2011

Universiteit Twente

Naam Student: Martijn Mensink
Studentnummer: 0098469
Onderwijsinstelling: Universiteit Twente
Studierichting: Bedrijfswetenschappen
Begeleider: Prof. dr. P.B. Boorsma
Tweede begeleider: Prof. dr. ir. J.I.M. Halman
Soort opdracht: Bacheloropdracht

RISICOMANAGEMENT

RISICOMANAGEMENT EN RISK MATURITY IN DE PRAKTIJK

Samenvatting

Deze scriptie beschrijft een onderzoek op het gebied van risicomanagement en risk maturity dat is gedaan ter afronding van de bachelor bedrijfskunde aan de Universiteit Twente. De aanleiding voor het doen van een onderzoek op het gebied van risicomanagement is de verschijning van het ISO31000 risicomanagementraamwerk, waardoor mijn interesse in dit steeds belangrijker wordende vakgebied is ontstaan. De doelstelling voor het onderzoek is de *risk maturity* van een vijftal organisaties in kaart te brengen en tevens om te onderzoeken wat deze organisaties in concreto gedaan hebben om het risicomanagement binnen hun organisatie te verbeteren.

Middels literatuurstudie is onderzocht wat risicomanagement is en aan welke criteria organisaties met een goed ontwikkeld risicomanagement te herkennen zijn. Op basis van de literatuur met daarin centraal de ISO31000 is een lijst met beoordelingscriteria opgesteld, op grond waarvan vervolgens een lijst met enquêtevragen is samengesteld. Deze enquête is voorgelegd aan de risicomanagers van de vijf organisaties. De vragen zijn hoofdzakelijk geformuleerd als stellingen waarvan de respondent middels een Likertschaal kon aangeven in welke mate de stelling van toepassing is op de organisatie. De enquête diende bovendien om te onderzoeken welke concrete maatregelen de organisaties gedurende de afgelopen twee jaar hebben genomen om het risicomanagement van hun organisatie te verbeteren.

Op basis van de resultaten van de enquête zijn scores toegekend aan de vijf organisaties. Twee van de vijf organisaties scoren uitgesproken hoog op risk maturity; beide organisaties hadden een score die nagenoeg op de grens tussen niveaus 4 en 5 ligt. Twee van de overige organisaties zijn ingedeeld in niveau 4 en één organisatie is ingedeeld in niveau 3. Alle vijf onderzochte organisaties blijken formeel risicomanagement toe te passen, dat de basis vindt in het *Enterprise Risk Management Framework* (ERMF) van COSO.

Naast het in kaart brengen van de *risk maturity* van de vijf organisaties, is onderzocht wat zij gedurende de afgelopen twee jaar in concreto gedaan hebben om risk maturity te verbeteren. De vijf organisaties hebben gedurende de afgelopen twee jaar allerlei verschillende maatregelen genomen om het risicomanagement binnen hun organisatie te verbeteren. Drie specifieke maatregelen werden genoemd door de risicomanagers van meerdere van de organisaties. Dat is ten eerste het duidelijker toewijzen van verantwoordelijkheden, ten tweede het consistenter toepassen van het risicomanagementproces in projecten en ten slotte het benadrukken van en extra aandacht schenken aan de belangrijkste risico's.

Inhoudsopgave

1 Introductie: Onderzoeksvoorstel

1.1 Inleiding risicomanagement

Onder risicomanagement verstaan we de gecoördineerde activiteiten om een organisatie te sturen en beheersen met betrekking tot risico (ISO/IEC 2002). Dit is vrij vertaald de definitie zoals omschreven in de ISO Guide73, de woordenlijst voor risicomanagement die de *International Organisation for Standardization* (ISO) heeft opgesteld. De ISO is een internationaal instituut dat internationale standaarden ontwikkelt en bepleit. De organisatie bestaat uit vertegenwoordigers van vele nationale standaardisatie-instituten en ontwikkelt op velerlei gebied internationale standaarden. De Guide73 heeft tot doel er voor te zorgen dat alle spelers in het risicomanagement dezelfde vaktaal spreken. In 2009 gepubliceerde de ISO een risicomanagementstandaard met de naam ISO31000. Hierin is de consensus zoals die tot dusver binnen het domein van de toepassing van risicomanagement bestaat samengepakt. Daarom zal ik in dit onderzoek zo veel mogelijk gebruik maken van de definities en methoden zoals gedefinieerd door de ISO in Guide73 en de ISO31000.

De ISO31000 zou een paraplufunctie moeten gaan vervullen, zodat reeds bestaande risicomanagementsystemen zoals dat van COSO en de ISO-Guide73 – Risk Management Vocabulary – onder één paraplu vallen. Een groot voordeel is dat de ISO een wereldwijd gerespecteerd instituut is. De ISO31000 is dan ook het resultaat van consensus tussen een groot aantal experts op het gebied van risicomanagement vanuit de hele wereld. Als de ISO31000 op grote schaal geaccepteerd wordt, wordt het voor wetenschappers en mensen uit het bedrijfsleven mogelijk om wereldwijd middels dezelfde vaktaal te communiceren.

Binnen dit onderzoek zullen risicomanagement en *risk maturity* centraal staan. *Risk maturity* is een maat voor de invoering en integratie van risicomanagement. Organisaties kunnen worden ingedeeld in verschillende niveaus van *risk maturity*, waarbij het laagste niveau van *risk maturity* correspondeert met een organisatie zonder enige vorm van risicomanagement en waarbij het hoogste niveau overeenkomt met een volledige inbedding en integratie van risicomanagement binnen de organisatie (Hillson 1997). Het doel van dit onderzoek is te bepalen welke concrete acties een vijftal geselecteerde organisaties heeft ondernomen om risicomanagement binnen hun organisatie naar een hoger niveau van *risk maturity* te brengen.

Het eerste deel van dit onderzoek zal derhalve bestaan uit een literatuurstudie, gevolgd door een empirisch deel met betrekking tot de praktijk van risicomanagement. Voor het empirische onderdeel zijn vijf organisaties bereid gevonden om hun medewerking te verlenen.

1.2 Aanleiding

In 2009 publiceerde de Internationale Organisatie voor Standaardisatie de ISO31000. Deze standaard definieert algemene richtlijnen en begrippen ten behoeve van adequate toepassing en implementatie van risicomanagement. De ISO31000 vertegenwoordigt de consensus tussen managementprofessionals en -wetenschappers wereldwijd.

De naderende verschijning van de ISO31000 prikkelde mijn nieuwsgierigheid naar risicomanagement. Gedurende mijn bachelorperiode van bedrijfswetenschappen aan de

Universiteit Twente zijn veel verschillende disciplines uit de bedrijfswetenschap aan bod gekomen, maar vreemd genoeg is risicomanagement nooit uitgebreid behandeld. Mede door onvoorziene gebeurtenissen zoals de aanslagen van 9/11, omvangrijke boekhoudschandalen en de huidige economische crisis, is gedurende het afgelopen decennium steeds meer aandacht voor risicomanagement gekomen. In het kader van mijn bacheloropdracht zou ik graag meer te weten willen komen over deze steeds belangrijker wordende discipline binnen de bedrijfswetenschap.

1.3 Probleemstelling

Het onderzoek zal betrekking hebben op wat *risk maturity* inhoudt, hoe verschillen in *risk maturity* kunnen worden onderscheiden en wat organisaties doen om een hoger niveau van *risk maturity* te bereiken. Het onderzoek dient zowel wetenschappelijke als praktisch relevante waarde hebben, en theoretische kennis en een zelf te verrichten empirisch onderzoek zullen daarin samenkomen. Derhalve zal het bestaan uit een theoretisch deel en een empirisch deel. In het theoretische deel zal worden ingegaan op wat risicomanagement in het algemeen inhoudt en wat *risk maturity* is. Op basis van de beschreven theorie zal een enquête worden opgesteld, waarmee de *risk maturity* van een organisatie in kaart gebracht kan worden en waarmee in kaart kan worden gebracht wat in concreto gedaan is om *risk maturity* te verbeteren.

1.4 Onderzoeksvragen

De centrale onderzoeksvraag waarop een antwoord gezocht zal worden is als volgt geformuleerd:

- Hoe *risk mature* zijn vijf geselecteerde organisaties en wat hebben deze organisaties gedaan om hun *risk maturity* to doen toenemen?

Er zal worden onderzocht hoe *risk mature* de vijf organisaties op dit moment zijn en daarnaast wordt – gestoeld op de theorie met betrekking tot risicomanagement en *risk maturity* – onderzocht welke stappen zij hebben ondernomen om een hoger niveau van *risk maturity* te bereiken.

Daarnaast zijn de volgende deelvragen geformuleerd:

1) Wat is risicomanagement volgens algemeen geaccepteerde wetenschappelijke literatuur?
2) Wat is *risk maturity* en welke fasen kunnen daarin worden onderscheiden?
3) Hoe *risk mature* zijn een vijftal geselecteerde organisaties?
4) Wat hebben deze vijf organisaties gedaan om de *risk maturity* van hun organisatie te verbeteren?

1.5 Methoden

Hieronder zal worden uitgewerkt met behulp van welke methoden de deelvragen beantwoord zullen worden.

1) *Wat is volgens algemeen wetenschappelijk geaccepteerde literatuur goed risicomanagement?*

   Deze vraag zal op basis van literatuurstudie beantwoord worden. In het hoofdstuk waarin deze vraag behandeld wordt, zal worden uitgelegd wat risicomanagement is en zal het risicomanagementproces worden beschreven. Naast wetenschappelijke literatuur zal ook gebruik worden gemaakt van standaarden en raamwerken als ISO en COSO. Risicomanagement richt zich achtereenvolgens op risico-identificatie, risico-evaluatie, en de beslissing van het beheersen van risico's en het zelf dragen of out-sourcen van risico's (P.F. Claes 1997; ISO/FDIS 2009). Deze onderdelen zullen in dit hoofdstuk aan bod komen.

