



**Handreiking  
Risicomanagement  
voor  
beleggingsinstellingen  
en  
beleggingsondernemingen**



**Copyright DUFAS 2011**

In geval van distributie of reproductie van informatie afkomstig uit deze publicatie dient de informatie accuraat te zijn en dient DUFAS als bron te worden vermeld. Indien de gebruiker een wijziging in de informatie aanbrengt of de informatie transformeert, dient dit duidelijk te worden vermeld, onder vermelding dat de bron voor de informatie DUFAS is. Indien de informatie wordt gebruikt in documenten ter commercieel gebruik, dient degene die de informatie aldus gebruikt de koper voorafgaand aan de totstandkoming van de overeenkomst te informeren dat de informatie gratis verkrijgbaar is voor leden van DUFAS.



## Voorwoord

Den Haag, maart 2011

Voor u ligt een handreiking van de Dutch Fund and Asset Management Association (DUFAS) over risicomanagement voor financiële instellingen die zich met individueel of collectief vermogensbeheer bezighouden.

DUFAS wil met deze handreiking bereiken dat financiële instellingen risicobewust handelen, gestructureerd nadenken over de risico's en dit ook in de eigen organisatie uitstralen. De handreiking biedt een handvat voor de vraag hoe kan worden omgegaan met risicobeheer en op welke wijze de bedrijfsvoering kan worden ingericht. De financiële crisis onderstreept het belang van een gedegen bedrijfsvoering en daarmee het voeren van risicomanagement.

De inhoud is met zorg samengesteld door DUFAS in samenwerking met een representatieve selectie van marktpartijen en externe adviseurs, van wie wij hier Ernst & Young en Charco & Dique willen noemen.

Wij hopen met deze handreiking een waardevolle bijdrage te leveren aan een goed risicomanagement door financiële instellingen in Nederland.

Zoals altijd vernemen wij gaarne eventuele opmerkingen van de gebruikers van deze handreiking, zodat wij daar bij actualisering gebruik van kunnen maken.

Wij vertrouwen erop u hiermee van dienst te zijn.

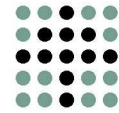
Dutch Fund and Asset Management Association (DUFAS)

Mr. J.H.M. Janssen Daalen  
Algemeen Directeur

dutch fund and asset

---

MANAGEMENT ASSOCIATION



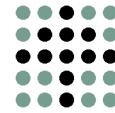


## inhoudsopgave

	pag.
<b>Samenvatting</b>	7
<b>1. Inleiding</b>	9
<b>2. Reikwijdte</b>	10
<b>3. Proportionaliteitsbeginsel en ‘kleine’ instellingen</b>	10
<b>4. Algemene eisen</b>	11
4.1. Doorzichtige zeggenschapsstructuur	11
4.2. Beheerste en integere bedrijfsvoering	11
4.3. Beheersen van bedrijfsprocessen en bedrijfsrisico's	12
4.4. Handelen in het belang van de beleggers	12
<b>5. Rolverdeling AFM en DNB</b>	13
<b>6. Bestuur en organisatie</b>	13
6.1. Het risicomangementbeleid	14
6.1.1. Doelstelling en deliverables	14
6.1.2. Systematische analyse en integratie in bedrijfsprocessen	14
6.1.3. Schriftelijke vastlegging	15
6.1.4. Goedkeuring door de hoogste leiding van de onderneming	15
6.1.5. Interne communicatie	16
6.1.6. Implementatie en toetsing	16
6.1.7. Bijstelling van tekortkomingen of gebreken	16
6.1.8. Inhoud risicomangementdocument	16
6.1.9. Risicobehandelingsplan	17
6.2. De risicomangementfunctie	18
6.2.1. Passende en proportionele invulling	18
6.2.2. Beloning risicomangementfunctie	18
6.2.3. Gezag van de risicomangementfunctie	19
6.3. Taken van de risicomangementfunctie	20
6.3.1. Implementeren, beheren, adviseren en rapporteren	20
6.3.2. Beloningsbeleid	20
6.3.3. Advies aan de leiding van de onderneming	21
6.3.4. Intrinsieke waardebeoordeling	21
6.4. Uitbesteding van de risicomangementfunctie	21
<b>7. Het risicomangement proces</b>	22
7.1. Schriftelijke vastlegging	23
7.2. Vaststellen context	24
7.3. Risicoprofiel	24
7.4. Risicolimieten	25
7.5. Risicoweging	26
7.6. Risicocategorieën (risico-dashboard)	27
7.7. Risicoboordeling	28
7.8. Risicobehandeling	29
7.9. Risicomangement en het beleggingsproces	30



7.10.	Monitoren en beoordelen	31
7.11.	Incidentenregister	31
7.12.	De rol van de interne of externe accountant	32
<b>Bijlage I: Risico inventarisatie</b>		<b>33</b>
1.	<i>Marktrisico</i>	33
	1.1. <i>Concentratierisico</i>	34
	1.2. <i>Derivatenrisico</i>	34
	1.3. <i>Leverage risico</i>	34
	1.4. <i>Valutarisico</i>	35
2.	<i>Kredietrisico</i>	35
	2.1. <i>Tegenpartijrisico en faillissementsrisico</i>	35
	2.2. <i>Securities lending risk</i>	36
	2.3. <i>Concentratierisico</i>	36
3.	<i>Liquiditeitsrisico</i>	36
4.	<i>Operationeel risico</i>	38
	4.1. <i>Uitbestedingrisico</i>	39
	4.2. <i>Juridisch risico</i>	40
	4.3. <i>Model risico</i>	40
	4.4. <i>Onderpandrisico (collateral risk)</i>	41
5.	<i>Integriteitsrisico</i>	41
	5.1. <i>Risico van belangenverstrengeling</i>	41
	5.2. <i>Personeelsrisico</i>	41
	5.3. <i>Witwasrisico en risico van terrorismefinanciering</i>	41
	5.4. <i>Afwikkelingsrisico</i>	44
6.	<i>Restrisico</i>	44
<b>Bijlage 2: Begrippen</b>		<b>45</b>
<b>Eindnoten</b>		<b>47</b>



## Samenvatting

Deze samenvatting is tevens een checklist voor financiële instellingen die zich met individueel en collectief vermogensbeheer bezig houden, die aangeeft wat zij op grond van de huidige wetgeving ten minste moeten doen.

1. Zorg voor een integriteits- en risicobewuste *tone at the top* [hfdst 6].
2. Het risicomanagement moet de volgende doelstellingen dienen:
  - (i) beheerste en integere bedrijfsvoering,
  - (ii) naleven van wet- en regelgeving, en
  - (iii) handelen in het belang van de beleggers c.q. de zorgplicht [par. 7.2.].
3. Maak een schriftelijk stuk, getiteld “Risicomanagementbeleid” [par. 6.1.].

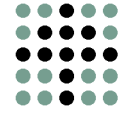
De inhoud van dit stuk bestaat tenminste uit [par. 6.1.7.]:

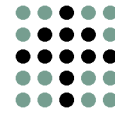
  - a. Wie doet wat inzake de risicomanagementfunctie [par. 6.2.];
  - b. De structuren van de risicoprofielen en de top-level limieten [par. 7.3.], eventueel aangevuld met een systeem van risicolimieten [par. 7.4.];
  - c. Een beschrijving van de rapportage arrangementen aan de toezichthouder en de hoogste leiding van de onderneming (wat wordt hoe vaak gerapporteerd);
  - d. Een beschrijving van de risicomeetinstrumenten en -technieken
  - e. Een analyse per beleggingsinstelling van de materiële, d.w.z. belangrijkste, risico's, waarbij in elk geval aandacht wordt besteedt aan de door de wet genoemde risico's [bijlage 1].
    - (i) Bestudeer de risico's met behulp van bijlage 1;
    - (ii) Bepaal welke voor uw organisatie materieel zijn (en zorg dat u de toezichthouder desgevraagd kunt uitleggen waarom de andere dat niet zijn);
    - (iii) Bepaal per materieel risico de kans en impact, eventueel aan de hand van de eenvoudige schema's in deze handreiking [par. 7.5.].
    - (iv) Bepaal per risico of dit laag genoeg is, dan wel dat u er een risicobehandelstrategie [zie par. 7.8.] op wilt toepassen.
4. Laat dit risicomanagementbeleid document goedkeuren door de hoogste leiding van de onderneming [par. 6.1.4.]
5. Implementeer het risicomanagementbeleid document, toets het jaarlijks [par. 6.1.6.] en stel het zo nodig bij [par. 6.1.7.]. D.w.z. bepaal of de risicobehandelstrategie adequaat is geweest om het risico tot een aanvaardbaar niveau terug te brengen.
6. Leg de uit het risicomanagementbeleid voortvloeiende maatregelen en procedures vast in de AO/IC [par. 6.1.2.].

dutch fund and asset

---

MANAGEMENT ASSOCIATION





## I. Inleiding

Deze handreiking geeft aan hoe de wettelijke vereisten met betrekking tot risico management door financiële instellingen die zich met individueel of collectief vermogensbeheer bezighouden, moeten worden ingevuld. De handreiking zelf is echter niet juridisch bindend. De tekst is afgestemd met de Autoriteit Financiële Markten (AFM). Het is een gids door de wettelijke verplichtingen inzake risicomanagement, met suggesties en aanbevelingen voor implementatie.

Uiteraard kan een instelling afwijken van deze suggesties en aanbevelingen, als hij maar aan de desbetreffende (open) wettelijke normen voldoet. Uitsluitend waar deze handreiking directief geformuleerd is (“moeten”, “is”, “zijn”) is sprake van een wettelijke norm, waarvan de nuances in de diverse paragrafen worden uitgelegd.

Voor het implementeren van risicomanagementbeleid binnen uw instelling, dient u de volgende drie onderdelen te onderscheiden:

- De bestuurlijke inrichting en organisatie van het risicomanagementproces (zie hoofdstuk 6);
- De identificatie en meting van relevante risico's binnen de instelling (zie hoofdstukken 7.1 t/m 7.9 en bijlage 1);
- De monitoring en rapportage van deze risico's (zie hoofdstukken 7.10 en 7.11).

De inrichting van een goed risicomanagement is maatwerk, dat dient te zijn toegesneden op de aard, omvang en complexiteit van uw onderneming, haar activiteiten en risico's. De wetgever heeft daarmee rekening gehouden en het zogenaamde proportionaliteitsbeginsel in de wet vastgelegd. Dat belangrijke uitgangspunt vindt u beschreven in hoofdstuk 3 hieronder.

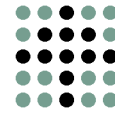
In hoofdstuk 2 hebben wij nader aangegeven op welk type instellingen en activiteiten deze handreiking van toepassing is.

In hoofdstuk 4 hebben wij de algemene eisen aangegeven die de wetgever stelt aan de bedrijfsvoering van beleggingsinstellingen en beleggingsondernemingen.

Het toezicht op het risicomanagement van financiële instellingen is thans verdeeld tussen AFM en DNB. Die onderlinge rolverdeling wordt beschreven in hoofdstuk 5.

Voor beter begrip van de eventuele toepasselijkheid van voorschriften op uw instelling, noopt dit tot het onderstaande begrippenkader:

- Waar de term “beleggingsinstelling(en)” wordt gebruikt, wordt ook hun (fonds)beheerder bedoeld.
- Waar de term “beleggingsondernemingen” wordt gebruikt, worden de individueel vermogensbeheeractiviteiten bedoeld.
- Waar de term “hoogste leiding van de onderneming” wordt gebruikt, wordt bedoeld de directie van de fondsbeheerder of als er geen separate fondsbeheerder is, de directie van de zelfstandige beleggingsinstelling.



## 2. Reikwijdte

Deze handreiking behandelt de wettelijke verplichtingen met betrekking tot het risicomanagement van fondsbeheerders (collectief beheer) en financiële instellingen, groot of klein, die zich met individueel vermogensbeheer bezig houden. Met individueel vermogensbeheer mogen zich zowel fondsbeheerders, banken, als beleggingsondernemingen bezig houden. De risicomanagement regels gelden voor alle typen fondsbeheer: beleggingsinstellingen met of zonder aparte beheerder, UCITS of non-UCITS, open-end of closed-end, vastgoedfondsen en *alternatives*.

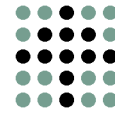
De reden voor de brede reikwijdte van deze handreiking vloeit voort uit de wet. Op het eerste gezicht zijn strikt formeel-juridisch de eisen die worden gesteld aan het risicomanagement van beleggingsinstellingen en beleggingsondernemingen niet identiek. Dit uit zich onder meer in het feit dat in het geval van beleggingsinstellingen de AFM wel ontheffingen kan verlenen en in het geval van beleggingsondernemingen niet. Maar de wet staat het een beheerder van een UCITS toe om tevens als individueel vermogensbeheerder op te treden,<sup>1</sup> en de regels voor beleggingsondernemingen gelden voor de activiteit “verlenen van beleggingsdiensten” en niet voor een bepaalde categorie vergunninghoudende instellingen. Derhalve is het in de praktijk niet zinvol om onderscheid te maken tussen de eisen die kunnen worden gesteld aan beleggingsinstellingen en hun beheerders enerzijds en individueel vermogensbeheer anderszijds.

De reikwijdte van de wettelijke bepalingen omtrent risicomanagement is naar huidig recht niet eenduidig, voornamelijk als gevolg van de reikwijdtebepalingen van de Wet op het financiële toezicht (Wft) en de vrijstellingsregeling Wft.<sup>2</sup> Naar het zich laat aanzien zal een aantal veranderingen worden aangebracht door de Wijzigingswet Financiële Markten 2010,<sup>3</sup> de Implementatiewet UCITS IV<sup>4</sup> en de implementatie van de Alternative Investment Fund Management Directive (AIFMD),<sup>5</sup> waardoor een behoorlijk ingericht risicomanagement voor alle fondsbeheerders, inclusief vastgoedfondsen en thans vrijgestelde institutionele beheerders, verplicht zal worden en onder toezicht zal gaan vallen. In deze handreiking wordt thans daarom niet ingegaan op uitzonderingen op de wettelijke verplichtingen, omdat die naar verwachting binnen afzienbare tijd zullen zijn verdwenen.<sup>6</sup>

De wetgeving definieert het begrip ‘risico’ niet. Risico kan volgens DUFAS worden gezien als een effect van onzekerheid op het behalen van doelstellingen.

## 3. Proportionaliteitsbeginsel en “kleine” instellingen

Voor het gehele risicomanagement van beleggingsinstellingen en beleggingsondernemingen geldt het proportionaliteitsbeginsel.<sup>7</sup> Hoe groter, complexer en geavanceerder een belegginginstelling of beleggingsonderneming is, des te hoger zullen de verwachtingen zijn betreffende de kwantificering, consistentie, systematische aard en documentatie van het proces,<sup>8</sup> en andersom. Dit kan het beste worden beoordeeld aan de hand van factoren als omvang van de onderneming, expertise, com-



plexiteit van de beleggingsstrategieën, het aantal en de soort beleggingsinstellingen c.q. cliënten en de omvang van de belegde activa.

Er zijn geen eenduidige criteria te geven voor de vraag wanneer een organisatie kan worden beschouwd als “klein”, of beter gezegd, “niet-complex”. Hiervoor dient u uw eigen afwegingen te maken, gebaseerd op de omvang van uw organisatie, de complexiteit van uw beleggingsactiviteiten en de daarmee gemoeide risico’s. Daarnaast mogen de onderstaande richtsnoeren gelden.

Voor toepassing van het proportionaliteitsbeginsel zal de mate van betrokkenheid van bestuurders bij relevante bedrijfsprocessen<sup>9</sup> een rol kunnen spelen. Wanneer de organisatie minder mensen telt, zijn communicatielijnen korter en ziet de leiding en ook de voor het risicomanagement verantwoordelijke meer, waardoor minder rapportages nodig zijn. Bij organisaties met minder mensen zijn risico’s als het personeelsrisico en het operationele risico in het algemeen ook minder groot, omdat de “teller” kleiner is. Anderzijds zal er bij kleine organisaties sneller een *key man* risico kunnen optreden.

Het proportionaliteitsbeginsel kan ook risico georiënteerd worden benaderd. Naar mate er minder van de in bijlage I genoemde risico’s materieel moeten worden geacht, zullen de inspanningen die voor goed risicomanagement moeten worden verricht, geringer zijn.

Voor beleggingsondernemingen geldt dat ook de frequentie en omvang van de ICAAP evaluatie door DNB wordt afgestemd op de aard, omvang en complexiteit van de onderneming,<sup>10</sup> maar hij moet in ieder geval ten minste één keer per jaar worden geactualiseerd.<sup>11</sup>

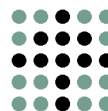
## 4. Algemene eisen

### 4.1. Doorzichtige zeggenschapstructuur

In de eerste plaats is het een wettelijke eis dat een beleggingsinstelling en beleggingsonderneming een formele of feitelijke zeggenschapstructuur heeft die niet zo ondoorzichtig is dat deze een belemmering vormt of kan vormen voor het adequaat uitoefenen van toezicht door de AFM.<sup>12</sup> Dit is voor beleggingsinstellingen nader uitgewerkt en betekent dat een beheerder voor iedere door hem beheerde beleggingsinstelling die hij beheert afzonderlijk een bedrijfsvoering moet inrichten.<sup>13</sup> In de bedrijfsvoering van de beheerder moet een scheiding worden aangebracht tussen de administratie van de beheerder zelf en van de diverse beleggingsinstellingen die hij beheert. Hiermee wordt voorkomen dat de administraties van de verschillende beleggingsinstellingen ondoorzichtig worden.<sup>14</sup>

### 4.2. Beheerste en integere bedrijfsuitoefening

Daarnaast moet de bedrijfsvoering<sup>15</sup> van beleggingsinstellingen en beleggingsonder-



nemingen zodanig worden ingericht dat deze een beheerste en integere uitoefening van het bedrijf waarborgt.<sup>16</sup> Dit is een doelgerichte of “principle based” benadering. Binnen de kaders van de regels van het Besluit gedragstoezicht financiële ondernemingen (Bgfo) moet de beleggingsinstelling en/of beleggingsonderneming bepalen welke maatregelen in de bedrijfsvoering moeten worden getroffen, gelet op de risico’s die de onderneming loopt<sup>17</sup> en wenst te lopen. Elke beleggingsinstelling en beleggingsonderneming zal dus zelf een analyse moeten maken van de risico’s en haar bedrijfsvoering daarnaar inrichten. Zie hierover hoofdstuk 7 van deze handreiking.

