

Risicomanagement voor bestuurders en toezichthouders

Carla van der Weerdt-Norder,
Alice Jansen-van den Tillaart en
Frank van Egeraat

Risicomanagement voor bestuurders en toezichthouders

Carla van der Weerdt-Norder
Alice Jansen-van den Tillaart
Frank van Egeraat

Leeswijzer

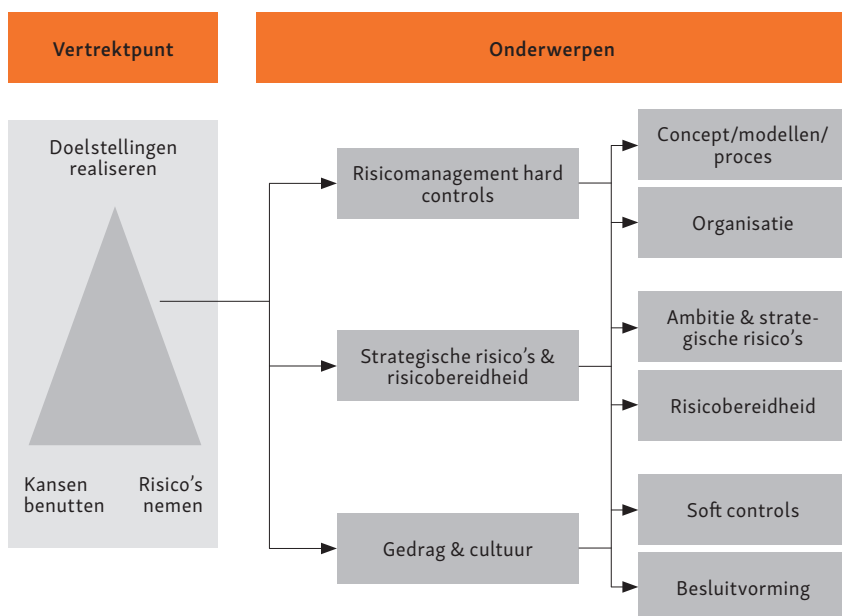
In dit boek worden veel facetten van risicomanagement behandeld en krijgt u als commissaris of bestuurder een groot aantal concrete tips om vanuit uw rol de juiste vragen te stellen over dit onderwerp. In de veelheid van facetten kan de vraag opkomen ‘waar moet ik beginnen?’ In onze ogen begint risicomanagement bij de strategie van de organisatie. Risicomanagement draait om doelstellingen realiseren, kansen benutten en risico’s effectief beheersen.

Commissarissen en toezichthouders proberen zicht te krijgen op drie hoofdonderwerpen binnen het risicomanagement:

1. de kwaliteit en effectiviteit van de risicomanagementorganisatie;
2. de strategische risico’s en risicobereidheid;
3. de heersende risicocultuur en de werking van *soft controls* (cultuur en gedrag, de psychologie achter het nemen van risico’s).

Dit is weergegeven in figuur 1. Bestuurders willen daarnaast ook zien dat het risicomanagement is verankerd in de afwegingskaders en de operationele processen.

Wat we hierin belangrijk vinden, is dat risicomanagement niet alleen draait om de negatieve aspecten, maar ook om het optimaal benutten van kansen. Door het onderwerp vanuit die invalshoek te benaderen, kan er een ander gesprek ontstaan in de boardroom. Wij hopen u met dit boek de juiste handvatten te bieden om vanuit verschillende invalshoeken vragen te stellen over investeringsvoorstellen of strategische beleidsvoorstellen en u in staat te stellen om bij te dragen aan een betere kwaliteit van besluitvorming in organisaties waarin u als bestuurder of toezichthouder actief bent.



FIGUUR 1 OVERZICHT VAN ONDERWERPEN IN RISICOMANAGEMENT

Dit boek bestaat uit twee delen:

1. *Deel 1: Basisinzichten voor bestuurder en toezichthouders*

Dit deel bevat de belangrijkste concepten van risicomanagement die als 'minimumbagage' worden beschouwd voor bestuurders en toezichthouders.

2. *Deel 2: Verdiepende inzichten voor bestuurders en leden van de auditcommissie*

Dit deel bevat een verdieping voor bestuurders en toezichthouders die behoefte hebben aan meer achtergrondinformatie voor een verdere versterking van hun rol.

Door de hoofdstukken heen hebben we aandachtspunten opgenomen. Ze bevatten korte samenvattingen van de relevantie in het werk van bestuurders en toezichthouders en tips voor vragen die toezichthouders kunnen stellen. Bij het stellen van deze vragen moet u rekening houden met de aard en de omvang van uw organisatie.