2) *Wat is risk maturity en wat kan een organisatie doen om een hoger niveau van risk maturity te bereiken?*

   De term en het achterliggende concept zijn nog betrekkelijk jong en in boeken over risicomanagement is derhalve nog niet veel te vinden over *risk maturity*. Modellen en theorieën over *risk maturity* komen vooralsnog hoofdzakelijk vanuit het bedrijfsleven en consultancybureaus. Met betrekking tot de empirische onderbouwing van de modellen en theorieën is de spoeling uiterst dun (Staveren 2009). Bestaande modellen zullen daarom uitgebreid onder de loep worden genomen en worden gecontroleerd op een logische onderbouwing, voordat elementen worden overgenomen.
   Risk maturity gaat over de mate waarin risicomanagement is geïntegreerd in organisaties, waarbij niveau één correspondeert met een organisatie zonder een formeel risicobeleid en het hoogste niveau overeenkomt met een volledige inbedding en integratie van risicomanagement in de gehele organisatie (Hillson 1997). In het hoofdstuk waarin de tweede deelvraag wordt beantwoord, zal worden gezocht naar manieren waarop organisaties een hoger niveau van *risk maturity* kunnen bereiken.

3) *Hoe Risk Mature zijn een vijftal geselecteerde organisaties?*

   Daartoe dient empirisch onderzoek gedaan te worden bij de drie geselecteerde organisaties. Op basis van de eerder geformuleerde criteria en bijbehorende enquêtevragen zal geprobeerd worden de organisaties te kwalificeren met betrekking tot de mate van *risk maturity*. De uitdaging zal liggen in het selecteren van de meest relevante toetsingscriteria.

4) *Wat hebben de vijf geselecteerde organisaties gedaan om de risk maturity van hun organisatie te verbeteren?*

   Op basis van de antwoorden op de eerste twee deelvragen, aangevuld met verder literatuuronderzoek, zal een model opgesteld worden waarin eigenschappen van een goed risicomanagementsysteem vanuit het oogpunt van *risk maturity* verwerkt zullen worden. Op basis van dit model zullen enquêtevragen opgesteld worden met behulp waarvan bepaald kan worden hoe een onderneming in praktijk omgaat met risicomanagement. Een model is per definitie een versimpelde weergave van de

werkelijkheid – hetzelfde geldt voor modellen van *risk maturity*. Werkelijk bestaande organisaties zullen wat bepaalde aspecten betreft in te delen zijn in het ene niveau, maar wat andere aspecten betreft in te delen zijn in een ander niveau. Het zal daarom een grote uitdaging worden om te bepalen in welk niveau van *risk maturity* de drie geselecteerde organisaties ingedeeld moeten worden. Naast het in kaart brengen van de *risk maturity*, wordt onderzocht wat de organisaties in concrete zin ondernomen hebben om de *risk maturity* te verbeteren.

1.6 Indeling scriptie

Hieronder volgt de geplande indeling van het verslag.

Samenvatting
De samenvatting zal maximaal één pagina beslaan. Hierin zal een zo beknopt mogelijke, maar toch ook zo volledig mogelijke samenvatting van het gehele onderzoeksverslag gegeven worden. Tevens zullen de belangrijkste termen en begrippen gedefinieerd worden.

Hoofdstuk 1 Introductie: Onderzoeksvoorstel
Dit hoofdstuk geeft de aanleding tot het onderzoek, de probleemstelling, de onderzoeksvragen en de gebruikte methoden. Voor het eindverslag zal deze tekst als gevolg van voortschrijdend inzicht mogelijk worden uitgebreid en aangevuld. Verder zal dit hoofdstuk bestaan uit een korte beschrijving van het onderzoeksdomein. De probleemstelling is een concrete formulering van de vraag waarop het onderzoek een antwoord poogt te vinden. Deze probleemstelling is verder onderverdeeld is deelvragen, welke gezamenlijk de hoofdvraag pogen te beantwoorden. De methoden en methodologie die zullen worden aangewend bij het beantwoorden van de vragen worden vervolgens benoemd en uitgelegd.

Hoofdstuk 2 Risico & Risicomanagement
In dit hoofdstuk zal een antwoord worden gezocht op de volgende deelvraag: Wat is risicomanagement volgens algemeen wetenschappelijk geaccepteerde literatuur?

Hoofdstuk 3 Het risicomanagementproces
In dit hoofdstuk wordt de kern van risicomanagement beschreven, het risicomanagementproces.

Hoofdstuk 4 Enterprise Risk Management en Risk Maturity
In dit hoofdstuk zal een antwoord worden gezocht op de volgende deelvraag: Wat is *risk maturity* en wat kan een organisatie doen om een hoger niveau van *risk maturity* te bereiken? In dit hoofdstuk zullen de belangrijkste algemene kenmerken van een goed risicomanagement-systeem worden beschreven en er worden beoordelingscriteria geformuleerd waarmee de mate van *risk maturity* van een organisatie in kaart gebracht kan worden.

Hoofdstuk 5 Resultaten: Risk Maturity in de praktijk
In dit hoofdstuk wordt de voor dit onderzoek samengestelde enquête beschreven en worden de resultaten hiervan besproken. Op basis van de antwoorden op de enquête wordt de mate van *risk maturity* van de vijf geselecteerde organisaties in kaart gebracht. De enquête dient

daarnaast om duidelijkheid te krijgen met betrekking tot wat de geselecteerde organisaties hebben gedaan om *risk maturity* te verbeteren.

Hoofdstuk 6 Conclusie en discussie
De belangrijkste bevindingen zullen in dit hoofdstuk worden benoemd. Het is bijvoorbeeld interessant om te beschouwen welke aspecten van risicomanagement de drie geselecteerde organisaties beter of minder goed beheersen.

2 Risico & Risicomanagement

2.1 Ontstaan Risicomanagement

Er zijn voorbeelden bekend uit de jaren ’40 en ’50 van de vorige eeuw waarbij risicomanagement een centraal onderdeel vormde van het besluitvormingsproces (Dickinson 2001). Risicomanagement bestaat in zijn huidige vorm echter pas vanaf de jaren ‘60 (Hedges 1965; Denenberg and Ferrari 1966; Dickinson 2001). Organisaties hebben altijd al te maken gehad met risico’s. Tegen veel risico’s konden organisaties zich ook vroeger al verzekeren, zoals tegen brand, overstroming, diefstal en persoonlijke fouten. Het is dan ook niet gek dat risicomanagement zijn oorsprong vond in het verzekeringswezen (Dickinson 2001). De verzekeringswereld realiseerde zich met de tijd dat verzekeren niet de enige oplossing was om risico het hoofd te bieden, maar dat ook maatregelen getroffen konden worden om risico’s zelf, of de impact van risico’s te verminderen (Olson 2007).

Hoewel de ontwikkeling van risicomanagement sinds de zestiger jaren geleidelijk is voortgezet (Snider 1991), is de opgang in een stroomversnelling terechtgekomen vanaf het begin van de jaren negentig, toen de *Committee of Sponsoring Organizations of the Treadway Commission (COSO)* naar aanleiding van een aantal boekhoudschandalen en gevallen van fraude het rapport *Internal Control – Integrated Framework (ICIF)* publiceerde (Knechel 2007). In dit document uit 1992 werd een raamwerk[1] gepresenteerd op basis waarvan organisaties hun *internal control* kunnen vormgeven en beoordelen. *Internal control* heeft tot doel er voor te zorgen dat een organisatie op de hoogte is van de stand van zaken met betrekking tot productieprocessen, financiële rapportage en de relevante wet- en regelgeving (COSO 1992).

In het begin van het nieuwe millennium waren er in de Verenigde Staten een aantal zeer omvangrijke fraudeschandalen, waarvan die bij Enron en WordCom twee van de bekendste zijn. Naar aanleiding van die schandalen besloot de Amerikaanse overheid strengere wetten te formuleren en streng toezicht te houden op naleving van die wetten. Deze wetten en regels werden verzameld in de *Sarbanes-Oxley Act* (SOA) uit 2002 (Sarbanes-Oxley 2002 ; Beasley, Clune et al. 2005). In Europa zijn vergelijkbare codes opgesteld. Zo kennen de Duitsers het *Gesetz zur Kontrolle und Transparanz im Unternehmens-bereich* (KonTraG), hebben de Engelsen het *Turnbull report*, de Fransen de *Loi sur la Sécurité Financière* (LSF) en kennen we in Nederland de *Code Tabaksblat*. Hoewel COSO’s ICIF in het eerste decennium na publicatie zeker een belangrijke rol speelde in de verdere opkomst van risicomanagement, werd het raamwerk pas tien jaar later – toen de Sarbanes-Oxley Act in werking trad – echt populair (Bowling and Rieger 2005).

Inmiddels is het ICIF raamwerk uitgegroeid tot het wereldwijde standaardwerk voor interne controle (Paape 2006). In 2004 publiceerde COSO het rapport *Enterprise Risk Management – Integrated Framework (ERMF)*. Dit rapport bouwt voort op *ICIF*, waarbij meer de nadruk wordt gelegd op risicomanagement in een breder perspectief. Het rapport beoogt organisaties te ondersteunen in het opzetten of verbeteren van hun *Enterprise Risk Management (ERM*). ERM is een systematische en organisatiebreed geïntegreerde methode

[1] Het Engelse woord *framework* wordt in dit verslag vertaald als raamwerk.

om alle risico's waar een organisatie mee te maken krijgt te kunnen managen (Dickinson 2001). In Nederland is de ERMF van COSO met ruim driekwart verreweg de meest gebruikte risicomanagementstandaard (Paape 2006).