Voor wat betreft beleggingsondernemingen is er de verplichting om de bedrijfsvoering zodanig in te richten dat de soliditeit van de onderneming wordt gewaarborgd.<sup>18</sup> Onder “soliditeit” wordt daarbij onder meer verstaan het beheersen van financiële risico’s (o.a. marktrisico, kredietrisico, verzekeringsrisico en liquiditeitsrisico<sup>19</sup>) en andere risico’s,<sup>20</sup> zoals juridische risico’s, het risico dat ontvangen garanties of onderpand niet afdwingbaar zijn omdat de juridische vormgeving tekortschiet, of operationele risico’s.<sup>21</sup> Daarbij merkt de regering in de Nota van toelichting op dat, ondanks het feit dat geen liquiditeitseisen worden gesteld aan beleggingsondernemingen, het belangrijk is dat zij over adequate procedures beschikken voor het waarborgen van de liquiditeitspositie.<sup>22</sup>

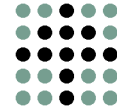
Een belangrijk uitgangspunt van risicomanagement is daarom dat het moet bijdragen aan het beheersen van de bedrijfsvoering met het oog op de met beleggers afgesproken risico/rendement verhouding en het behouden van waarde.

### 4.3. Beheersen van bedrijfsprocessen en bedrijfsrisico’s

De algemene regel van beheerste en integere bedrijfsvoering is nader uitgewerkt in het Bgfo.<sup>23</sup> Daar worden regels gesteld met betrekking tot het beheersen van bedrijfsprocessen en bedrijfsrisico’s. Beheersen bevat het hele traject van vaststellen, besturen, monitoren en bijsturen van doelstellingen en processen. De beleggingsinstelling en beleggingsonderneming moet voor het beheersen van bedrijfsprocessen onder meer beschikken over een duidelijke organisatiestructuur en heldere rapportagelijnen. Een dergelijke bedrijfsvoering levert namelijk inzichtelijke en betrouwbare rapportages op: het systeem van maatregelen en procedures waarborgt de kwaliteit van de *output*.<sup>24</sup> Zo’n systeem van maatregelen en procedures wordt meestal de AO/IC genoemd. Daarnaast zijn er nadere regels voor het optreden van beleggingsinstelling en beleggingsonderneming op markten in financiële instrumenten, zoals de regels inzake bestrijding van marktmisbruik en de melding van zeggenschap.

### 4.4. Handelen in het belang van de beleggers

De (beheerder van de) beleggingsinstelling is wettelijk verplicht om te handelen in het belang van de deelnemers in de beleggingsinstelling.<sup>25</sup> Bij de beoordeling van het risicomanagement zal de toezichthouder ook de belangen van de belegger als uitgangspunt nemen. Deze norm is een uitwerking van de zorgplicht, die voor beleggingsondernemingen separaat is uitgewerkt.



## 5. Rolverdeling AFM en DNB

Het toezicht op het risicomanagement wordt niet alleen door de AFM gedaan, maar óók door De Nederlandsche Bank (DNB).<sup>26</sup> De wetgever heeft in zijn toelichting gezegd dat daarbij de AFM op de gedragsaspecten moet letten en DNB op de prudentiële aspecten. Die prudentiële aspecten uiten zich in de verplichting van beleggingsondernemingen (maar niet beleggingsinstellingen en hun beheerders of bewaarders) om een *Internal Capital Adequacy Assessment Process* (ICAAP) op te stellen. Indien kleinere beleggingsondernemingen in bijzondere gevallen geen ICAAP wensen uit te voeren, beveelt DUFAS aan dat men in overleg treedt met DNB.

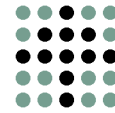
Het ICAAP evaluatieproces is van toepassing op beleggingsondernemingen.<sup>27</sup> Als deze onderneming dochter van een vergunninghoudende bank met zetel in Nederland is en wordt meegenomen in de consolidatie van deze bank, dan moet men voor het opstellen van het ICAAP aansluiten bij het ICAAP van de moederinstelling. In alle andere gevallen is de beleggingsonderneming verplicht zelf een ICAAP op te stellen voor de eigen onderneming dan wel, zich aan te sluiten bij het ICAAP voor de groep van beleggingsondernemingen waarvan hij deel uitmaakt.<sup>28</sup>

De door de beleggingsonderneming opgestelde ICAAP wordt vervolgens in het kader van het door Basel II ingevoerde *Supervisory Review and Evaluation Process* door de Nederlandsche Bank beoordeeld. De door de Nederlandsche Bank uitgevoerde *supervisory review* moet ten minste betrekking hebben op het valutarisico, grondstoffenrisico en operationeel risico, het renterisico bij niet-handelsactiviteiten, de blootstelling aan en het beheer van het concentratierisico, het liquiditeitsrisico en grote posities, en de impact van de diversificatie-effecten en de wijze waarop dergelijke effecten in het systeem van risicometing worden verwerkt.<sup>29</sup>

De ICAAP van DNB geldt niet voor beleggingsinstellingen. Toch houdt in het kader van risicomanagement niet alleen de AFM toezicht op beleggingsinstellingen, maar ook DNB. Met het oog op de bewaking en beheersing van solvabiliteitsrisico's moet de bedrijfsvoering van een UCITS beheerder in ieder geval voorzien in de bewaking en beheersing van de aard en omvang van de activa en passiva, niet uit de balans blijvende verplichtingen en resultaatontwikkeling, uitgesplitst naar de onderscheiden bedrijfsactiviteiten en bedrijfsonderdelen,<sup>30</sup> met andere woorden de voor hem in verband met zijn bedrijfsvoering bestaande risico's voor zover die impact kunnen hebben op de solvabiliteit. De UCITS-beheerder moet in staat zijn een verband te leggen tussen de risico's en het aanwezige eigen vermogen. De inrichting van de bedrijfsvoering moet daartoe de mogelijkheid bieden.<sup>31</sup>

## 6. Bestuur en organisatie

Risicomanagement kan worden omschreven als het geheel van gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot risico's. Een belangrijk uitgangspunt van risicomanagement is dat het onderdeel uitmaakt van het besturen van de organisatie en de besluitvorming. Risicomanagement helpt bestuurders een onderbouwde keuze te maken, prioriteiten te stellen en onderscheid



te maken tussen alternatieve oplossingsrichtingen, met name gericht op de beheersing van risico's en het bewust kiezen voor welke risico's de organisatie loopt.

Een integriteitsbewuste bedrijfscultuur<sup>32</sup> is van eminent belang. Een cultuur waarbij risicomanagement belangrijk wordt gevonden staat of valt met de *tone at the top*. Niet alleen zal de hoogste leiding van de onderneming zelf het goede voorbeeld moeten geven, ook zal hij het belang van een goed risicomanagement steeds onder de aandacht van de medewerkers moeten brengen. Een gestructureerd en integraal risicomanagement werkt alleen als iedereen in de organisatie is doordrongen van het belang daarvan.

Het startpunt van het bestuur en de organisatie van het risicomanagement van beleggingsinstellingen en beleggingsondernemingen is volgens DUFAS daarom het document waarin het risicomanagementbeleid is vastgelegd. Daarin zou het bestuur en organisatie moeten zijn beschreven. Daarbij gaat het kort samengevat om de inrichting van de risicomanagementfunctie en het toezicht daarop, de rapportagelijnen en de taken van de risicomanagementfunctie.

Daarbij adviseert DUFAS integraal risicomanagement (*enterprise risk management*). Voor wat betreft de toezichthouders gaat het echter om risico's die de belangen van de beleggers kunnen raken.

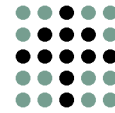
## 6.1. Het risicomanagementbeleid

### 6.1.1. Doelstelling en deliverables

Risicomanagementbeleid kent geen wettelijke definitie, maar kan worden omschreven als een uitleg van de algemene bedoelingen en het uiteindelijk nastreven, behouden, nemen of vermijden van risico's. Volgens de Nota van toelichting op het Bgfo moet uit het risicomanagementbeleid blijken dat de betreffende onderneming (a) zodanig georganiseerd is dat de integriteitrisico's zoveel mogelijk beperkt zijn en (b) dat de onderneming adequaat kan optreden tegen eventuele incidenten.<sup>33</sup> Deze weergave van de doelstelling is naar de mening van DUFAS een praktisch bruikbare formulering van de *deliverables* van de *principles based* geformuleerde wettelijke verplichtingen rond het risicomanagementbeleid. Het gaat dus om het risicomanagement van de gehele onderneming, dus in het geval van een beheerder van beleggingsinstellingen om zowel de beheerder als de beleggingsinstellingen.

### 6.1.2. Systematische analyse en integratie in bedrijfsprocessen

Een beleggingsinstelling en beleggingsonderneming moet ervoor zorgen dat er een systematische analyse van integriteitrisico's plaatsvindt,<sup>34</sup> en dat die zijn neerslag vindt in procedures en maatregelen.<sup>35</sup> De formulering kan de schijn wekken dat het hier uitsluitend gaat om integriteitrisico's, maar uit de wetsystematiek volgt dat het gaat om alle risico's die de integriteit van de bedrijfsvoering kunnen schaden. Volgens de toelichting moet men beschikken over "helder geformuleerde beleidsuitgangspunten ter beheersing van integriteitrisico's".<sup>36</sup> Volgens de Nota van toelichting gaat het bij een "systematische analyse" om het doorlichten van de eigen



organisatie om te bezien bij welke bedrijfsonderdelen er gevaar op integriteitrisico's bestaat. Naar aanleiding van deze analyse moet de beleggingsinstelling en beleggingsonderneming zijn beleid formuleren en moet hij dit indien nodig aanpassen om de integere uitoefening van het bedrijf blijvend te waarborgen.<sup>37</sup>

Volgens de Nota van toelichting is het verder van belang dat het beleid en de procedures en maatregelen ten aanzien van integriteit worden geïntegreerd in de bedrijfsprocessen en op die manier bijdragen aan een integriteitsbewuste bedrijfscultuur.<sup>38</sup> Hoewel dit laatste strikt genomen geen juridische verplichting is, beveelt DUFAS aan om de risicomangementprocedures en -maatregelen onderdeel te laten uitmaken van de AO/IC (de beschrijving van de processen en procedures van de bedrijfsvoering). Dit is namelijk een voor de hand liggende manier om te zorgen dat de inrichting van de bedrijfsvoering een beheerste en integere uitoefening van het bedrijf waarborgt.<sup>39</sup> Het risicomangementbeleid past echter strikt genomen niet goed in de AO/IC, omdat de AO/IC niet gaat over beleid maar over processen (die uiteraard wel voortvloeien uit het risicomangementbeleid).

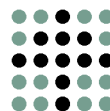
#### 6.1.3. Schriftelijke vastlegging

DUFAS beveelt aan dat het risicomangementbeleid wordt neergelegd in een apart document. Daarnaast moeten de daaruit voortvloeiende procedures en maatregelen ter beheersing van relevante risico's worden geïntegreerd in de bedrijfsprocessen.<sup>40</sup> De schriftelijke vastlegging is uitdrukkelijk verplicht voor wat betreft beleggingsondernemingen.<sup>41</sup> Voor beleggingsinstellingen herleidt de AFM dit uit artikel 4:14, Wft, omdat er een up-to-date en adequate beschrijving van de AO moet zijn.<sup>42</sup>

Met CESR<sup>43</sup> beveelt DUFAS (beheerders van) beleggingsinstellingen daarom aan om het risicomangementbeleid schriftelijk vast te leggen. Het lijkt DUFAS in de praktijk ook heel moeilijk om behoorlijk intern toezicht te organiseren op het risicomangement als het beleid terzake niet schriftelijk is vastgelegd. Op die vastlegging is het proportionaliteitsbeginsel van toepassing,<sup>44</sup> wat niet wil zeggen dat kleinere organisaties niets hoeven vast te leggen, slechts dat zij minder uitgebreid hoeven vast te leggen.

#### 6.1.4. Goedkeuring door de hoogste leiding van de onderneming

Om dezelfde reden is goedkeuring van het risicomangementbeleid door de hoogste ondernemingsleiding van belang. DUFAS beveelt dan ook aan dat de hoogste leiding van de onderneming het risicomangement beleidsdocument goedkeurt. Het lijkt DUFAS in de praktijk niet goed mogelijk om een behoorlijk intern toezicht te organiseren op het risicomangement, als de desbetreffende medewerkers niet weten wat er van hen verlangd wordt. DUFAS beveelt beleggingsinstellingen en beleggingsondernemingen dan ook aan om het risicomangementbeleid op een passend niveau te laten goedkeuren. Dat kan de directie van het fonds zijn maar ook de directie van de beheerder.



#### 6.1.5. Interne communicatie

Interne communicatie over het beleid, de procedures en de maatregelen aan alle relevante bedrijfsonderdelen is dan ook verplicht,<sup>45</sup> omdat integriteitsrisico's kunnen voortvloeien uit activiteiten, relaties en handelingen van bijna alle geledingen van beleggingsinstellingen en beleggingsondernemingen.<sup>46</sup> In de Nota van toelichting wordt overigens wel erkend dat het ene onderdeel van een onderneming wellicht een groter risico vormt dan het andere. Het is aan de beleggingsinstellingen en beleggingsondernemingen zelf om hier een juiste inschatting van te maken. In de Nota van toelichting wordt nog opgemerkt dat scholing of opleiding belangrijke instrumenten zijn om het bewustzijn met betrekking tot het integer handelen binnen de onderneming te vergroten.<sup>47</sup> DSI biedt hiervoor een aantal praktische hulpmiddelen.

#### 6.1.6. Implementatie en toetsing

Het beleid, de procedures en de maatregelen van beleggingsinstellingen en beleggingsondernemingen moeten ook worden uitgevoerd en systematisch worden getoetst,<sup>48</sup> en daarop moet "onafhankelijk toezicht"<sup>49</sup> worden gehouden.<sup>50</sup> De tekst van de bepaling maakt niet duidelijk door wie en waaraan dan moet worden getoetst, maar volgens de Nota van toelichting gaat het daarbij om de onderneming die toetst aan "de vigerende wet- en regelgeving".<sup>51</sup> Het is naar de mening van DUFAS goed voorstelbaar dat men van tijd tot tijd beziet of er nieuwe regels van kracht zijn geworden die om implementatie vragen. Gezien de frequentie van wijziging van Nederlandse regels met betrekking tot asset management beveelt DUFAS aan dat dit tenminste éénmaal per jaar geschiedt.

Naast toetsing aan de wettelijke verplichtingen is het naar de mening van DUFAS ook van belang om ook de risico-inventarisatie, de beoordeling van de risico's, de modellen etc. van tijd tot tijd opnieuw onder de loupe te nemen. Wat de juiste frequentie is, hangt af van de aard, omvang en complexiteit van de organisatie. DUFAS beveelt aan dat ook dit tenminste éénmaal per jaar geschiedt.<sup>52</sup>

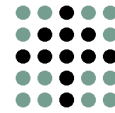
#### 6.1.7. Bijstelling van tekortkomingen of gebreken

Tenslotte moeten beleggingsinstellingen en beleggingsondernemingen beschikken over procedures die erin voorzien dat gesignaleerde tekortkomingen of gebreken met betrekking tot de integere uitoefening van het bedrijf tot een gepaste bijstelling leiden.<sup>53</sup> Risicomanagement helpt dus bij het verbeteren van de organisatie.

In het geval van beleggingsondernemingen (maar op dit moment nog niet beleggingsinstellingen) speelt de compliancefunctie<sup>54</sup> hier ook een rol. Met de inwerkingtreding van de UCITS IV richtlijn op 1 juli 2011 zal de compliancefunctie ook verplicht worden voor UCITS en waarschijnlijk ook voor alle non-UCITS.<sup>55</sup> Overigens betekent de verplichte compliancefunctie niet dat er ook een separate functionaris (compliance officer) moet worden benoemd.

#### 6.1.8. Inhoud risicomanagement document

Samenvattend zou het document inzake het risicomanagementbeleid voor beleg-



gingsinstellingen, zo adviseert CESR,<sup>56</sup> de volgende inhoud kunnen hebben:

- (a) identificatie en allocatie van de functies en verantwoordelijkheden van de verschillende onderdelen van het risicomanagementproces, zoals uitgewerkt in de risicomanagementfunctie;
- (b) beschrijving van de uitgangspunten en methoden voor de periodieke identificatie van de relevante risico's;
- (c) beschrijving van de randvoorwaarden van de interactie tussen de risicomanagementfunctie en de investment management functies om het risicoprofiel te beheersen en in overeenstemming te houden met het beleggingsbeleid (risicolimieten);
- (d) beschrijving van de rapportage arrangementen aan de toezichthouder en de hoogste leiding van de onderneming;
- (e) beschrijven van de technieken en gereedschappen die geschikt worden geacht voor het meten van de relevante risicofactoren die verbonden zijn met het beleggingsbeleid en de asset management stijl.

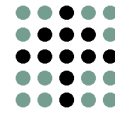
Daarnaast kan het document, teneinde het risicomanagement beter te plaatsen en in te kaderen, desgewenst (i) een toelichting geven over de reden(en) dat de organisatie risico's wil managen; (ii) een uitleg geven over de samenhang tussen de doelstelling van de organisatie en het risicomanagementbeleid; (iii) een toelichting op de wijze waarop risicomanagement belangenconflicten beheerst en (iv) de manier waarop de prestaties van risicomanagement worden gemeten.

#### 6.1.9. Risicobehandelingsplan

Risicobehandeling kan worden omschreven als het proces waarmee een risico wordt aangepast. ICAAP vereist de vastlegging door beleggingsondernemingen van een overzicht van alle materiële risico's, hun impact, kans en gehanteerde risicobeheersingsmaatregelen, met een toelichting. In dat kader moet in elk geval aandacht worden besteed aan de volgende risico's: het concentratierisico, krediet- en tegenpartijrisico, liquiditeitsrisico, marktrisico, operationeel risico, renterisico voortvloeiend uit niet-handelsactiviteiten, restrisico, securitisatierisico, verzekeringsrisico en de risico's die voortvloeien uit de macro-economische omgeving waarin de onderneming actief is en die verband houden met de stand van de conjunctuurcyclus.<sup>57</sup>

De wet vereist van beleggingsinstellingen wel de vastlegging in het prospectus van een overzicht van alle materiële risico's,<sup>58</sup> maar de lijst met risico's waaraan aandacht moet worden besteed verschilt van de elders in de wet genoemde risico's. Uit bijlage I blijkt dat deze risico's wel weer in wat andere gedaanten c.q. onder andere namen terugkomen in het risicomanagement.