Inhoud

Voorwoord 7

Leeswijzer 9

1. **Introductie** 15

DEEL 1: BASISINZICHTEN VOOR BESTUURDERS EN TOEZICHTHOUDERS 19

2. **Risicomanagement – een algemeen overzicht** 21

2.1 **Definities van het begrip ‘risico’** 21

2.2 **Basisproces risicomanagement** 22

2.3 **Relatie tussen risico en rendement** 24

2.4 **Governance van risicomanagement** 25

2.4.1 Three lines of defence-model 25

2.4.2 Uitdagingen bij het toepassen van het three lines of defence-model 27

2.4.3 Rol van de interne toezichthouder 27

2.5 **Risicomanagement volwassenheidsniveaus** 29

3. **Risicomanagement in de planning- en controlcyclus** 33

3.1 **Risicomanagement op drie verschillende niveaus** 33

3.2 **Risicomanagement borgen in de planning- en controlcyclus** 35

3.3 **In control statement** 38

4. **Risico's identificeren en analyseren** 41

4.1 **Risicoraamwerk** 41

4.2 **Methoden voor het identificeren van risico's** 43

4.3 **Analyseren van risico's** 45

4.3.1 Kwalitatieve methoden 46

4.3.2 Kwantitatieve methoden 48

5.	Risico's evalueren en behandelen	51
5.1	Risicobereidheid	51
5.1.1	Risicofilosofie	52
5.1.2	Strepen in het zand trekken	53
5.1.3	Toepassen van risicobereidheid op de begroting, investeringsbeslissingen en strategische beslissingen	55
5.2	Risicoreacties	57
5.3	Beheersmaatregelen treffen	59
5.3.1	Typologie van maatregelen volgens BIV/AO	59
5.3.2	Typologie van maatregelen volgens Simons' levers of control	60
5.3	Risk & control framework	61
5.4	Signalen voor onvoldoende risicobeheersing	63
6.	Risico's monitoren en beoordelen	65
6.1	Permanente monitoring met indicatoren	65
6.2	Separate evaluaties/audits	68
7.	Risico's communiceren en rapporteren	71
7.1	Risicomangement in de kwartaalrapportage aan de RvC	71
7.2	Risicomangement in het bestuursverslag	72
7.3	In-control statement	73
8.	Risicocultuur en soft controls in organisaties	77
8.1	Het begrip risicocultuur	77
8.2	Hard controls en soft controls	78
8.3	Aandacht voor risicocultuur en soft controls groeit	80
8.4	Model om risicocultuur inzichtelijk te maken	81
8.4.1	Leiderschap	83
8.4.2	Beleidskaders	84
8.4.3	Medewerkers	85
8.4.4	Inzicht en besluitvorming	85
8.4.5	Organisatie	86
8.5	Risicocultuur beïnvloeden	87

- 9. De psychologie van het nemen van risico's** 89
 - 9.1 Persoonlijke risicobereidheid** 89
 - 9.2 Risicoperceptie** 90
 - 9.3 Risicoattitude** 97
 - 9.4 Relevantie voor bestuurders en commissarissen** 97
 - 9.5 Risico's in besluitvorming verminderen** 98

DEEL 2: VERDIEPENDE INZICHTEN VOOR BESTUURDERS EN LEDEN VAN DE AUDITCOMMISSIE 101

- 10. Risicomanagementmodellen** 103
 - 10.1 NEN-ISO 31000 Risicomanagement** 103
 - 10.2 COSO Enterprise Risk Management** 106
- 11. Uitdagingen in het three lines of defence-governance-model** 109
 - 11.1 Zuivere splitsing 'three lines of defence'** 109
 - 11.2 Recente kritiek op 3LoD** 113
- 12. Risicocategorieën en risicoanalysetechnieken** 115
 - 12.1 Strategie** 115
 - 12.1.1 Model van Porter** 116
 - 12.1.2 DESTEP-model** 118
 - 12.2 Operationele activiteiten** 119
 - 12.2.1 Frauderisico** 121
 - 12.2.2 Klanten, producten en marktbenadering** 126
 - 12.2.3 Medewerkers en veiligheid op de werkvloer** 126
 - 12.2.4 Schade aan bedrijfsmiddelen** 127
 - 12.2.5 Bedrijfsonderbreking en systeemfalen** 128
 - 12.2.6 Uitvoeringsfouten en procesbeheersing** 136
 - 12.3 Financiële positie** 140
 - 12.4 Financiële verslaggeving** 145
 - 12.5 Wet- en regelgeving** 146
 - 12.6 Reputatierisico** 148

13.	Methoden om risico's te analyseren	151
13.1	Kwalitatieve methoden	151
13.2	Kwantitatieve methoden	155
14.	Mitigeren van risico's bij belangrijke investeringsbesluiten	159
14.1	Factoren in een afwegingskader	159
14.2	Praktisch invulling geven aan het afwegingskader	161
14.3	Toepassen van het afwegingskader	166
	Gebruikte afkortingen	167
	Literatuur en bronnen	169
	Over de auteurs	173

1. Introductie

Risicomanagement raakt alle facetten in het leven, zowel de persoonlijke als de zakelijke. Dagelijks zijn we bezig met het nemen van beslissingen waarin onzekerheden een rol spelen. Deze onzekerheden zijn vaak onvermijdbaar. Dat maakt het maken van keuzes soms moeilijk, maar het leidt ook tot plezier als we de juiste keuze hebben gemaakt en we onze wensen en doelstellingen hebben gerealiseerd.