Was risicomanagement oorspronkelijk primair een middel om risico's te beheersen, tegenwoordig ontwikkelt het zich daarnaast in toenemende mate tot een middel om aan de buitenwacht te laten zien dat een onderneming op een verantwoorde manier opereert en zich aan de regels houdt. Hierdoor ontstaat het risico dat risicomanagement leidt tot een afvinkmentaliteit (Paape 2006).

2.2 Wat is risico?

Risico wordt in ISO/IEC Guide73 – *Risk Vocabulary* omschreven als het effect van onzekerheid op doelstellingen (ISO/IEC 2002). Een vergelijkbare definitie is die van Chapman en Ward: risico is de mogelijkheid van nadelige afwijkingen van verwachtingen (Chapman and Ward 2004). Kaplan en Garrick omschrijven risico als het product van onzekerheid en mogelijke schade als gevolg van deze onzekerheid (Kaplan and Garrick 1981).

Hoewel er vele verschillende definities van risico bestaan (Christensen, Andersen et al. 2003), bevat de definitie vaak een element met betrekking tot onzekerheid – de kans op een bepaalde gebeurtenis – en een element met betrekking tot de verwachte uitkomsten van die eventuele gebeurtenis, i.e. een gevolg-component (Aven and Renn 2009). Andere wetenschappers nemen in de definitie een element op dat aangeeft dat risico ook positieve effecten kan hebben; de zogenaamde *upside* van een risico (Jaafari 2001; Hillson 2002; Haimes 2009). Dit zijn risico's die bewust worden geaccepteerd, wetende dat negatieve consequenties kunnen volgen, maar waarbij wordt gespeculeerd op een positieve uitkomst. Dergelijke risico's worden speculatieve risico's – of meer gebruikelijk – ondernemersrisico's genoemd (Claes P.F. 1997). De opneming van positieve effecten in de definitie van risico is echter controversieel – niet in de laatste plaats vanwege de strijdigheid met de betekenis van het woord in alledaags gebruik, waar het woord een negatieve connotatie heeft (March and Shapira 1987). Hoewel belangrijke instituten zoals de COSO de mogelijk positieve effecten van risico opnemen in hun definitie, beperk ik mij in dit werk tot de zogenaamde zuivere risico's. Dit zijn risico's die enkel een negatieve uitkomst kunnen hebben (Claes P.F. 1997). Voorbeelden van zuivere risico's zijn brand, diefstal en het kapot gaan van productiemachines.

Door risico als een slechts tweedimensionaal fenomeen te beschouwen – dat bestaat uit een kans-component en een gevolg-component – ligt het wellicht voor de hand om risico uit te drukken in een getal dat ontstaat door kans en gevolg met elkaar te vermenigvuldigen (Kaplan and Garrick 1981). Hoewel deze mathematische benadering zinvol kan zijn, zijn veel wetenschappers tegenwoordig van mening dat hierbij voorzichtigheid geboden is, omdat het kan leiden tot een irreëel beeld van risico als te veel waarde wordt gehecht aan de cijfermatige uitkomst (Williams 1996; Ward 1999). Het toepassen van een dergelijke methode om risico te classificeren zou er bijvoorbeeld toe kunnen leiden dat een simpele regenbui en een tsunami als even risicovol worden beoordeeld: de kans dat een regenbui zich voordoet is groot maar de gevolgen zijn doorgaans onbeduidend, terwijl de kans op een tsunami juist klein is maar het effect desastreus kan zijn (Heijden 2006). Het enkel werken

met een dergelijke mathematische benadering kan er daarom toe leiden dat extreme situaties niet worden opgemerkt. Een kwalitatieve benadering is daarom nog steeds noodzakelijk om de tsunami van de normale regenbui te onderscheiden. Hoewel het toekennen van een getalmatige waarde aan risico's zeer nuttig kan zijn om een globaal beeld van risico te vormen, is het raadzaam gebruik te maken van zowel kwalitatieve als kwantitatieve methodes. Alleen dan kan een risico juist worden beoordeeld en kan effectief bepaald worden hoe het risico behandeld moet worden (Ward 1999; Haimes 2009).

2.3 Wat is risicomanagement?

Net als het geval is met het woord risico, bestaan er veel verschillende definities van risicomanagement. In de ISO/IEC Guide73 – *Risk Vocabulary* wordt risicomanagement gedefinieerd als de gecoördineerde activiteiten om een organisatie te sturen en beheersen met betrekking tot risico (ISO/IEC 2002). Claes definieert risiciomanagement als volgt: "Risicomanagement betreft een systematisch en regelmatig onderzoek naar de risico's die mensen, materiële en immateriële belangen en activiteiten bedreigen en de formulering en implementatie van een geïntegreerd beleid met betrekking tot risicoreductie, risico-overdracht en risicofinanciering" (P.F. Claes 1997).

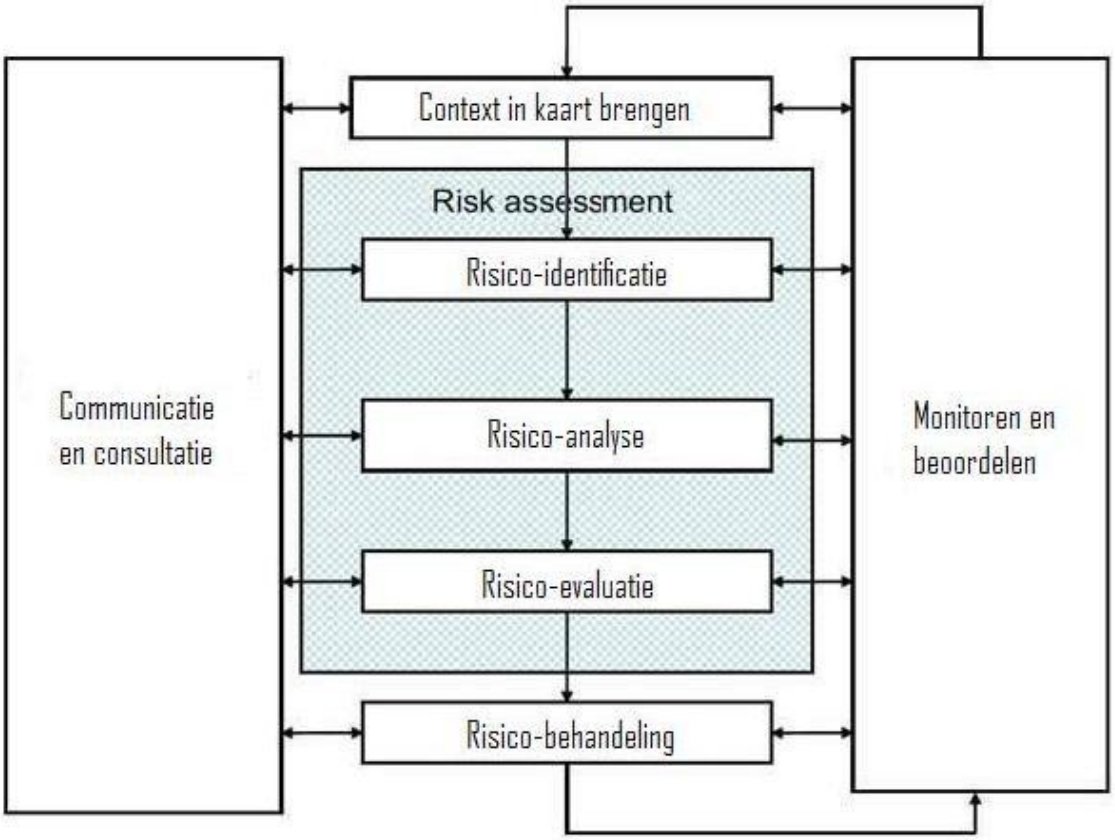
Risicomanagement is niet een geïsoleerde managementpraktijk, maar een organisatiebreed, constant proces (ISO/IEC 2002). Risicomanagement dient een constant proces te zijn omdat de context constant verandert, waardoor bestaande risico's evolueren en nieuwe risico's ontstaan (Power 2001). De term risicomanagement verwijst naar de zogenaamde architectuur voor het managen van risico's. Deze architectuur bestaat uit geformaliseerde raamwerken en processen, welke zijn gebaseerd op algemeen geaccepteerde theorieën met betrekking tot risicomanagement (ISO/FDIS 2009).

Op dit moment is COSO's ERMF in ieder geval in Nederland (Paape 2006), maar waarschijnlijk ook wereldwijd het meest gebruikte risicomanagementraamwerk (Simkins and Ramirez 2007). In dit verslag staat echter het meer recente raamwerk ISO31000 centraal. De onderlinge afstemming tussen de vele bestaande raamwerken is niet altijd even goed, mede doordat niet iedereen dezelfde definities van begrippen hanteert (Barateiro and Borbinha 2011). De ISO heeft met de ISO31000 gepoogd de gemene deler van de belangrijkste van de bestaande raamwerken te vatten. Op het eerste oog lijken de ERMF en ISO31000 heel verschillend, maar in de basis zijn ze eigenlijk zeer vergelijkbaar. Een belangrijk verschil is dat de ISO31000 zich in hoofdzaak richt op de zuivere risico's, terwijl in de ERMF de zogenaamde *upside* een centrale rol speelt.

