

Risk management systemen van niet-financiële ondernemingen en de in het Groenboek genoemde 'key societal risks'

In het in de afgelopen zomer verschenen Groenboek inzake het EU corporate governance framework wordt de vraag gesteld of het risicomanagement van een onderneming zich ook dient uit te strekken tot 'key societal risks'. Hoe zou dit zich verhouden tot de 'risk appetite' als onderdeel van een risicomanagementsysteem, en tot 'compliance'? Welke mate van beleidsvrijheid heeft het management bij de bepaling van de 'risk appetite' en de inrichting van een compliance systeem van een onderneming? In deze bijdrage wordt op die vragen ingegaan.



1. Inleiding

Onderwerp van deze bijdrage¹ is de vraag naar een spillover van de nieuwe regels voor financiële instellingen naar andere sectoren. Ik wil me daarbij in het bijzonder richten op de reikwijdte van het risicomanagement voor niet-financiële instellingen en de risico's die daarbij moeten worden bestreken. Allereerst ga ik in op de redenen voor een zwaarder regime voor banken, en de vraag of die ook voor niet-financiële instellingen geacht kunnen worden te gelden. Vervolgens sta ik stil bij de vraag of het risicomanagement zich ook dient uit te strekken tot 'key societal risks' zoals voorgesteld in het recent verschenen Groenboek inzake het EU corporate governance framework. Hoe zou zich dit verhouden tot begrippen als 'risk appetite' als onderdeel van een risicomanagementsysteem, alsook tot compliance? Daarbij wordt ingegaan op vragen naar de analyses en waarderingen die in het kader van een compliance systeem dienen te worden gemaakt. Ten slotte wordt ingegaan op enige in het Groenboek genoemde 'key societal risks' ten aanzien waarvan het de vraag is of, en in welke mate, vandaag de dag zorgplichten van de onderneming geacht kunnen worden te gelden.

2. Redenen voor zwaarder regime voor banken

Het Groenboek van de Europese Commissie inzake Corporate Governance and Financial Institutions (Brussel, 2 juni 2010) noemt een aantal kenmerken van de 'financial industry' die nopen tot de verhoogde eisen die worden gesteld aan de corporate governance van deze ondernemingen. Daarin wordt geschetst dat de traditionele definitie van corporate governance betrekking heeft

op de relaties tussen het management, de board, de aandeelhouders en andere stakeholders, zoals werknemers en hun vertegenwoordigers. Bij een financiële instelling is deze scope van stakeholders ruimer. Vanwege de aard van haar activiteiten en 'interdependencies within the financial system', kan het faillissement van financiële instelling een domino-effect opleveren, resulterend in andere faillissementen in de 'financial industry'. Op haar beurt kan dit resulteren in een economische crisis vanwege het daaruit voortvloeiend gebrek aan financieringsmogelijkheden in de economie. Dit leidt ertoe dat overheden zullen bijspringen met belastinggeld, teneinde hun financiële stabiliteit zo veel mogelijk te waarborgen. Daarnaast geldt dat de crediteuren van banken in het algemeen gebaat zullen zijn bij een laag risicoprofiel van de onderneming.²

Het in Engeland verschenen *The Turner Review* noemt een drietal onderscheidende kenmerken voor de financiële industrie:

- de rol van banken 'as providers of maturity transformation, holding longer tenor assets than liabilities and thus enabling non bank sectors in total to hold longer liabilities than assets', wat van essentieel belang is voor de economie, maar dat grote risico's loopt in geval van een bank run;
- het eerdergenoemde domino-effect;

* Prof. mr. A.F. Verdam is hoogleraar Ondernemingsrecht aan de Vrije Universiteit Amsterdam en juridisch adviseur bij Koninklijke Philips Electronics N.V.

1. Het betreft een bewerking van een voordracht gehouden op het congres 'Crisiswetgeving voor financiële instellingen en ondernemingen' van deze zomer, georganiseerd door het Zuidas Instituut voor Financieel recht en Ondernemingsrecht (ZIFO) van de VU te Amsterdam, waarvan tevens een congresbundel wordt uitgebracht in de ZIFO-reeks van het instituut.