Een leven zonder risico's is ondenkbaar. Dat geldt ook voor organisaties. Voor iedere organisatie is het benutten van kansen en het effectief beheersen van risico's essentieel om haar doelstellingen te realiseren. In de beheersing van risico's hebben organisaties vaak de neiging om zich vooral te richten op de risico's op operationeel en tactisch niveau, en risicomanagement instrumenteel aan te pakken.

Risicomanagement staat wel op de agenda, maar dan gaat het meer om de governance van risicomanagement in de organisatie en signalen van de controller en de externe accountant. Daarbij ontstaat het gevaar dat risicomanagement op de agenda van het bestuur 'verzandt' in discussies over operationele issues, waarna de aandacht voor het risicomanagement bij de bestuursleden verdwijnt. Lijstjes worden ingevuld en afgevinkt, maar het goede gesprek wordt niet gevoerd. Dit heeft tot gevolg dat de risicomanagementinspanningen niet resulteren in daadwerkelijke verbetering van de beheersing ervan.

Het bestuur en de RvC zouden zich vooral moeten richten op risicomanagement op strategisch niveau. In dit boek laten we zien hoe u risicomanagement op een effectieve wijze op de RvC-vergadering kunt bespreken en geven we daarnaast verdiepende inzichten waarmee bestuurders het risicomanagement goed vorm kunnen geven.

Risicomanagement wordt verschillende keren genoemd in de Nederlandse Corporate Governance Code:³

Principe 1.2 Risicobeheersing

De vennootschap beschikt over adequate interne risicobeheersings- en controlesystemen. Het bestuur is verantwoordelijk voor het identificeren en beheersen van de risico's verbonden aan de strategie en de activiteiten van de vennootschap.

Principe 1.4 Verantwoording over risicobeheersing

Het bestuur legt verantwoording af over de effectiviteit van de opzet en de werking van de interne risicobeheersings- en controlesystemen.

Principe 1.5 Rol raad van commissarissen

De raad van commissarissen houdt toezicht op het beleid van het bestuur en de algemene gang van zaken in de vennootschap en de met haar verbonden onderneming. Hierbij richt de raad zich tevens op de effectiviteit van de interne risicobeheersings- en controlesystemen van de vennootschap en de integriteit en kwaliteit van de financiële verslaggeving.

Ook in sectorspecifieke governance-codes staat de rol van het bestuur en de interne toezichthouder ten aanzien van risicomanagement benoemd. Hieronder geven we enkele voorbeelden.

Governancecode Woningcorporaties, 2020 (Aedes/VTW, 21 november 2019)

- Artikel 5.1: Het bestuur is zich bewust van de risico's die verband houden met de activiteiten van de woningcorporatie, brengt deze in kaart en hanteert een inzichtelijk beleid voor het beheersen van die risico's. De corporatie verantwoordt zich hierover in het jaarverslag.
- Artikel 5.4: De RvC houdt in het licht van de maatschappelijke doelen van de corporatie specifiek toezicht op alle inspanningen om risico's inzichtelijk te maken en te beheersen. Het bestuur verschaft de RvC alle relevante informatie voor (het toezicht op) de risicobeheersing.

3 Monitoring Commissie Corporate Governance Code, 8 december 2016.

Governancecode Zorg, 2017 (Branchevereniging Zorg, 2017)

- Artikel 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.
- Artikel 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.

Governancecode Cultuur, 2019 (Cultuur+Ondernemen, 2019)

- Artikel 6.1: Het bestuur is verantwoordelijk voor de naleving van wet- en regelgeving, het artistiek en zakelijk beleid en het beheersen van de risico's die verbonden zijn aan de activiteiten van de organisatie en haar medewerkers. Het bestuur voert hierin een op de organisatie toegesneden beleid, in het bijzonder voor risicobeheersing en controle.
- Artikel 7.3: De toezichthoudende taak heeft in ieder geval betrekking op: ... de bedrijfsvoering, het risicobeheer en het zakelijk beleid.

In hoofdstuk 2 vindt u een toelichting op de basisbeginselen van risicomanagement. Hoofdstuk 3 positioneert risicomanagement in de organisatorische context als onderdeel van de planning- en controlcyclus. De hoofdstukken 4 t/m 7 behandelen de elementen van het risicomanagementproces zoals in hoofdstuk 2 is beschreven. De hoofdstukken 8 en 9 gaan in op cultuur en gedrag. De eerste 9 hoofdstukken samen vormen de basis die iedere commissaris nodig heeft om zijn toezichthoudende rol goed te kunnen invullen. Voor bestuurders en financiële commissarissen en leden van de auditcommissie hebben wij op onderdelen verdere verdieping aangebracht in de hoofdstukken 10 t/m 14, waarbij hoofdstuk 12 ook kan worden gebruikt als naslagwerk bij het identificeren van soorten risico's in organisaties.

A large, stylized orange number '1' that serves as a background for the title text.