3 Het risicomanagementproces

Risicomanagement is een complexe zaak. Het nemen van beslissingen waarbij onzekerheid een rol speelt behelst elk facet van onze levens en is derhalve ook verbonden aan elk proces binnen organisaties. Risico en onzekerheid zijn overal en daarom is het lastig om te bepalen welke risico's extra aandacht verdienen en op welke manier ze behandeld moeten worden. Het is onmogelijk om alle risico's te beschouwen en beheersen. Daarom is de selectie van nader te onderzoeken risico's cruciaal. Een tweede oorzaak van de complexiteit van risicomanagement is de multidisciplinairiteit ervan. Risico en onzekerheid treden op bij elk bedrijfsonderdeel – elk bedrijfsonderdeel heeft te maken met andersoortige risico's en houdt er vaak een eigen benadering op na (Haimes 2009).

Het risicomanagementproces bestaat uit de systematische toepassing van managementbeleid, procedures en praktijken met betrekking tot de activiteiten van communiceren, consulteren, het in kaart brengen van de context, het identificeren, het analyseren, het evalueren, het behandelen en het monitoren en herbeschouwen van risico's (ISO 2009). Een centraal onderdeel van het risicomanagementproces behelst het in kaart brengen van risico's en het behandelen van die risico's. Er bestaan gestandaardiseerde methoden om risicomanagement effectief en efficiënt aan te pakken, maar dit betekent niet dat risicomanagement kan worden bedreven op een kookboekmanier. Elke organisatie is uniek en daarom dient ook het risicomanagement van elke organisatie uniek te zijn, afgestemd op de specifieke omstandigheden van de organisatie (Chopra and Sodhi 2004; ISO/FDIS 2009).



Figuur 1 Risicomanagementproces (bewerkt naar ISO/FDIS, 2009)

Figuur 1 is een bewerking van een schema van het risicomanagementproces uit ISO31000. Hierin wordt weergegeven uit welke elementen het risicomanagementproces bestaat en hoe deze zich tot elkaar verhouden. Bovenaan in deze figuur staat het *in kaart brengen van de context*. De volgende stap is *risk assessment*, i.e. het in kaart brengen van risico's. Bij gebrek aan een Nederlandse term die de lading voldoende dekt, zal in dit verslag voor het in kaart brengen en beoordelen van risico's de Engelse term *risk assessment* worden gebruikt. *Risk assessment* wordt onderverdeeld in *risico-identificatie, risico-analyse en risico-evaluatie*. De laatste stap van het risicomanagementproces is het *behandelen van risico*. Aan weerzijden van de kolom met de centrale processen staan blokken met daarin *communicatie en consultatie* en *monitoren en beoordelen.* Deze balken staan in verbinding met elk ander blokje en dus met elk element van risicomanagement. Via monitoren en beoordelen treedt bovendien terugkoppeling naar het eerste element van risicomanagement op - het in kaart brengen van de context. Op deze wijze wordt een kringloop gesloten.

3.1 Context

Om een goed risicomanagementplan op te stellen en te implementeren dient rekening gehouden te worden met de specifieke eigenschappen en behoeften van een organisatie: haar doelstellingen, structuur, operationele activiteiten, processen, functies, projecten, producten, diensten en bezit (ISO/FDIS 2009). Daarom begint risicomanagement niet met de risico's waar de organisatie mee te maken heeft, maar met de organisatie zelf – om

risicomanagement te doen slagen is het van groot belang het risicomanagement precies af te stemmen op de betreffende organisatie en derhalve de zogenaamde *context* in kaart te brengen (Chopra and Sodhi 2004; ISO/FDIS 2009). Wat in de ISO31000 context wordt genoemd, komt grofweg overeen met wat in COSO's ERMF wordt geschaard onder de noemers *interne omgeving*, *doelstellingen* en *risk appetite* (Bowling and Rieger 2005). *Risk appetite* wordt ook genoemd in de ISO73 en ISO31000. De *risk appetite* van een organisatie zegt iets over het soort risico's dat de organisatie wil nemen en over de mate waarin zij bereid is risico's te nemen.

Het in kaart brengen van de context staat bovenaan in *figuur 1*. De context wordt lang niet altijd met nadruk genoemd in de literatuur. De nadruk ligt meestal op *risk assessment*. *Risk assessment* wordt echter een stuk eenvoudiger als de context helder is. Bovendien behoort de context te worden meegenomen bij het bepalen van het risicobeleid van een organisatie (ISO 2009).

3.2 Risk assessment

Risk assessment is de tweede stap in het risicomanagementproces. Aangaande risk assessment stellen Kaplan en Garrick de volgende drie hoofdvragen (Kaplan and Garrick 1981):

- Wat kan gebeuren?
- Hoe groot is de kans dat het gebeurt?
- Gegeven dat het gebeurt, wat zijn de consequenties?

In de ISO31000 worden grofweg dezelfde vragen gesteld, maar de ISO ziet *risk* assessment breder – de analyse van de risico's wordt ook tot *risk assessment* gerekend. In de ISO31000 wordt *risk assessment* onderverdeeld in de volgende drie delen: *risico-identificatie*, risico-analyse en *risico-evaluatie*.

3.2.1 Risico-identificatie

Bij *risico-identificatie* worden alle mogelijke risico's geïdentificeerd. Deze fase van *risk assessment* behelst het aanwijzen van bronnen van risico, mogelijke scenario's en de gevolgen. Deze stap zou moeten leiden tot een uitgebreide lijst van mogelijke gebeurtenissen die een invloed zouden kunnen hebben op het behalen van de doelstellingen van een organisatie. Risico-identificatie dient op een systematische wijze gedaan te worden en periodiek herhaald te worden (ISO 2009). Omdat risico's in oneindig veel zaken kunnen schuilen, is risico-identificatie een zeer arbeidsintensieve aangelegenheid; vooral ook omdat men constant alert dient te zijn op nieuw ontstane risico's (Claes P.F. 1997). Vaak worden checklists en stappenschema's gebruikt om risico's te identificeren. Er bestaan verschillende benaderingen en invalshoeken van waaruit de checklists de organisatie en zijn risico's benaderen. De keuze van één of meerdere van deze benaderingen is afhankelijk van de specifieke situatie van de organisatie (Claes P.F. 1997).

3.2.2 Risico-analyse

Risico-analyse heeft tot doel er voor te zorgen dat de organisatie begrip krijgt van de risico's waaraan ze wordt blootgesteld. Bij deze stap van *risk assessment* worden de kans op-, en de mogelijke gevolgen van de geïdentificeerde risico's onderzocht. Op basis van de kans en de mogelijke gevolgen kunnen risico's worden gecategoriseerd, waarbij risico's met een hoge kans en/of een grote impact hoger op de lijst komen te staan dan risico's met een lage kans en/of beperkte gevolgen. Het doorgronden en beschrijven van de aard van een risico is een lastig proces. Kansen en gevolgen zijn vaak moeilijk in te schatten.

Claes en Meerman onderscheiden op basis van de kans op schade en ernst van de gevolgen vier risicocategorieën, zoals te zien in figuur 2 (Claes P.F. 1997). Een frequentie/omvang-matrix met vier cellen zoals deze is een instrument dat dient om een grove schifting te maken waaruit naar voren komt welke risico's prioriteit hebben.

	Gering schadebedrag	Hoog schadebedrag
Kleine kans op schade	I	II
Grote kans op schade	III	IV

Figuur 2 Frequentie/omvang-matrix (Claes & Meerman, 1997)

Vaak worden grotere matrices toegepast, zoals het 5x5 diagram in figuur 3, afkomstig van de website van de PM&C, de adviesraad voor de Australische overheid. Een groter diagram maakt een preciezere categorisering mogelijk, waardoor de selectie van de te behandelen risico's makkelijker wordt. In de praktijk worden echter ook de resolutie van matrices van deze afmetingen nog wel eens te beperkt gevonden. Bovendien zijn er wetenschappers die waarschuwen voor het gebruik van risicomatrices, omdat de beperkingen te ernstig zouden zijn. Zo noemt Cox Jr. de beperkte resolutie, de mogelijkheid van foutief indelen en subjectiviteit bij het indelen als belangrijk nadelen (Cox Jr 2008).

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

Figuur 3 Risicomatrix (PM&C)

Wat betreft de vraagtekens die Cox Jr. plaatst bij de mogelijkheid risico's objectief te beoordelen en analyseren, staat hij niet alleen. Ook (Klinke and Renn 2002) betwijfelen of een methodische analyse werkelijk objectieve waarschijnlijkheden en kansen oplevert, of dat het slechts een afspiegeling geeft van de conventies van een elite groep risico-experts.

Risico-experts hebben net als alle andere mensen te maken met vooringenomenheid, waardoor hun oordeel gekleurd is (Hubert, Barny et al. 1991; Skjong and Wentworth 2001).

3.2.3 Risico-evaluatie

Risicocriteria zijn criteria die samen een referentiekader vormen op basis waarvan een risico op zijn belang getoetst kan worden (ISO 2009). De risicocriteria vloeien voort uit het risicobeleid van de organisatie en dienen derhalve aan te sluiten bij de waarden, doelstellingen en middelen van de organisatie. Organisaties hebben per definitie te maken met meer risico's dan ooit behandeld kunnen worden. Daarom dient een organisatie risico's voor behandeling te selecteren. Bij risico-evaluatie worden de resultaten van risicoanalyse vergeleken met de risicocriteria. De risicocriteria geven aan waar de risicotoleranties van de organisatie liggen. Daarbij wordt gekeken of een risico acceptabel is en dus aansluit bij de mate van *risk appetite* van de organisatie, of dat behandeling noodzakelijk is. Het is gebruikelijk om voorrang te geven aan grotere risico's; de risico's met een groter product van kans en gevolg. Hoewel de gevolgen van een voorval binnen grenzen doorgaans redelijk kunnen worden ingeschat, blijft het lastig om de kans van optreden in te schatten. Klinke en Renn stellen voor gebruik te maken van een combinatie van harde data en subjectieve schattingen door experts (Klinke and Renn 2002).

