingericht kan en mag worden dan bij een grote landelijk opererende zorginstelling.




De uitkomst van deze 'verschillen analyse' tussen het huidige niveau en het ambitieniveau van risicomanagement geeft aan welke onderdelen voldoende uitgewerkt zijn en welke onderdelen nog moeten worden opgepakt om de geformuleerde ambitie te realiseren. Deze uitkomsten zullen de basis vormen om te komen tot een 'roadmap' voor risicomanagement. In deze roadmap wordt aangegeven welke ontbrekende risicomanagement activiteiten dienen te worden opgepakt en/of verder geprofessionaliseerd om het gewenste ambitieniveau te realiseren. Zo is er altijd een compleet overzicht van de voortgang van de invoering van het integraal risicomanagement model.

# 2 Integraal risicomanagement

Er zijn vele methoden en instrumenten om risicomanagement concreet handen en voeten te geven. Bij de keuze van de juiste methode is het van groot belang om ervoor te zorgen dat deze aansluit op de dagelijkse bedrijfsvoering en niet, zoals vaak, los staat van reguliere strategische, tactische en operationele sturing, beheersing en verantwoording van de zorginstelling.
Het succes van integraal risicomanagement hangt in belangrijke mate af van de mate waarin risicomanagement echt onderdeel uitmaakt van de bedrijfsvoering en bedrijfscultuur. Door een model te hanteren dat nauw aansluit bij de beleidscyclus van de zorginstelling kan risicomanagement optimaal geïntegreerd worden in de reguliere sturing en beheersing.
Een model dat hierbij gehanteerd kan worden is de risicomanagement cyclus zoals beschreven in onderstaande figuur, de Risico8Baan. Onze werkwijze sluit aan bij de reguliere sturing van een zorginstelling en legt zo de verbinding tussen risicomanagement en bedrijfsvoering.

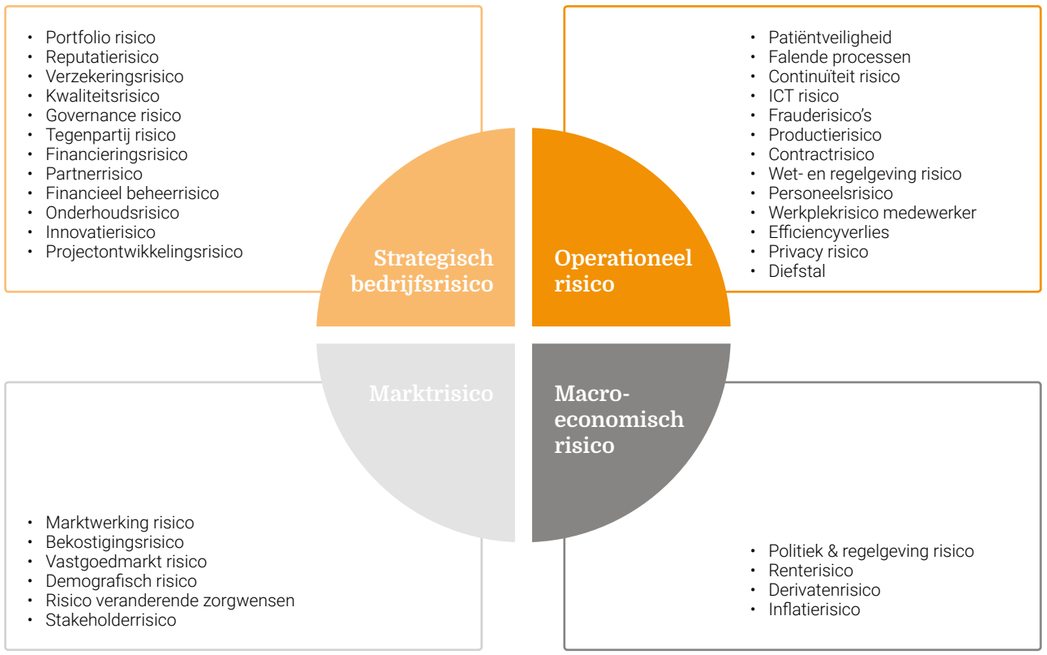



In de rest van dit hoofdstuk doorlopen we de achtbaan en beschrijven we hoe de risicomanagement cyclus in de organisatie kan worden ingevoerd en geïntegreerd in de beleidscyclus van de zorginstelling.

## 2.1 Strategisch risicomanagement

### 2.1.1 Strategische risico's bepalen

Het startpunt van zowel de strategische sturing als risicomanagement zijn de (maatschappelijke) doelstellingen van de zorginstelling, volgend uit het ondernemingsplan. Doelstellingen zijn richtinggevend voor goede en verantwoorde zorg. Verantwoorde zorg moet veilig, doeltreffend, doelmatig en cliëntgericht zijn. Goede zorg moet merkbaar zijn voor de cliënt en hun naasten. Het gaat om de betrokkenheid, de manier waarop professionals omgaan met de mensen die zich aan de zorg van de instelling toevertrouwen en hoe de instellingen zich plooien rondom wat cliënten wensen en nodig hebben. Integraal met dit proces kan de zorginstelling de strategische risico's rondom het behalen van de (maatschappelijke) doelstellingen in kaart brengen door middel van een 'strategische risicokaart'. Deze strategische risico's kunnen worden bepaald aan de hand van een generiek raamwerk van risico's en risicocategorieën waarmee zorginstellingen geconfronteerd kunnen worden.
Bij de discussies over de risico's werken wij in eerste aanleg met een generiek risicoraamwerk. Het door ons ontwikkelde raamwerk geeft inzicht in de meest voorkomende risico's in de zorgsector. Gedurende de discussies kan het raamwerk verder worden aangepast aan de specifieke situatie van de zorginstelling.



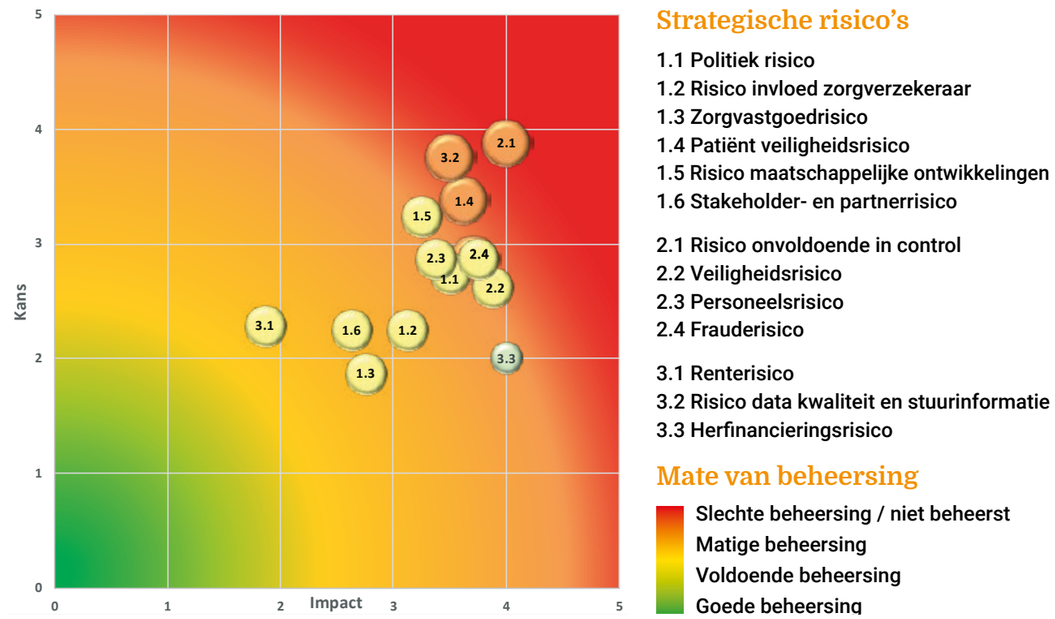

Op basis van het risicoraamwerk en met behulp van assessments en interviews wordt een strategische risicokaart uitgewerkt, waarin de kans en de mogelijke impact van alle geïdentificeerde risico's worden aangegeven (een groslijst van risico's). Om een goede focus te houden neemt de organisatie aan de hand van het risicoraamwerk de 10 tot 15 risico's die de meeste gevolgen voor de organisatie hebben, in een verdere analyse en werkt deze uit in een strategische risicokaart.