DEEL 1
BASISINZICHTEN
VOOR BESTUURDERS EN
TOEZICHTHOUDERS

2. Risicomanagement – een algemeen overzicht

2.1 Definities van het begrip ‘risico’

In de literatuur en in het dagelijks woordgebruik worden verschillende definities en interpretaties van het woord ‘risico’ gebruikt. Voor sommigen heeft ‘risico’ een negatieve connotatie; voor anderen klinkt het meer als een combinatie van kansen en onzekerheden.

De Nederlandse betekenis van het woord ‘risico’ is sinds 1525 ‘gevaar van schade of verlies’;⁴ een vrij negatieve betekenis. Het woord ‘*rysigo*’ had in de zestiende eeuw in het Duits de betekenis ‘durven te ondernemen, hoop op economisch succes’. Het Arabische woord ‘*rizq*’ had de betekenis ‘het zoeken van opportuniteit, voordeel of geluk’. Deze twee laatste definities hebben een veel positievere connotatie.

Aangezien wij risicomanagement bekijken als een onderdeel van strategisch management, gaan wij uit van onzekerheden die het behalen van de strategie en doelstellingen kunnen belemmeren. Hierbij zijn zowel de negatieve als de positieve definities van risico relevant. Er is onderscheid te maken tussen *pure risico’s* (risico’s met alleen een potentiële negatieve uitkomst) en *speculatieve risico’s* (kansen/opportunities die ook een potentieel negatief effect hebben). De speculatieve risico’s hebben in aanvang meer aandacht gekregen in boardrooms dan de pure risico’s, omdat er met die laatste niets te winnen valt.⁵

4 Van Dale etymologisch woordenboek.

5 Van den Tillaart, *Controlling Operational Risk*, hoofdstuk ‘Evolution of the Concepts and Practices of Risk Measurement’, 2003.

Wij definiëren risico's waarmee een organisatie te maken kan krijgen als volgt:

Risico = een onzekere gebeurtenis die het behalen van de strategie en doelstellingen van een organisatie negatief kan beïnvloeden.

Risicomanagement in organisaties is dan:

Risicomanagement = het proces om risico's zodanig te beheersen dat meer zekerheid bestaat dat de organisatie haar doelstelling(en) zal realiseren.

In principe is er een relatie tussen risico en rendement: meer rendement (maatschappelijk, financieel of anderszins) vereist vaak het nemen van meer risico. Dit lichten we toe in paragraaf 2.3.

Het vak risicomanagement wordt vaak geassocieerd met modellen, statistiek en financiën. Dat is niet terecht. De kern van het risicomanagement ligt in het maken van inschattingen van toekomstige gebeurtenissen en trendbreuken. Ook is het van belang ons te realiseren dat besluitvorming ten dele niet rationeel is. Mensen maken onverwachte keuzes en hieruit komen nieuwe onzekerheden voort.

2.2 Basisproces risicomanagement

Risicomanagement wordt conform de hiervoor gegeven definitie dus gezien als een *proces*. Het risicomanagementproces kent in de basis een zestal stappen, die zijn samengevat in figuur 2.1:

- identificeren;
- analyseren;
- evalueren;
- behandelen;
- monitoren & beoordelen;
- communiceren & rapporteren.

Identificeren

Risicomanagement start met het identificeren van risico's. Dit kan plaatsvinden op verschillende niveaus in de organisatie (strategisch, tactisch, operationeel; zie ook hoofdstuk 3) en kan betrekking hebben op een breed scala aan risicocategorieën (zie hoofdstuk 4). Soms beperkt de identificatie zich tot een specifieke risicocategorie, zoals frauderisico of compliance-risico. Het is belangrijk dat het bestuur en de RvC vooral naar de risico's kijken die het realiseren van de strategie en doelstellingen van de organisatie in gevaar kunnen brengen.

Analyseren

De volgende stap in het risicomanagementproces is het analyseren van de risico's die geïdentificeerd zijn. Het analyseren van risico's kan op verschillende manieren, waarbij de analysemethoden grofweg ingedeeld kunnen worden in *kwalitatieve methoden* en *kwantitatieve methoden*. In hoofdstuk 4 lichten we een aantal methoden toe.

Evalueren

Nadat de risico's geanalyseerd zijn, moeten de risico's geëvalueerd worden. Daarbij staat de vraag centraal of de risico's passen binnen de bereidheid van de organisatie om de betreffende risico's te lopen (*risk appetite*). Hierop gaan we in hoofdstuk 5 nader in.

Behandelen

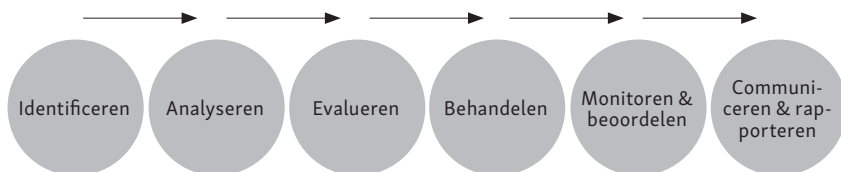
Afhankelijk van de uitkomsten van de evaluatie moet de organisatie een besluit nemen over de wijze waarop ze met de risico's om wil gaan. Daarbij heeft de organisatie de keuze uit verschillende risicoreacties. Deze lichten we toe in hoofdstuk 5.