2. Green Paper, Corporate governance in financial institutions and remuneration policies, COM(2010) 284/3, (gepubliceerd op http://ec.europa.eu/internal_market/consultations/2010/governance_en.htm), p. 3 en 4. Zie over dit Groenboek o.a. H.J. Bruisten, *FR* 2010-10, p. 258 e.v.

- het kenmerk dat het gevolg van een 'bank failure' of een 'bank system failure' zeer ernstige gevolgen kan hebben voor de economie.³

Een en ander heeft geleid tot regelgeving, of voorstellen tot regelgeving, onder andere met betrekking tot het risicomangement bij een financiële instelling.

3. Gelden die redenen ook voor andere ondernemingen?

Het ligt voor de hand om de vraag naar de wenselijkheid van spillover-effecten naar andere sectoren primair te benaderen vanuit een tegenvraag: zijn er nog andere sectoren waar men ook zo'n combinatie ziet van nutsfunctie, potentieel domino-effect van het omvallen van een onderneming op de positie van branchegenoten, en de zeer serieuze impact van het omvallen van zodanige ondernemingen voor de maatschappij als geheel?

Een aantal sectoren met zo'n nutsfunctie is gemakkelijk aan te duiden. Te denken is aan de leveranciers van gas, water, elektriciteit, de netbeheerder, de ophaler van huisafval, openbaar vervoer. Maar de combinatie met de andere genoemde kenmerken van de financiële industrie (domino-effect bij het omvallen van een onderneming, zeer serieuze impact op economie als geheel) en daarmee de cumulatie van deze drie, is niet op voorhand evident. Aldus bezien zou het argument luiden dat er niet zo gemakkelijk andere sectoren zijn aan te wijzen waarvoor zo'n spillover-effect gerechtvaardigd zou zijn. Andere sectoren nemen nu eenmaal niet zo snel zo'n speciale positie in de maatschappij in, als de financiële instellingen.

4. Dient risicomangement zich ook uit te strekken tot 'key societal risks'?

Het is de vraag of je zo'n hoge drempel voor een spillover-effect van de regelgeving naar andere sectoren of ondernemingen moet opwerpen. Immers, men kan ook meer algemeen de vraag stellen of in het risicomangement van de onderneming⁴ niet dienen te worden meegenomen de potentiële gevaren voor de maatschappij die voortvloeien of samenhangen met de operaties van de onderneming. Dus los van een eventueel domino-effect, los van een eventuele zeer zware impact op de economie: wat zijn de potentieel serieuze gevaren voor de maatschappij die zich in het kader van bepaalde ondernemingsactiviteiten kunnen voordoen?

Aan de hand van recente krantenkoppen, is het niet zo moeilijk hierbij voorbeelden te noemen van ernstige gevaren, zoals het gevaar van milieuschade aan kustgebieden in bepaalde landen ten gevolge van de risico's bij oliebo-

ringen op zee, en de schade aan milieu en gezondheid ten gevolge van bepaalde risico's die bewaarheid worden bij een kernenergiecentrale.

De deur in die richting wordt op een behoorlijke kier gezet door het in april van dit jaar verschenen Groenboek inzake het EU corporate governance framework.⁵ Het gaat hier dus niet om de corporate governance van financiële instellingen, maar van ondernemingen in het algemeen.⁶

Daarin wordt onder het kopje 'Risk management' geschetst dat sommige ondernemingen ook te doen hebben met risico's:

'(...) that significantly affect society as a whole; risks related to climate change, to the environment (...), health, safety, human rights, etc.'

Deze risico's worden aangeduid met 'relevant key societal risks'. Daaronder worden ook begrepen ondernemingsactiviteiten die betrekking hebben op 'critical infrastructure, the disruption or destruction of which could have major cross-border impacts'.