Het gaat bij opname in het prospectus van de beleggingsinstelling om de materiële risico's, namelijk elk risico dat "van betekenis en relevant is in het licht van de gevolgen en de waarschijnlijkheid ervan". Deze beschrijving moet in het prospectus een korte en begrijpelijke uitleg te bevatten over ieder specifiek risico dat voortvloeit uit een gegeven beleggingsbeleid of dat verband houdt met specifieke voor de beleggingsinstelling relevante markten of beleggingen.<sup>59</sup> De wet vereist echter niet



van beleggingsinstellingen dat zij van de risico's die in het prospectus moeten worden genoemd de impact, kans en gehanteerde risicobeheersingmaatregelen schriftelijk vastleggen. Dat is wel vereist voor de risico's genoemd in bijlage I, voor zo ver zij materieel zijn.

DUFAS beveelt beleggingsinstellingen en beleggingsondernemingen aan om risicobehandelsmaatregelen op een passend niveau te laten goedkeuren: wanneer het bijvoorbeeld gaat om het imago of de reputatie van de onderneming, zou dat de hoogste leiding zijn, maar wanneer het bijvoorbeeld een computervirus betreft, kan dat beter worden overgelaten aan de leidinggevende inzake IT.

Zie voor een praktische uitwerking van het risicobehandelingsplan hoofdstuk 7.

## 6.2. De risicomangementfunctie

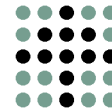
### 6.2.1. *Passende en proportionele invulling*

Bij beleggingsinstellingen moet de risicomangementfunctie, als het passend en proportioneel is in relatie tot de aard, omvang en complexiteit van de onderneming en de beleggingsinstellingen die hij beheert, hiërarchisch en functioneel onafhankelijk zijn van de operationele diensten.<sup>60</sup> Als dat niet passend en proportioneel is, adviseert CESR om er wel op te letten dat de onderneming kan aantonen dat er specifieke waarborgen zijn tegen belangenverstremming die een onafhankelijke uitoefening van de risicomangement activiteiten mogelijk maken.<sup>61</sup> Dergelijke waarborgen om belangenverstremming tegen te gaan moeten er volgens de Nederlandse wetgeving sowieso zijn,<sup>62</sup> en implementatie van de UCITS IV richtlijn per 1 juli 2011 zal deze eisen nog nader invullen.<sup>63</sup>

Met de "risicomangementfunctie" wordt in de wet- en regelgeving bedoeld degene die de beslissingen neemt en verantwoordelijk is inzake risicomangement, niet de medewerkers die ter zake slechts monitoren, rapporteren of adviseren. De risicomangement analyse- en adviestaken kunnen daarom als een staffunctie worden ingevuld onder verantwoordelijkheid van degene die beslissingen neemt en verantwoordelijk is inzake risicomangement, de "risicomangementfunctie". Bij kleinere of niet-complexe organisaties zal de risicomangementfunctie daarentegen veelal zijn ondergebracht bij het bestuur of één van de bestuurders. Binnen het bestuur beveelt DUFAS een zodanige functiescheiding aan dat het risico management en de beleggingen aan separate bestuurders toebedeeld zijn.

### 6.2.2. *Beloning risicomangementfunctie*

In het kader van de onafhankelijkheid van de risicomangementfunctie bij beleggingsinstellingen en beleggingsondernemingen let de toezichthouder ook op de wijze waarop de beloning van de risicomangementfunctie wordt bepaald. CESR adviseert dat het niet "waarschijnlijk" mag zijn dat de wijze van beloning de objectiviteit van de risicomangementfunctie in gevaar kan brengen.<sup>64</sup> De Nederlandse beleidsregels inzake beloning zijn concreter: variabele beloning voor hen mag slechts in beperkte mate afhankelijk zijn van commerciële resultaten en de commerciële lijnver-



antwoordelijke mag niet over de toekenning ervan gaan (maar er wel input voor leveren).<sup>65</sup> Dat wil niet zeggen dat variabele beloning voor de risicomanagementfunctie verboden is, integendeel, hij is toegestaan, maar “is afhankelijk van een passende verhouding van de prestaties van de medewerker, de afdeling en/of de onderneming als geheel”.<sup>66</sup>

### 6.2.3. Gezag van de risicomanagementfunctie

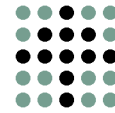
De risicomanagementfunctie moet bij beleggingsinstellingen over het nodige gezag, “de nodige autoriteit” beschikken en de nodige toegang hebben tot alle dienstige informatie om zijn taken te kunnen vervullen<sup>67</sup> (dit voorschrift geldt niet voor beleggingsondernemingen). Dit zou kunnen worden bewerkstelligd door (1) risicoeigenaren te benoemen die verantwoordelijkheid en bevoegdheid hebben bij het managen van risico’s en (2) duidelijk vast te leggen wie verantwoordelijk is om de elementen van het risicomanagement-raamwerk te onderhouden en waar nodig te verbeteren. Naar de mening van DUFAS volgt de bedoelde autoriteit uit bijvoorbeeld de onafhankelijke adviesfunctie van de risicomanagementfunctie, de bevoegdheid om toegang te hebben tot “alle dienstige informatie”, of uit de uitbestedingsovereenkomst, of uit de leidinggevende positie van de persoon die de risicomanagementfunctie uitoefent.

CESR adviseert dat de risicomanagementfunctie bij beleggingsinstellingen passende middelen dient te hebben en voldoende vakbekwaam en efficiënt moet zijn.<sup>68</sup> Deskundigheid van de dagelijksbeleidsbepalers van beleggingsinstellingen en beleggingsondernemingen is ook een wettelijke eis,<sup>69</sup> maar de wet bepaalt niet wanneer een risicomanagementfunctionaris voldoende deskundig is.

DUFAS is van mening dat de nodige deskundigheid in elk geval kan blijken uit de volgende genoten opleidingen en/of behaalde certificaten c.q. titels:

- Financial Risk Manager (FRM), een titel die men na het met succes afleggen van een toets van de Global Association of Risk Professionals (GARP) mag gebruiken.<sup>70</sup>
- Professional Risk Manager (PRM), een titel die men na het met succes afleggen van een toets van de Professional Risk Managers International Association (PRMIA) mag gebruiken.<sup>71</sup>
- Het Enterprise Risk Management programma van de Universiteit van Amsterdam;<sup>72</sup>
- Het Risk Management for Financial Institutions programma van de Vrije Universiteit;<sup>73</sup>
- Het Master of Science in Risk Management for Executives programma van het Amsterdam Institute of Finance;<sup>74</sup>

Daarnaast zijn er ook andere erkende opleidingen met vergelijkbare curriculae. Voorts kan de nodige deskundigheid ook blijken uit relevante werkervaring. Bij een kleine belegginginstelling c.q. een organisatie met weinig personeel zal werkervaring doorgaans de belangrijkste bron van deskundigheid zijn. Uiteraard kan deskundigheid, indien en voor zover nodig, ook extern worden ingehuurd.



Dit wil niet zeggen dat de persoon die met de risicomanagementfunctie is belast, zelf onder alle omstandigheden een daarvoor specifieke opleiding moet hebben genoten. Hij/zij kan zich uiteraard ook laten adviseren door een deskundige en hij/zij kan het risico management deels of geheel uitbesteden aan een deskundige buiten de eigen organisatie. Zie daarvoor paragraaf 6.4.

### 6.3. Taken van de risicomanagementfunctie

#### 6.3.1. Implementeren, beheren, adviseren en rapporteren

De taken van de risicomanagementfunctie zijn vanaf 1 juli 2011<sup>75</sup> voor wat betreft beleggingsinstellingen nauwkeuriger omschreven dan voorheen:

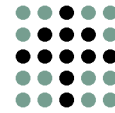
- (a) het implementeren van het risicomanagementbeleid en het risicobeheer;
- (b) het beheren van het risicolimietensysteem;
- (c) adviseren met betrekking tot het risicoprofiel;
- (d) op gezette tijden<sup>76</sup> rapporteren aan de hoogste leiding van de onderneming en (wanneer die bestaat) de toezichtfunctie,<sup>77</sup> (dat is afhankelijk van de structuur de directie/commissarissen, bewaarder of accountant). Die rapportage moet gaan over:
  - (i) de verhouding van het feitelijke risico tot het risicoprofiel van de beleggingsinstelling;
  - (ii) de naleving van de relevante risicolimietensystemen;
  - (iii) de deugdelijkheid en effectiviteit van de risicobeheerprocedure, waarbij met name moet worden aangegeven of passende maatregelen zijn genomen om eventuele onvolkomenheden te verhelpen.<sup>78</sup>

Dit betekent onder meer dat het niet per sé zo is dat de hoogste leiding van de onderneming en eventueel de toezichtfunctie het risicomanagement doet. Dat is echter wel een optie. Bij grotere, complexere organisaties verdient het concept van drie “lines of defence” de voorkeur: de uitvoerende lijn, de risicomanagementfunctie en tenslotte de toezichtfunctie. Bij kleinere of minder complexe organisaties is doorgaans geen ruimte voor een dergelijke taak- en functieverdeling en komt meer werk neer op de schouders van minder mensen, waardoor het voor de hand ligt dat een lid van de hoogste leiding van de onderneming verantwoordelijk is voor het risicomanagement.

Of de risicomanagementfunctie het beste zou kunnen rapporteren aan de toezichtfunctie, kan het beste worden beoordeeld aan de hand van factoren als omvang van de onderneming, expertise, complexiteit van de beleggingsstrategieën, het aantal fondsen c.q. cliënten en de omvang van de belegde activa.

#### 6.3.2. Beloningsbeleid

Daarnaast heeft de risicomanagementfunctie ook een taak in het beloningsbeleid van de beleggingsinstelling en beleggingsonderneming: het analyseren van de effecten van een variabele beloningsstructuur op het risicoprofiel van de onderneming en het bewaken van de beheersing daarvan.<sup>79</sup> De risicomanagementfunctie kan –



maar dat is niet wettelijk verplicht – het risicomanagement voorbereiden door bijvoorbeeld concepten voor de documentatie te maken<sup>80</sup> (maar dat kan uiteraard ook een ander doen).

De verplichtingen van beleggingsinstellingen en beleggingsondernemingen ten aanzien van het beloningsbeleid zijn te vinden in de *Principes voor beheerst beloningsbeleid* van de AFM en DNB van mei 2009, het Besluit Beheerst Beloningsbeleid<sup>81</sup> en de Beleidsregels inzake Beloningsbeleid<sup>82</sup> van DNB. Zodra de AIFM richtlijn wordt geïmplementeerd zullen soortgelijke regels vermoedelijk ook voor beleggingsinstellingen gaan gelden. Ook zullen de beloningsregels uit de Code Banken van de NVB hoogstwaarschijnlijk mutatis mutandis gaan gelden voor beleggingsinstellingen en beleggingsondernemingen. Tenslotte moet opgemerkt worden dat sedert 1 januari 2011 meer specifieke regels uit de *Regeling beheerst beloningsbeleid Wft 2011* gelden voor banken, verzekeraars en beleggingsondernemingen en hun dochtermaatschappijen.<sup>83</sup>

#### 6.3.3. Advies aan de leiding van de onderneming

De wet verplicht de risicomanagementfunctie niet om te adviseren<sup>84</sup> aan de hoogste leiding van de onderneming over de identificatie van alle relevante risico's. Naar de mening van DUFAS brengt de verplichting om te komen tot een systematische analyse van integriteitrisico's<sup>85</sup> mee dat dit wel een goede optie is. Zie voor de risico-inventarisatie verder bijlage I.

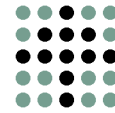
#### 6.3.4. Intrinsieke waardebeoordeling

CESR adviseert om de risicomanagementfunctie van de beleggingsinstelling te betrekken bij de intrinsieke waardebeoordeling. Zij zou het proces kunnen beoordelen (review) en indien nodig passende ondersteuning kunnen bieden bij het waarderingsproces met betrekking tot *exposures* aan activa die complexe evaluatie vereisen, zoals illiquide activa, gestructureerde producten en derivaten.<sup>86</sup> De risicomanagementfunctie zou volgens het advies van CESR ook grondig kunnen checken of bij het meten van de risico's van met name illiquide activa de risico-schattingen robuust genoeg zijn, door de gebruikte data te beoordelen. Om het waarderingsproces te begrijpen kan het nuttig zijn om de risicomanagementfunctie te laten deelnemen in het *Valuation Committee* van de onderneming – als dat er is.<sup>87</sup>

DUFAS beveelt aan dat de betrokkenheid van de risicomanagementfunctie, zeker in kleinere organisaties, niet nodig is. Wel moeten uiteraard de wettelijke regels omtrent IW-bepaling (zie bijlage 3) worden nageleefd.

## 6.4. Uitbesteding van de risicomanagementfunctie

De risicomanagementfunctie mag geheel of gedeeltelijk worden uitbesteed. De verantwoordelijkheid ervoor kan echter niet worden uitbesteed. Onder uitbesteding wordt kort gezegd verstaan het laten uitvoeren van werkzaamheden door derden.<sup>88</sup> Dit kan zowel bij grotere als bij kleinere organisaties een optie zijn. De beweegredenen kan bijvoorbeeld zijn harmonisatie van risicobeheer binnen de grotere groep van ondernemingen waartoe de individueel vermogensbeheerder of beheerder van



beleggingsinstellingen behoort, kosten / baten overwegingen, of het inhuren van vakkenis en/of capaciteit teneinde de functie in te vullen.

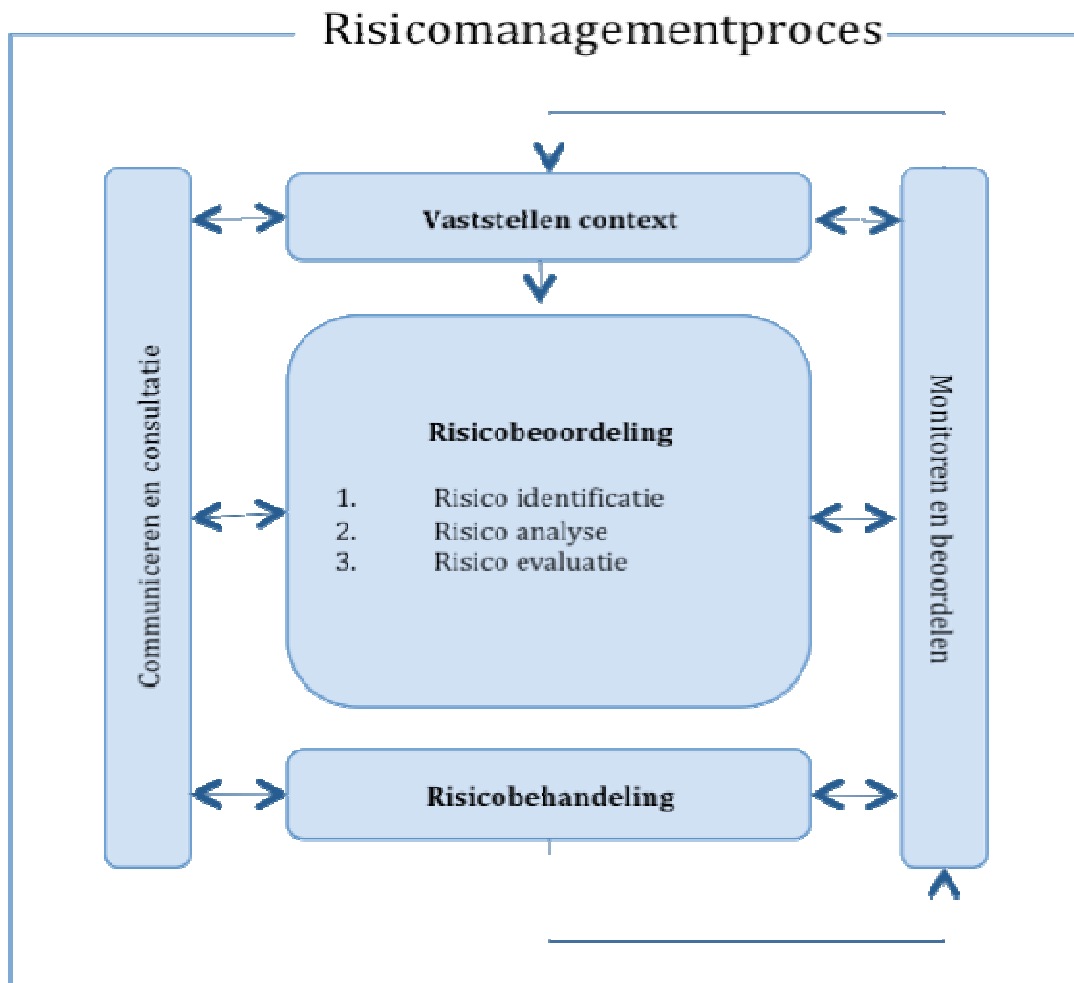
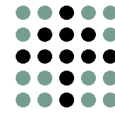
De wetgever stelt een hele reeks eisen aan de uitbesteding, niet alleen van risicomanagement maar van allerlei andere activiteiten ook. Deze regels kunnen worden beschouwd als de minimale invulling van de beheersing van het uitbestedingsrisico. De regels gelden zowel voor individueel vermogensbeheerders<sup>89</sup> als voor (beheerders van) beleggingsinstellingen,<sup>90</sup> en verschillen op een aantal punten van elkaar. Hiervoor zij verwezen naar een binnenkort te verschijnen handreiking uitbesteding van DUFAS.

Wanneer de wettelijke regels voor uitbesteding (van de risicomanagementfunctie) zijn nageleefd, is het uitbestedingsrisico in het algemeen naar de mening van DUFAS voldoende gereduceerd.

## 7. Het risicomanagementproces

Het begrip “risicomanagementproces” is niet wettelijk gedefinieerd. Het kan worden opgevat als het systematisch toepassen van beleidslijnen, procedures en werkwijze op de activiteiten met betrekking tot communicatie en het identificeren, analyseren, evalueren, behandelen monitoren en beoordelen van risico's. Risicomanagement kan worden begrepen als een proces: het geheel van acties gericht op (i) het identificeren en meten van de relevant risico's; (ii) het beoordelen van hun consistentie met het risicoprofiel; (iii) monitoren van de effectiviteit van de genomen maatregelen; en (iv) het nemen van maatregelen in geval van gebreken; (v) één en ander via de daarvoor aangewezen rapportage kanalen.<sup>91</sup>

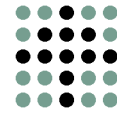
Het risicomanagementproces kan als volgt schematisch worden weergegeven:



### 7.1. Schriftelijke vastlegging

In verband met doeleinden van interne communicatie binnen de onderneming en in verband met het geheugen van de verantwoordelijke leidinggevenden in de onderneming acht DUFAS het verstandig dat ook het risicomanagementproces wordt gedocumenteerd. CESR adviseert dat ook.<sup>92</sup> DUFAS is van mening dat het risicomanagementproces deel uitmaakt van het risicomanagementbeleid. Dit beleid dient al schriftelijk te worden vastgelegd. DUFAS beveelt aan om dat document ook de titel “risicomanagementbeleid” te geven.