Monitoren & beoordelen

De organisatie moet vervolgens de risico's en de ontwikkelingen daarin bewaken en periodiek opnieuw beoordelen. De wijze waarop een organisatie dit kan doen, beschrijven we in hoofdstuk 6.

Communiceren & rapporteren

De laatste stap in het risicomanagementproces is het periodiek communiceren en rapporteren over de risico's. Dit betreft zowel interne rapportages aan de RvC als externe rapportages aan belangenhouders en het brede publiek. Dit lichten we toe in hoofdstuk 7.



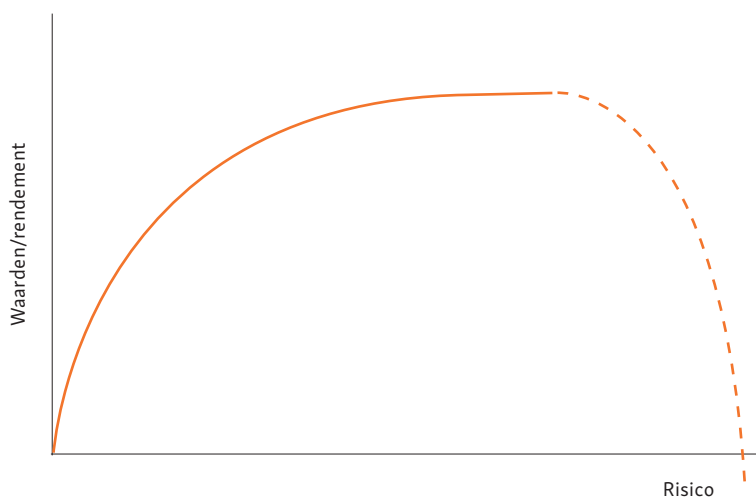
FIGUUR 2.1 DE ZES STAPPEN VAN HET RISICOMANAGEMENTPROCES

2.3 Relatie tussen risico en rendement

Een belangrijk principe in risicomanagement is het risico-rendement-principe (*risk-reward principle*). Dit principe stelt dat een laag niveau van risico gepaard gaat met een relatief laag rendement en een relatief hoog rendement gepaard gaat met navenant hoger risico (zie ook figuur 2.2). Uit dit principe volgt ook dat het realiseren van een bepaald rendement niet mogelijk is zonder een zekere mate van risico te lopen.

Iedereen zal dit principe herkennen vanuit de beleggingswereld: de rente op een spaarrekening is lager dan het rendement op een bedrijfsobligatie en dat rendement is (meestal) weer lager dan het beleggingsrendement op een aandeel. Dit principe gaat over het algemeen ook op voor andere situaties waarin een afweging en keuze gemaakt moeten worden tussen verschillende alternatieven. Als een organisatie bijvoorbeeld een strategische keuze moet maken tussen verschillende product-marktcombinaties (PMC's), dan zullen de PMC's die een hoog rendement beloven ook een hoger risico met zich meebrengen. Strategische keuzes of activiteiten die een risicoloos rendement beloven, bestaan (in principe) niet.

Het is belangrijk voor een commissaris om dit principe in het achterhoofd te houden. Als een bestuurder u een project voorspiegelt waarmee een hoog rendement gerealiseerd kan worden tegen een beperkt risico, dan moet u dat met de nodige argwaan bekijken. En als in een kwartaalrapportage fantastische rendementen gepresenteerd worden (rendementen die veel hoger liggen dan bij branchegenoten), dan moet u zich afvragen welke risico's de organisatie daarbij loopt of gelopen heeft.



FIGUUR 2.2 EEN SCHEMATISCHE WEERGAVE VAN HET RISICO-RENDEMENTPRINCIPE

De afweging tussen risico en rendement (of waarde) verloopt niet volgens een rechte lijn, maar als een curve. Aan het begin van de curve kan een organisatie met iets meer risico een beduidend hoger rendement of een hogere waarde realiseren. Maar verder op de risico-rendementcurve neemt de opbrengst van meer risico nemen af en moet een organisatie disproportioneel veel risico nemen om een (iets) hoger rendement te realiseren. Uiteindelijk komt er een punt dat het nemen van nog meer risico niet leidt tot meer rendement, maar juist tot een afbraak van rendement of waarde, met als ultiem verlies de discontinuïteit (het faillissement) van de organisatie.

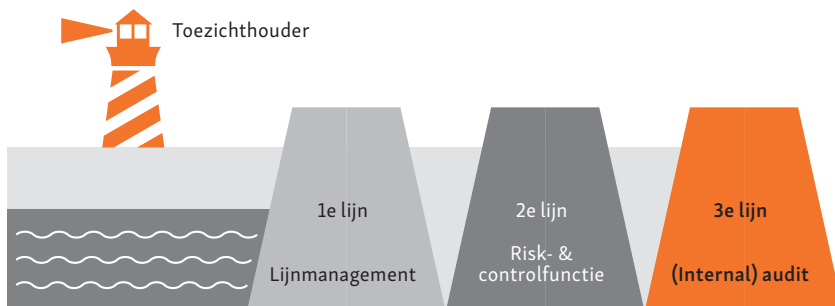
2.4 Governance van risicomanagement

2.4.1 *Three lines of defence-model*

Governance van risicomanagement gaat over de vraag hoe taken, bevoegdheden en verantwoordelijkheden voor het nemen en beheersen van risico's in een organisatie zijn belegd. Het *three lines of defence-model* (3LoD-model), dat zo'n 20 jaar geleden is ontwikkeld binnen de financiële sector, is het breed geaccepteerde model voor de inrichting van risicomanagement en interne beheersing (control) binnen organisaties.