In dat kader worden in het Groenboek de volgende vragen gesteld:

1. 'Do you agree that the board should approve and take responsibility for the company's risk appetite and report it meaningfully to shareholders?'

En hier meer van belang: 'Should these disclosure arrangements also include relevant key societal risks?'

2. 'Do you agree that the board should ensure that the company's risk management arrangements are effective and commensurate with the company's risk profile?'

Ik ga hierna (slechts) op een paar aspecten in die bij de beantwoording van die vragen relevant zijn.

5. Opbouw risicomangementsysteem; hoe verhouden 'key societal risk' zich tot 'risk appetite'?

Risicobeheersingssystemen zijn veelal opgezet volgens het zogenaamd COSO-systeem en met name bij Engelse bedrijven conform de zogenaamde Turnbull Guidance. In het COSO-systeem ziet het risicomangementsysteem op een systeem – ik citeer Strik:

- 'designed to identify potential events that may affect the entity, and
- manage risks to be within it's risk appetite,
- to provide reasonable assurance regarding the achievement of entity objectives.'⁷

3. *The Turner Review*, 'A regulatory response to the global banking crisis, Financial Services Authority', maart 2009 (gepubliceerd op de website van de FSA), p. 52.

4. Gemakshalve en met verwijzing naar het spraakgebruik verwijs ik in deze bijdrage vooral naar 'onderneming', daarbij in het midden latend welke vennootschap of welk vennootschapsorgaan in een constellatie van ondernemingen daarbij in het geding is.

5. Green Paper, The EU corporate governance framework, COM(2011)164, Brussel 5 april 2011 (gepubliceerd op http://ec.europa.eu/internal_market/company/docs/modern/com2011-164_en.pdf).

6. Het Groenboek stelt eerder de vraag of ook voor niet-beursgenoteerde ondernemingen corporategovernanceregels opgesteld zouden moeten worden.

7. Zie D.A.M.H.W. Strik, *Grondslagen bestuurdersaansprakelijkheid* (diss. Rotterdam), Deventer: 2010 (hierna: Strik 2010), p. 224, alsook D.A.M.H.W. Strik (i.s.m. B.F. Assink), 'Aansprakelijkheid voor falend risicomangement', in: *Ondernemingsbestuur en risicobeheersing*

Het is de vraag hoe de 'key societal risks' hierin passen. De vraag is allereerst hoe bedoelde 'key societal risks' zich verhouden tot het begrip 'risk appetite' dat een belangrijk onderdeel is van een risicomanagementsysteem, en dat in het Groenboek ook in dit kader wordt genoemd. Strik schetst in haar proefschrift (en daarvoor in het preadvies voor de Vereniging 'Handelsrecht') zo mooi voor de jurist hoe een risicomanagementsysteem is opgebouwd en welke rol de 'risk appetite' daarin speelt.⁸ De risk appetite is dan (in de woorden van de Code Banken) 'de mate van redelijkerwijs voorzienbaar risico die de onderneming gezien haar activiteiten bereid is te accepteren bij het nastreven van haar doelstellingen'.⁹

De risk appetite is dus een beleidskeuze en daarin heeft de onderneming in beginsel een zekere beleidsvrijheid.

Aan die beleidsvrijheid zitten grenzen, zo heeft Strik in de vergadering van de Vereniging 'Handelsrecht' naar voren gebracht, zoals wet- en regelgeving, de aard van de ondernemingsactiviteiten die tot een bepaalde prudentie kan nopen, daar waar het belang van derden in het geding is. Wat betreft het laatste geeft zij aan dat er nog een verschil in zit of bij die plannen eigenlijk vrijwillig gevaarzetting optreedt of dat die gevaren vrijwillig worden aangevaard door derden of niet.¹⁰

In de discussie daarover komt de complexiteit naar voren van 'risk appetite' en de beleidsvrijheid daarbij, in verhouding tot de belangen van derden. Timmerman stelt in dat verband – als ik hem goed begrijp – dat hij het idee heeft dat de bepaling van de 'risk appetite' een veel minder vrije beslissing is gezien de belangen van buitenstaanders.¹¹ Hammerstein stelt dat het hele begrip risicobeheersing al zit in het *Kelderluik*-arrest. Hij zegt: je zet een luik open en op het moment dat je dat doet moet je je al gaan afvragen wat daarvan de risico's zijn en hoe snel je ze kunt beheersen.¹² Dat is in feite de leer van de gevaarzetting en de zorgplichten die daaruit voortvloeien.