3.3 Het beheersen en behandelen van risico's

De derde stap in het risicomanagementproces is het behandelen van risico's. Bij risico-analyse wordt bepaald of een risico binnen de risicocriteria valt of dat behandeling noodzakelijk is. Blijkt uit analyse dat een risico behandeling vereist, dan wordt een geschikte manier van behandelen geselecteerd en uitgevoerd. Na het behandelen van het risico wordt het risico opnieuw geanalyseerd en bepaald of het risicoresidu verdere behandeling vereist (ISO 2009). Op deze wijze wordt een cyclisch risicomanagementproces gecreëerd (zie figuur 1).

Bij het behandelen van risico's zijn er kortweg vier alternatieven te duiden: vermijden, verminderen, overdragen of zelf dragen (P.F. Claes 1997). De meest drastische van deze vier alternatieven is het vermijden van een risico. De andere alternatieven richten zich op het terugdringen van de kans of het gevolg van risico's, maar het vermijden van een risico elimineert het risico in zijn geheel. In de praktijk betekent dit doorgaans dat de organisatie de activiteit waaruit het risico voortkomt afstoot of drastisch verandert. De tweede behandelingsoptie is het verminderen van het risico. Dit kan op twee manieren gedaan worden: de kans van optreden kan verkleind worden, of het gevolg kan beperkt worden. De derde behandelingsoptie is het overdragen van risico. In de eerste plaats rekenen we het verzekeren van risico hier onder. Een andere manier om risico over te dragen is door de activiteit waarbij het risico ontstaat uit te besteden aan een andere organisatie, waardoor deze er verantwoordelijk voor wordt. Ten slotte kan gekozen worden het risico zelf te dragen. Dit gebeurt doorgaans hoofdzakelijk in het geval van kleine risico's.

4 Enterprise Risk Management (ERM)

De laatste jaren wordt het belang van een holistische benadering van risicomanagement steeds meer benadrukt. Waar risicomanagement vroeger vaak werd uitgevoerd door een aparte afdeling of manager, wordt het tegenwoordig steeds vaker geïntegreerd in alle lagen van een organisatie (Chapman and Ward 2004). Risico's werden vaak min of meer als opzichzelfstaand beschouwd en vervolgens ad hoc behandeld, terwijl tegenwoordig wordt gepleit voor een organisatiebrede aanpak die van bovenaf wordt gecoördineerd (Simkins and Ramirez 2007).

Het op een holistische wijze en organisatiebreed geïntegreerd bedrijven van risicomanagement wordt ook wel *Enterprise Risk Management* (ERM) genoemd. Echter, net als het geval is met bijvoorbeeld de termen 'risico' en 'risicomanagement', is er ook niet echt één algemeen geaccepteerde definitie van ERM. Dickinson omschrijft ERM als de systematische en geïntegreerde benadering van het managen van het totaal aan risico's waar een organisatie mee te maken heeft (Dickinson 2001). De COSO definieert ERM als: "een proces dat wordt beïnvloed door de raad van bestuur van een organisatie, het management en ander personeel, en dat wordt toegepast bij het bepalen van de strategie en in de gehele onderneming, dat is ontwikkeld met tot doel het identificeren van potentiële gebeurtenissen die de organisatie kunnen beïnvloeden, en het managen van risico zodat het binnen de mate van *risk appetite* past, om zo een redelijke zekerheid te bieden met betrekking tot het behalen van de doelstellingen van de organisatie" (COSO 2004). Dit is een brede en specifieke definitie van ERM. Algemene overeenkomsten tussen de vele verschillende definities van ERM zijn dat het gaat om een constant proces dat organisatiebreed geïntegreerd is (Kleffner, Lee et al. 2003).

De ISO Guide73 – Risk Management Vocabulary, de ISO31000 en de ISO31010 maken geen van allen melding van de term ERM. De ISO definieert risicomanagement als de gecoördineerde activiteiten om een organisatie te sturen en beheersen met betrekking tot risico (ISO 2002). In de ISO31000 staat dat risicomanagement een integraal onderdeel van alle organisationele processen is, en dat risicomanagement verwijst naar de architectuur (principes, raamwerken en processen) voor het effectief managen van risico's (ISO 2009). Het lijkt er op dat *Enterprise Risk Management* door de ISO wordt beschouwd als een pleonasme; risicomanagement is per definitie een organisatiebreed geïntegreerd en constant proces. Afgezien van dit semantische verschil komen ERM – zoals beschreven door de COSO – en risicomanagement – zoals beschreven door de ISO – inhoudelijk in grote lijnen met elkaar overeen.

In dit verslag zal de term ERM gebruikt worden, omdat zo een beter onderscheid gemaakt kan worden tussen risicomanagement als bedrijfskundige discipline en risicomanagement als organisatiebreed geïntegreerd en constant proces.

4.1 Risk maturity

Risk Maturity is ontstaan vanuit het *Process Maturity Framework* (PMF) dat is ontwikkeld door Humprey c.s. binnen IBM (Humphrey 1989). Bij het Software Engineering van de Carnegie Mellon Universiteit Institute ontwikkelden Humprey en zijn collega's later het *Capability Maturity Model* (CMM), dat voortborduurt op het PMF (Paulk, Weber et al. 1993). *Maturity* laat zich in het Nederlands vertalen als rijpheid of volwassenheid. In de context van

*maturity*modellen staat het woord voor de mate van formalisering en optimalisering van een proces. Op basis van het CMM kan een proces worden gecategoriseerd in één van vijf niveaus van toenemende *maturity*: *initial, repeatable, defined, managed* en *optimizing.* Het CMM is ontwikkeld voor gebruik bij het ontwikkelen van software, maar het model wordt tegenwoordig steeds vaker ook voor andere toepassingen gebruikt. Risicomanagement is één van die toepassingsgebieden (website: Software and Engineering Institute).

Hillson heeft op basis van het CMM een *maturity* model ontwikkeld dat is toegespitst op risicomanagement, een zogenaamd *Risk Maturity Model* (RMM) (Hillson 1997). Organisaties kunnen op basis van dat model worden beoordeeld en gecategoriseerd met betrekking tot de mate van ontwikkeling van risicomanagement binnen de organisatie. Het laagste niveau van *risk maturity* correspondeert met een organisatie zonder enige vorm van formeel risicomanagement, het hoogste niveau komt overeen met een volledige inbedding en integratie van risicomanagement binnen de gehele organisatie. Waar het CMM vijf niveaus onderscheidt, kent het model van Hillson vier niveaus: *Naive, Novice, Normalized* en *Natural*. Hillson bepaalt de *risk maturity* door organisaties te scoren op de aspecten cultuur, proces, ervaring en toepassing van risicomanagement. Om organisaties meer onderscheidend en specifieker te kunnen categoriseren, onderscheiden andere onderzoekers meer niveaus, zoals Ren en Yeo (2004) en Liaqat en Shah (2009). Ren en Yeo benoemen de verschillende niveaus van *risk maturity* met dezelfde termen als in het CMM gedaan wordt (i.e. *initial, repeatable, defined, managed* en *optimizing*) en merken daarbij op dat dit de standaard vijf niveaus zijn. Liaqat en Shah nemen eveneens de vijf niveaus van *risk maturity* van het CMM als beginsel, maar hebben het model iets aangepast en uitgebreid met een zesde niveau. Zij onderscheiden de niveaus: *incomplete, performed, managed, defined, quantatively managed* en *optimizing*.
In dit onderzoek zal worden gewerkt met de vijf niveaus van *risk maturity* zoals ook gebruikt in het CMM.

Niveau 1: Initial
Organisaties op dit niveau van *risk maturity* zijn zich niet bewust van de noodzaak van risicomanagement. Men is niet bewust bezig met het leren van risico-ervaringen of om zich voor te bereiden op risico en onzekerheid in de toekomst.

Niveau 2: Repeatable
Organisaties op dit niveau van *risk maturity* experimenteren met toepassingen van risicomanagement, maar niet op een gestructureerde en geformaliseerde manier. Risicomanagement wordt gedragen door één of enkele individuen.

Niveau 3: Defined
Organisaties op dit niveau van *risk maturity* passen geformaliseerd risicomanagement toe bij de meeste routineprocessen en projecten. Algemene risicoprocessen zijn geformaliseerd en worden op verschillende plekken in de organisatie toegepast, hoewel ze wellicht niet consequent worden gerealiseerd.

Niveau 4: Managed
Organisaties op dit niveau van *risk maturity* passen risicomanagement toe bij bijna alle routineprocessen en projecten. Informatie omtrent risico wordt op een actieve wijze gebruikt

om processen binnen de organisatie te verbeteren, om zo een competitief voordeel te bewerkstelligen.

Niveau 5: Optimizing

Organisaties op dit niveau van *risk maturity* hebben een proactieve benadering van risicomanagement in alle lagen van de onderneming. Risicomanagement is volledig ingebed in de cultuur van de onderneming en speelt een rol bij alle processen en projecten binnen de organisatie. Het risicomanagement proces is een geïntegreerd onderdeel van besluitvormingsprocessen.