Dit model is geïntegreerd in governance-codes en in het breed toegepaste COSO-model (verder toegelicht in hoofdstuk 10).

Het three lines of defence-model (3LoD-model) verduidelijkt de rollen en verantwoordelijkheden voor de beheersing van risico's (zie figuur 2.3).



FIGUUR 2.3 HET THREE LINES OF DEFENCE-MODEL

De *eerste lijn* wordt gevormd door het bestuur⁶, het management en de proceseigenaren in de organisatie. Zij zijn de risico-eigenaren (*risk owners*) en uit dien hoofde integraal verantwoordelijk voor de beheersing van de risico's (inclusief het voldoen aan wet- en regelgeving) binnen hun respectievelijke verantwoordelijkheidsgebieden, processen of activiteiten. Dit omvat onder andere:

1. het integreren van risicomanagement in de besluitvorming, procesinrichting, producten en systemen;
2. het zorgen voor een effectieve risk en control-omgeving;
3. het zorgen voor voldoende mensen en middelen om risico te beheersen;
4. het promoten en onderhouden van de juiste risicocultuur.

⁶ Het bestuur maakt deel uit van de eerste lijn, maar is verantwoordelijk voor zowel de eerste, de tweede als de derde lijn en moet zorgdragen voor een goede inrichting en effectiviteit van alle lijnen!

De *tweede lijn* wordt gevormd door (staf)functies op het gebied van *risk & control*, die zich richten op het stellen van kaders, het faciliteren en het toetsen van de interne risicobeheersing (*risk oversight*). Dit zijn specialistische functies op het vakgebied van risicomanagement (inclusief compliance), die onafhankelijk van de eerste lijn functioneren. Zij zijn de sparringpartners van de eerste lijn en ondersteunen de lijnmanagers en proceseigenaren bij de inrichting van het risicomanagement, risicoanalyses, het ontwikkelen van hulpmiddelen, het inrichten van beheersmaatregelen en de managementinformatie.

De *derde lijn* wordt gevormd door de functie die, onafhankelijk van de eerste twee lijnen, het bestuur en de RvC zekerheid verschaft over de adequaatheid van de interne risicobeheersing (*risk assurance*). Deze functie wordt vervuld door de (interne) auditfunctie. De auditfunctie voert periodiek audits uit en vormt zich een onafhankelijk oordeel over de opzet, het bestaan en de werking van het risicomanagement. De uitkomsten van de audits zijn input voor de eerste en tweede lijn om het risicomanagement te verbeteren.

2.4.2 *Uitdagingen bij het toepassen van het three lines of defence-model*

In de praktijk lopen veel organisaties tegen uiteenlopende uitdagingen aan bij het goed toepassen van het three lines of defence-model. In deel 2 van dit boek (hoofdstuk 11) behandelen we een aantal van die uitdagingen en de bijbehorende oplossingsrichtingen. We gaan daarbij in op:

- zuivere splitsing three lines of defence;
- onvoldoende functioneren van de eerste lijn;
- rolduidelijkheid tweede en derde lijn;
- kennis in de derde lijn.

Mede naar aanleiding van schandalen in de financiële sector in het verleden, is er ook kritiek op het functioneren van dit model. Er is echter nog geen goed alternatief ontwikkeld. In hoofdstuk 11 gaan we kort in op de kritiek en de consequenties daarvan voor de toezichthouder.

2.4.3 *Rol van de interne toezichthouder*

Bij de governance van risicomanagement wordt de RvC soms de *vierde lijn* genoemd. Conform de Corporatie Governance Code houdt de RvC onder

andere toezicht op de effectiviteit van de interne risicobeheersings- en controlesystemen van de organisatie, de integriteit en kwaliteit van de financiële verslaggeving, en de activiteiten van het bestuur om een cultuur gericht op waardecreatie op de lange termijn (gezonde risicocultuur) vorm te geven.

De RvC bespreekt minimaal jaarlijks de strategie en de risicoanalyse. Bestuurders vragen de RvC ook om goedkeuring voor (veranderingen in) de risicobereidheid, een aantal belangrijke kaderdocumenten en het auditplan. Voorbeelden van belangrijke kaderdocumenten zijn:

- investeringskader;
- treasurystatuut;
- gedrags- en integriteitscode (inclusief klokkenluidersregeling);
- beheersingskader frauderisico's.