6. Risk appetite: waar manifesteren zich de eventuele gevolgen van een risico?

We lijken wat te worstelen bij de mate van beleidsvrijheid bij de bepaling van de 'risk appetite' van een onderneming, als daarbij de belangen van derden in het geding zijn. Om welke belangen gaat het dan? Ik denk dat de gedachtevorming rond 'risk appetite' en de vaststelling daarvan aan duidelijkheid wint als je een onderscheid maakt al naargelang waar de gevolgen van een als risico ingeschat gevaar zich manifesteren. Gaat het om de effec-

ten binnen de onderneming, of zie je met name op de effecten buiten de onderneming?

Vanouds gaat het bij het begrip 'risicomanagement' bij ondernemingen naar mijn idee om risico's in die mate dat die een negatieve neerslag kunnen hebben binnen de onderneming.¹³

Daarbij is te denken aan de gevolgen voor de resultaten van de onderneming of haar balanspositie, en eventueel voor de reputatie van de onderneming of haar producten of diensten. Ten aanzien van die risico's zal de onderneming een keuze en beoordeling maken in welke mate het de moeite waard is om die risico's te nemen. Die beoordeling wordt bepaald door een afweging tussen mogelijke opbrengsten en kosten, de wijze waarop die risico's door de betrokkenen worden gepercipieerd en de bereidheid van de betrokkenen om risico's te nemen.¹⁴

Bij het laatste zal – zo dunkt me – weer een rol spelen hoe groot de eventuele schade zal zijn, wat het zal kosten om die schade en eventuele gevolgschade ongedaan te maken, en wellicht ook in welke mate dat verzekerd of verzekeraar is.¹⁵

Uiteraard is de aldus bepaalde 'risk appetite' van invloed op het risicoprofiel van de onderneming. En dat is dus voor aandeelhouders relevant. Om die reden wordt in de Code en door Eumedion aandacht besteed aan de transparantie van de onderneming op dit punt.¹⁶

Maar aldus bezien is er een grote mate van beleidsvrijheid voor het management in het beleid ten aanzien van de 'risk appetite'. In de praktijk is te zien dat ondernemingen soms ten aanzien van bepaalde producten, de risico's of gebreken daarin, het klachtenbeleid en de klachtenafhandeling, een verschillende koers varen. Sommigen zeilen nu eenmaal scherper aan de wind. Dat kan denk ik, ook al is het niet altijd even plezierig voor de klant. Men leze er de rubriek 'Stekeligheden' in de *Consumentengids* maar op na.

7. Gevaren voor derden: geen kwestie van 'risk appetite', maar van compliance

Die beleidsvrijheid is evenwel van een geheel andere orde als het gaat om de risico's van gevaren die zich buiten de onderneming manifesteren, bijvoorbeeld als het gaat om risico's van ernstige schade voor milieu of ernstig letsel. Er is geen beleidsvrijheid ten aanzien van het accepteren van risico's van productgebreken (zoals lekken) in waterkruiken die je in je winkel verkoopt. Strik zegt dat een bedrijf dat voedingsmiddelen levert in het algemeen een

op de drempel van een nieuw decennium: een ondernemingsrechtelijke analyse (Preadvies van de Vereniging 'Handelsrecht' 2009), p. 201 e.v.