CESR adviseert dat de hoogste leiding van de onderneming het risicomanagementproces goedkeurt, periodiek beoordeelt en zo nodig herziet.<sup>93</sup> Dit omdat CESR van mening is dat zij verantwoordelijk moeten worden gehouden voor het opzetten en implementeren van een robuuste en diepgaande en algemeen verspreide risicocultuur in de onderneming.<sup>94</sup> DUFAS beveelt aan om dat éénmaal per jaar te doen (zie ook par. 6.1.6).



## 7.2. Vaststellen context

Met het vaststellen van de context wordt bedoeld dat het goed zou zijn om inzichtelijk te maken wat de doelstellingen van de organisatie zijn en met welke interne en externe variabele rekening gehouden moet worden bij het managen van risico's. Bij beleggingsinstellingen en beleggingsondernemingen zal het daarbij doorgaans in elk geval gaan om de volgende doelstellingen:

1. Beheerste en integere bedrijfsvoering
2. Naleven van wet- en regelgeving
3. Handelen in het belang van de beleggers
4. De doelstellingen uit het fondsprospectus.

Het leidt tot criteria aan de hand waarvan risico's worden beoordeeld en geven richting aan de wijze waarop risico's worden behandeld. De risicocriteria moeten in lijn zijn met het risicomanagementbeleid en ze moeten worden vastgesteld c.q. goedgekeurd aan het begin van het risicomanagementproces. Belangrijke risicocriteria zijn het risicoprofiel, de risicolimieten (en risiconiveau), en de risicorapportage (bijvoorbeeld aan de hand van een risicodashboard).

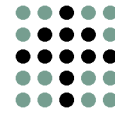
## 7.3. Risicoprofiel

Een risicoprofiel is een beschrijving van een verzameling risico's. Bij beleggingsondernemingen bestaan geen wettelijke verplichtingen met betrekking tot het risicoprofiel. Veel van hetgeen hieromtrent verplicht is gesteld voor beleggingsinstellingen zou echter naar de mening van DUFAS goed passen in een risicomanagementbeleid van een beleggingsonderneming en zou dan betrekking kunnen hebben op de modelportefeuilles (maar niet zozeer op de individuele cliëntportefeuilles).

Risico-identificatie, het proces waarmee risico's worden opgespoord, herkend en beschreven, is de noodzakelijke eerste fase van het samenstellen van een risicoprofiel. Hiervoor kan gebruik worden gemaakt van de risicobeschrijvingen in bijlage I. CESR adviseert de hoogste leiding van de onderneming het risicoprofiel van elke UCITS te laten goedkeuren.<sup>95</sup> Hierover zouden zij advies kunnen vragen aan de risicomanagementfunctie.<sup>96</sup> DUFAS is van mening dat dit betekent dat de hoogste leiding van de onderneming de structuur van het risicoprofiel en de top-level limieten zou moeten goedkeuren, maar niet de gehele set van gedetailleerde parameters en limieten. Die laatsten zouden kunnen worden goedgekeurd en gemanaged door de risicomanagementfunctie.

Bij latere wijzigingen zou deze hoogste leiding van de onderneming volgens het advies van CESR in elk geval moeten worden geïnformeerd. De risicomanagementprocedures moeten er dan voor zorgen dat het feitelijke risiconiveau consistent blijft binnen de grenzen van het risicoprofiel.<sup>97</sup> Elders adviseert CESR dat de hoogste ondernemingsleiding het beste advies kan vragen aan de risicomanagementfunctie over wijziging van het risicoprofiel.<sup>98</sup>

DUFAS beveelt aan dat de hoogste leiding van de onderneming vooral zou moeten worden geïnformeerd als het door hen goedgekeurde *overall* risicoprofiel waar-



schijnlijk zal worden doorbroken of waarschijnlijk niet meer passend zal zijn. Als de risicomanagementfunctie vervolgens rapporteert dat het feitelijk risiconiveau van de beleggingsinstelling niet overeenkomt met het ten doel gestelde risicoprofiel, moet de hoogste leiding van de onderneming passende maatregelen te nemen in het belang van de beleggers.<sup>99</sup>

Het risicoprofiel houdt volgens DUFAS verband met de risicobereidheid (*risk appetite*) van de beleggingsinstelling. Het risicoprofiel van een beleggingsinstelling zou, zo adviseert CESR, het niveau moeten weergeven van de geïdentificeerde relevante risico's die voortvloeien uit diens beleggingsstrategie, en tevens de interactie en concentratie van die risico's op het niveau van de beleggingsportefeuille.<sup>100</sup> Bij het samenstellen van het risicoprofiel beveelt DUFAS aan om ook rekening te houden met juridische en contractuele beperkingen (en eventuele andere interne beperkingen of limieten die de onderneming oplegt), met het universum en de technieken die gebruikt worden, de mate van tolerantie van leverage, het al dan niet gebruiken van derivaten, concentratie van instrumenten en liquiditeit.

#### 7.4. Risicolimieten

In verband met de verplichting om het risicomanagementbeleid vast te leggen<sup>101</sup> wil de wetgever in de Nota van toelichting dat de beleggingsonderneming (maar niet beleggingsinstelling) op instellingsbrede basis limieten stelt aan de te nemen risico's en ze op overschrijdingen bewaakt. Limieten die nader zijn uitgewerkt naar werkzaamheden of bedrijfsonderdelen moeten consistent zijn met de limieten die op het niveau van de onderneming zijn vastgesteld. Ook hier geldt weer het proportionaliteitsbeginsel: de procedures en maatregelen moeten worden afgestemd op de aard, omvang en complexiteit van de financiële onderneming en er moet rekening worden gehouden met het soort bedrijf en de risico's die daarbij worden gelopen.<sup>102</sup>

DUFAS adviseert verder dat de beheerder voor elke beleggingsinstelling indien opportuun en praktisch mogelijk een systeem van risicolimieten inricht betreffende de maatregelen die gebruikt worden om de relevante risico's te monitoren en te beheersen, teneinde binnen het goedgekeurde risicoprofiel te blijven.<sup>103</sup> Deze risicolimieten zouden het beste goedgekeurd kunnen worden door de hoogste leiding van de onderneming.<sup>104</sup>

Het systeem van risicolimieten zou, zo adviseert CESR, het beste consistent kunnen zijn met het beleggingsbeleid van de beleggingsinstelling en zowel juridische als contractuele limieten omvatten, naast andere interne limieten die de onderneming stelt.<sup>105</sup> Het limietensysteem zou volgens CESR het beste kunnen refereren aan het risicoprofiel van de specifieke beleggingsinstelling en passende limieten stellen voor alle potentieel relevante risicofactoren. Dat wil zeggen dat het alle risico's moet bestrijken waar een limiet aan kan worden gesteld en rekening moet houden met de interactie tussen die risico's.<sup>106</sup>

Bij interne limieten kan gedacht worden aan maximale exposure op bepaalde tegenpartijen, beleggingsrestricties (van de UCITS of in het prospectus), *Value at Risk*



gegevens, tracking error data, etc.

De wet stelt geen concrete eisen aan het risicolimietsysteem. In verband met doeleinden van interne communicatie binnen de beleggingsinstelling en beleggingsonderneming en de AO/IC beveelt DUFAS aan dat het risicolimietsysteem wordt gedocumenteerd. CESR adviseert dat ook.<sup>107</sup> Dat impliceert dat wanneer vastgestelde limieten worden overschreden, de genomen actie wordt geregistreerd.

## 7.5. Risicoweging

Bij het wegen van risico's is het belangrijk dat betrokkenen een eenduidig beeld hebben van de begrippen kans (waarschijnlijkheid) en impact (gevolg). Bij het verduidelijken van kansen kan een schaalverdeling (bijv. 5 puntschaal) worden gebruikt die inzichtelijk gemaakt kan worden aan de hand van de dimensie van de kans, de frequentie van het optreden en een absoluut bedrag (of percentage). Dit kan als volgt geïllustreerd worden.

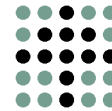
### Kans

Schaal	1	2	3	4	5
<b>Dimensie</b>	Zeer onwaarschijnlijk	Onwaarschijnlijk	Waarschijnlijk	Meer dan waarschijnlijk	Zeer waarschijnlijk
<b>Frequentie</b>	Minder dan ..x per jaar	... x per jaar	... tot .. x per jaar	... tot .. x per jaar	... tot .. x per jaar
<b>Absolute bedrag of percentage</b>	0-1%	1-10%	10-25%	25-50%	50-100%

Een kleine kans wil niet zeggen dat het risico kan worden genegeerd. Een kleine kans kan worden gebruikt als leidraad in de prioritering van beheersingsmaatregelen. Impact is evenwel veel beter te beoordelen en daarmee een beter sturingsmiddel dan kans. Voor impact geldt eveneens dat een schaalverdeling kan worden aangebracht. Dit kan als volgt worden geïllustreerd.

### Impact

Schaal	1	2	3	4	5
<b>Consequentie</b>	Verwaarloosbaar	Klein	Matig	Groot	Zeer groot
<b>Regulering</b>	Licht overtreding van wetgeving die intern kan worden opgelost en waarbij geen belegger is benadeeld.	...	...	...	Sancties door externe toezichthouder
<b>Integriteit</b>	Handeling van medewerker die leidt tot aantekening in personeelsdossier	...	...	...	Inbreuk op integriteit van de organisatie die leidt tot ontslag van betrokkenen. Beleggers benadeeld.
<b>Reputatie</b>	Niet verwijtbare	...	...	...	Organisatie komt



	gebeurtenis komt in vakpers. Sprake van immateriële schade.				negatief in de pers door toerekenbare fout die hebben geleid tot (grote) schade bij betrokkenen (bijv. beleggend publiek of organisatie zelf).
<b>Financieel (€)</b>					

Eveneens moet worden bepaald het tijdbestek waarbinnen de kans of de impact zich openbaart.

### 7.6. Risicocategorieën (risico-dashboard).

Het rapporteren van risico's kan op grond van het proportionaliteitsbeginsel zowel geaggregeerd als in detail plaatsvinden. Om eenduidigheid en consistentie te waarborgen kan men overwegen om te verduidelijken op welke wijze individuele gebeurtenissen en risico's geaggregeerd worden naar eenduidige risicocategorieën. De lijst met risico's in bijlage I kan hier behulpzaam bij zijn. Terwijl de wetgever wel bepaalde risico's benoemt en sommige definieert, wordt er aan risicocategorisering geen eisen gesteld.

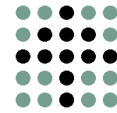
#### Financiële risico's

<p><b>Marktrisico</b></p> <ul style="list-style-type: none"> <li>• Concentratierisico</li> <li>• Derivatennisico</li> <li>• Leverage risico</li> <li>• Valutarisico</li> </ul>	<p><b>Kredietrisico</b></p> <ul style="list-style-type: none"> <li>• Tegenpartijrisico</li> <li>• Faillissementsrisico</li> <li>• Securities lending risico</li> <li>• Concentratierisico</li> </ul>	<p><b>Liquiditeitsrisico</b></p>
--	--	----------------------------------

#### Niet-financiële risico's

<p><b>Operationeel risico</b></p> <ul style="list-style-type: none"> <li>• Uitbestedingsrisico</li> <li>• Juridisch risico</li> <li>• Modelrisico</li> <li>• Onderpandrisico</li> </ul>	<p><b>Integriteitsrisico</b></p> <ul style="list-style-type: none"> <li>• Risico van belangenverstrengeling</li> <li>• Personeelsrisico</li> <li>• Witwassen en risico van terrorismebestrijding</li> <li>• Afwikkelingsrisico</li> </ul>
---	---

Er zijn veel verschillende opvattingen over hoe risico's het beste kunnen worden ingedeeld en gecategoriseerd. Risicocategorieën kunnen worden ingedeeld naar niveau (strategisch, tactisch en operationeel) of naar herkomst/doel (omgeving, proces en beslissingsinformatie). Daarbinnen kunnen deelgebieden worden onderkend.



Een eenvoudige indeling van de risico's die de wetgeving noemt (zie bijlage I) zou ook volgens bijgaand schema kunnen.

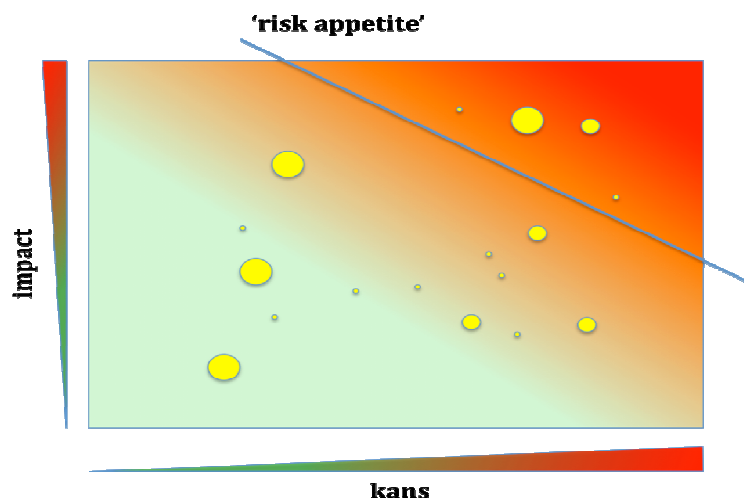
### 7.7. Risicobeoordeling

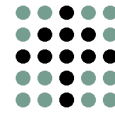
Het begrip risicobeoordeling is niet wettelijk gedefinieerd, maar kan worden omschreven als het gehele proces van risico-identificatie, risicoanalyse en risico-evaluatie. Het doel van de processen/werkzaamheden is om een overzicht te krijgen van risico's (en kansen) die van invloed zijn op het behalen van de doelstellingen (zowel wettelijk opgelegde doelstellingen (integriteit, solvabiliteit etc.) als organisatiedoelstellingen). De organisatie mag zelf bepalen op welke wijze de risico's worden geïdentificeerd waarbij DUFAS adviseert dat gebruik wordt gemaakt van actuele informatie die waar nodig en mogelijk is voorzien van voldoende achtergrondinformatie. Ook voor de risicobeoordeling geldt het proportionaliteitsbeginsel.

Het analyseren van de geïdentificeerde risico's richt zich onder meer op de kans en de impact van risico's. Een goede analyse zorgt ervoor dat het inzicht in een risico wordt verbeterd zodat ook inzicht komt in de factoren die van invloed zijn op de kans en impact. Tevens zal beoordeeld moeten worden of gebeurtenissen meerdere gevolgen kan hebben en meerdere doelstellingen kan beïnvloeden. Bij het analyseren adviseert DUFAS om zoveel mogelijk uitgaan van de bestaande beheersmaatregelen. Veelal wordt gesproken over netto risico's, risico's die al zijn beïnvloed door beheersmaatregelen.

Het evalueren van de risico's is bedoeld om te bepalen of risicobehandeling nodig is (zijn risico's toegestaan, tolereerbaar?). Hierbij dient onder meer te worden uitgegaan van het risicoprofiel van de organisatie, eisen opgelegd door wet- en regelgeving en de risicolimieten.

De uitkomsten van de risicobeoordeling zullen in ieder geval op een op geaggregeerd niveau, maar indien nodig ook op een meer gedetailleerd niveau inzichtelijk moeten worden gemaakt.





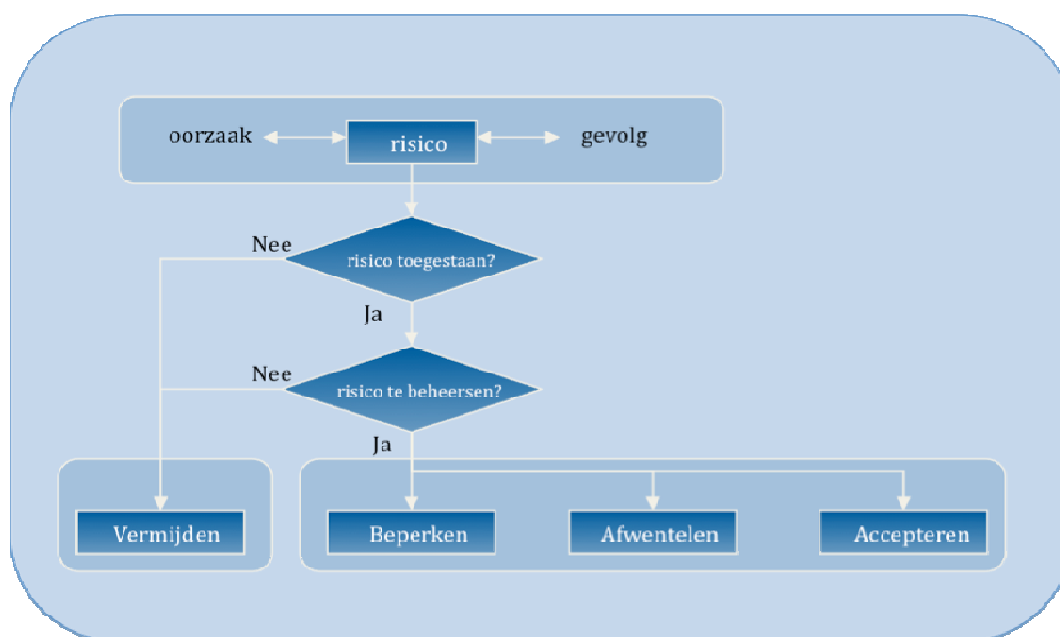
De presentatie van de uitkomsten kan gebeuren overeenkomstig de hierboven beschreven risicoweging en risicocategorieën (maar men mag uiteraard ook een eigen risico-indeling en eigen definities gebruiken). Tevens moet duidelijk zijn hoe de uitkomsten zich verhouden tot het risicoprofiel. Dat vraagt vaak om een geconcretiseerde *'risk appetite'*, ofwel risicobereidheid, die weergegeven moeten worden zodat inzichtelijk is welke risico's zich buiten het risicoprofiel begeven en behandeld moeten worden. Ook adviseert DUFAS om de ontwikkelingsrichting van risico's weer te geven zodat het monitoring plan rekening kan houden met risico's die wellicht op korte termijn onaanvaardbaar worden.

Het bepalen van de risicobereidheid is een taak voor de hoogste leiding van de onderneming en is gerelateerd aan de strategie en doelstellingen van de organisatie. Bij het bepalen van de risicobereidheid zullen diverse onderwerpen betrokken moeten worden, zoals solvabiliteit, liquiditeit, resultaten (en volatiliteit), credit rating, de reputatie, nieuwe producten(fondsen), klantgroepen, distributie, verdienmodel, overnames, corporate governance en naleving wet- en regelgeving.