**Strategische Risicokaart**

Om te komen tot een voor een zorginstelling specifieke strategische risicokaart, worden in onze werkwijze de volgende stappen ondernomen:

1. Wat is de bruto kans en de bruto impact van het risico. Bruto betekent dat het risico wordt bepaald zonder dat rekening wordt gehouden met de beheersing. Dit bepaalt de positie in de kaart.
2. Wat zijn de door de zorginstelling genomen beheersmaatregelen (veelal ook afhankelijk van de mate van invloed die een zorginstelling heeft op het risico). Dit bepaalt de kleur in de kaart.
3. Op basis van de kans en impact en beheersing van een risico wordt het restrisico vastgesteld.

Onderstaand zie u een voorbeeld van een 'risicokaart', met een selectie van een top 10 strategische risico's.



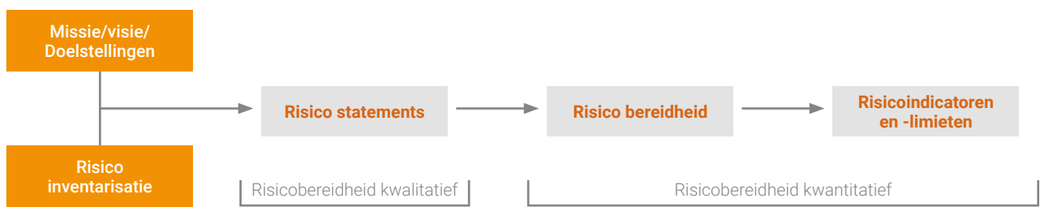

**Scenario-analyses**

Een deel van de top 10 strategische risico's laat zich vertalen in scenario's waarmee in de formulering van het zorgplan en de financiële meerjarenplanning rekening gehouden moet worden. Te denken valt aan het strategisch vastgoed beleid waarin keuzes te maken zijn of locaties in eigen bezit moeten blijven, verkocht of herontwikkeld kunnen worden of mogelijke sales & leaseback constructies etc. Denk bijvoorbeeld aan financiële risico's, zoals renterisico, herfinancieringsrisico en liquiditeitsrisico. Maar ook operationele risico's kunnen soms desastreus zijn voor het vertrouwen in de zorginstelling, zoals een aantal fraude incidenten in het verleden hebben aangetoond.
De scenario-analyses kunnen leiden tot een besluit om meer of andere maatregelen te nemen die de kans en/of impact van het risico beperken. De organisatie gebruikt deze scenario-analyse vervolgens voor de meerjarenbegroting en liquiditeitsplanning.

### 2.1.2 Risicobereidheid bepalen

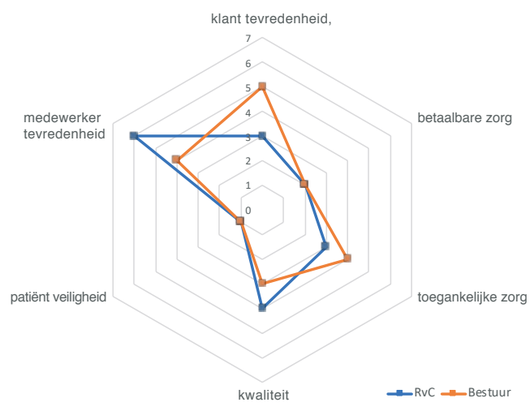
Een belangrijke volgende stap in het strategisch risicomanagement is het formuleren van de risicobereidheid van de zorginstelling in relatie tot de gesignaleerde strategische risico's. De risicobereidheid van een zorginstelling geeft uitdrukking aan de aard en omvang van de risico's die een zorginstelling bereid is aan te gaan bij het realiseren van haar doelstellingen. De risicobereidheid heeft vaak een kwalitatieve dimensie, waarmee de zorginstelling uitdrukking kan geven aan aspecten als haar grondhouding ten opzichte van het nemen van risico's. De risicobereidheid kan ook uitgedrukt worden in kwantitatieve dimensies, veelal in de vorm van (minimaal acceptabele) financiële ratio's zoals een minimaal noodzakelijk geachte rentedekkingsgraad, solvabiliteit, liquiditeit, of leencapaciteit.

Een belangrijke vraag bij het bepalen van de risicobereidheid is hoe dicht de zorginstelling "langs de rand" van de criteria van onder andere IGJ, Zorgautoriteit of Waarborgfonds voor de Zorg (WfZ) kan en wil opereren. Anders gezegd, wat is de minimale financiële flexibiliteit die de zorginstelling na wil streven? Dit vormt belangrijke input voor het bepalen van het meerjarenplan en de begroting. Als blijkt dat de beoogde plannen niet realiseerbaar zijn binnen de door de zorginstelling vastgestelde financiële kaders, dan kan stapsgewijs via verschillende scenario's een meerjarenplan uitgewerkt worden dat wel haalbaar is binnen de risicobereidheid van de zorginstelling. Het is belangrijk dat er consistentie is tussen de strategie, de doelstellingen, de risicobereidheid en de genomen maatregelen.




Om de risicobereidheid vast te kunnen stellen, zullen assessments en interviews worden georganiseerd, waarbij intensief gediscussieerd moet worden over de risico's die de organisatie bereid is te accepteren rondom haar verschillende doelstellingen. Hoe belangrijker de doelstelling of organisatorische randvoorwaarde, hoe lager de risicobereidheid. Voor de meest essentiële doelstellingen of randvoorwaarden geldt dat een zorginstelling het risico van het niet halen van die doelstelling c.q. het overschrijden van de randvoorwaarden zo veel mogelijk zal willen beperken, en dus een lage risicobereidheid hierop heeft.

Hiernaast geven we een voorbeeld wat de risicobereidheid van een zorginstelling is op de haar verschillende doelstellingen (en hoe bijvoorbeeld een RvT en Bestuur risicobereidheid verschillend interpreteren).




## 2.2 Tactisch risicomanagement

Risicomanagement vindt plaats op drie niveaus in de organisatie, te weten op strategisch, tactisch en operationeel niveau.

Risicomanagement op tactisch niveau gaat een stap verder dan strategisch risicomanagement en betreft de risicobeheersing op bedrijfsonderdeel- of afdelingsniveau. Daar waar de risico's op strategisch niveau gerelateerd zijn aan het ondernemingsplan, zijn de risico's op tactisch niveau veelal gerelateerd aan de plannen van de verschillende bedrijfsonderdelen. Deze risico's op tactisch niveau kunnen het behalen van de doelstellingen van de betreffende bedrijfsonderdeel of afdeling in gevaar brengen.

### 2.2.1 Sturingskader voor risicobeheersing op tactisch niveau

De vastgestelde risicobereidheid van de zorginstelling wordt ten behoeve van het risicomanagement in de organisatie op tactisch niveau omgezet in relevant beleid, statuten en afwegingskaders. Dit zijn bij voorkeur geen afzonderlijke beleidsdocumenten, statuten of afwegingskaders. De onderwerpen worden zo veel als mogelijk geïntegreerd in bestaand beleid. Te denken valt aan financiële sturingskaders, afwegingskaders voor investeringen en kwaliteitskaders. Daarnaast is er beleid gericht op de beheersing van specifieke risico's, zoals patientveiligheidsbeleid, een informatiebeveiligingsbeleid of een fraude- en integriteitsbeleid.