8. Zie ook de aangehaalde definitie in het COSO-raamwerk, genoemd door Strik 2010, hoofdstuk 8.

9. Strik 2010, p. 227.

10. Verslag van de vergadering van de Vereniging 'Handelsrecht' van 8 december 2009, p. 14.

11. A.w., p. 30.

12. A.w., p. 51.

13. Vergelijk ook het verband met insurance management: verzekeren we het risico ja of nee, zie Strik 2010, p. 222.

14. Strik 2010, p. 220.

15. Zie B.C.J.M. van Beurden & P.M. van der Zanden, 'Perikelen in de financiële verslaggeving', *TvOB* 2011-1, p. 1 e.v., die uitleggen dat het bestuur van de onderneming risico's moet nemen om een hoger rendement te behalen voor de aandeelhouders dan staatsobligaties, en daar inzicht in moet verschaffen. Of zoals ook wel wordt gezegd: 'Ondernemen is het nemen van beheersbare risico's'.

16. Zie Nederlandse corporate governance code 2008, die in Principe II.1 spreekt van de strategie met het bijbehorende risicoprofiel, en de Eumedion Speerpuntenbrief 2010 (te vinden op <http://eumedion.nl/home.html>).

lage 'risk appetite' zal hebben op het gebied van voedselveiligheid. Maar het is de vraag of het concept van de 'risk appetite' die de onderneming bepaalt, in dit verband wel passend is. Bij 'risk appetite' is mijns inziens met name te denken aan de 'appetite' ten aanzien van de interne financiële gevolgen of gevolgen voor de reputatie van incidenten. En daarbij kan een rol spelen de verzekeraarbaarheid, de mogelijkheden tot vervanging van het product of het uit de handel nemen daarvan, zeg maar de afgrenzing van de schade.

Maar waar het gaat om de risico's van gevaren die zich buiten de onderneming manifesteren, zoals letsel aan personen of milieuschade, past niet een beleidskeuze inzake 'risk appetite' als onderdeel van risicomanagement. Het gaat dan naar mijn idee om het door Hammerstein genoemde *Kelderluik*-arrest, met andere woorden: om de normen die voortvloeien voor de onderneming uit de gevaarzettingsleer. Aan die normen heeft de onderneming zich te houden.¹⁷ Dit is in feite het onderwerp van compliance met wet- en regelgeving.

8. Compliance: waarderingen, analyses en zorgplicht

Compliance wordt vaak gezien als een onderdeel van risicomanagement, maar wordt ook wel behandeld als een aparte categorie. Eijsbouts ziet compliance met name in relatie tot de reputatie van de onderneming.¹⁸ Impliceert compliance dat er ten aanzien van de naleving van normen geen waardering van het risico meer plaatsvindt in het kader van het risicomanagement?

Die waardering heeft nog wel een plaats, te weten als onderdeel van de risicoanalyse.¹⁹ Ingeschat moet worden hoe groot het risico is van een normschending, of het risico van aansprakelijkheid in geval van risicoaansprakelijkheid voor bijvoorbeeld gevaarlijke stoffen.

Een waardering is ook nodig met betrekking tot de naleving van zorgplichten ten aanzien van een veiligheidssituatie. De waardering dient dan om te komen tot een invulling van de zorgplicht in de concrete situatie: het gaat dan om de afweging van de zorg tegen de omvang van het risico.

In de leer van de gevaarzetting zijn er immers twee relevante factoren wat betreft de zorg:

1. de aard en het nut van de zorggedraging; in relatie tot
2. het bezwaar tot het treffen van die zorg.

En wat betreft de omvang van het risico zijn van belang:

1. de ernst van de schade; en
2. de waarschijnlijkheid van de schade.²⁰

Dáár is dus een waardering nodig om te zien hoever de zorgplicht strekt.

9. Hoever strekt de zorgplicht ten aanzien van het compliance systeem?

Het Groenboek stelt aan de orde of 'relevant key societal risks' onderdeel moeten worden van het risicomanagementsysteem van ondernemingen, ook van niet-financiële ondernemingen. Tot zover heb ik betoogd dat waar het daarbij gaat om risico's van gevaren die zich niet zozeer binnen de onderneming manifesteren maar daarbuiten, jegens derden, het niet zozeer gaat om algemeen risicomanagement, maar meer specifiek om compliance (als species van het genus risicomanagement). Voor de vaststelling van een 'risk appetite' is daar geen plaats. Maar er vindt wel een zekere waardering plaats van het risico, als onderdeel van de risicoanalyse.