De bij de risico-inventarisatie en beoordeling gesignaleerde (deel) risico's worden afgezet tegen de risicobereidheid voor de betreffende risico's. Dit kan zowel per risico, risicocategorie of op een hoger aggregatieniveau worden weergegeven. In de figuur hierboven zijn de verschillende risico's schematisch weergegeven afgezet tegen de kans en de impact die deze risico's hebben op een doelstelling. De weergegeven risicobereidheid geeft weer tot aan welk niveau de risico's acceptabel zijn, dus zodanig zijn dat de doelstellingen waarschijnlijk kunnen worden gerealiseerd. De verwachte ontwikkeling van een specifiek risico kan worden weergegeven door grote of kleinere cirkels.

## 7.8. Risicobehandeling

De risicobehandeling moet ertoe leiden dat de uitkomsten van de risicobeoordelingen structureel worden behandeld zodat, indien nodig, het risico wordt gewijzigd en binnen tolereerbare grenzen wordt gebracht dan wel wordt vermeden. Het proces dat weergeeft welke opties voor risicobehandeling het meest geschikt is, is onderstaand schematisch weergegeven.



Bij het bepalen van de behandelstrategie adviseert DUFAS dat een afweging wordt gemaakt tussen de kosten van de strategie en de voordelen die het oplevert. Hierbij moet wel rekening worden gehouden met de minimale eisen die voortvloeien uit wet- en regelgeving.

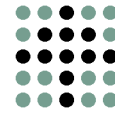
**Behandelstrategieën**

Behandelstrategie	Te nemen acties (kernbegrippen)
Vermijden	Beëindigen, beveiligen, elimineren, afstand bewaren, verbieden, stoppen
Beperken	Behandelen, verspreiden, controleren, diversificeren, verdelen
Afwentelen	Verzekeren, herverzekeren, compenseren (hedgen)
Accepteren	Nemen, toewijzen, verlengen, reorganiseren, prijzen, arbitrerende, heronderhandelen, beïnvloeden

De risicobehandeling is een cyclisch proces waarbij ook na aanpassingen in de beheersmaatregelen beoordeeld en gemonitord moet worden of risico's binnen acceptabele niveaus blijven en als dit niet het geval is, moet worden bepaald welke acties aanvullend getroffen moeten worden.

**7.9. Risicomanagement en het beleggingsproces**

De portfolio manager is verantwoordelijk voor het nemen van beleggingsbeslissingen in overeenstemming met het systeem van risicolimieten. Het meten van de bijbehorende risico's en het monitoren van de risicolimieten is een taak van de risicomanagementfunctie. Het risicomanagementproces opereert dus parallel aan en is intrinsiek gebonden aan het beleggingsproces. Om het proces effectief te laten functioneren beveelt DUFAS aan dat de onderneming er -- indien het proportionaliteitsbeginsel daartoe noopt -- voor zorgt dat communicatiekanalen bestaan en regelmatig gebruikt worden tussen de risicomanagementfunctie en de portfolio manager. Dat impliceert, zo adviseert CESR<sup>108</sup> een voortdurend, dynamisch proces, in



plaats van louter periodieke beoordelingen.

### 7.10. Monitoren en beoordelen

Het monitoren en beoordelen van het risicomanagementproces is erop gericht om vast te stellen dat beheersmaatregelen effectief zijn, (nieuwe) gebeurtenissen (incidenten, trends, veranderingen in interne en externe omgeving etc.) tijdig worden beoordeeld op relevantie (en leiden tot de noodzakelijke aanvullende acties) en eventueel nieuwe risico's te identificeren.

Uit het raamwerk en de beschrijving van de risicomanagementfunctie moet blijken wie verantwoordelijk is voor het monitoren en beoordelen. Welke werkzaamheden moeten worden uitgevoerd ten behoeve van het monitoren en beoordelen van het proces verschilt per organisatie.

Ook hier geldt het proportionaliteitsbeginsel.<sup>109</sup> De werkzaamheden kunnen een combinatie zijn tussen onder meer het verrichten van eigen analyses, het gebruik maken van cijfermatige analyses, rapporten over risicolimieten (geoorloofde en ongeoorloofde overschrijdingen), verrichten van deelwaarnemingen (operationele risico's/performance), portfoliorapporten etc. DUFAS is het ermee eens dat het risicomanagementproces een continue proces is, maar wil waarschuwen voor een misverstand: het betekent niet dat met de hoogst mogelijke frequentie moet worden gemeten en beoordeeld. Het risicomanagementproces moet de onderneming *in staat stellen* "to monitor and measure at any time the risk...".<sup>110</sup> Dat het proces het mogelijk maakt om op elk moment te kunnen meten, betekent echter nog niet dat ook continu moet worden gemeten. DUFAS adviseert de onderneming om de meetfrequentie risicogeorieënterd te bepalen.

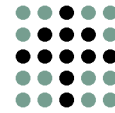
De resultaten van het monitoren en beoordelen moeten worden vastgelegd en gerapporteerd. In het risicomanagementbeleid zal moeten zijn bepaald met welke frequentie en aan wie moet worden gerapporteerd.

### 7.11. Incidentenregister

Een belangrijke bouwsteen van de monitoring en rapportage van het risico management is het incidentenregister. Dit is wettelijk verplicht.

Een (beheerder van een) beleggingsinstelling en/of een beleggingsonderneming moet beschikken over procedures en maatregelen met betrekking tot de omgang met en vastlegging van incidenten,<sup>111</sup> moet naar aanleiding van een incident maatregelen nemen die zijn gericht op het beheersen van de opgetreden risico's en het voorkomen van herhaling,<sup>112</sup> en moet de Autoriteit Financiële Markten onverwijld informeren omtrent incidenten.<sup>113</sup>

Het begrip "incident" wordt gedefinieerd als een "gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van een financiële onderneming"<sup>114</sup> De Nota van toelichting beperkt dit nog en spreekt van incidenten die "ernstige gevolgen hebben voor de integere uitoefening van het bedrijf en



daarmee (...) het vertrouwen in de financiële onderneming of de financiële markten als geheel schaden”.<sup>115</sup>

Volgens de Nota van toelichting moet worden voorkomen dat (beheerders van) beleggingsinstellingen en/of beleggingsondernemingen betrokken raken bij strafbare feiten of anderszins gedragingen (handelen of nalaten) verrichten die ingaan tegen hetgeen in het maatschappelijk verkeer betamelijk wordt geacht.<sup>116</sup> De toelichting verwijst met de zinsnede “hetgeen in het maatschappelijk verkeer betamelijk wordt geacht” naar de civielrechtelijke onrechtmatige daad. Naar de mening van DUFAS gaat het hier daarom om alles dat de wet verbiedt, of het nu strafrecht, civiel recht of administratief recht (inclusief belastingrecht) betreft. Maar opname in het wettelijk vereiste incidentenregister wordt pas vereist indien sprake is van een incident dat een “ernstig gevaar vormt voor de integere uitoefening van het bedrijf”.

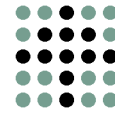
Daarbij moet worden bedacht dat de combinatie van de persoon en het feit gezamenlijk bepaalt of het om een “incidentenregisterwaardig” feit gaat. Volgens de Nota van toelichting maakt het namelijk niet uit door wie een dergelijke handeling wordt verricht. Het kan hierbij gaan om gedragingen van personeelsleden, bestuurders, personen die onderdeel zijn van het orgaan dat is belast met het toezicht op het beleid en de algemene gang van zaken van de financiële onderneming of van natuurlijke of rechtspersonen die werkzaamheden verrichten ten behoeve van de betrokken onderneming.<sup>117</sup>

## 7.12. De rol van de interne of externe accountant

Op dit moment is er geen formeel wettelijke rol voor de externe accountant om zich uit te spreken over risk management anders dan de algemene werkzaamheden die de accountants in het kader van de controle van de jaarrekening verricht (kennis nemen van de interne organisatie op relevante onderdelen, bespreken van interne beheersingsmaatregelen, eventueel rapporteren aan management en toezichthoudend orgaan over de bevindingen etc.).

De hoogste leiding van de onderneming moet ervoor zorgen dat alle elementen van het risicomanagement proces onderworpen zijn aan een passende review.<sup>118</sup> Zo'n review kan intern worden uitgevoerd, bijvoorbeeld door een interne accountant-functie en/of door externe accountants. Hierbij kan gedacht worden aan de volgende werkzaamheden:

- beoordelen van de inrichting van het risicobeheersingssysteem op de onderdelen:
  - governance en organisatie;
  - identificeren en meten van risico's;
  - monitoringssystematiek en rapportage;
- beoordelen van de risicomanagement rapportages en kennisnemen van eventuele notulen van risicocommittees en beoordelen of aan eventuele tekortkomingen c.q. bevindingen voldoende follow-up is gegeven.



## Bijlage I: Risico inventarisatie

Deze bijlage bevat alle risico's waar de wet- en regelgever gewag van maakt. Daarbij wordt tevens aandacht besteed aan de lijst van risico's waaraan in het prospectus van een beleggingsinstelling aandacht moet worden besteed.<sup>119</sup>

De wetgever brengt zelf geen classificatie aan en definieert de meeste risicocategorieën ook niet. Dit kan de (beheerder van een) beleggingsinstelling en/of een beleggingsonderneming uiteraard wel doen. Wie deze lijst van risico's doorneemt zal overlap constateren. De lijst is dan ook alleen maar een hulpmiddel en niet directief bedoeld, zodat risico's anders geordend en genoemd mogen worden. Er is ook overlap mogelijk in de sfeer van risico-reducerende maatregelen; het is denkbaar dat één maatregel meerdere risico's adequaat reduceert.

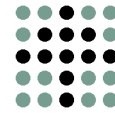
De financiële toezichtwetgeving beschrijft een groot aantal risico's en geeft ook voorschriften omtrent het risicomanagement ten aanzien van een aantal specifieke risico's. De beleggingsinstelling en beleggingsonderneming zal zich derhalve moeten afvragen of die risico's ook spelen in zijn organisatie en indien dat niet het geval is dat moeten motiveren. Daarnaast moeten de wettelijke verplichtingen uiteraard worden nagekomen als zij van toepassing zijn, ongeacht de vraag of het naar het inzicht van de beleggingsinstelling of beleggingsonderneming om een reëel risico gaat.

### I. Marktrisico

Marktrisico wordt gewoonlijk omschreven als het risico van fluctuaties in de marktwaarde van financiële instrumenten, die in de tijd kan variëren (zgn. clusters van volatiliteit) als gevolg van verschillende marktomstandigheden.<sup>120</sup> In het kader van ICAAP gaat het hier bijvoorbeeld om prijsvolatiliteit, marktliquiditeit, concentratie en correlatie.<sup>121</sup> Het marktrisico omvat het prijsrisico, het renterisico en het valutarisico.<sup>122</sup>

In het geval van beleggingsinstellingen geeft de wet gedetailleerde regels voor het berekenen van het marktrisico.<sup>123</sup> Dit risico moet, indien van toepassing, tevens in het prospectus worden vermeld.<sup>124</sup> In het prospectus moet ook, indien van toepassing, worden vermeld het sterk verwante “rendementsrisico”, dat wordt gedefinieerd als “mede omvattende het feit dat het risico kan variëren op grond van de keuzes die mogelijk zijn op grond van het beleggingsbeleid, alsmede het bestaan of ontbreken van, dan wel de beperkingen op eventuele waarborgen van derden”.<sup>125</sup> Tevens verwant zijn de “risico's voor het vermogen, met inbegrip van het potentiële risico van erosie als gevolg van intrekkingen van rechten van deelneming en winstuitkeringen die hoger zijn dan het beleggingsrendement”, die indien van toepassing ook in het prospectus moeten worden vermeld.<sup>126</sup> Tenslotte is nog verwant aan het marktrisico het inflatierisico,<sup>127</sup> dat ook, indien van toepassing, moet worden vermeld in het prospectus.<sup>128</sup>

Het marktrisico kan zich naast financiële instrumenten ook voordoen bij onroerend goed, commodities, etc.



### 1.1. Concentratierisico

Het concentratierisico is bij belegginginstellingen het risico dat is verbonden aan een grote concentratie van de beleggingen in bepaalde soorten of op bepaalde markten, moet indien van toepassing, in het prospectus worden vermeld.<sup>129</sup> Concentratierisico wordt door de prudentiële regels die door DNB worden gehandhaafd, gedefinieerd als een onderdeel van het marktrisico en is als zodanig ook een ander risico. Zie daarvoor punt 2.3 van deze bijlage.

Bij UCITS zijn er wettelijke voorschriften voor in de vorm van de beleggingsrestricties. Voor non-UCITS zijn die beleggingsrestricties er niet, maar is het wel van belang dat men zich bewust is van het concentratierisico en dat men heeft nagedacht over wat er gedaan moet worden indien dit risico zich voordoet.

### 1.2. Derivatennisico

Derivaten worden meestal afgesloten om het marktrisico af te dekken. Een derivaat heeft meestal niet precies dezelfde kenmerken als de onderliggende waarde. Een transactie in derivaten kan onderpand vereisen als de positie verlies oplevert. Derivaten worden vaak niet op de beurs verhandeld maar *over the counter* (OTC). OTC-derivaten zijn soms minder goed verhandelbaar dan beursgenoteerde derivaten. Bovendien creëert een onderhandse transactie tegenpartijrisico.

Mogelijke risicoreductiemaatregelen zijn:

- Expliciteer beleid voor het gebruik van derivaten en benoem daarin de doelen, het type instrumenten, de toegestane complexiteit, de tegenpartijen en de omvang.
- Houd bij het liquiditeitsbeheer rekening met de gevolgen. Abrupte koersveranderingen kunnen de behoefte aan onderpand en de behoefte aan kasgeld vergroten wanneer derivatenposities tot grote verliezen of kasbetalingen leiden.
- Zorg voor inzichtelijke rapportages over strategische derivatenposities en het effect op balansrisico, beleggingsrisico en liquiditeitsrisico in extreme marktomstandigheden. Rapporteer ook over spreiding van tegenpartijrisico.

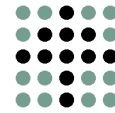
### 1.3. Leverage risico

Ook het *leverage* risico heeft te maken met het marktrisico. Leverage van beleggingen biedt een grotere blootstelling aan winst of verlies op dezelfde hoeveelheid belegd vermogen, zodat het potentiële verlies ook groter wordt. In extreme gevallen kan een schuld overblijven.

Indien de beleggingsinstelling belegt met (namens of voor rekening en risico van de deelnemers) geleend geld moet daar over een aantal zaken in het prospectus worden vermeldt.<sup>130</sup>

Mogelijke risicoreductiemaatregelen zijn:

- Het vaststellen van voorwaarden voor beleggingen en producten met (indirecte) leverage, en in welke mate zijn ze toegestaan. Toets de mandaten voor het



vermogensbeheer aan deze uitgangspunten.

- Houd bij de beoordeling van het risicoprofiel van de beleggingsportefeuille ook rekening met economische leverage. De scheiding tussen financiële leverage en economische leverage is niet absoluut. Een aandeel in een onderneming die met veel schuld is gefinancierd kan hetzelfde risicoprofiel hebben als een deels met geleend geld gekocht aandeel in een onderneming zonder vreemd vermogen.

#### 1.4. Valutarisico

Valutarisico is het risico dat de waarde van een belegging wordt beïnvloed door wisselkoersschommelingen. Dit risico moet, indien van toepassing, in het prospectus worden vermeld.<sup>131</sup>

## 2. Kredietrisico

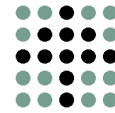
Bij kredietrisico gaat het om de bestaande of toekomstige bedreiging van vermogen en resultaat van de beleggingsinstelling en beleggingsonderneming als gevolg van het niet nakomen van een financiële of andere contractuele verplichting door de tegenpartij, met inbegrip van de mogelijkheid van beperkingen of belemmeringen bij het overmaken van betalingen vanuit het buitenland.<sup>132</sup>

### 2.1. Tegenpartijrisico en faillissementsrisico

Dit risico speelt een rol bij zgn. OTC transacties: de onderneming achter de onderliggende instrumenten kan bijvoorbeeld failliet gaan, zelfs wanneer dat een financiële onderneming is die onder prudentieel toezicht staat. Tegenpartijrisico kan ook een rol spelen bij structured products, maar die kunnen ook beursgenoteerd zijn, in welk geval een dreigende déconfiture van de onderneming meestal wordt beschouwd als marktrisico.

In het geval van UCITS-beleggingsinstellingen<sup>133</sup> geeft de wet gedetailleerde regels voor het berekenen van het tegenpartijrisico.<sup>134</sup> Het tegenpartijrisico wordt daarbij omschreven als het “maximale potentiële verlies voor de beleggingsinstelling wanneer de tegenpartij in gebreke blijft”.<sup>135</sup> Hoewel de hier genoemde berekeningsregels niet gelden voor niet-UCITS is het voor elke beleggingsinstelling en beleggingsonderneming van belang om te beoordelen of er zich in zijn organisatie dergelijke risico’s voordoen. Dit kan het geval zijn bij custodian banks, clearinginstellingen en dergelijke maar ook bij andere belangrijke toeleveranciers, bijvoorbeeld inzake software en ook bij de beleggingen zelf. Ook is het van belang te bezien of een samenloop van faillissementen van enkele van hen nog aanvullende risico’s behelzen (een concentratierisico). Dit risico moet ook in het prospectus worden vermeld.<sup>136</sup>

Tegenpartijrisico kan tevens een rol spelen bij bewaring van financiële instrumenten. Dit specifieke tegenpartijrisico moet, indien van toepassing, ook in het prospectus worden vermeld. Het wordt dan gedefinieerd als “het risico van verlies van in bewaring gegeven activa als gevolg van insolventie, nalatigheid of frauduleuze handelingen van de bewaarnemer of van een onderbewaarnemer”.<sup>137</sup>



Daarnaast moet een sterk verwant risico, indien van toepassing, ook in het prospectus van een beleggingsinstelling worden vermeldt, namelijk “de afhankelijkheid van de prestaties van een aanbieder of een garantieggever, indien de belegging in het product een rechtstreekse belegging bij een aanbieder inhoudt in plaats van een belegging die door de aanbieder worden [sic!] aangehouden”.<sup>138</sup>

Mogelijke maatregelen ter mitigering van het risico zijn (1) het vragen van onderpand, (2) spreiding, (3) goede uitbestedingscontracten, (4) due diligence van tegenpartijen, (5) eisen m.b.t. bijvoorbeeld kredietwaardigheid aan tegenpartijen waaraan wordt uitbesteed, (6), limieten bij beleggingen.