Verder is het aan te bevelen om een risicomanagement statuut op stellen, met daarin duidelijk vastgelegd wat de taken, bevoegdheden en verantwoordelijkheden van functionarissen binnen de organisatie ten aanzien van risicomanagement zijn. Op deze wijze wordt gezorgd dat eigenaarschap met betrekking tot risicomanagement voor een iedereen helder en duidelijk zijn verwoord.

### 2.2.2 Tactische besluitvorming

Bij de besluitvorming omtrent nieuwe investeringen of grote projecten is het belangrijk de juiste afweging te maken. Daarbij spelen verschillende factoren een rol. Bij deze factoren valt te denken aan de mate waarin de investering of het project bijdraagt aan de doelstelling van de organisatie, wat de financiële en niet-financiële rendementen zijn, de mogelijke risico's als gevolg van de

investering of het project en de vraag of aan andere randvoorwaarden wordt voldaan. Bij deze randvoorwaarden kunnen we denken aan afspraken met gemeenten, financiers, zorgverzekeraars of andere belangenhouders, de van toepassing zijnde wetgeving, normen van toezichthouders en mogelijke interne randvoorwaarden (zoals een treasury- of investeringsstatuut).

Meestal betrekt een zorginstelling de genoemde factoren impliciet wel bij de afweging van een voorstel, maar worden de afwegingen niet altijd expliciet vastgelegd. Daardoor is niet voor alle betrokkenen (zowel externe als interne stakeholders) duidelijk of en hoe deze factoren in de besluitvorming zijn meegenomen. Met een gestructureerde afweging van de voorstellen waarin zowel de rendementen als de risico's worden meegenomen, wordt het risico van onzorgvuldige, onvolledige en/of onduidelijke besluitvorming bij veranderingen gemitigeerd.

## 2.3 Operationeel risicomanagement

Risicomanagement op operationeel niveau is het dagelijkse risicobeheer in de primaire en ondersteunende processen of in projecten. Dit zijn met name operationele risico's (risico's als gevolg van het falen van mensen, systemen of processen zoals medicatie verstrekking, zorgverlening, patientadministratie), maar het kan bijvoorbeeld ook de dagelijkse monitoring van bezetting zijn.

### 2.3.1 Risico's identificeren

Het operationeel risicomanagement proces start met het identificeren van de risico's in de verschillende processen van de organisatie. Dit gebeurt onder andere door gebruik te maken van operationele indicatoren zoals bijvoorbeeld incidenten, klachten, maar ook verloop- en verzuimratio's. Deze helpen vaak om in een vroeg stadium risico's in beeld te krijgen. Het is belangrijk dat medewerkers in een vroeg stadium van het risicomanagement proces worden betrokken. Op deze manier wordt ook het risicobewustzijn van de medewerkers verhoogd.
Daarvoor kan de zorginstelling gebruik maken van verschillende methoden en technieken, zoals brainstormsessies, raadplegen van externe bronnen en overzichten, inzetten van kennis van externe experts, etc. Wij maken veelal gebruik van Risk & Control Self Assessment. Deze 'self assessments' vinden plaats in workshop vorm, waarbij wij vaak een methode om het operationele proces van begin tot einde in kaart te brengen hanteren, de zogenaamde waardestroomanalyse of "Makigami" methode. Daarbij worden de functies (rollen), activiteiten, informatiedragers, risico's, verspillingen en mogelijke beheersmaatregelen in één overzicht in kaart gebracht (zie onderstaande figuur).

### 2.3.2 Beheersmaatregelen treffen, key controls definiëren en periodiek toetsen

Op basis van een Risk & Control Self Assessment kan beoordeeld worden of het treffen van beheersmaatregelen noodzakelijk is. Een zorginstelling kan er bijvoorbeeld voor kiezen om de risico's die een lage kans hebben en weinig schade opleveren (voor nu) te laten en zich te focussen op risico's met een grote kans op veel schade. Het hebben van een vooraf gedefinieerde en helder uitgewerkte risicobereidheid is van groot belang voor het maken van de juiste keuzes.

Ten aanzien van de gesignaleerde en geselecteerde operationele risico's zal de zorginstelling moeten vaststellen welke actie gewenst is. In alle gevallen moeten de kosten van de maatregel(en) worden afgewogen tegen het potentiële risico (het verlies). De acties vallen in één van de vier generieke categorieën:

1. Vermijden: het volledig vermijden van het risico door de activiteit waarmee het risico verbonden is te beëindigen, bijvoorbeeld het stoppen van bepaalde activiteiten;
2. Reduceren: het beïnvloeden van de kans op optreden of de impact. Onder "reduceren" valt een veelheid aan risicobeheersingsmaatregelen zoals het inrichten van procedures en richtlijnen, het treffen van maatregelen op het gebied van informatiebeveiliging, het inrichten van adequate functiescheidingen in de organisatie, etc.
3. Delen: het beïnvloeden van het effect in het geval van optreden, bijvoorbeeld verzekeren.
4. Accepteren: het accepteren van het risico zonder verdere maatregelen te treffen.

Bij het opvoeren van beheersmaatregelen zal continue de afweging gemaakt moeten worden of de kosten van de maatregel opwegen tegen de risico's die gemitigeerd worden. Het heeft immers geen zin om meer kosten te maken voor het beheersen van een risico dan het potentiële verlies dat geleden kan worden. Daarnaast zal gewaakt moeten worden voor een overregulering voor de patiënten en mensen op de werkvloer. Meer is niet altijd beter. Men moet een goede balans zien te vinden tussen effectiviteit en efficiëntie. Het gevaar is dat een schijnwerkelijkheid wordt gecreëerd door veel beheersmaatregelen en controles op te voeren, die onvoldoende of zelfs in het geheel niet de onderliggende oorzaken van de risico's adresseren. Een goed werkende controle, die de onderliggende oorzaak van een risico niet aanpakt, heeft in feite geen enkele toegevoegde waarde. Een bowtie analyse maakt de relaties tussen een risicogebeurtenis, de onderliggende oorzaken en de potentiële gevolgen inzichtelijk:

Aan de hand van de keuzes die gemaakt zijn, worden de beheersmaatregelen inclusief de key controls ingevoerd in de processen. Dit hoeft geen activiteit op zich te zijn, maar kan heel goed geïntegreerd worden binnen bestaande activiteiten van zorginstellingen om te komen tot betere sturing en beheersing. De uitkomst van deze keuzes wordt vaak vastgelegd in een risk & control framework.

Het risk & control framework kan de zorginstelling laten zien dat het risicomanagement wel of niet goed op orde is. Wel dient dit framework periodiek te worden getoetst (in relatie tot het in-control statement) op bijvoorbeeld de onderstaande vragen:

- Doen we nog steeds met elkaar wat we afgesproken hebben?
- Zijn de controls die we uitvoeren nog wel de juiste?
- Voeren we überhaupt die controles nog wel uit en zo ja, doen we dat ook op de juiste manier en op het juiste moment?