Compliance als een onderdeel van risk management of van corporate governance, is op zich ook te zien als een zorgplicht van de onderneming om een goed compliance bouwwerk op te zetten. Hoe goed het compliance bouwwerk ook is, je kunt niet garanderen dat bepaalde normen binnen de onderneming door een werknemer niet worden geschonden. Maar je kunt er wel op worden aangesproken als binnen de organisatie niet de nodige maatregelen zijn getroffen om normovertreding zo veel mogelijk te voorkomen.

En hoe groot is die zorgplicht dan met betrekking tot het compliance bouwwerk? Er zal nu eenmaal een andere (voor)zorg worden verwacht van het management ten aanzien van normen waarvan de niet-naleving grote schade kan opleveren, zoals de niet-naleving van normen inzake het lozen van giftige stoffen, dan ten aanzien van de norm die geldt voor de bedrijfschauffeur om voldoende geld in de parkeermeter te stoppen.

Ik denk dat voor de zorgplicht voor het compliance bouwwerk soortgelijke criteria gelden als bij de vermogensrechtelijke leer van gevaarzetting. Ook hier gaat het om de ernst, gevaarlijkheid en waarschijnlijkheid van de schade als die zich realiseert, en de aard en het nut van het compliance systeem afgezet tegen het praktische bezwaar bij het treffen van zulke maatregelen.

Bij het opzetten van een compliance bouwwerk dienen dus steeds dit soort afwegingen en waarderingen te worden gemaakt.

10. 'Key societal risk': grote maatschappelijke gevolgen van eigen disfunctioneren

Bij compliance gaat het over de naleving van wet- en regelgeving die op de onderneming van toepassing is, zoals zorgplichten met betrekking tot veiligheid. Gelden zulke

17. Duidelijkheidshalve: bij bijvoorbeeld het risico van lekkende waterkruiken moet dus worden onderscheiden tussen het risico van gevaren voor derden en het risico van gevaren die ten gevolge van door derden geleden schade of letsel voor de onderneming dreigen zoals verhaalsacties en reputatieschade. Het concept van 'risk appetite' past wel bij het laatst bedoelde risico, maar niet bij het risico van gevaren voor derden.

18. A.J.A.J. Eijsbouts, 'Elementaire beginselen van Maatschappelijk Verantwoord Ondernemerschap', in: *Maatschappelijk verantwoord ondernemen* (Preadviezen Nederlandse Juristen-Vereniging 2010), p. 95-96; zie ook zijn beschouwingen over preventief beleid in het kader van het in aanmerking komen voor strafvermindering als het onverhoopt toch fout gaat, op p. 96.

19. Zie voor verschillende onderdelen van het risicomanagement, waaronder risicoanalyse, Strik 2010, p. 226.

20. Zie C.C. van Dam, *Aansprakelijkheidsrecht*, Den Haag: 2000, hoofdstuk 8.

zorgplichten ten aanzien van alle 'key societal risks' waarop het Groenboek doelt? Het Groenboek noemt:

'(...) risks that significantly affect society as a whole: risks related to climate change, to the environment (...), health, safety, human rights, etc.'

Voorts spreekt het Groenboek van ondernemingen die:

'(...) operate critical infrastructure, the disruption or destruction of which could have major cross-border impacts.'²¹

Ten aanzien van twee categorieën risico's is het mijns inziens de vraag of die vandaag de dag onder een zorgplicht van de onderneming vallen.

Ten eerste noem ik de categorie van het risico van de grote impact op de maatschappij als geheel van het omvallen of disfunctioneren van de eigen onderneming, de 'major cross border impacts van de critical infrastructure operations' waarvan het Groenboek spreekt. Het gaat om risico's die vergelijkbaar zijn met de risico's die geschetst worden in de verschillende vormen van (voorstellen tot) regelgeving voor financiële instellingen: grote maatschappelijke gevolgen van het disfunctioneren of omvallen van de instelling.