## 2.2. *Securities lending risk*

De risico's van securities lending zijn (1) het risico dat de lener de stukken niet terugbetaalt (kredietrisico), of (2) dat hij dat geheel of gedeeltelijk later dan afgesproken doet (liquiditeitsrisico), (3) het risico dat de uitleenvoorwaarden door zich ontwikkelende marktomstandigheden ongunstiger worden (marktrisico), (4) een faillissement van de lener kan de uitlener opzadelen met een ongedekte marktpositie of een marktpositie waarop hij ongerealiseerde winsten moet laten schieten (tegenpartijrisico), (5) bij cash als onderpand bestaat het risico dat ofwel de termijn of het rentepercentage van de lening niet overeenkomt met dat van de cash (renterisico), of (6) het risico dat de bewaarder van de effecten failliet gaat, dat daar fouten worden gemaakt of fraude wordt gepleegd (bewaarder risico).<sup>139</sup>

Indien de beleggingsinstelling financiële instrumenten in- of uitleent, moet daar over een aantal zaken in het prospectus worden vermeld.<sup>140</sup>

Mogelijke risicoreductiemaatregelen zijn:

- Laat periodiek (minimaal maandelijks) onafhankelijk vaststellen wat de exposure is op elk van de tegenpartijen, in welke richting deze zich beweegt en welke zekerheden hiervoor in de plaats geboden worden.
- Vraag onderpand.

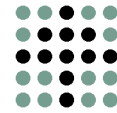
## 2.3. *Concentratierisico*

Onder concentratierisico wordt verstaan de risico's die voortvloeien uit vorderingen op wederpartijen, groepen van verbonden wederpartijen en wederpartijen van dezelfde economische sector of geografische regio, dan wel uit dezelfde activiteit of grondstof, de toepassing van technieken voor de vermindering van het kredietrisico, en met name grote indirecte kredietrisico's.<sup>141</sup>

DUFAS gaat ervan uit dat de Nederlandsche Bank de beleggingsonderneming hier in elk geval naar zal vragen.<sup>142</sup>

## 3. Liquiditeitsrisico

Liquiditeitsrisico kan worden omschreven als de bestaande of toekomstige bedreiging van vermogen en resultaat van de onderneming als gevolg van de mogelijkheid dat zij op enig moment niet in staat zal zijn aan haar korte termijn betalingsverplicht-



tingen te voldoen zonder dat dit gepaard gaat met onaanvaardbare kosten en verliezen.<sup>143</sup> DNB houdt toezicht op de liquiditeit van (open-end) beleggingsinstellingen en van beleggingsondernemingen.

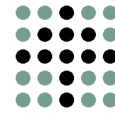
Voor wat betreft de meldingsplicht in het prospectus voor zover relevant voor het fonds wordt een andere definitie gebruikt:<sup>144</sup> het risico dat een positie niet tijdig tegen een redelijke prijs kan worden geliquideerd. Daarnaast moet een sterk verwant risico ook, voor zover van toepassing, in het prospectus worden vermeld, namelijk “de uit het product zelf voortvloeiende inflexibiliteit met inbegrip van het risico van voortijdige afkoop en beperkingen op het overschakelen op andere aanbieders”.<sup>145</sup> Het gaat hierbij niet om de liquiditeit van de onderlinge beleggingen, maar die van de deelnemingsrechten zelf.

Een open-end beleggingsinstelling moet altijd voldoende liquiditeit aanhouden tegenover de deelnemingsrechten zodat zij op korte termijn aan haar betalingsverplichtingen kan voldoen. Daarom moet de bedrijfsvoering van een open-end belegginginstelling zo zijn ingericht dat het liquiditeitsrisico kan worden bewaakt en beheerst.<sup>146</sup> Daarom moet de bedrijfsvoering onder meer voorzien in autorisatieprocedures, limietstellingen, limietbewaking en procedures en maatregelen voor noodsituaties met betrekking tot de liquiditeitspositie.<sup>147</sup>

Bij beleggingsondernemingen moeten de procedures en maatregelen die zijn gericht op het liquiditeitsrisico betrekking hebben op het beheer van de actuele en toekomstige netto financiële positie en behoeften.<sup>148</sup> De beleggingsonderneming moet alternatieve scenario's in overweging nemen en de hypothesen die aan beslissingen betreffende de netto financiële positie ten grondslag liggen, regelmatig aan een nieuw onderzoek onderwerpen.<sup>149</sup>

Er zijn verschillende technieken voor het beoordelen van de liquiditeit van een beleggingsinstelling, vooral afhankelijk van de aard van de beleggingen in de beleggingsportefeuille, de handelsfrequentie in het kapitaal van het fonds, de mate van concentratie van beleggers en, in mindere mate, afhankelijk van de marktomstandigheden (d.w.z. overspannen marktomstandigheden in plaats van normale). Bij deze beoordelingen zou het volgens DUFAS goed zijn om te letten op de structuur van de beleggingsportefeuille om ervoor te zorgen dat niet alle hoge kwaliteitsbeleggingen geliquideerd worden om uitstappende beleggers uit een fonds terug te betalen, en zodoende de gemiddelde waarde voor de achterblijvende beleggers materieel te verlagen.

M.m. speelt hetzelfde probleem uiteraard voor een verzameling individuele portefeuilles van cliënten van beleggingsondernemingen. De laatste kredietcrisis toonde dat ook cliënten van beleggingsondernemingen in tijden van grote financiële spanningen op de financiële markten liquiditeitsrisico's kunnen lopen. Alternatieve beleggingen (vastgoed, private equity, hedge funds) zijn vaak minder liquide, en veel obligaties (niet alleen hypotheekgerelateerde, de zgn. collateralised debt obligations) ook. En wanneer men derivaten gebruikt kan het gebeuren dat bij marktonrust in-



eens meer onderpand moet worden bijgestort, juist wanneer het verkopen van beleggingen om de betreffende liquide middelen te verkrijgen heel moeilijk is. Het verkopen van de derivatencontracten is niet altijd een optie, zo is in de kredietcrisis van 2008 gebleken: er was toen geen markt voor.

Beleggingsinstellingen en beleggingsondernemingen hebben in de praktijk kredietlijnen bij banken, maar in de omstandigheden van de kredietcrisis van 2008 realiseerde zich een *liquidity funding risk*: de banken deden hun contracten van geldlening niet altijd gestand.

Liquiditeitskwesaties komen alleen in extreme marktsituaties voor. De kans is klein, maar de impact kan groot zijn. De risico's zijn onder meer een neerwaartse spiraal (bij gebruik van derivaten) en het niet meer goed kunnen uitvoeren van het afgesproken beleggingsbeleid.

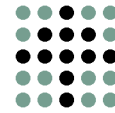
Mogelijke maatregelen zijn stress tests, het beperken van de maximale derivaten exposure (en bij overschrijding innemen van fysieke posities) en afspraken met banken over kredietlijnen. Daarnaast is operational hedging mogelijk als bijvoorbeeld twee of drie doelgroepen (particuliere beleggers, family offices en institutionele beleggers) van de belegginginstelling of beleggingsonderneming tegengesteld gedrag vertonen voor wat betreft in- en uitstappen, kan het een goed idee zijn om deze elk voor een ongeveer gelijk deel als cliënt te hebben.

#### 4. Operationeel risico

Operationeel risico wordt door de Capital Adequacy Directive omschreven als "het risico van verliezen als gevolg van tekortschietende of falende interne procedures en systemen of als gevolg van externe gebeurtenissen. Juridische risico's worden er ook toe gerekend".<sup>150</sup> Deze definitie is ook overgenomen in het Besluit prudentiele regels. Hieronder valt niet het reputatierisico en het strategie risico. Voor de beleggingsinstelling en beleggingsonderneming zijn in relatie tot de financiële toezichthouder uiteraard vooral die operationele risico's van belang die tevens de belangen van de beleggers raken omdat zij daar direct gevolgen voor hebben.<sup>151</sup>

Basel II geeft een nadere onderverdeling van de typen risico die hieronder vallen:

- Interne fraude (verduistering van activa, belastingontduiking, opzettelijk verkeerd voorstellen van posities, omkoping);
- Externe fraude (diefstal van informatie, schade door computer hacking diefstal en vervalsing door derden);
- Arbeidspraktijken en arbeidsomstandigheden (discriminatie, beloning van werknemers, gezondheid en veiligheid van werknemers);
- Cliënten, producten en bedrijfsvoering (marktmanipulatie, mededinging, oneerlijke handelspraktijken, mankementen aan producten, inbreuk op fiduciaire verplichtingen, churning);
- Schade aan fysieke activa (natuurrampen, terrorisme, vandalisme);
- Business disruption & systems failures (van gas, water, licht, software en hardware);



- Execution, delivery, & process management (fouten bij data-invoer, boekhoudkundige fouten, fouten inzake verplichte rapportages, verwijtbaar verlies van stukken en gelden van cliënten).

Operationeel risico is anders van karakter dan financiële risico's: er is geen risicorendement relatie, risicoreductie is procesgedreven in plaats van wiskundig en het risico is heel moeilijk te kwantificeren, omdat het vaak om lage-frequentie incidenten met grote impact gaat.<sup>152</sup> Sommigen hebben daarom kritiek op statistische analyse van operationele risico's en zeggen dat zij alleen de symptomen meten, maar niet de onderliggende causaliteitsketen en zij dus niet in staat zijn om de structurele en systemische effecten van de (rapportage van) heterogene data op de omvang en frequentie van de verliezen vast te stellen.<sup>153</sup>

De procedures en maatregelen die zijn gericht op het beheersen van het operationeel risico bij een beleggingsonderneming moeten mede zijn gericht op zelden voorkomende, zeer ernstige gebeurtenissen.<sup>154</sup> De beleggingsonderneming moet aangeven wat hij naast de wettelijke definitie<sup>155</sup> verder onder operationeel risico verstaat,<sup>156</sup> in de beschrijving van de procedures en maatregelen ter beheersing van relevante risico's.<sup>157</sup>

Een belangrijk onderdeel van operationeel risico is volgens de Nota van toelichting voor beleggingsondernemingen het IT-risico. IT-risico kan worden omschreven als de bestaande of toekomstige bedreiging van vermogen en resultaat van de financiële onderneming als gevolg van een ontoereikende strategie en beleid of van tekortkomingen in de toegepaste technieken en/of gebruik inzake informatieverwerking en communicatie, welke zich vertalen in strategische, beleids-, beveiligings-, beheersbaarheids- en continuïteitsrisico's.<sup>158</sup>

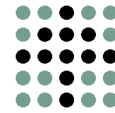
Op het gebied van vooral operationeel risico zijn zgn. loss data consortia<sup>159</sup> ontstaan, waarbij ondernemingen (vooral banken en verzekeraars) samenwerken om data te verzamelen om het grote statistische probleem te adresseren van de lage-frequentie/hoge impact karakteristieken van veel operationele risico's.

Voor wie zich verder wil verdiepen in operationeel risico biedt het Institute of Operational Risk nader materiaal.<sup>160</sup>

Belangrijke instrumenten die zouden kunnen worden gebruikt zijn een loss database, risk self assessment, key risk indicators, new product approval en action tracking.

#### 4.1. Uitbestedingsrisico

Uitbesteden kan de continuïteit, integriteit en/of kwaliteit van de uitbestede werkzaamheden schaden. De beleggingsinstelling en beleggingsonderneming moet daarom beleid vaststellen om de risico's die samenhangen met de uitbesteding van bedrijfsprocessen te beheersen. Het naleven van de vele gedetailleerde wettelijke voorschriften daaromtrent staat daarbij voorop.



De beleggingsinstelling en beleggingsonderneming kan bij wijze van risicoreductie-maatregel aan degene aan wie wordt uitbesteed vragen om periodiek verantwoording af te leggen over de beheersing van de processen, bijvoorbeeld met een ISAE 3402 (voorheen SAS70 type II) rapportage.<sup>161</sup>

#### 4.2. Juridisch risico

DUFAS gaat ervan uit dat de Nederlandsche Bank de beleggingsonderneming hier in elk geval naar zal vragen.<sup>162</sup> Het risico kan worden omschreven als het risico van niet (op tijd) naleven van wet- en regelgeving, het risico dat de beleggingsonderneming aansprakelijk wordt gesteld (claim risico), en het contractueel risico, dat wil zeggen het risico dat men een contract niet kan nakomen.

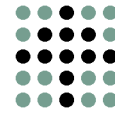
#### 4.3. Model risico

Dit risico wordt in de wetgeving niet van voorschriften voorzien, maar CESR bevestigt er in zijn guidance inzake beleggingsinstellingen wel aandacht aan. Het modelrisico kan worden omschreven als het risico dat een model en/of een risicomeet-techniek kwetsbaar is.<sup>163</sup>

Naar de mening van DUFAS is ook hier het proportionaliteitsbeginsel van groot belang. Het zou goed zijn als het risicomodel dat men gebruikt past bij de mate van complexiteit van de beleggingsportefeuille. Het raamwerk waarmee de risico's gemeten worden zou wat CESR betreft onderworpen moeten zijn aan continue beoordeling en (naar DUFAS aanneemt: waar nodig) aanpassing, en de technieken, gereedschappen en mechanismen die gebruikt worden zouden adequaat gedocumenteerd moeten zijn.<sup>164</sup>

Het zou goed zijn als de kwaliteit van de voorspellingen op basis van het risicomodel aantoonbaar beoordeeld wordt, door middel van gedocumenteerde testen om te verifiëren of de voorspellingen op basis van het model met een passende confidence level kloppen met werkelijke waarden van de risicometingen (*back-testing*).<sup>165</sup> Waar dat passend is kan *back-testing* ook uitgevoerd worden op de risicomeettechnieken. Dat kan voorafgaand aan het in gebruik nemen (calibratie en interne validatie) en daarna periodiek, om er zeker van te zijn dat het risicomeetingsraamwerk levensvatbaar en robuust blijft door de tijd heen.<sup>166</sup> Ondernemingen zouden ook de validity range, marktomstandigheden en inherente of aangenomen limieten van hun risicometingen (die over het algemeen voortvloeien uit de aannames die bij de modellen horen of bij de inschatting van de parameters van de modellen) vóóraf moeten beoordelen. Indien nodig kunnen deze beoordelingen worden gedaan met behulp van stress tests. Ondernemingen zouden hun risicomanagementmethoden moeten review-en wanneer dat maar nodig is.<sup>167</sup>

Stress tests zijn niet wettelijk verplicht voor beleggingsinstellingen en beleggingsondernemingen.<sup>168</sup> Stress tests zijn gewoonlijk bedoeld om de mogelijkheid van zeldzame hoge verliezen te vangen, die zich kunnen voordoen gedurende marktschokken en die waarschijnlijk niet gemeten kunnen worden met de modellen, omdat die



gewoonlijk de structurele breuken in de functionele relaties tussen marktvariabelen volgen (plotselinge verschuivingen van cruciale parameters van de modellen).<sup>169</sup> Wanneer beleggingsinstellingen en beleggingsondernemingen stress tests willen toepassen, zouden deze stress tests het beste alle kwantificeerbare risico's kunnen dekken die materiële invloed hebben op de intrinsieke waarde van de beleggingen, met bijzondere aandacht voor de risico's die niet met voldoende precisie in de gebruikte risicomodellen zitten. Daarbij kan gedacht worden aan bijvoorbeeld onverwachte veranderingen in prijsrelaties of in de liquiditeit van de activa of zelfs de hele markt.<sup>170</sup>

Stress tests kunnen subjectieve scenario-hypothesen betreffen die gebaseerd zijn op empirische gegevens met betrekking tot handelscondities en marktcondities (met betrekking tot hetzij specifieke financiële instrumenten of een gehele portefeuille) in historische perioden van marktonrust. Dergelijke scenario's zouden echter niet alleen maar historische omstandigheden moeten simuleren, maar ook voortborduren op de aanname dat een vergelijkbare dynamiek de risicofactoren kan beïnvloeden die voortvloeien uit de outstanding exposures van de beleggingsportefeuille.<sup>171</sup> Als de beleggingsstrategie is gebaseerd op specifieke handelmodellen of portefeuillemodellen en algoritmen, dan moet de risicomanagementfunctie adequaat zijn om hun beheer en gebruik te beoordelen.<sup>172</sup>

#### 4.4. *Onderpand risico (collateral risk)*

Onderpand is bedoeld om risico's te verminderen, maar levert zelf ook (residuele) risico's op. Het kan zijn dat het geleverde onderpand onvoldoende waarde heeft om mogelijk verlies volledig op de tegenpartij te kunnen verhalen. Er is een (her)beleggingsrisico als de liquide middelen die als onderpand zijn verkregen worden herbelegd om een hoger rendement te genereren dan de verschuldigde rentevergoeding.

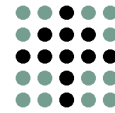
Mogelijke risicoreductiemaatregelen zijn:

- Vooraf duidelijk vastleggen welk onderpand men wel en niet accepteert.
- Ter voorkoming van (her)beleggingsrisico kan men kiezen om alleen effecten als onderpand te accepteren, of zelfs alleen zeer liquide stukken te accepteren, eventueel met een bepaalde afslag (*haircut*) als extra zekerheid.
- Verhoog eventueel de frequentie van monitoren en aanpassen van het benodigde onderpand.

## 5. Integriteitsrisico

### 5.1. *Risico van belangenverstremeling*

De wetgever heeft in artikel 18, Bgfo<sup>173</sup> aan het risico van belangenverstremeling gedacht waar het gaat om verstremeling van de privébelangen van personen die het beleid van de beleggingsinstelling en beleggingsonderneming bepalen, personen die onderdeel zijn van een orgaan dat is belast met toezicht op het beleid en de algemene gang van zaken van de beleggingsinstelling en beleggingsonderneming, andere werknemers, of andere personen die in opdracht van de betrokken onderneming op structurele basis werkzaamheden voor haar verrichten met haar belangen of die



van haar deelnemers.