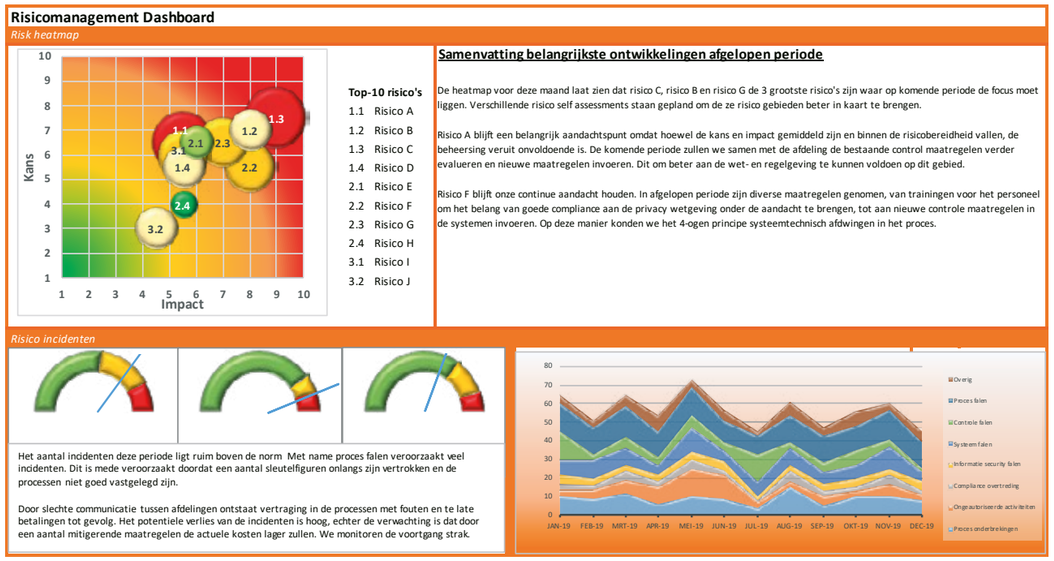
### 2.3.3 Risico's bewaken en rapporteren

Monitoring en beoordeling omvat het periodiek beoordelen van de risico's en de effectiviteit van risicobeheersing. De verantwoordelijkheid hiervoor ligt om te beginnen bij het lijnmanagement. Zij dienen zelf met enige regelmaat vast te stellen of risico's binnen het eigen verantwoordelijkheidsgebied adequaat beheerst worden. Sommige organisaties kiezen ervoor dit te formaliseren in de vorm van een zelfevaluatie (control self assessment) met bijbehorende "in control statement".

Een andere vorm van periodieke beoordeling is het uit (laten) voeren van audits. Bij zorginstellingen van enige omvang is vaak een eigen interne audit functie ingericht. Bij kleinere zorginstellingen wordt deze functie veelal extern belegd.

Voor een effectieve sturing is het hebben van kwalitatief goede informatie van belang. Dat geldt ook voor de beheersing van risico's. Risicomanagement is ook gebaat bij een systematiek van rapporteren op basis van een eenduidige set parameters en indicatoren. Hier is integratie met de reguliere beleidscyclus van een zorginstelling mogelijk. Zo kunnen in sommige gevallen indicatoren met betrekking tot bijvoorbeeld de bezetting ook indicaties van (verhoogd) risico geven. Een samenhangende rapportage, bijvoorbeeld in de vorm van een dashboard, kan dan behulpzaam zijn. Door te werken met een eenduidige systematiek voor de rapportage, is het mogelijk om de informatie geschikt te maken op zowel operationeel, tactisch als strategisch niveau. Daarnaast is het mogelijk om de data uit de organisatie om te zetten in relevante stuurinformatie in de verschillende geledingen van de zorginstelling. Hiernaast een voorbeeld van een 'risico dashboard' waar wij mee werken.

Een risico dashboard is een effectieve en efficiënte manier om een risicorapportage in te richten. In een dergelijke rapportage wordt de informatie over risico's op een overzichtelijke en gestructureerde wijze gepresenteerd. De lezer kan de informatie in één oogopslag tot zich nemen. Door middel van kleuren en iconen wordt de aandacht van de lezer gericht op die onderdelen van het rapport die zijn aandacht vragen.




Vaak wordt in deze rapportages gebruik gemaakt van Key Risk Indicators (KRIs). Een KRI is een kwantitatieve maatstaf (bijvoorbeeld een absoluut getal of een ratio) dat de mate van risico weergeeft. Het is een indicator van de kans van optreden van een risico, de mogelijke schade bij optreden, of beide. Een KRI is vergelijkbaar met een Key Performance Indicator (KPI) met dien verstande dat een KPI iets zegt over de mate waarin prestaties gerealiseerd worden terwijl een KRI iets zegt over de mate waarin toekomstige risico's zich kunnen materialiseren.

### 2.3.4 Risicomanagement evalueren en herijken.

Voor het evalueren van het risicomanagement kan de zorginstelling vaak steunen op reeds aanwezige informatiebronnen. Ook hier geldt dat integratie met de reguliere beleidscyclus gewenst en mogelijk is. Naast de reguliere interne rapportages valt daarbij te denken aan de management letter van de accountant, het visitatierapport of de oordeelsbrieven van sectorinstituten als NZa, WfZ of de IGJ. Maar soms is een specifieke beoordeling nodig, zoals een diepgaande audit op de beheersing van de IT omgeving, een analyse van de gevolgen van eventuele "stress situaties" (bijvoorbeeld een verandering in de financieringstromen) of een beoordeling van eventuele frauderisico's. Op basis van deze bronnen kan de zorginstelling het risicomanagement periodiek evalueren en herijken waar nodig, waarmee de cyclus rond is.
Met behulp van een risico gestuurde auditagenda wordt jaarlijks vastgesteld welke specifieke onderwerpen extra aandacht behoeven. Op deze manier wordt geborgd dat de betreffende onderwerpen ook daadwerkelijk aan bod komen, maar ook dat niet ieder jaar dezelfde audits worden uitgevoerd. Gegeven de steeds veranderende omgeving, zal regelmatig moeten worden vastgesteld welke onderwerpen extra aandacht behoeven.

# 3 Risicocultuur & soft controls

Voor iedere organisatie is het beheersen van risico's essentieel om te waarborgen dat de doelstellingen van de organisatie gerealiseerd worden. Steeds meer groeit het besef bij bestuurders en toezichthouders dat een eenzijdige focus op risicobeheersings- en controlesystemen – de harde kant van risicomanagement – niet voldoende is. Het succes van risicomanagement staat of valt met de houding en het gedrag in de organisatie ten aanzien van risico's: de risicocultuur.
Organisaties voelen steeds meer de behoefte om een gezonde risicocultuur na te streven omdat dit bijdraagt aan een hogere klantwaarde, het voorkomen van incidenten en betere en meer voorspelbare financiële prestaties. Daarnaast ondersteunt een gezonde risicocultuur de mogelijkheid om organisaties platter te maken en verantwoordelijkheden laag in de organisatie te beleggen. Organisaties worden daardoor wendbaarder en kunnen beter het hoofd bieden aan de toenemende mate van verandering, onzekerheid en complexiteit in de wereld van vandaag. Bovendien moeten organisaties beantwoorden aan de groeiende druk van buiten om meer transparantie en zichtbare aandacht te geven aan zogenaamde 'soft controls'.
Ondanks het groeiende besef dat de risicocultuur in de organisatie van belang is, komen veel organisaties vaak niet verder dan een oppervlakkige discussie over het belang van risicocultuur. Het is een moeilijk tastbaar begrip waar geen universeel geaccepteerde aanpak voor bestaat om het begrip te kaderen, te meten en te bewaken. Het onderwerp leent zich niet gemakkelijk om KPIs op te formuleren en een PDCA cyclus op toe te passen.
Veel organisaties zijn dus op zoek naar manieren om de risicocultuur inzichtelijk te maken en daarop te sturen. In dit hoofdstuk beschrijven wij onze visie en werkwijze om 'grip' te krijgen op risicocultuur (3.1), waarbij we onder 'risico en gedrag' (3.2) wat langer stilstaan bij de menselijke drijfveren van het management en personeel in de zorginstelling, omdat deze voor een belangrijk deel bepalend zijn voor het gedrag ten aanzien van risico's.