Naarmate die maatschappelijke impact groter is, dient het risicomanagementsysteem als geheel op een hoger plan te worden getild. De Code Banken voorziet in dit verband in het volgende:

- een sterkere betrokkenheid van de raad van commissarissen bij het risicomangement;
- binnen het bestuur is één lid daarvan in het bijzonder belast met besluiten op het gebied van risicomangement;
- een goedkeuringsproces van nieuwe producten in het kader van risicomangement.²²

Het resulteert in feite in een op een hoger plan tillen van het risicomangement als geheel, dat ook gevolgen heeft voor de mate van beleidsvrijheid bij het bepalen van de 'risk appetite'.²³

De vraag dringt zich op, op welke ondernemingen dit daadwerkelijk van toepassing is. Geldt hier de eis van een domino-effect? Of van een moeilijke vervangbaarheid van de toelevering van de producten en/of diensten? Zoals bijvoorbeeld kan gelden voor het functioneren van de nationale luchthaven die cruciaal is voor de logistiek in het land? Het voert te ver om hierop in te gaan, maar nadere overdenking leidt mogelijk tot de vraag of het hierbij niet vooral om publieke functies gaat, met de vervolgvraag of de bescherming daarvan niet met name gezocht moet worden in het als overheid in eigen hand

houden van die functies, of in het stellen van strenge regels – o.a. ter zake van risicomangement – in geval van privatisering.

Overigens is het de vraag hoe je moet omgaan met de beoordeling of het disfunctioneren van de eigen onderneming wel leidt tot zulke grote maatschappelijke gevolgen, als hier bedoeld. Wie bepaalt of dat het geval is? Ondernemingen kennen zichzelf nog wel eens een belangrijke maatschappelijke functie toe, maar dat zou wel eens anders kunnen zijn als het gaat om de vraag naar de gevolgen van het eigen disfunctioneren, met name indien het antwoord daarop leidt tot een aanzienlijke verzwaring van het eigen risicomanagementsysteem – met alle kosten van dien – en een inperking van de beleidsvrijheid op dat gebied. Het komt me voor dat het met het oog op een *level playing field* wenselijk is dat de criteria voor de beantwoording van deze vraag op EU-niveau worden vastgesteld.

11. 'Key societal risks': human rights: reikwijdte verplichtingen?

Een tweede categorie van risico's waarbij vragen kunnen rijzen ten aanzien van (in het bijzonder de precieze inhoud en reikwijdte van) de zorgplicht is die van 'human rights' waaraan het Groenboek refereert. Goed denkbaar zijn immers situaties dat er niet rechtens een zorgplicht op de onderneming rust, terwijl de operaties van de onderneming, of het enkele plaatsvinden daarvan mogelijk wel een directe of indirecte invloed heeft op de lokale mensenrecht situatie.

Kent de onderneming een eigen gedragscode voor verantwoord ondernemen, dan mag zij denk ik worden aangesproken op een compliance systeem ten aanzien van de handhaving daarvan.²⁴ Maar voor het overige is het gebied van mensenrechten een gebied dat zeer moeilijk is af te bakenen met betrekking tot de precieze verplichtingen dienaangaande van de onderneming. Zo getuige ook het vele denkwerk dat daarover inmiddels is verricht; zie bijvoorbeeld de preadviezen voor de Nederlandse Juristen Vereniging en de dissertatie van Lambooy.²⁵ Hetzelfde geldt voor het bredere onderwerp van maatschappelijk verantwoord ondernemen, dat in feite aan de orde is als het gaat om onderwerpen als 'climate change' en 'environment' als door het Groenboek genoemd.²⁶ Ook hier komt de vraag naar voren of de zorgplichten op deze gebieden voldoende nauwkeurig zijn afgebakend, om de naleving daarvan in te bedden in het risicomanagementsysteem. Ik denk dat daarvoor eerst een nadere afbakening, bijvoorbeeld in de vorm van voor de onderneming geldende 'business principles' nodig is. Zo'n code wordt ook juist opgesteld als positiebepaling van de onderneming naar aanleiding van een interne discussie en een externe dialoog met 'interest groups' over hoever die verantwoordelijk-