Het beleid van een beleggingsinstelling en beleggingsonderneming ten aanzien van belangenverstrengeling moet volgens de Nota van toelichting duidelijk maken hoe er bijvoorbeeld moet worden omgegaan met persoonlijke, professionele en financiële belangen in relatie tot het omgaan met deelnemers en andere relaties, het omgaan met (vertrouwelijke) informatie, het aangaan van cliëntrelaties, het verrichten van transacties in de privésfeer en het uitoefenen van nevenactiviteiten.<sup>174</sup>

### 5.2. *Personeelsrisico*

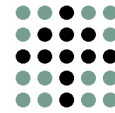
De beleggingsinstelling en beleggingsonderneming is wettelijk verplicht om onderbouwd te beoordelen of de betrouwbaarheid<sup>175</sup> van de dagelijks beleidsbepaler die hij wil benoemen buiten twijfel staat. Deze beoordeling geldt alleen voor bestuurders en personen die onderdeel zijn van het orgaan dat is belast met het toezicht op het beleid en de algemene gang van zaken van de beleggingsinstelling en beleggingsonderneming. Zo'n beoordeling moet ook plaatsvinden voor integriteitsgevoelige functies.<sup>176</sup> Met integriteitsgevoelige functies wordt bedoeld (i) degenen die hiërarchisch dicht onder "de top" zitten, het zogeheten tweede echelon en (ii) andere personen die, hoewel niet horend tot het (hogere) management, werkzaamheden verrichten die van invloed kunnen zijn op de integere bedrijfsvoering.<sup>177</sup>

Om een beoordeling met betrekking tot de betrouwbaarheid te maken, zal de beleggingsinstelling en beleggingsonderneming onder andere de identiteit van de betrokkenen moeten vaststellen en eventuele referenties moeten controleren op juistheid en volledigheid. Bij deze beoordeling zal in veel gevallen het recente arbeidsverleden een belangrijke rol spelen, zeker indien de betrokkene werkzaam is geweest bij een andere financiële onderneming.<sup>178</sup> Deze verplichting geldt ook bij uitbesteding van die functie.

Een belangrijke tool voor de beleggingsinstelling en beleggingsonderneming is hierbij de Pre Employment Screening door het DSI, waarbij DSI de potentiële medewerker toetst aan zijn eigen registers, het identiteitsbewijs controleert, een Verklaring Omtrent het Gedrag (VOG) opvraagt, een eigen verklaring over de integriteit afgeeft, de juistheid van de referenties over de laatste 5 jaar checkt, relevante diploma's checkt en beziet of de persoon in kwestie bij faillissementen betrokken is geweest.<sup>179</sup>

### 5.3. *Witwasrisico en risico van terrorismefinanciering*

De normen met betrekking tot *Customer Due Diligence* ("ken uw cliënt" hierna: CDD) hangen nauw samen met de bestrijding van witwassen en terrorismefinanciering. De normen zijn echter ook relevant voor de integere bedrijfsvoering van beleggingsinstellingen; door een goed zicht op de eigen deelnemers te houden kan voorkomen worden dat de integriteit van een beleggingsinstelling in gevaar komt. Verder is CDD een belangrijk onderdeel van het risicomangement.<sup>180</sup> M.m. geldt naar de mening van DUFAS hetzelfde voor de beleggingsonderneming en zijn cliënten.



CDD valt uiteen in vier belangrijke onderdelen: (i) de acceptatie van deelnemers; (ii) de identificatie en verificatie van deelnemers; (iii) monitoring en review van deelnemers, rekeningen en transacties en (iv) risicomangement.<sup>181</sup>

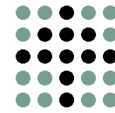
Een beleggingsinstellingen moet een beleid hebben met betrekking tot acceptatie van deelnemers in beleggingsinstellingen c.q. cliënten.<sup>182</sup> Er moeten daarom procedures zijn om deze te identificeren en om de identiteit te verifiëren.<sup>183</sup> Als niet overeenkomstig de vastgelegde procedures is geïdentificeerd, mag de deelnemer c.q. cliënt niet geaccepteerd worden.<sup>184</sup> De wet maakt een uitzondering op deze verplichting voor kortweg “beursgenoteerde fondsen”, of preciezer: beleggingsinstellingen waarbij niet voorafgaand aan de toe- of uittreding wordt beslist omtrent de acceptatie van deelnemers, zoals bij distributie via de Euronext Fund Service.<sup>185</sup>

In dit verband moeten de beleggingsinstellingen beschikken over procedures en maatregelen die betrekking hebben op risicoclassificaties ten aanzien van cliënten, producten of diensten,<sup>186</sup> en voor wat betreft beleggingsondernemingen over procedures met betrekking tot de analyse van gegevens van cliënten, mede in relatie tot de door de cliënt afgenomen producten en diensten, en de detectie van afwijkende transactiepatronen.<sup>187</sup>

Voor de verschillende risicocategorieën moeten verschillende procedures met betrekking tot de acceptatie gelden.<sup>188</sup> Afhankelijk van het risico moeten de gegevens en achtergrond van meer personen of entiteiten worden geverifieerd. Bij het witwassen van geld wordt vaak gebruik gemaakt van allerlei constructies om de ware herkomst van het geld (of andere waarden) te verhullen. Voor een correct beeld en een goed begrip van een transactie is het daarom van belang dat de financiële onderneming weet wie de uiteindelijk belanghebbende (*ultimate beneficial owner*, UBO) in kwestie is.<sup>189</sup>

Monitoring en review is ook van belang. De frequentie en diepgang hangt af van de risicosituatie van de deelnemer respectievelijk cliënt van de beleggingsinstelling respectievelijk beleggingsonderneming. Het is van belang om te toetsen of de situatie en het risicoprofiel van de deelnemer/cliënt na het moment van acceptatie veranderd is, aan de hand van analyse van gegevens van deelnemers/cliënten en detectie van afwijkende transactiepatronen. Een integraal inzicht in de situatie van een deelnemer/cliënt is noodzakelijk voor het opmerken van afwijkend (transactie)gedrag.<sup>190</sup> DUFAS is van mening dat het derhalve is aan te bevelen om de CDD uit te besteden aan een in het kader van de vermogensscheiding dienstverlenende bank (behoudens bij exchange traded fondsen<sup>191</sup>) of een onafhankelijke fonds-administrateur.

Eén en ander moet worden gedocumenteerd en vastgelegd.<sup>192</sup> Dergelijke gegevens dienen, op grond van de Wet ter voorkoming van witwassen en financieren van terrorisme net als op basis van de oude Wid, vijf jaar bewaard te worden na de dienstverlening of beëindiging van de relatie.<sup>193</sup>



Een beleggingsinstelling en beleggingsonderneming is ook verplicht in zijn administratie te zoeken of er bepaalde personen of instellingen voorkomen die van terroristische activiteiten verdacht worden.<sup>194</sup> Als dat het geval is, moet dat aan de AFM gemeld worden,<sup>195</sup> zodat kan worden overgegaan tot bevrozing van tegoeden.<sup>196</sup> Ook moet altijd worden nagegaan of het bedrag niet afkomstig is van een bank uit een land dat op de NCCT-lijst van de Financial Action Task Force staat.

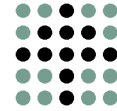
De identificatie van een persoon en verificatie daarvan geschiedt veelal aan de hand van een paspoort of een rijbewijs. DUFAS adviseert daarbij ook de nationaliteit(en) van de cliënt te registreren, omdat de Amerikaanse FATCA wetgeving<sup>197</sup> – naar het voorbeeld van de Europese Spaarrenterichtlijn – belastingontduiking door aldaar belastingplichtigen via (onder meer) Europese beleggingsinstellingen wil voorkomen. Daarnaast zal naar verwachting het Belastingplan 2011 een wettelijke grondslag geven voor het renseignering door beleggingsinstellingen en beleggingsondernemingen aan de Nederlandse Belastingdienst omtrent niet ingezetenen.<sup>198</sup>

#### 5.4. Afwikkelingsrisico

Het afwikkelingsrisico is het risico dat een afwikkeling via een betalingssysteem niet plaatsvindt zoals verwacht, omdat de betaling of levering van de financiële instrumenten door een tegenpartij niet of niet op tijd of zoals verwacht plaatsvindt. Dit risico moet, indien van toepassing, in het prospectus worden vermeld.<sup>199</sup>

#### 6. Restriscico

Onder restriscico wordt begrepen het risico dat de toegepaste en erkende technieken voor de vermindering van de risico's minder doeltreffend blijken dan verwacht. De Nederlandsche Bank spits het daarbij toe op het kredietrisico.<sup>200</sup>



## Bijlage 2: Begrippen

**Risico** is een effect van onzekerheid op het behalen van doelstellingen

**Risicomanagement** zijn gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot risico's

**Risicomanagementbeleid** is een uitleg van de algemene bedoelingen en het uiteindelijk nastreven, behouden, nemen of vermijden van risico's.

**Risicomanagementproces** is het systematisch toepassen van beleidslijnen, procedures en werkwijze op de activiteiten met betrekking tot communicatie en het identificeren, analyseren, evalueren, behandelen monitoren en beoordelen van risico's.

**Risicobeoordeling** is het gehele proces van risico-identificatie, risicoanalyse en risico-evaluatie.

**Risico-identificatie** is het proces waarmee risico's worden opgespoord, herkend en beschreven.

**Risicoprofiel** is een beschrijving van een verzameling risico's

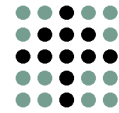
**Risicoanalyse** is het proces dat tot doel heeft de aard van het risico te begrijpen en het risiconiveau vast te stellen.

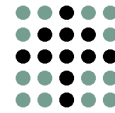
**Risiconiveau** is de omvang van een risico of combinatie van risico's, uitgedrukt als combinatie van gevlogen en hun waarschijnlijkheid (impact & likelihood)

**Risico-evaluatie** is het proces waarin de resultaten van een risicoanalyse worden vergeleken met risicocriteria om vast te stellen of het risico en/of de omvang ervan aanvaardbaar of toerekenbaar is.

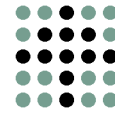
**Risicobehandeling** is het proces waarmee een risico wordt aangepast

**Beheersmaatregelen** zijn maatregelen waarmee een risico wordt gewijzigd. Dit kan elke vorm van een proces, beleid, voorziening, werkwijze of andere maatregel zijn waarmee een risico wordt gewijzigd.

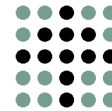




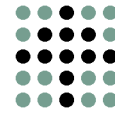
- <sup>1</sup> Art. 4:59, lid 2, en art. 2:97, lid 3, Wft. Daarvoor moet dan uiteraard wel een aparte vergunning worden aangevraagd.
- <sup>2</sup> Zie de artikelen 1:12 en 4:12, Wft, en artikel 4 en 34 Vrijstellingsregeling Wft..
- <sup>3</sup> Kamerstuk 32.036.
- <sup>4</sup> Kamerstuk 32.622. De Nederlandstalige tekst van de UCITS IV richtlijn (Pb L302, p. 32 van 17 november 2009) en de implementatierichtlijn 2010/43/EU van de Europese Commissie (Pb L 176, p. 42 van 10 juli 2010) bieden qua formulering dermate weinig beleidsruimte aan de Lidstaten dat DUFAS zich in deze handreiking voor wat betreft de verplichtingen die uit UCITS IV zullen voortvloeien baseert op de richtlijnteksten.
- <sup>5</sup> Voor wat betreft de AIFMD zijn op het moment van schrijven alleen nog maar Engelstalige en Franstalige teksten beschikbaar. Zodra er ook een Commissierichtlijn beschikbaar is, zal DUFAS deze handreiking aanpassen.
- <sup>6</sup> Ook de bevoegdheid van de AFM om ontheffing te verlenen van de wettelijke verplichtingen (op grond van artikel 4:14, lid 4, Wft) wordt niet nader besproken, omdat die ontheffing alleen verleend kan worden wanneer “de aanvrager aantoont dat daaraan redelijkerwijs niet kan worden voldaan en dat de doeleinden die dit artikel beoogt te bereiken anderszins worden bereikt”. De wettelijke eisen omtrent risicomangement zijn dermate principle based geformuleerd, dat het aanvragen van een ontheffing in de praktijk niet snel nodig zal zijn. De AFM kan overigens geen ontheffing verlenen van de regels in het Bgfo indien die regels betrekking hebben op beleggingsondernemingen, waaronder individueel vermogensbeheerders, omdat de MiFID de mogelijkheid van een ontheffing niet toelaat.
- <sup>7</sup> Zie de de Memorie van Toelichting bij de Wft en het Bgfo, alsmede de UCITS IV Commissierichtlijn 2010/43/EU en CESR, *Risk Management Principles for UCITS*, art 15, AIFMD en annex II van de AIFMD. Ook de MiFID richtlijn spreekt van proportionele implementatie (zie D. Busch, C.M. Grundman-van de Krol, *Handboek Beleggingsondernemingen*, Kluwer, 2009, p. 345-348).
- <sup>8</sup> Kamerstuk 30 672, nr. 3.
- <sup>9</sup> Dit criterium is ook gebruikt in de DUFAS Handreiking AO/IC verklaring.
- <sup>10</sup> Art 3:18a, lid 3, Wft.
- <sup>11</sup> Art 3:18a, lid 4, Wft.
- <sup>12</sup> Art. 4:13, lid 1, Wft.
- <sup>13</sup> Art 34, lid 4, Bgfo.
- <sup>14</sup> Nota van toelichting, Stb 2006, nr. 520.
- <sup>15</sup> In tegenstelling tot de bepalingen in de oude sectorale wetten wordt in artikel 4:14 Wft niet meer de formulering “administratieve organisatie en interne controleprocedures” (AO/IC) gehanteerd ter voorkoming van verwarring met het gelijklopende maar naar strekking beperktere begrip AO/IC dat accountants bijvoorbeeld in het kader van de controle van de jaarrekening hanteren. In plaats daarvan wordt het begrip “bedrijfsvoering” gehanteerd. (Kamerstuk 29.709, nr. 19).
- Uit de parlementaire geschiedenis van de totstandkoming van de Wft blijkt overigens dat het niet de bedoeling is geweest van de wetgever om inhoudelijk iets te wijzigen. In een wetgevingsoverleg op 29 mei 2006 zei de minister van Financiën (Zalm): “Mevrouw Van Egerschot vroeg of het begrip “bedrijfsvoering” nu verruimd is. Ten opzichte van de bestaande wetgeving is de reikwijdte van het toezicht op de bedrijfsvoering niet verruimd. Het is een puur terminologische kwestie dat wij ‘administratieve organisatie en interne controle’ hebben gewijzigd in ‘bedrijfsvoering’. Daarmee wordt niets anders of meer geregeld dan nu het geval is. ‘Bedrijfsvoering’ is ook de term die wij in de rijksbegroting gebruiken. Dit is een modernisering qua jargon” (kamerstuk 29.708, nr.45, p. 17). Dit heeft de minister van Financiën daarna in een brief van 12 juni 2006 aan de Tweede Kamer herhaald: “Dufas merkte ten eerste op dat de reikwijdte van het toezicht op de bedrijfsvoering te ruim is. In artikel 4:14 wordt namelijk niet meer gesproken van ‘administratieve organisatie en interne controle (AO/IC)’, maar van ‘bedrijfsvoering’. Wordt het toezicht op de bedrijfsvoering hiermee verruimd? De reikwijdte van het toezicht op de bedrijfsvoering is ten opzichte van de bestaande toezichtwetten niet verruimd. De wijziging van ‘admi-



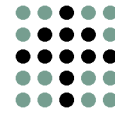
- nistratieve organisatie en interne controle' in 'bedrijfsvoering' betreft een puur terminologische kwestie" (kamerstuk 29.708, nr 47, p. 1).
- 16 Art. 4:14, lid 1, Wft.
- 17 Kamerstuk 29.709, nr. 19.
- 18 Art 3:17, lid 2, sub c jo. lid 3 en kamerstuk 29 708, nr. 10.
- 19 Kamerstuk 29 708, nr. 10.
- 20 Art. 3:17, lid 2, sub c, Wft.
- 21 Kamerstuk 29 708, nr. 10.
- 22 Kamerstuk 29 708, nr. 10.
- 23 Op grond van art. 4:14, lid 2, Wft.
- 24 Kamerstuk 29.709, nr. 19.
- 25 Art. 83, lid 1, Bgfo.
- 26 Op grond van artikel 3:17, lid 4, Wft
- 27 Art. 3:18a, 3:57, Wft, jo. art 3, Bpr.
- 28 Zie de brief van De Nederlandsche Bank d.d. 16 augustus 2007, kenmerk BB/2007/00440/coe inzake Pijler 2 voor beleggingsondernemingen, bijlage 1.
- 29 Art 25a, lid 1, Bpr.
- 30 Art 26, lid 2, Bpr.
- 31 Stb. 2006, nr. 519.
- 32 Nota van toelichting, Stb. 2006, nr. 520.
- 33 Nota van toelichting, Stb. 2006, nr. 520.
- 34 Art. 17, lid 1, Bgfo en art 23, lid 6, Bpr.
- 35 Art. 17, lid 2, Bgfo en 23, lid 1, Bpr.
- 36 Nota van toelichting, Stb. 2006, nr. 520.
- 37 Nota van toelichting, Stb. 2006, nr. 520.
- 38 Nota van toelichting, Stb. 2006, nr. 520.
- 39 Zoals vereist door art. 4:14, lid 1, Wft.
- 40 Art 23, lid 3, Bpr.
- 41 Art 23, lid 3, Bpr.
- 42 Dit is wat slordig opgeschreven in art. 17, lid 2, Bgfo. De norm is dat het beleid, inzake integere bedrijfsuitoefening "zijn neerslag" moet vinden in procedures en maatregelen (art 17, lid 2, Bgfo). Het woord "neerslag" betekent volgens het woordenboek Van Dale "het geheel van gevoelens, ervaringen, indrukken die men heeft opgedaan en die later *verbaal* [cursivering DUFAS] worden weergegeven".
- 43 CESR, *Risk Management Principles for UCITS*, p. 12, par. 9: "The risk management policy should ideally take the form of a separate document. However, in light of the principle of proportionality, it can also be documented within the existing organisational and procedural rules. In the latter case, the different documents should allow for a clear identification of risk management roles, responsibilities and operating procedures." Zie tevens art. 4, lid 1 (a); 18, lid 1; en 38, lid 1 van Commissierichtlijn 2010/43/EU.
- 44 Zie art. 38, lid 1 van Commissierichtlijn 2010/43/EU.
- 45 Art. 17, lid 3, Bgfo eist dit van beleggingsinstellingen en hun beheerders en bewaarders, maar art. 23 Bgfo eist dit niet van individueel vermogensbeheerders. Niettemin beveelt DUFAS aan om het wel te doen, omdat integriteitrisico's kunnen voortvloeien uit activiteiten, relaties en handelingen van bijna alle geledingen van financiële ondernemingen.
- 46 Nota van toelichting, Stb. 2006, nr. 520.
- 47 Nota van toelichting, Stb. 2006, nr. 520.
- 48 Art. 17, lid 4, Bgfo eist dit van beleggingsinstellingen en hun beheerders en bewaarders, maar art. 23 Bgfo eist dit niet van beleggingsondernemingen. DUFAS acht een gewetensvolle naleving van de regels echter onmogelijk voor een beleggingsinstelling en beleggingsonderneming die zich niet op gezette tijden op de hoogte stelt van veranderingen in de vigerende wet- en regelgeving.
- 49 Volgens de *DUFAS Fund Governance Principles* kan een onafhankelijke toezichthouder bestaan uit een externe accountant of een onafhankelijke bewaarder (depository). Goede commissarissen zijn voor kleine organisaties vaak moeilijk te vinden. Indien er voor wordt gekozen deze functie