## 3.1 Risicocultuur en soft controls

Onder risicocultuur verstaan wij: "de normen, de houding en het gedrag van individuen en groepen in de organisatie die bepalen hoe zij omgaan met het identificeren, begrijpen, bespreken, en acteren op de risico's waarmee de organisatie geconfronteerd wordt c.q. die de organisatie neemt".
Risicocultuur kent vele facetten, is een mix van formele en informele processen, en ontwikkelt zich continu. Wij werken met een risicocultuur model dat de dimensies en aspecten van risicocultuur weergeeft en logisch bij elkaar brengt. De dimensies in het model zijn:

1. Leiderschap: gewenste risicohouding en -gedrag in de organisatie (normen en waarden) en de mate waarin de leiding hierin het juiste voorbeeldgedrag vertoont.
2. Beleidskaders: het gehanteerde risicobeleid (inclusief risicobereidheid), procedures en systemen, en de mate waarin deze begrijpelijk en uitvoerbaar zijn en nageleefd worden.
3. Medewerkers: de wijze waarop prestaties van medewerkers beoordeeld en beloond worden en medewerkers ondersteund worden in hun ontwikkeling en de invloed daarvan op de risicohouding en het gedrag van medewerkers.

4. Inzicht & besluitvorming: de risicorapportage- en besluitvormingsprocessen in de organisatie, en de mate waarin kritische bevraging en tegenspraak georganiseerd en gewaardeerd wordt.
5. Organisatie: de wijze waarop verantwoordelijkheden in de organisatie belegd zijn en gehandhaafd worden en de volwassenheid van de risicocompetenties in de organisatie.

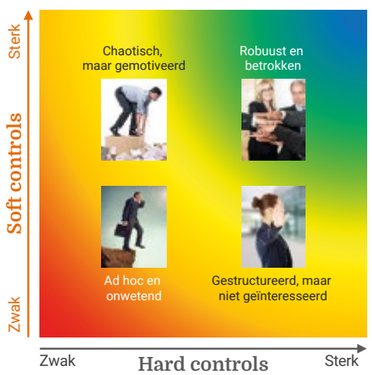
**Risicocultuurkaart**

Aan de hand van de dimensies van het risicocultuur model worden de 'hard controls' (structuur) en de 'soft controls' ('gedrag') benoemd en beoordeeld. De optelsom van de 'hard & soft controls' en de wijze waarop deze worden beleefd is bepalend voor de risicocultuur.
De 'hard controls zijn maatregelen die een organisatie treft om het gewenste gedrag direct of indirect 'af te dwingen' en ongewenst gedrag te beperken of te voorkomen, bijvoorbeeld procedures, codes, beleid, KPIs, governance, en besluitvorming.

De soft controls zijn maatregelen die de motivatie, loyaliteit, integriteit, inspiratie en normen en waarden van medewerkers beïnvloeden, zoals helderheid, voorbeeldgedrag, verbondenheid, uitvoerbaarheid, transparantie, bespreekbaarheid en aanspreekbaarheid, naleving en handhaving.
Op basis van een inschatting van de zorginstelling zelf worden de dimensies van de risicocultuur beoordeeld langs de assen van de hard & soft controls, met andere woorden, in hoeverre zijn de hard controls en soft controls in voldoende mate ontwikkeld en geborgd in de organisatie. Dit leidt uiteindelijk tot een risicocultuurkaart zoals hiernaast afgebeeld.

**Risicocultuurprofiel**

Op basis van de Risicocultuurkaart wordt uiteindelijk het huidige en het geambieerde risicocultuurprofiel gedefinieerd.




Onze aanpak is gebaseerd op research van internationale standaarden en best practices op het gebied van risicomanagement en cultuur en omvat een gestructureerde methode om de risicocultuur van de organisatie in beeld te brengen, te beoordelen en interventies te plegen om de risicocultuur op het geambieerde niveau te krijgen.
In onze aanpak hanteren wij verschillende methoden en technieken om het beeld op deze onderwerpen op te halen en bespreekbaar te maken, zoals enquêtes, focus interviews en gefaciliteerde workshops. Uiteindelijk resulteert de aanpak in een duidelijk beeld van de huidige risicocultuur en de gebieden waarin verbetering noodzakelijk is.

## 3.2 Risico en gedrag

De risicocultuur binnen een organisatie en het gedrag van mensen wordt voor een belangrijk deel bepaald door de menselijke drijfveren van het management en medewerkers. Diverse onderzoekers hebben modellen ontwikkeld waarin de drijfveren van mensen worden beschreven en gecategoriseerd. Een van deze onderzoekers is de psycholoog Clare Graves. De resultaten van zijn onderzoek bieden inzicht in de innerlijke 'filters' waarmee we het leven interpreteren en begrijpen. Zijn onderzoek is door verschillende organisaties verder vertaald in modellen om inzicht te geven in de drijfveren van personen of de dynamiek in groepen of organisaties.
Graves onderscheidde 8 drijfveren, waarvan 6 veel worden gebruikt in de 'drijfveermodellen'. De drijfveren van een persoon zijn van invloed op de "risico-acceptatie" van die persoon. Onder "risico-acceptatie" verstaan we de mate waarin iemand risico's durft te nemen. In grote lijnen kunnen we verschillende niveaus van "risico-acceptatie" verbinden aan de kleuren uit het drijfverenmodel. Dit hebben wij in onderstaande figuur samengevat.

| Kleur | Belangrijkste drijfveren | Risico-acceptatie |
|---|---|---|
| Geel | Analyseren, begrijpen, doorgronden | Gemiddelde risico-acceptatie voor de organisatie - nieuwe ontwikkelingen en verbeteringen kunnen niet worden gerealiseerd zonder risico's te nemen. Deze risico's moeten echter goed geanalyseerd en volstrekt begrepen worden. |
| Groen | Mensen en sociale verbanden voorop stellen | Relatief lage risico-acceptatie voor de organisatie – grote risico's kunnen de zwakkeren het hardst raken en kan de harmonie binnen de groep beschadigen. |
| Oranje | Resultaten en prestaties willen laten zien | Hoge risico-acceptatie voor de organisatie - wij willen doelen realiseren en daarbij moeten we risico's nemen. Als het fout gaat, neem ik op tijd maatregelen om alsnog mijn doelen te realiseren. |
| Blauw | Zekerheid en duidelijkheid creëren | Relatief lage risico-acceptatie voor de organisatie - te grote risico's kunnen de organisatie en de structuur in gevaar brengen en de uitkomsten kunnen onzeker zijn. |
| Rood | Durf, tempo en kracht | Hoogste risico-acceptatie voor de organisatie – lef vereist het nemen van risico's. |
| Paars | Veiligheid en thuisgevoel zoeken | Laagste risico-acceptatie voor de organisatie – risico's brengen de veiligheid en de traditie in gevaar. |

Met deze typering van drijfveren en de daaraan gerelateerde risico-acceptatie is het interessant om te kijken naar organisaties en de risico's die door en in deze organisaties worden genomen. Als we bijvoorbeeld kijken naar de zorgsector, dan waren de traditionele drijfveren bij zorginstellingen Groen (maatschappelijk belang), Blauw (regelgeving) en Paars (hechte bedrijfscultuur en tradities) ruim vertegenwoordigd bij de mensen binnen deze sector. Na de introductie van marktwerking in de zorg (minder directe invloed van de overheid), kwam ook een verschuiving van de drijfveren bij de bestuurders. De invloed van Geel, Rood en Oranje werd groter. Dit heeft gevolgen voor de risicobereidheid van de organisatie. Met name door de rode en oranje drijfveer kan deze risicobereidheid groter worden. Dat hoeft geen probleem te zijn mits deze risicobereidheid past bij de

doelstellingen van de organisatie. Zijn de doelstellingen zeer ambitieus, dan vereist dat het beheerst nemen van risico's en dus ook een hogere mate van risicobereidheid bij de bestuurders. Zijn de doelstellingen niet ambitieus, dan is het niet verstandig om een bestuurder aan het roer te zetten die een (zeer) grote risicobereidheid heeft.