4.2 Kenmerken en eigenschappen van effectief ERM

Om een organisatie te beoordelen op de mate van *risk maturity* is het allereerst zaak concrete criteria te formuleren op basis waarvan *maturity* getoetst kan worden. In deze paragraaf zullen de belangrijkste kenmerken en eigenschappen van effectief ERM worden beschreven. Op basis van deze kenmerken zullen vervolgens de enquêtevragen worden geformuleerd, welke er toe dienen te bepalen in welke mate een organisatie effectief is op het gebied van ERM, oftewel – om de *risk maturity* van de organisatie te bepalen. De lijst met kenmerken en eigenschappen van goed ERM zijn hoofdzakelijk gebaseerd op de ISO31000. De ISO31000 komt voort uit de consensus van risicomanagementspecialisten wereldwijd. De meeste belangrijke criteria en voorwaarden voor risicomanagement die in andere literatuur vermeld worden, komen ook naar voren in de ISO31000. Om deze redenen wordt de ISO31000 gebruikt als de primaire bron voor de kenmerken van goed een organisatie met een grote mate van *risk maturity*.

De belangrijkste resultaten van ERM zijn:

- De organisatie heeft actuele, accurate en uitvoerige kennis van haar risico's.
- De risico's van de organisatie vallen binnen haar risicocriteria.

Deze twee punten worden in de ISO31000 verder uitgesplitst en gespecificeerd. Het voert te ver om alle in de ISO31000 genoemde aspecten hier te reproduceren. Belangrijke aspecten zijn onder meer: het hebben van een duidelijke risicomanagementfilosofie, mandaat en toewijding om risicomanagement te implementeren, coördinatie van bovenaf, het werken met een risicomanagementraamwerk, het werken met concrete risicocriteria, toepassing van het risicomanagementproces, goede verslaglegging en communicatie, het constant proberen risicomanagement te verbeteren, het werken met concrete doelstellingen, het meten van de resultaten en constante terugkoppeling.

Op basis van de ISO31000 is de volgende lijst met beoordelingscriteria opgesteld:

- *In het topmanagement is mandaat en toewijding aanwezig om risicomanagement te implementeren en blijvend van de benodigde resources te voorzien.*
- *Risicomanagement wordt vanuit het topmanagement gecoördineerd.*
- *Er is een Chief Risk Officer (CRO) of iemand met een vergelijkbare functie, met directe toegang tot de RvB.*
- *Er is een separate afdeling voor risicomanagement.*

- *Er is door het topmanagement een risicomanagementbeleid[2] geformuleerd en gecommuniceerd.*
- *Er wordt gebruik gemaakt van een risicomanagemenraamwerk[3] dat aansluit bij de eigen specifieke situatie van de organisatie.*
- *Er zijn concrete risicocriteria[4] geformuleerd.*
- *Er wordt een volledig en up-to-date risicobestand (riskfile) bijgehouden.*
- *De risico's waaraan de organisatie wordt blootgesteld, zijn geïdentificeerd, geanalyseerd en geëvalueerd op basis van de risicocriteria.*
- *Het bepalen en in kaart brengen van de prestaties van het risicomanagement is een integraal onderdeel van het meten en in kaart brengen van de prestaties van de organisatie.*
- *Er wordt nadrukkelijk gepoogd risicomanagement continu te verbeteren door het formuleren van organisationele prestatiedoelstellingen, metingen, beoordelingen en het vervolgens aanpassen van processen, systemen, middelen, bekwaamheid en vaardigheden.*
- *Risicomanagement omvat uitvoerig en volledig gedefinieerde, toegewezen en geaccepteerde verantwoordelijkheid voor risico's en risicobeheers- en behandelingstaken.*
- *De organisatie zet zich in om er voor te zorgen dat alle leden van de organisatie zich volledig bewust zijn van de risico's, de beheersmiddelen en de taken waarvoor zij verantwoordelijk zijn[5].*
- *Er zijn aangewezen individuen verantwoordelijk gemaakt om risico's in de gaten te houden, te beheersen en om de beheersmaatregelen te verbeteren – deze aangewezen individuen beschikken over de autoriteit, tijd, training, middelen en competenties die nodig zijn om hun verantwoordelijkheden te kunnen nakomen en zij zijn in staat om effectief met interne en externe betrokkenen te communiceren over risico's en het management daarvan.*
- *De definities van taken en verantwoordelijkheden met betrekking tot risicomanagement zijn onderdeel van alle introductieprogramma's[6] van de organisatie.*
- *Bij alle beslissingen die binnen de organisatie genomen worden, wordt – onafhankelijk van het niveau of de mate van belangrijkheid – in gepaste mate expliciet rekening gehouden met risico's en de toepassing van risicomanagement.*
- *Bij belangrijke processen en beslissingen binnen de organisatie zijn alle componenten van het risicomanagementproces[7] vertegenwoordigd; e.g. voor beslissingen met*

---

[2] Typische elementen die in een risicomanagementbeleid worden opgenomen zijn de visie en doelstellingen, taken, verantwoordelijkheden, de risicobereidheid (ook wel 'risk appetite' genoemd) en een korte beschrijving van het risicomanagementraamwerk.
[3] Bijvoorbeeld Enterprise Risk Management van COSO.
[4] Risicocriteria zijn beoordelingscriteria die samen een referentiekader vormen op basis waarvan een risico op zijn belang getoetst kan worden. De risicocriteria vloeien voort uit het risicobeleid van de organisatie en geven de grenzen van de 'risk appetite' aan. De criteria dienen aan te sluiten bij de waarden, doelstellingen en middelen van de organisatie.

[5] *Doorgaans worden deze zaken opgenomen in taak- of functieomschrijvingen, databases of informatiesystemen.*
[6] *Een programma dat nieuwe werknemers moeten doorlopen, waarin zij kennis maken met de organisatie en worden voorbereid op hun nieuwe rol en taken.*
[7] *I.e. risico-identificatie, risico-analyse, riciso-evaluatie, risico-behandeling, terugkoppeling, duidelijke toekenning van verantwoordelijkheden en de volgorde en timing van de verschillende activiteiten.*

betrekking tot grote projecten, de toewijzing van budgetten, herstructurering en organisatieveranderingen – dit kan worden aangetoond met behulp van notulen van vergaderingen en documentatie van beslissingen waarbij risico's expliciet aan de orde gekomen zijn.

- *Communicatie met interne en externe belanghebbenden wordt beschouwd als een integraal en essentieel component van risicomanagement.*
- *Als onderdeel van goede governance is er sprake van uitvoerige rapportage met betrekking tot het functioneren van het risicomanagement.*
- *Risicomanagement wordt binnen de gehele organisatie algemeen beschouwd als een centraal en integraal onderdeel van het managementproces.*
- *Effectief risicomanagement wordt door managers beschouwd als essentieel voor het behalen van de doelstellingen van de organisatie. Dit blijkt uit het taalgebruik van managers en uit belangrijk geschreven materiaal in de organisatie, waarin de termen onzekerheid en risico worden genoemd in relatie tot doelstellingen.*

5 Risicomanagement in de praktijk

5.1 Beschrijvend onderzoek *risk maturity* in een vijftal praktijksituaties

De identiteiten van de vijf Nederlandse ondernemingen die bereid zijn gevonden hun medewerking te verlenen aan dit onderzoek worden in verband met privacy niet genoemd in dit verslag. Het handelt om een havenbedrijf (organisatie A), een bedrijf in de chemische industrie (organisatie B), een nutsbedrijf (organisatie C), een infrastructuurbeheerder (organisatie D) en een persoenbeheerder (organisatie E).

Het empirisch onderzoek is tweeledig; enerzijds zal de *risk maturity* van de geselecteerde organisaties worden getoetst, anderzijds zal onderzocht worden wat de organisaties in concreto gedaan hebben om hun *risk maturity* te verbeteren.

De data zijn vergaard met behulp van een enquête welke is ingevuld door de risicomanager van de betreffende organisaties. De enquête bestaat uit tweeëntwintig genummerde vragen, waarvan sommige zijn gesplitst in deelvragen, zie bijlage A. De vragen zijn direct afgeleid van de beoordelingscriteria zoals vermeld in paragraaf 4.2 De meeste vragen zijn geformuleerd als stelling. De respondenten is gevraagd middels een vijfpunts Likert-schaal aan te geven in welke mate zij vinden dat de stelling van toepassing is op de eigen organisatie. De antwoordalternatieven zijn ‘volledig eens’, ‘eens’, ‘neutraal’, ‘oneens’ en ‘volledig oneens’. Op enkele stellingen konden de respondenten slechts antwoorden met ‘ja’ of ‘nee’. Daarnaast zijn een aantal open vragen opgenomen. De respondenten kregen bij elke vraag de mogelijkheid om opmerkingen te plaatsen voor in het geval de vraagstelling onduidelijk was of als zij vonden dat extra informatie noodzakelijk was.

Om de organisaties in te kunnen delen in een *risk maturity* niveau zijn op basis van de antwoorden op de gesloten vragen punten toegekend. Om te kunnen rekenen met de resultaten wordt aangenomen dat de schaal niet slechts ordinaal verdeeld is, maar ook intervalgeschaald. Waar een respondent ‘volledig’ eens heeft ingevuld zijn vier punten toegekend, ‘eens’ leverde drie punten op, ‘neutraal’ twee punten, ‘oneens’ leverde één punt op en ‘volledig oneens’ leverde geen punten op. Bij vragen die zijn gesplitst in verschillende onderdelen, is de gemiddelde score bepaald. In totaal konden 92 punten behaald worden. Die maximale score komt tot stand door het aantal van tweeëntwintig vragen te vermenigvuldigen met de maximale vier punten per vraag, plus vier extra punten voor vraag drie. Op basis van de somscore is het niveau van *risk maturity* van de organisaties bepaald, zoals te zien in tabel 1.