- te laten vervullen door een externe accountant, kan worden afgesproken dat de accountant deze werkzaamheden (grotendeels) verricht gelijktijdig met zijn reguliere controlewerkzaamheden ten behoeve van het jaarrekeningwerk voor de beleggingsinstelling(en). Hierdoor kunnen de additionele kosten zo veel mogelijk beperkt blijven. Beursgenoteerde closed-end vastgoedfondsen voldoen al aan het vereiste van een onafhankelijke toezichthouder doordat ze op grond van de op hen van toepassing zijnde Code Tabaksblat dienen te beschikken over een raad van (externe) commissarissen.
- 50 Art. 17, lid 5, en 23, lid 2, Bgfo.
- 51 De Nota van toelichting (Stb. 2006, nr. 520) spreekt niet van “systematisch toetsen”, maar van “doorlopend toetsen”, wat iets anders is. “Doorlopend” wil zeggen “niet onderbroken”, terwijl “systematisch” wil zeggen “volgens een systeem van werkwijzen of handelingen”.
- 52 Dit o.a. omdat art 15, lid 2, AIFMD zal te zijner tijd waarschijnlijk tenminste éénmaal per jaar een review van de risk management systemen eisen.
- 53 Art. 17, lid 6 en art. 23, lid 2, Bgfo.
- 54 Art. 23, lid 2, Bgfo.
- 55 Art. 10, lid 2, Commissierichtlijn 2010/43/EU.
- 56 CESR, *Risk Management Principles for UCITS*, p. 12, par. 10 en p. 16, Box 6. Zie ook ibid. p. 13, par. 12.
- 57 Art 23, lid 2, Bpr.
- 58 Art 118, lid 1, Bgfo jo. Bijlage E, Bgfo, punt 8.2. en punt 8.3.
- 59 Art 118, lid 1, Bgfo jo. Bijlage E, Bgfo, punt 8.2. en 8.3.
- 60 Art. 12, lid 2, Commissierichtlijn 2010/43/EU en CESR, *Risk Management Principles for UCITS*, p. 12, Box 3. In dezelfde zin waarschijnlijk art 15, lid 1, AIFMD; zie ook annex II van de AIFMD. Ook de MiFID richtlijn spreekt van proportionele implementatie (zie D. Busch, C.M. Grundman-van de Krol, *Handboek Beleggingsondernemingen*, Kluwer, 2009, p. 345-348).
- 61 CESR, *Risk Management Principles for UCITS*, p. 13, par. 16.
- 62 Zie art 4:14, lid 2, Wft en art. 18 Bgfo.
- 63 Zie art 17-20 Commissierichtlijn 2010/43/EU.
- 64 CESR, *Risk Management Principles for UCITS*, p. 13, par. 15. In dezelfde zin waarschijnlijk ook art 13, AIFMD.
- 65 Principe 6 plus toelichting van de *Principes voor beheerst beloningsbeleid*, AFM, DNB, mei 2009.
- 66 Principe 8c plus toelichting van de *Principes voor beheerst beloningsbeleid*, AFM, DNB, Mei 2009.
- 67 Art. 12, lid 4, Commissierichtlijn 2010/43/EU.
- 68 CESR, *Risk Management Principles for UCITS*, p. 12, Box 3.
- 69 Zie art. 4:9, lid 1, Wft.
- 70 Zie verder [www.garp.org](http://www.garp.org)
- 71 Zie verder [www.prmia.org](http://www.prmia.org)
- 72 Zie verder <http://www.feb.uva.nl/emerm/home.cfm>
- 73 Zie verder <http://www.feweb.vu.nl/nl/opleidingen/postgraduate-opleidingen/risk-management-for-financial-institutions/index.asp>
- 74 Zie verder <http://www.aif.nl/programs/executivemastersinriskmanagement.htm>
- 75 De datum waarop UCITS IV en de bijbehorende Commissierichtlijn 2010/43/EU in werking treedt.
- 76 Art 15, lid 2, AIFMD zal te zijner tijd waarschijnlijk tenminste éénmaal per jaar een review van de risk management systemen eisen.
- 77 Art. 12, lid 3, Commissierichtlijn 2010/43/EU en Risk Management Principles for UCITS, p. 12, Box 3.
- 78 Art. 12, lid 3, sub d) Commissierichtlijn 2010/43/EU.
- 79 Principe 5 en 5b van de *Principes voor beheerst beloningsbeleid*, AFM, DNB, Mei 2009.
- 80 CESR, *Risk Management Principles for UCITS*, p. 13, par. 17.
- 81 Stb. 2010, nr. 806.
- 82 Richtlijn 2006/48/EU. Zie met name artikel 22 en Annex V. Voor een uitgebreide bespreking van de inhoud van de toekomstige regels en hun samenhang zie de *Guidelines on Remuneration Policies and practices* d.d. 10 december 2010 van het Committee of European Banking Supervisors.



- 83 Stcrt 2010, nr. 20931 d.d. 24 december 2010.
- 84 CESR adviseert dat (*Risk Management Principles for UCITS*, p. 13, par. 17).
- 85 Art. 17, lid 1, Bgfo eist dit van beleggingsinstellingen en hun beheerders en bewaarders, maar art. 23, lid 1, Bgfo eist dit niet van individueel vermogensbeheerders. Niettemin acht DUFAS het moeilijk om zonder de juiste analyse tot effectieve procedures en maatregelen te komen.
- 86 CESR, *Risk Management Principles for UCITS*, p. 18, Box 8 en p. 19, par. 45.
- 87 CESR, *Risk Management Principles for UCITS*, p. 19, par. 45.
- 88 Kamerstuk 29 708, nr. 19. De wettelijke definitie is nauwkeuriger: het door een financiële onderneming verlenen van een opdracht aan een derde tot het ten behoeve van die financiële onderneming verrichten van werkzaamheden (a) die deel uitmaken van of voortvloeien uit het uitoefenen van haar bedrijf of het verlenen van financiële diensten of (b) die deel uitmaken van de wezenlijke bedrijfsprocessen ter ondersteuning daarvan (art. 1:1, Wft). Catering, schoonmaakwerkzaamheden en bijvoorbeeld de aanschaf van kantoorinventaris worden niet door de bepalingen van Deel 4 Wft geregeld en behoren niet tot de uitoefening van het bedrijf. Het laten uitvoeren van dergelijke werkzaamheden wordt niet beheerst door de bepalingen inzake uitbesteding (Stb 2006, nr. 520).
- 89 Art. 3:18, Wft en art. 27-32a Besluit prudentiële regels (Bpr).
- 90 Art. 4:16, 4:36, Wft, 38-38d, Bgfo.
- 91 CESR, *Risk Management Principles for UCITS*, p. 19, par. 48. CESR stelt dat het “risicomanagement beleid” moet heten.
- 92 CESR, *Risk Management Principles for UCITS*, Box 2.
- 93 CESR, *Risk Management Principles for UCITS*, Box 2. Dit advies wordt gegeven in een passage over het risicomanagement proces, maar er wordt gesproken van “risicomanagement beleid”.
- 94 CESR, *Risk Management Principles for UCITS*, Box 2.
- 95 CESR, *Risk Management Principles for UCITS*, p. 19, Box 9.
- 96 CESR, *Risk Management Principles for UCITS*, p. 20, par. 49.
- 97 CESR, *Risk Management Principles for UCITS*, p. 19, Box 9.
- 98 CESR, *Risk Management Principles for UCITS*, p. 20, par. 49.
- 99 Art. 83, lid 1, Bgfo.
- 100 CESR, *Risk Management Principles for UCITS*, p. 19, par. 47.
- 101 Art 23, lid 3, Bpr.
- 102 Stb. 2006, nr. 519.
- 103 CESR, *Risk Management Principles for UCITS*, p. 20, par. 51.
- 104 CESR, *Risk Management Principles for UCITS*, p. 20, Box 10.
- 105 CESR, *Risk Management Principles for UCITS*, p. 20, par. 51.
- 106 CESR, *Risk Management Principles for UCITS*, p. 20, par. 53.
- 107 CESR, *Risk Management Principles for UCITS*, p. 20, par. 54.
- 108 CESR, *Risk Management Principles for UCITS*, p. 13-14, par. 18.
- 109 CESR, *Risk Management Principles for UCITS*, Box 2.
- 110 Art. 21, UCITS.
- 111 Art. 19, lid 1 en 24, lid 1, Bgfo.
- 112 Art. 19, lid 2 en 24, lid 2, Bgfo.
- 113 Art. 19, lid 3 en 24, lid 3, Bgfo.
- 114 Art. 1, Bgfo.
- 115 Nota van toelichting, Stb. 2006, nr. 520.
- 116 Nota van toelichting, Stb. 2006, nr. 520.
- 117 Nota van toelichting, Stb. 2006, nr. 520.
- 118 Art. 17 en 23, Bgfo. Zie ook par. 6.1.6.
- 119 Eén risico dat in het prospectus moet worden vermeld past niet goed in een handreiking over risicomanagement van de beleggingsinstelling, namelijk “het risico van onzekerheid over externe factoren zoals het toepasselijke belastingregime”, genoemd Bijlage E, punt 8.3. onder f. Dit risico hangt namelijk van de omstandigheden van de belegger af en niet van de omstandigheden van de beleggingen of het beleggingsvehikel.
- 120 CESR, *Risk Management Principles for UCITS*, p. 8, par. 3.



- 121 Zie de brief van De Nederlandsche Bank d.d. 16 augustus 2007, kenmerk BB/2007/00440/coe  
inzake Pijler 2 voor beleggingsondernemingen, p. 4.
- 122 Stb. 2006, nr. 662.
- 123 Art. 5:3 en 5:4 Nrgfo.
- 124 Art. 118, lid 1, Bgfo jo. Bijlage E, punt 8.2., onder a.
- 125 Art. 118, lid 1, Bgfo jo. Bijlage E, punt 8.3., onder a.
- 126 Art. 118, lid 1, Bgfo jo. Bijlage E, punt 8.3., onder b.
- 127 Inflatie is in de Keynesiaanse visie de stijging van het algemeen prijspeil (prijsinflatie), als gevolg  
van relatieve veranderingen in vraag en aanbod op de markt. Inflatie is in de monetaristische vi-  
sies een verandering in de geldvoorraad ten opzichte van de voorraad goederen (monetaire infla-  
tie). Monetaristen bestrijden die monetaire inflatie door de rentetarieven die centrale banken  
aan het bankwezen berekenen te veranderen, m.a.w. de prijs van geld te veranderen.
- 128 Art. 118, lid 1, Bgfo jo. Bijlage E, punt 8.3., onder e.
- 129 Art. 118, lid 1, Bgfo jo. Bijlage E, punt 8.2., onder g.
- 130 Art. 118, lid 1, Bgfo jo. Bijlage E, punt 8.7.
- 131 Art. 118, lid 1, Bgfo jo. Bijlage E, punt 8.2., onder e.
- 132 Stb. 2006, nr. 662.
- 133 Art. 133, 134, Bgfo. Dit is de wettelijke basis voor de bepalingen in de Nrgfo.
- 134 Art. 5:5 t/m 5:9, Nrgfo.
- 135 Art. 5:5, Nrgfo.
- 136 Art. 118, lid 1, Bgfo jo. Bijlage E, punt 8.2., onder b.
- 137 Art. 118, lid 1, Bgfo jo. Bijlage E, punt 8.2., onder f.
- 138 Art. 118, lid 1, Bgfo jo. Bijlage E, punt 8.3., onder c.
- 139 Zie voor een overzicht van de risico's en risicomanagement technieken *Securities Lending Trans-  
actions: Market Development and Implications*, BIS/IOSCO, July, 1999, p. 40-47; *An Introduction to  
securities lending*, International Securities Lending Association, March 2004, chapter 5.
- 140 Art. 118, lid 1, Bgfo jo. Bijlage E, punt 8.6.
- 141 Stb. 2006, nr. 662.
- 142 Zie de brief van De Nederlandsche Bank d.d. 16 augustus 2007, kenmerk BB/2007/00440/coe  
inzake Pijler 2 voor beleggingsondernemingen, p. 4.
- 143 Stb. 2006, nr. 662.
- 144 Art. 118, lid 1, Bgfo jo. Bijlage E, punt 8.2., onder d.
- 145 Art. 118, lid 1, Bgfo jo. Bijlage E, punt 8.3., onder d.
- 146 Stb. 2006, nr. 519.
- 147 Art 26, lid 3, Bpr.
- 148 Art 23b, lid 1, Bpr.
- 149 Art 23b, lid 2, Bpr.
- 150 Art 4, CRD.
- 151 Zie ook CESR, *Risk Management Principles for UCITS*, p. 9, par. 9.
- 152 Andreas A. Jobst, *The credit crisis and operational risk, implications for practitioners and regulators*,  
*Journal of Operational Risk*, vol. 5, no. 2, summer 2010.
- 153 Andreas A. Jobst, *Constraints of consistent operational risk measurement and regulation: data collec-  
tion and loss reporting*, *Journal of Financial Regulation and Compliance*, 2007.
- 154 Art 23c, lid 1, Bpr.
- 155 Art 1, Bpr: "risico van verliezen als gevolg van tekortschietende of falende interne procedures  
en systemen of als gevolg van externe gebeurtenissen, met inbegrip van juridische risico's".
- 156 Art 23c, lid 2, Bpr.
- 157 Stb. 2006, nr. 662. Zie art. 23, lid 4.
- 158 Stb. 2006, nr. 662.
- 159 De meest bekende voorbeelden zijn de Global Operational Loss Database (GOLD) van de Bri-  
tish Bankers' Association, het Operational Risk Insurance Consortium (ORIC) van de Associati-  
on of British Insurers, OpBase van Aon, en de database van de Operational Riskdata eXchange  
Association (ORX). (Andreas A. Jobst, *Constraints of consistent operational risk measurement and  
regulation: data collection and loss reporting*, *Journal of Financial Regulation and Compliance*, 2007.)



- <sup>160</sup> <http://www.ior-institute.org/education/sound-practice-guidance>. Ook nuttig is <http://operationalrisk.blogspot.com/>
- <sup>161</sup> In een Type I verklaring evalueert de accountant de inspanningen van de dienstverlener op het moment van de audit om boekhoudkundige inconsistenties, fouten en verkeerde voorstellingen van zaken te voorkomen. De accountant beoordeelt ook de kans dat deze inspanningen de gevraagde resultaten zullen genereren. Een Type II verklaring bevat daarnaast ook nog een poging van de accountant om de effectiviteit te beoordelen van overeengekomen controls sinds hun implementatie. Type II verklaringen omvatten mede data die gedurende een specifiek tijdvak zijn verzameld. Overigens gaat de naam van het SAS-70 rapport in de toekomst wijzigen in ISAE3402.
- <sup>162</sup> Zie de brief van De Nederlandsche Bank d.d. 16 augustus 2007, kenmerk BB/2007/00440/coe inzake Pijler 2 voor beleggingsondernemingen, p. 4.
- <sup>163</sup> CESR, *Risk Management Principles for UCITS*, p. 17, Box 7, nr. 1.
- <sup>164</sup> CESR, *Risk Management Principles for UCITS*, p. 17, Box 7, nr. 2.
- <sup>165</sup> CESR, *Risk Management Principles for UCITS*, p. 17, par. 38.
- <sup>166</sup> CESR, *Risk Management Principles for UCITS*, p. 17-18, par. 39. CESR adviseert back testing “on an ongoing basis”, maar DUFAS is van mening dat dat ook heel goed periodiek kan, zolang het tijdsinterval tussen de tests niet te lang is. In de daarop volgend paragraaf heeft CESR het name-lijk over review “wanneer nodig”.
- <sup>167</sup> CESR, *Risk Management Principles for UCITS*, p. 18, par. 40.
- <sup>168</sup> Als de eigenaar van de asset manager een bank is, kan dat anders zijn.
- <sup>169</sup> CESR, *Risk Management Principles for UCITS*, p. 18, par. 41.
- <sup>170</sup> CESR, *Risk Management Principles for UCITS*, p. 18, par. 42.
- <sup>171</sup> CESR, *Risk Management Principles for UCITS*, p. 18, par. 43.
- <sup>172</sup> CESR, *Risk Management Principles for UCITS*, p. 18, par. 44.
- <sup>173</sup> voor wat betreft de beheerder, bewaarder of beleggingsinstelling.
- <sup>174</sup> Nota van toelichting, Stb. 2006, nr. 520.
- <sup>175</sup> Art 12-16, Bgfo.
- <sup>176</sup> Art. 20 en 25, Bgfo.
- <sup>177</sup> Stb. 2006, nr. 520.
- <sup>178</sup> Stb. 2006, nr. 520.
- <sup>179</sup> Zie verder [www.dsi.nl](http://www.dsi.nl). De registratie in de DSI registers betreft niet de integriteit maar de vak-bekwaamheid van de persoon.
- <sup>180</sup> Stb. 2006, nr. 520.
- <sup>181</sup> Stb. 2006, nr. 520.
- <sup>182</sup> Art 21, lid 1 en 26, lid 1, Bgfo.
- <sup>183</sup> Art 21, lid 2 en 26, lid 2, Bgfo.
- <sup>184</sup> Art 21, lid 2 en 26, lid 2, Bgfo.
- <sup>185</sup> Art. 21, lid 5, Bgfo.
- <sup>186</sup> Art 21, lid 3 en 26, lid 2, Bgfo.
- <sup>187</sup> Art 21, lid 4 en 26, lid 3, Bgfo.
- <sup>188</sup> Stb. 2006, nr. 520.
- <sup>189</sup> Stb. 2006, nr. 520.
- <sup>190</sup> Stb. 2006, nr. 520.
- <sup>191</sup> Art. 21, lid 5, Bgfo.
- <sup>192</sup> Art 21, lid 5 en 26, lid 4, Bgfo.
- <sup>193</sup> Stb. 2006, nr. 520.
- <sup>194</sup> Art 22, lid 1 en 27, lid 1, Bgfo.
- <sup>195</sup> Art 22, lid 2 en 27, lid 2, Bgfo.
- <sup>196</sup> Stb. 2006, nr. 520.
- <sup>197</sup> Foreign Account Tax Compliance Act, Subtitle A of Title V of Public Law 111 147.
- <sup>198</sup> Zie Kamerstuk 32.128, artikel XXIII inzake de WIB.
- <sup>199</sup> Art. 118, lid 1, Bgfo jo. Bijlage E, punt 8.2., onder c.
- <sup>200</sup> Stb. 2006, nr. 662.