### 3.3 Risicocultuur in relatie tot besluitvorming

De risicocultuur en het gedrag van mensen speelt ook een zeer belangrijke rol bij het nemen van besluiten binnen de organisatie. Het is belangrijk om te realiseren dat bij de presentatie en bespreking van bijvoorbeeld investeringsvoorstellen ook psychologische aspecten een belangrijke rol kunnen spelen, zoals framing en groepsdenken. Om het belang van deze psychologische aspecten en de risico's daarvan te benadrukken geven we in deze paragraaf een paar voorbeelden.

**Framing**
Framing is een techniek die (bewust of onbewust) wordt gebruikt bij het brengen van een boodschap en het overtuigen van mensen. Framing-effecten treden op indien gelijke voorstellen of situaties op verschillende wijzen worden beschreven en daarmee anders worden beoordeeld. De wijze en volgorde waarop informatie wordt gepresenteerd beïnvloedt de beoordeling. Een voorstel dat er mooi en degelijk uitziet, zonder taalfouten en met mooie grafieken, kan hierdoor meer kans maken dan een voorstel dat wellicht inhoudelijk beter is, maar er qua presentatie veel minder goed uitziet. Voorbeelden van 'framing' zijn:

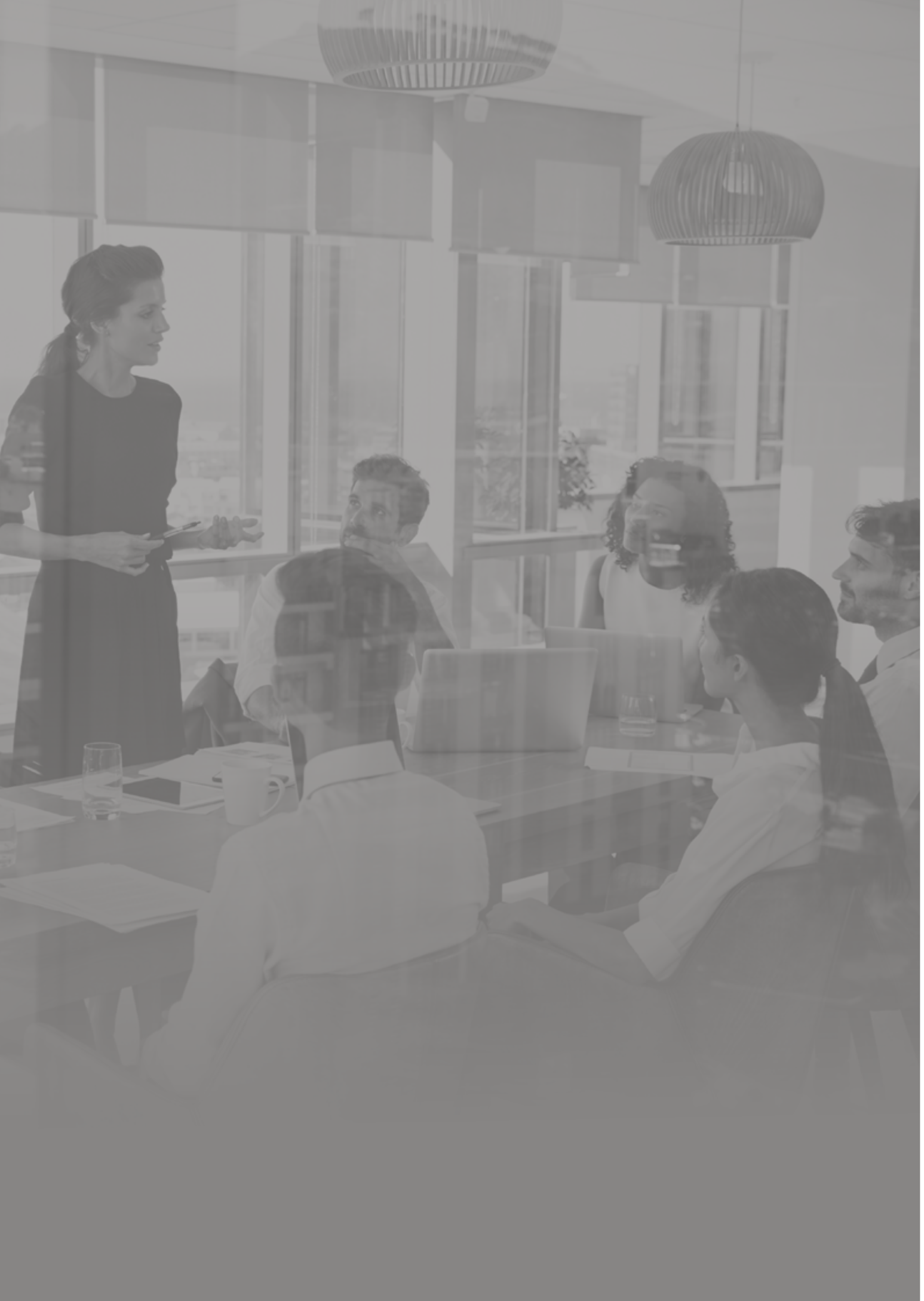
- Formuleren in termen van positieve kansen lijkt gunstiger dan een formulering in termen van mogelijke verliezen ('de kans op succes bij deze business case is 90%, de kans op falen bij de andere business case is 10%').
- Het gebruik van bepaalde termen (bijvoorbeeld 'uitdagingen' in plaats van 'risico's').
- De presentatie van informatie in een bepaalde volgorde (de risicoparagraaf komt altijd pas aan het einde van het investeringsvoorstel).
- Uitspraken van het bestuur, zoals: 'We moeten wel snel beslissen', 'Als we dit niet doen dan kunnen we verder wel ophouden', 'Als wij het niet doen staan er anderen klaar om het wel te doen' en 'Dit zouden we toch echt wel moeten willen doen'.

**Groepsdenken**
Groepsdenken is een denkwijze die plaatsvindt bij mensen die nauw met elkaar samenwerken. Zij hechten zoveel waarde aan een unanieme mening, dat deze unanimiteit belangrijker wordt geacht dan een kritische rationele instelling. De groepsleden leggen meer nadruk op het 'wij-gevoel' en zullen daardoor minder gemakkelijk kritiek uiten of informatie die de groepsvisie tegenspreekt, van zowel binnen als van buiten de groep, toelaten. Een belangrijk aspect in het groepsdenken is de 'risky shift'. Een 'risky shift' is het gegeven dat een groep meer risico neemt dan de gemiddelde risicobereidheid van de groepsleden zou toestaan. Als het fout gaat sta ik niet alleen want dan hebben we het samen fout gedaan.