21. Zie p. 10.

22. Zie Code Banken, par. 4. Zie hierover o.a. C.W.M. Lieverse, 'De Code banken', *FR* 2009-10, p. 391.

23. Zie hiervoor par. 3 e.v.

24. Zie Eijsbouts, a.w., p. 93.

25. Zie voornoemde Preadviezen Nederlandse Juristen-Vereeniging 2010, van de hand van A.J.A.J. Eijsbouts, F.G.H. Kristen, J.M. de Jongh, A.J.P. Schild & L. Timmerman, alsook T.E. Lambooy, *Corporate Social Responsibility* (diss. Leiden), Deventer: 2010.

26. Vergelijk bijvoorbeeld de door Lambooy in haar dissertatie in hoofdstuk 11 genoemde zorg ten aanzien van 'sustainable water use' door de onderneming.

heid van de onderneming moet strekken in de verschillende landen waar zij activiteiten uitoefent, en veelal niettegenstaande de lokale minder strenge normen op dit punt.²⁷

12. Afronding

In het Groenboek inzake het EU corporate governance framework wordt de suggestie gedaan dat het risicomanagementsysteem van de onderneming ook 'key societal risks' zou moeten bestrijken. Dat levert een aantal vragen op in verband met de tot nu toe gebruikelijke inrichting van een risicomanagementsysteem. Zo geldt mijns inziens dat de 'risk appetite' en de daarbij geldende beleidsvrijheid van de onderneming met name betrekking heeft op risico's met daaruit voortvloeiende gevaren voor de onderneming. Gaat het om gevaren die voor derden uit risico's voortvloeien, dan is – naar Nederlands recht – de vermogensrechtelijke leer van gevaarstelling in het geding, met inbegrip van de zorgplichten die daaruit voor de onderneming voortvloeien. Dat is een onderwerp voor het binnen de onderneming geldende systeem van compliance met wet- en regelgeving. Op zich betekent dat niet dat ten aanzien daarvan aan de onderneming geen beleidsvrijheid toekomt, maar die is wel anders en zeker beperkter van aard. Bij het inrichten van een compliance bouwwerk binnen de onderneming dienen een aantal waarderings- en analyses van eigen aard te worden gemaakt. Hetzelfde geldt voor de daaraan voorafgaande bepaling van de inhoud en reikwijdte van de zorgplicht van de onderneming.

Overigens is het ten aanzien van een aantal in het Groenboek genoemde categorieën van 'key societal risks' niet duidelijk of en in welke mate daarvoor vandaag de dag een zorgplicht van de onderneming geldt. Zo rijst een aantal vragen ten aanzien van de door het Groenboek genoemde situatie van ondernemingen die 'operate critical infrastructure, the disruption or destruction which could have major cross-border impact'. Ook ten aanzien van de categorie 'human rights' rijst de vraag of deze op dit moment reeds voldoende afgebakend zijn om geïncorporeerd te worden in het risicomanagementsysteem van de onderneming.

Een en ander geeft wel aan dat de materie van 'key societal risks' eerst verder moet worden doordacht voordat gekomen wordt tot regelgeving die ertoe verplicht deze risico's deel uit te laten maken van het risicomanagementsysteem van de onderneming.

27. In de interne verhoudingen binnen de onderneming zal de gedragscode nadere invulling geven aan de voor de bestuurders van de vennootschap geldende normen van behoorlijk bestuur; zie van mijn hand: 'De zorgplichten van de bestuurder van een rechtspersoon', *Onderneming en Financiering* 2010 (18) 2, p. 93 e.v., op p. 104.