Risicomanagement is onderdeel van de periodieke managementinformatie die de RvC bespreekt met het bestuur. Die managementinformatie bevat informatie over risico's op de verschillende niveaus, waarbij de RvC vaak te veel aandacht besteedt aan operationele risico's. Het is belangrijk om ervoor te zorgen dat ook de risico's op strategisch niveau op de juiste wijze worden geadresseerd.

Om zich een beter beeld te vormen van het risicobeheer en de risicocultuur spreekt de RvC (al dan niet via de auditcommissie) met de onafhankelijke internal auditor, controller of compliance officer en met de externe accountant. In deze gesprekken is het goed om ook een gevoel te krijgen bij de wijze waarop zij in hun werk wel of niet worden gesteund door de leiding in de organisatie en welk gevoel zij hebben over de opvolging in de organisatie van hun bevindingen en aanbevelingen.

De remuneratiecommissie geeft aandacht aan risicobeheer en risicocultuur in haar gesprekken met het bestuur. Daarnaast doet de remuneratiecommissie voorstellen voor het beloningsbeleid van het bestuur. Het is daarbij van belang om oog te hebben voor de invloed die het beloningsbeleid heeft op de mate waarin het bestuur risico's neemt of zal nemen.

Jaarlijks legt de RvC verantwoording af over deze taak in het jaarverslag.



Aandachtspunten!

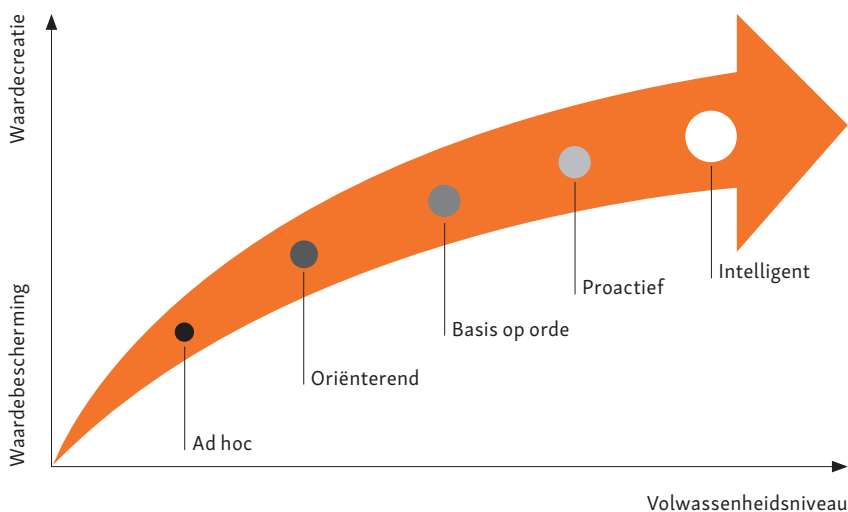
- Vraag het bestuur om uit te leggen hoe het risicomanagement in de organisatie is geïntegreerd in de planning- en controlcyclus. Let daarbij op of een goed onderscheid wordt gemaakt tussen risicomanagement op strategisch niveau, op tactisch niveau en op operationeel niveau.
- Risico's op strategisch niveau kunnen ook niet-strategische risico's zijn. Het zou kunnen dat bepaalde operationele risico's of de risico's in een bepaalde businessunit zo groot zijn geworden dat we hier kunnen spreken van risico's op strategisch niveau die een gevaar kunnen vormen voor de continuïteit van de organisatie. In de praktijk zijn hier vele voorbeelden van.
- Organiseer een goede discussie over de risicobereidheid van de organisatie (per risicogebied) en bespreek wat hiervan de consequenties zijn voor de organisatie.
- Het is meestal voldoende om één keer per jaar te bespreken hoe de organisatie de risico's op tactisch en operationeel niveau beheerst; daarbij hoeft de RvC niet in te gaan op de details van deze risicobeheersing. Risico's op strategisch niveau staan ten minste één keer per jaar op de agenda, maar verdienen per risico vaak ook aandacht in de reguliere vergaderingen als het gaat om een groot risico dat een gevaar vormt voor de continuïteit van de organisatie.
- Bevraag het bestuur op de inrichting en het functioneren van de three lines of defence. Is er sprake van een zuivere splitsing tussen de drie rollen? Zo niet, hoe waarborgt het bestuur de kwaliteit en de onafhankelijkheid van iedere rol? Zo ja, hoe wordt bewaakt dat alle belangrijke risicogebieden door de tweede en derde lijn goed worden afgedekt?

2.5 Risicomanagement volwassenheidsniveaus

Risicomanagement kan op veel manieren worden ingericht, van heel beknopt en ad hoc tot geavanceerd. In de jaren negentig zijn er verschillende modellen ontwikkeld om de volwassenheid van het risicomanagement te kunnen beoordelen om zo het benchmarken van organisaties mogelijk te maken. Elk volwassenheidsmodel omvat *fases* (4 of 5) en maakt onderscheid tussen verschillende aspecten van risicomanagement. Het model dat hieraan ten basis ligt, is in de meeste gevallen het

model van Hillson.⁷ Hij onderscheidt vier *volwassenheidsniveaus* (*naive, novice, normalised, natural*) en meet deze aan de hand van vier aspecten van risicomanagement (cultuur, proces, ervaring en toepassing). Het model van Hillson is in eerste instantie ontwikkeld voor risicomanagement in een projectmanagementomgeving. Naast het model van Hillson met vier volwassenheidsniveaus, kennen we verschillende modellen waarin het niveau 4 is opgesplitst en er zo vijf volwassenheidsniveaus ontstaan.