**Heuristiek**
Heuristieken zijn efficiënte vereenvoudigingsmechanismen met een sterk selectief karakter. Ze zijn zeer bruikbaar bij het nemen van complexe beslissingen maar zij kunnen leiden tot fouten. Deze fouten ontstaan door 'cognitieve biases' in het gebruik van de heuristieken en kunnen soms grote gevolgen hebben. Een cognitieve bias, een denkfout, is een irrationele gedachtegang. Door deze denkfout kunnen conclusies over mensen, situaties of voorstellen op een onlogische manier worden getrokken als gevolg van (i) een te pessimistische of te optimistische beoordeling (ii) het niet onderkennen of niet in overweging nemen van andere alternatieven en (iii) een foutieve inschatting van waarschijnlijkheden (kansen) en/of mogelijke uitkomsten (impact)

Er zijn veel vormen van biases, maar de drie meest voorkomende voorbeelden van biases zijn:

1. De overconfidence bias. De 'overconfidence bias', ook wel overmoedigheid genoemd, heeft betrekking op de neiging van mensen om een hoger (subjectief) vertrouwen toe te kennen aan de eigen prestaties en oordeelsvorming dan de (objectieve) feitelijke prestaties en oordeelvorming
2. Confirmation bias. De 'confirmation bias', in het Nederlands voorkeur voor bevestiging genoemd, verwijst naar de neiging van mensen om meer aandacht en waarde te hechten aan informatie die de eigen ideeën of hypotheses bevestigt. Tegelijkertijd is er de neiging om minder aandacht te besteden aan informatie die de eigen ideeën tegenspreekt. De bias houdt verder in dat mensen niet alleen zoeken naar informatie die hun ideeën bevestigt, maar nieuwe informatie ook interpreteren op een manier die in lijn is met de eigen ideeën.
3. Sunk cost fallacy. De 'sunk cost fallacy' heeft betrekking op kosten die al gemaakt zijn en niet meer ongedaan te maken zijn. Toch spelen 'sunk costs' soms een rol bij investeringsbeslissingen, terwijl dit niet rationeel is.





# 4 Governance

'Good governance' gaat over besturen en beheersen, over verantwoordelijkheid en zeggenschap en over toezicht en verantwoording. Goede governance is een van de belangrijkste voorwaarden voor de continuïteit van zorginstellingen. Governance gaat onder meer over de verhouding tussen het bestuur en de Raad van Toezicht (RvT) van een zorginstelling. Op 1 januari 2017 is de nieuwe governancecode Zorg van kracht geworden. Deze governancecode biedt de sector een instrument om de governance zo in te richten dat die bijdraagt aan het waarborgen van de goede zorg, aan het realiseren van haar maatschappelijke doelstelling en daarmee aan het maatschappelijk vertrouwen. De code is gebaseerd op een zevental principes, te weten: Goede zorg, Waarden en normen, Invloed belanghebbenden, Inrichting governance, Goed bestuur, Verantwoord toezicht en Continue ontwikkeling.

In het kader van integraal risicomanagement zijn met name de principes Waarden en Normen (over risicocultuur en soft controls – zie hoofdstuk 3), Inrichting governance en Goed bestuur (zie onderstaande paragrafen) van belang. In Goed bestuur wordt in artikel 5.4 expliciet het belang van risicobeheersing benoemd:

> 5.4.1. De raad van bestuur is verantwoordelijk voor het beheersen van de risico's verbonden aan de strategie en de verschillende activiteiten van de zorgorganisatie, het handelen van medewerkers en de maatschappelijke positionering van de zorgorganisatie. De raad van bestuur draagt zorg voor goede en hanteerbare interne risicobeheersings- en controlesystemen, de bemensing daarvan en de werking van die systemen.

> 5.4.2. De raad van bestuur bespreekt en verantwoordt regelmatig de risicoanalyses en de werking van de risicobeheersingssystemen met de raad van toezicht, dit mede in het licht van de strategie en de effecten van die beheersing op de regeldichtheid in de organisatie.

## 4.1 Governance vanuit RvT

De RvT houdt toezicht op het beleid van het bestuur en de algemene gang van zaken in de organisatie. De Raad richt zich daarbij tevens op de effectiviteit van de interne risicobeheersings- en controlesystemen van de organisatie, de integriteit en kwaliteit van de financiële verslaggeving. De Raad ziet er bovendien op toe dat het bestuur in de organisatie vorm geeft aan een gezonde cultuur en bijbehorende soft controls, gericht op lange termijn waarde creatie.
De effectiviteit van het toezicht door de RvT wordt enerzijds bepaald door structuuraspecten. Heeft de RvT zijn toezicht- en toetsingskader op orde? Is sprake van goed voorbereide vergaderingen met heldere stukken? Is de besluitvorming op orde? Anderzijds bepaalt de houding en het gedrag van individuele leden van de

Raad, alsmede de interactie tussen de leden van de Raad als team, de mate waarin het toezicht effectief is. Hoe acteren raadsleden in de vergaderingen? Houden ze elkaar bij de les, of heeft ieder zo zijn eigen interesses en stokpaardjes?
Belangrijk in ieder geval is dat de RvT haar rolopvatting als toezichthouder, klankbord en werkgever, de onderlinge wisselwerking in rollen en de verhoudingen tussen het bestuur en de RvT vastlegt in een toezichtvisie en dit verder uitwerkt in een toezichts- en toetsingskader. Het toezichtskader beschrijft op hoofdlijnen het speelveld en de taken van de organisatie en omvat het geheel van spelregels die de RvT bij het uitoefenen van zijn taken volgt. Het toetsingskader omvat de besturings- en beheersingskaders waaraan de RvT bestuursvoorstellen en –besluiten inhoudelijk kan toetsen. We hebben een aanpak ontwikkeld die RvTs van zorginstellingen ondersteunt in hun functioneren. Dit betreft zowel de inrichting en uitvoering van het toezicht als het bevorderen van kennis en competenties.

### 4.2 Governance vanuit bestuur

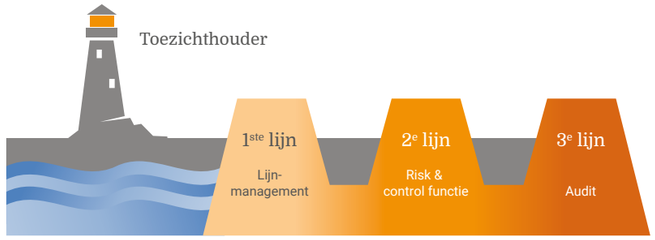
Het bestuur verschaft de RvT tijdig de informatie die nodig is voor de uitoefening van de taak. Het bestuur is verantwoordelijk voor de naleving van alle relevante wet- en regelgeving en voor het beheersen van de risico's verbonden aan de activiteiten van de zorginstelling. Het bestuur rapporteert hierover aan en bespreekt de interne risicobeheersings- en controlesystemen met de Raad van Toezicht, de commissie kwaliteit en veiligheid en zijn auditcommissie.
Naast het belang van relevante, juiste en tijdige informatie inzake risicomanagement, is het van belang dat er een goede discussie en besluitvorming plaatsvindt binnen het bestuur. Een kritische houding van de RvT is hierbij van essentieel belang, waarbij de leden van de RvT niet alleen een klankbord vormen voor het bestuur maar daar waar nodig ze van een kritisch weerwoord voorzien.

# 5 Organisatie inrichting

Bij de invulling van het risicomanagement dient tevens aandacht geschonken te worden aan de mate waarin risico's opgevangen en beheerst kunnen worden door de organisatie: de organisatie inrichting. Deze inrichting loopt uiteen van de verdeling van taken, bevoegdheden en verantwoordelijkheden tot het uitschrijven van een risicomanagement statuut. Het resultaat van een goede inrichting moet zijn dat de juiste beslissingen op het juiste tijdstip door de juiste mensen worden genomen.
Belangrijk bij de inrichting is dat deze aansluit bij de omvang, ambities en risicobereidheid van een zorginstelling. Een zorginstelling kan bijvoorbeeld een hoge ambitie hebben, een hoge risicobereidheid accepteren, maar moet dit niet alleen financieel maar ook organisatorisch kunnen dragen en op een adequate manier inrichten. Dit stelt andere eisen aan de inrichting van het risicomanagement dan bijvoorbeeld bij een kleine(re) zorginstelling. Een gebruikelijke inrichting, die wij in onze aanpak ook hanteren, is gebaseerd op het 'Three Lines of Defense'.