Tabel 1 Risk maturity niveaus behorende bij de verschillende scores

Score	Risk maturity niveau
0 – 19	Niveau 1: *Initial*
20 – 38	Niveau 2: *Repeatable*
39 – 56	Niveau 3: *Defined*
57 – 75	Niveau 4: *Managed*
76 – 95	Niveau 5: *Optimizing*

Naast de vragen om de organisaties in te delen in een bepaald level van *risk maturity* zijn er ook vragen opgenomen om te onderzoeken welke hulpmiddelen en maatregelen de organisaties gebruiken.

Op basis van de resultaten van de enquête zijn scores toegekend aan de *risk maturity* van de vijf organisaties. In de volgende paragrafen worden allereerst de scores en de indeling in *risk maturity* niveaus besproken. Vervolgens wordt ingegaan op de overeenkomsten en verschillen tussen de vijf organisaties. Aansluitend komen concrete maatregelen ter verbetering van *risk maturity* aan bod.

5.2 Resultaten

5.2.1 Risk maturity

Op basis van de resultaten van de enquêtes zijn de scores voor *risk maturity* berekend voor de vijf organisaties. De resultaten staan in tabel 2.

Tabel 2 Risk maturity scores en niveaus van de vijf onderzochte organisaties

Organisatie	Score	Risk maturity niveau
A	74	Niveau 4: *Managed*
B	75	Niveau 5: *Optimizing*
C	61	Niveau 4: *Managed*
D	48	Niveau 3: *Defined*
E	65	Niveau 4: *Managed*

Organisatie A wordt op basis van de behaalde score ingedeeld in niveau 4. Met een score van 74 punten zit de organisatie aan bovenkant niveau 4. Organisatie B daarentegen zit met een score van 75 net in niveau 5, het in dit model hoogste niveau van *risk maturity*. Als organisatie B slechts één punt minder gescoord zou hebben, zou het in niveau 4 worden ingedeeld en als organisatie A slechts één punt meer gescoord zou hebben, zou de organisatie in niveau 5 zijn ingedeeld. Bij de overige drie organisaties is minder sprake van ambiguïteit, omdat de scores min of meer in het midden van de 'range' van de verschillende categorieën zitten. Organisatie C zit met een score van 61 duidelijk in niveau 4 en organisatie D wordt met een score van 61 duidelijk ingedeeld in niveau 3. Organisatie E wordt met een score van 65 punten ingedeeld in niveau 4.

De eerste vijf vragen van de enquête dienden om te onderzoeken of de basale infrastructuur die past bij goed risicomanagement aanwezig is bij de organisaties. Alle onderzochte organisaties maken gebruik van een risicomanagementraamwerk. Door elk van de onderzochte organisaties wordt gebruik gemaakt van het raamwerk van de COSO. Bovendien wordt het risicomanagement in elk van de gevallen gecoördineerd vanuit het topmanagement. Door elk van de onderzochte organisaties wordt een risicobestand bijgehouden en ook worden risico's voor behandeling geselecteerd door middel van onder meer een risico-matrix. Uit deze resultaten blijkt dat bij deze vijf organisaties sprake is van formeel risicomanagement en dat de basale infrastructuur daarvoor aanwezig is.

Het is opvallend dat hoewel alle organisaties aangeven dat in het topmanagement een zekere mate van mandaat en toewijding aanwezig is en dat risicomanagement vanuit het

topmanagement wordt gecoördineerd, enkel organisatie E een *Chief Risk Officer* (CRO) heeft die is gezeteld in het topmanagement. Bij de overige organisaties bevindt de risicomanager zich in de tweede managementlaag en wordt gerapporteerd aan de *Chief Financial Officer* (CFO). Dit is temeer opvallend omdat bij organisatie E als enige van de vijf onderzochte organisaties juist geen formeel risicomanagementbeleid is geformuleerd en geen risicocriteria zijn opgesteld.

De verschillen tussen de organisaties die in dit onderzoek hoog scoren op *risk maturity* en organisaties met een gemiddelde score komen in belangrijke mate voort uit verschillen in het al dan of niet aanwezig zijn van een systeem voor constante verbetering van risicomanagement, het nadrukkelijk toekennen van verantwoordelijkheden omtrent risicomanagement, documentatie en vastlegging van toepassing van het risicomanagementproces, de activiteiten die de ondernemingen nemen om ervoor te zorgen dat werknemers beschikken over de benodigde kennis met betrekking tot risicomanagement, het integreren van risicomanagement in de gehele organisatie en het aanwezig zijn van een risicobewuste cultuur waarin het belang van risicomanagement organisatiebreed wordt erkend en ondersteund.

5.2.2 Concrete maatregelen ter verbetering van risk maturity

De enquête was tweeledig; enerzijds diende het om de *risk maturity* van de organisaties in kaart te brengen, maar het diende ook om te onderzoeken wat de organisaties in concreto gedurende de afgelopen twee jaar hebben gedaan om *risk maturity* te verbeteren. Het blijkt dat de vijf organisaties op veel verschillende vlakken hebben gepoogd het risicomanagement van de organisatie te verbeteren, maar er zijn ook een aantal overeenkomsten.

Organisatie A heeft risicomanagement meer verticaal geïntegreerd in de organisatie. Daarbij zijn verantwoordelijkheden geformuleerd en zijn mensen binnen de organisatie formeel eigenaar gemaakt van specifieke verantwoordelijkheden. De CRO heeft hierbij het voortouw genomen door de kaders te zetten. In samenwerking met de verantwoordelijke managers is vervolgens bepaald welke standaard-tools gebruikt zullen worden en hoe de veranderingen geïmplementeerd moeten worden. Een belangrijk element hierbij is de verscherpte rapportage en controle.

Binnen organisatie B is eveneens gepoogd verantwoordelijkheden duidelijker vast te leggen. Daarbij zorgt de organisatie er door middel van een recent herziene en uitgebreide *Code Of Business Conduct* met verplichte e-learningmodule voor alle werknemers voor dat de werknemers over de juiste kennis en vaardigheden beschikken. Bovendien zijn de risicocriteria aangescherpt, waarbij bepaalde belangrijke risico's speciaal zijn uitgelicht waardoor ze worden benadrukt ten opzichte van de rest. Daarnaast wordt risicomanagement strikter toegepast in projecten en bij overnames, acquisities en andere externe contracten, waarbij er op wordt toegezien dat de organisatie geen onnodige aansprakelijkheid op zich neemt. Er wordt recentelijk extra scherp toegezien op de mate van blootstelling aan risico's om verzekeringsniveaus te verifiëren. Ten slotte zet de organisatie zich in voor het verbeteren van risicomanagement in groeiregio's, waarbij specifieke aandacht uitgaat naar het beschermen van de intellectuele eigendommen van de organisatie – welke in de relevante regio's (o.m. China en India) frequent geschonden plachten te worden.

Organisatie C heeft onlangs een concreter risicomanagementbeleid geformuleerd. Tevens is het topmanagement meer betrokken bij risicomanagement en zijn de rapportage en evaluaties verzwaard. Net als bij organisatie B zijn ook bij organisatie C belangrijke risico's uitgelicht en wordt risicomanagement binnen projecten strikter toegepast. Het ERM-raamwerk van COSO is recentelijk meer volledig geïmplementeerd. Hiertoe is met name de rapportage met het oog op compliance aangescherpt, op alle niveaus binnen de organisatie. Belangrijk is ook dat de RvC sinds kort expliciet wordt betrokken bij het risicomanagement. Ten slotte wordt gepoogd om in meer situaties een financiële-impact-analyse te doen.

Organisatie D heeft een visie opgesteld en deze breed gedeeld. Bovendien wordt ook hier extra aandacht geschonken aan de belangrijkste risico's, in dit geval middels een speciaal daarvoor opgericht comité. Recentelijk is een niet nader omschreven risicomanagement-tool aangeschaft, maar deze moet nog geïmplementeerd worden. Ten slotte heeft organisatie D de beoordeling en terugkoppeling met betrekking tot risicobeheersmaatregelen verbeterd en hebben werknemers die verantwoordelijk zijn voor risicomanagement interne cursussen gevolgd.

Bij organisatie E is recentelijk een risicomanagementafdeling opgericht. Voorheen was risicomanagement een onderdeel van de financiële afdeling. Helaas is geen verdere informatie beschikbaar.

6 Conclusies en discussie

Gedurende het afgelopen decennium heeft risicomanagement zich ontwikkeld tot een niet meer weg te denken stroming binnen de bedrijfswetenschappen en de bedrijfskundige praktijk. Enerzijds komt dit door eisen die wet- en regelgevers naar aanleiding van enkele misstanden aan organisaties zijn gaan stellen, maar ook aandeelhouders en andere stakeholders eisen van ondernemingen dat zij op een verstandige wijze omgaan met de alomtegenwoordige risico's waaraan moderne organisaties worden blootgesteld. Organisaties maken voor de implementatie van risicomanagement doorgaans gebruik van een risicomanagementraamwerk, waarvan het ERMF van COSO mogelijk de bekendste en meest gebruikte is. Waar risicomanagement vroeger meer als opzichzelfstaande managementpraktijk gezien werd, wordt tegenwoordig het belang van Enterprise Risk Management onderkend – risicomanagement dient in de gehele organisatie geïntegreerd te worden. De ene organisatie heeft risicomanagement in grotere mate geïmplementeerd in de organisatie dan de andere. De *Risk maturity* geeft aan in welke mate het risicomanagement binnen een organisatie is ontwikkeld. In dit onderzoek is gewerkt met een model met vijf niveaus van *risk maturity*.