Wij gebruiken een model met vijf volwassenheidsniveaus in het risicomanagement van organisaties, aangezien dit organisaties meer richting en handvatten biedt bij het bepalen van de juiste ambitie. Niet elke organisatie streeft immers naar dezelfde mate van professionaliteit in risicomanagement (zie figuur 2.4).



FIGUUR 2.4 DE VIJF VOLWASSENHEIDSNIVEAUS IN HET RISICOMANAGEMENT

⁷ David Hillson, *Toward a Risk Maturity Model*, 1997.

Niveau 1: Ad hoc

Een organisatie die het risicomanagement *ad hoc* heeft ingericht, reageert op ongunstige gebeurtenissen op het moment dat ze zich voordoen. Risicomanagement vindt veelal incidenteel plaats (vaak na druk van buitenaf). Er is geen sprake van rapportages of van monitoring van risico's.

Niveau 2: Oriënterend

Een organisatie waarbij het risicomanagement in volwassenheidsniveau *oriënterend* zit, heeft een eerste aanzet gemaakt voor de inrichting van het risicomanagement. De focus ligt daarbij vooral op financiële en compliance-risico's. Een kleine groep mensen in de organisatie is zich ervan bewust hoe belangrijk risicomanagement is.

Niveau 3: Basis op orde

Een organisatie die de *basis op orde* heeft op het gebied van risicomanagement heeft alle elementen in de basis ingericht, maar is nog steeds voornamelijk reactief ten aanzien van risicomanagement. Risicomanagement ligt bij deze organisaties vooral bij het bestuur, het management en de bedrijfsvoering/control. Risicomanagement is nog een losstaand 'iets'. De verbindingen met strategie en beleid, cultuur en besluitvorming zijn nog beperkt.

Niveau 4: Proactief

Organisaties die het volwassenheidsstadium *proactief* hebben bereikt, hebben een gestructureerd risicomanagementproces op alle niveaus binnen de organisatie. Risicomanagement is een integraal onderdeel van de besluitvorming en belicht zowel kansen als bedreigingen. De risicobereidheid is benoemd, er wordt gebruikgemaakt van scenarioanalyses en er is een koppeling met prestatie management.

Niveau 5: Intelligent

Bij organisaties die het hoogste volwassenheidsniveau *intelligent* realiseren, is risicomanagement volledig geïntegreerd in de besluitvorming en wordt risicomanagement ook gebruikt om vooruit te kijken. Er is sprake van continue en actieve sturing op risico's op alle niveaus binnen de organisatie. Een aantal sleutelwoorden voor dit soort organisaties is 'integraliteit, professionaliteit, samenhang en optimalisatie'.

Het is niet voor elke organisatie passend om het hoogste niveau van volwassenheid na te streven. De mate van volwassenheid die een organisatie nastreeft, moet passen bij de omvang van de organisatie, het ambitieniveau en de complexiteit ervan en haar externe omgeving. Hoe groter, complexer en ambitieuzer een organisatie, hoe meer belang en baat zij heeft bij professioneler risicomanagement. Hoewel er geen vaste regels zijn voor wat een passend niveau van risicomanagement is, hanteren wij de vuistregels die zijn weergegeven in tabel 2.1.

Aspect	Ad hoc	Oriënterend	Basis op orde	Proactief	Intelligent
Omvang	< 10 FTE	10-50 FTE	50-100 FTE	100-250 FTE	>250 FTE
Ambities	Stabiel	Beperkt ambitieus	Gemiddeld	Aanzienlijk ambitieus	Zeer ambitieus/innovatief
Complexiteit	Overzichtelijk	Enigszins complex	Gemiddeld	Behoorlijk complex	Zeer complex

TABEL 2.1 VUISTREGELS VOOR HET BEPALEN VAN EEN PASSEND VOLWASSENHEIDSNIVEAU

Een grote organisatie (>250 fte) met gemiddelde ambities en een beperkte complexiteit in de organisatie en de externe omgeving (stabiele markt) kan volstaan met ‘basis op orde’. Een kleine organisatie (10-50 fte) in een zeer dynamische omgeving met grote (groei)ambities heeft echter baat bij een proactief risicomanagement.

In het volgende hoofdstuk, hoofdstuk 3, introduceren wij de risicomanagementachtbaan. Voor elk van de elementen van de risicomanagementachtbaan kan in kaart worden gebracht wat het huidige volwassenheidsniveau is.



Aandachtspunt!

Vraag de bestuurder waar hij vindt dat de organisatie staat op het gebied van risicomanagement en beoordeel of dit niveau passend is bij de omvang, complexiteit en ambitie van de organisatie.