## 5.1 Three Lines of Defence

Een veelvuldig gebruikt inrichtingsprincipe voor risicomanagement is het zogenaamde "Three Lines of Defence" model. In dit model worden de risico's binnen de organisatie beheerst vanuit drie verdedigingslinies:



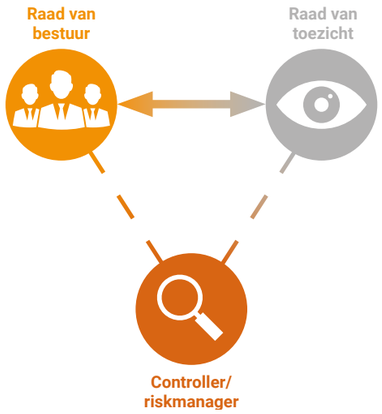

1. De eerste verdedigingslinie wordt gevormd door het management en de medewerkers van de organisatie. Zij zijn integraal verantwoordelijk voor de beheersing van de risico's binnen hun verantwoordelijkheidsgebied.
2. De tweede verdedigingslinie wordt gevormd door functies die zich richten op de ondersteuning van de eerste lijn bij het geven van invulling aan de beheersing van risico's. Te denken valt aan een specialistische risicomanagement functie, maar ook functies als Juridische Zaken & Compliance vallen hieronder. Deze functies kunnen bij een aparte afdeling belegd zijn (veelal bij grotere organisaties), maar kunnen ook een onderdeel vormen van het takenpakket van een functionaris (bijvoorbeeld de Manager Finance & Control). Deze functies zijn verantwoordelijk voor de kaderstelling, facilitering, monitoring en rapportage op het gebied van risicomanagement.
3. De derde verdedigingslinie wordt gevormd door de audit functie. De audit functie voert onafhankelijk van de eerste twee verdedigingslinies een beoordeling uit van de risico's en de risicobeheersing binnen de organisatie. De audit functie kan intern gepositioneerd zijn of kan door externe partijen ingevuld worden.

De inrichtingsprincipes van het "Three Lines of Defence" model houden niet in dat voor iedere "Line of Defence" een aparte afdeling ingericht wordt. In grotere organisaties is dat wel verstandig, maar in kleinere organisaties is dat niet altijd mogelijk. Het gaat erom dat de betreffende functies c.q. rollen onafhankelijk van elkaar zijn belegd binnen de organisatie (bijvoorbeeld bij een afdeling Finance & Control), of daarbuiten (bijvoorbeeld de audit functie).

Op ieder van de drie verdedigingslinies moet voldoende kennis en kunde aanwezig zijn om de verantwoordelijkheid op het gebied van risicomanagement goed in te vullen. Maar misschien nog wel belangrijker is dat er een open cultuur heerst om risico's bespreekbaar te maken. Niets is dodelijker voor goed risicomanagement dan een cultuur waarin het benoemen van risico's en fouten in de organisatie afgestraft wordt. Het is daarom bijvoorbeeld van belang dat in de eerste verdedigingslinie, bij het lijnmanagement en medewerkers, ruimte is om risico's te signaleren en daarop actie te ondernemen. Dit zijn juist de medewerkers die inhoudelijk het dichtst bij het werk betrokken zijn, waardoor zij beter dan wie dan ook in staat zijn om risico's in de operationele processen te onderkennen.

### 5.2 Controlfunctie in de driehoek

De controlfunctie vindt haar oorsprong in een door de Wetenschappelijke Raad voor Regeringsbeleid (WRR) opgesteld rapport – na een aantal incidenten - om het traditionele governance model van semipublieke instellingen (tweeluik-model: bestuur - raad van toezicht) te versterken door het organiseren en verstevigen van het interne weerwerk en tegenspraak. De controller of riskmanager moet het interne weerwerk en tegenspraak ('checks and balances') verstevigen, vooral in situaties waar het bewaken van de financiële stabiliteit, de integriteit van de organisatie en de kwaliteit van het primaire proces van belang zijn.




Wat opvalt is dat de WRR in één adem spreekt over 'controller / riskmanager'. Dat is relevant voor de vraag wat de rol en positie van de controller is binnen het stelsel van risicobeheersing bij een zorginstelling. In de praktijk zien wij dat de invulling van deze rol verschilt per zorginstelling, van een meer proces gestuurde, compliance rol tot aan een enterprise risk manager. In onze zienswijze heeft de controller een brede scope en kijkt naar de zogenaamde 'Enterprise Risks' vanuit een integraal perspectief, waarbij de functie zowel oog heeft voor de financiële als niet-financiële risico's, en zowel de hard controls als de soft controls.

### 5.3 Personele invulling

Uiteindelijk draait ook de inrichting om mensen. In een zorginstelling zal een adequate personele invulling van de risicomanagement functie een noodzaak zijn. Hierbij gaat het niet alleen om kennis en kunde van het personeel, maar ook om gedrag en de eerder genoemde drijfveren. Met regelmaat zullen er trainingen en workshops over risicomanagement worden gehouden, waarbij de risicomanager aan de hand van praktijkvoorbeelden laat zien wat risicomanagement inhoudt en wat er kan worden geleerd van voorvallen uit het verleden.  De risicomanagement functie zou eventueel ook kunnen worden ingevuld door de inhuur van een externe, gespecialiseerde risicomanager die een aantal dagen per week/per maand deze rol vervult.

# Meer weten? Neem dan contact op met:

**Marc Breij**
06 13 23 25 48
m.breij@accentadvies.nl

Marc werkte bij verschillende organisaties (ABN AMRO en Cordaid), met name op het gebied van Strategie en Risicomanagement, waarna hij partner werd bij Accent Organisatie Advies. Advies over governance en strategisch risicomanagement in de semipublieke sector hebben in zijn werk centraal gestaan. Marc is voormalig lid van de directie en bestuurder van het Waarborgfonds Sociale Woningbouw.

**Frank van Egeraat**
06 23 16 23 82
f.vanegeraat@accentadvies.nl

Frank van Egeraat is Register Controller en heeft ruim 20 jaar ervaring in de dienstverlening, waar hij functies heeft bekleed op het gebied van Operational Audit, Operational Risk Management en Finance. Advies over en implementatie van verbeteringen op het vlak van procesoptimalisatie, risicobeheersing en management van operationele en financiële performance hebben in zijn werk centraal gestaan.

**Over Accent**
Als Accent geloven wij dat organisaties met meer zekerheid hun doelstellingen kunnen realiseren en kansen kunnen benutten als mensen in de organisatie bewust risico's nemen en beheersen.

**Integraal risicomanagement**
Ons concept van integraal risicomanagement leidt tot een betere inrichting, besluitvorming en aansturing van een organisatie door strategische doelstellingen en risico's te verbinden aan de bedrijfsvoering op alle niveaus. Hierbij hebben we nadrukkelijk oog voor de invloed van mensen en hun gedrag op de risicobeheersing.

**Creatief en pragmatisch**
Wij helpen klanten op een andere wijze naar hun organisatie te kijken. Wij doen dat op een onafhankelijke, betrokken en interactieve manier. We komen met nieuwe inzichten, zijn creatief maar wel pragmatisch. Complexe vraagstukken zetten we om naar werkbare oplossingen. We stellen onszelf hoge kwaliteitsnormen.

Onze adviseurs zijn mensen uit de praktijk en hebben jarenlang ervaring in senior posities in de publieke en private sector, zowel op bestuurlijk als toezichthoudend niveau.

Accent
Organisatie Advies

www.accentadvies.nl
Amaliawolde, Amalialaan 126 E, 3743 KJ Baarn