Op basis van belangrijke wetenschappelijke literatuur en vakliteratuur met betrekking tot risicomanagement en *risk maturity* is een lijst met beoordelingscriteria voor goed risicomanagement opgesteld. Deze lijst heeft de grondslag gevormd voor een enquête waarmee de *risk maturity* van een organisatie getoetst kan worden. Middels deze enquête is de *risk maturity van een* vijftal organisaties in kaart gebracht. Twee van de vijf organisaties scoren uitgesproken hoog op *risk maturity* met beide een score die nagenoeg op de grens tussen niveaus 4 en 5 ligt. Twee van de overige organisaties zijn ingedeeld in niveau 4 en één organisatie is ingedeeld in niveau 3. Alle vijf onderzochte ondernemingen blijken formeel risicomanagement toe te passen, dat de basis vindt in het ERMF van COSO.

De organisaties met de hoogste mate *risk maturity* scoren in verhouding tot de aspecten waarop zij uitgesproken hoog scoren verhoudingsgewijs betrekkelijk laag op punten als het meten van het functioneren van risicomanagement, het constant verbeteren van het risicomanagement en op het beschikken over de vereiste competenties van de mensen die verantwoordelijk zijn voor risicomanagement. Dit zijn over het algemeen de punten waarop nog relatief grote verbeteringen mogelijk zijn.

Naast het in kaart brengen van de *risk maturity* van de vijf organisaties, is onderzocht wat zij gedurende de afgelopen twee jaar in concreto gedaan hebben om *risk maturity* te verbeteren. De vijf organisaties hebben gedurende afgelopen twee jaar allerlei verschillende maatregelen genomen om het risicomanagement binnen hun organisatie te verbeteren. Drie specifieke maatregelen werden genoemd door de risicomanagers van meerdere van de organisaties. Dat is ten eerste het duidelijker toewijzen van verantwoordelijkheden, ten tweede het consistenter toepassen van het risicomanagementproces in projecten en ten slotte het benadrukken en extra aandacht schenken aan de belangrijkste risico's.

De data voor dit onderzoek zijn vergaard met behulp van een enquête met daarin hoofdzakelijk vragen die zijn geformuleerd als stellingen. De respondenten konden aangeven in welke mate zij van mening waren dat de stelling van toepassing is op hun organisatie. Deze onderzoeksmethodiek heeft een aantal eigenschappen die hebben geleid tot de keuze hiervoor. Een enquête zoals deze maakt het bijvoorbeeld mogelijk de datavergaring te standaardiseren en in vergelijking met een alternatief zoals een interview is de benodigde tijd voor zowel de onderzoeker als de respondenten beperkt. Een interview zou waarschijnlijk voordelen hebben gehad voor het onderzoeken wat de organisaties hebben gedaan om *risk maturity* te verbeteren. Tijdens een interview kan om toelichting gevraagd worden als een antwoord niet geheel duidelijk is – iets wat afgezien van beperkte correspondentie via email niet mogelijk was binnen dit onderzoek.

De resultaten van zijn gebaseerd op de meningen van de risicomanagers van de vijf onderzochte organisaties. Dat betekent dat subjectiviteit een rol speelt. Bias is niet uit te sluiten, zoals bijvoorbeeld bias als gevolg van sociale wenselijkheid. Dat wil zeggen, het is mogelijk dat de respondenten hun organisatie beter willen doen voorkomen dan ze zijn. Daarnaast kan sprake zijn van individuele verschillen bij de manier van invullen – het kan voorkomen dat de ene respondent het antwoordalternatief ‘eens’ aankruist terwijl een andere respondent onder identieke omstandigheden ‘volledig eens’ zou hebben ingevuld. Het is overigens opvallend te noemen dat niet één keer ‘volledig oneens’ is aangekruist, terwijl ‘volledig eens’ veelvuldig is aangekruist. De scores op basis waarvan de organisaties zijn ingedeeld in een niveau van *risk maturity* konden enkel berekend worden op basis van de premisse dat de antwoordalternatieven intervalgeschaald zijn – i.e. dat tussen de opvolgende antwoordalternatieven telkens één punt verschil bestaat.

De vijf organisaties behaalden in dit onderzoek scores voor *risk maturity* die betrekkelijk dicht bij elkaar liggen. Het is bovendien moeilijk om de betrouwbaarheid van dit onderzoek te toetsen. De enquête lijkt een geschikte methode te zijn om eenvoudig en snel een grove inschatting van de *risk maturity* van een organisatie te kunnen maken, maar het op basis van enkel de behaalde scores vergelijken van deze organisaties zou een te simplistisch en beperkt beeld opleveren. Voor een hogere betrouwbaarheid en validiteit zou uitvoeriger onderzoek noodzakelijk zijn, met bijvoorbeeld interviews met individuen uit verschillende lagen van de organisatie en door het controleren van feiten zoals de aanwezigheid en toegankelijkheid van een risicobestand. Het zou een uitdaging voor toekomstig onderzoek kunnen zijn om de betrouwbaarheid van een enquête zoals toegepast in dit onderzoek te verifiëren door de uitkomsten te vergelijken met die van een uitvoeriger onderzoek.

Een belangrijke vraag die gedurende dit onderzoek begon op te spelen is of risicomanagement in het algemeen überhaupt werkt en zo ja, hoe een organisatie een goede keuze tussen kosten en baten kan maken. Het lijkt aannemelijk dat het nastreven van een grotere *risk maturity* vanaf een zeker *risk maturity*-niveau niet langer zinvol is voor een organisatie. Er zijn legio voorbeelden van situaties waarin risicomanagement grote problemen had kunnen voorkomen. Succesverhalen met betrekking tot invoering van risicomanagement zijn echter schaars. In de praktijk blijkt dat grootschalige veranderingen en organisationele innovaties binnen organisaties vaak slecht uitpakken. Uit onderzoek bij vijftig Nederlandse organisaties blijken de gestelde doelstellingen in minder dan de helft van de gevallen gehaald te worden (Cozijnsen, Vrakking et al. 2000). Andere onderzoekers schatten het aandeel van gevallen waarin organisatieverandering succesvol genoemd kan worden nog lager in (Staveren 2009). Volgens Aken is management theorie doorgaans

bewezen maar te triviaal om enige praktische relevantie te hebben, of relevant maar zonder voldoende wetenschappelijke rechtvaardiging (Aken 2004). Dit laatste lijkt te gelden voor het domein van het risicomanagement. Hopelijk zal toekomstig wetenschappelijk onderzoek op dit gebied de praktijk en theorie van risicomanagement dichter bij elkaar brengen.

Literatuurlijst

Aken, van. (2004). “Management research based on the paradigm of the design sciences: The quest for field-tested and grounded technological rules.” Journal of Management Studies **41:** 219-246.

Aven, T. and O. Renn (2009). "On risk defined as an event where the outcome is uncertain." Journal of Risk Research **12**(1): 1-11.

Barateiro, J. and J. Borbinha (2011). "Integrated management of risk information." Proceedings of the Federated Conference on Computer Science and Information Systems. ISBN 978-83-60810-22-4. p799–806.

Beasley, M.S., R. Clune, et al. (2005). “Enterprise risk management: An empirical analysis of factors associated with the extent of implementation.” Journal of Accounting and Public Policy **24**(6)**:** 521-531.

Bowling, D.M. and L.A. Rieger (2005). “Making sense of COSO’s new Framework for Enterprise Risk Management.” Bank Accounting & Finance **18:** 29-34.

Chapman, C. and S. Ward (2004). “Why risk efficiency is a key aspect of best practice projects.” International Journal of Project Management. **22:** 619-632.

Chopra, S. and M.M.S. Sodhi (2004). "Supply-Chain Breakdown." MITSLOAN Management Review **45**(1).

Christensen, F.M., O. Andersen, et al. (2003). "Risk terminology--a platform for common understanding and better communication." Journal of Hazardous Materials **103**(3): 181-203.

Claes P.F. and H.J.J.M. Meerman (1997). Risk Management - inleiding tot het risicobeheersproces. ISBN 9020720821. Stenfert Kroese, Houten

COSO (1992). “Internal Control – Integrated Framework (Executive Summary).”

COSO (2004). "Enterprise Risk Management — Integrated Framework (Executive Summary)."

Cox Jr, A.T. (2008). “What's wrong with risk matrices?” Risk Analysis **28:** 497-512.

Cozijnsen, A.J., W.J. Vrakking, et al. (2000). “Success and failure of 50 innovation projects in Dutch companies.” International Journal of Innovation Management **3:** 150-159.

Denenberg, H.S. and J.R. Ferrari (1966). “New perspectives on risk management: The search for principles.” The Journal of Risk and Insurance **33:** 647-661.

Dickinson, G. (2001). "Enterprise Risk Management: Its Origins and Conceptual Foundation." The Geneva Papers on Risk and Insurance **26**: 360 - 366.

Haimes, Y.Y. (2009). Risk Modeling, Assessment, and Management. ISBN 0470282371 Virginia, Wiley.

Hedges, B.A. (1965). “A Methodology for a Course in Risk Management” The Journal of Risk and Insurance **32:** 609-615.

Hillson, D.A. (1997). "Toward a Risk Maturity Model." The International Journal of Project & Business Risk Management **1**(1): 35-43.

Hillson, D.A. (2002). "Extending the risk process to manage opportunities." International Journal of Project Management **20** (3): 235-240.

Hubert,P., M.H. Barny, et al. (1991). “Elicitation of Decision Makers Preferences for Management of Major Hazards.” Risk Analysis **11:** 199-206.

ISO (2002). "Guide 73: Risk management — Vocabulary."

ISO (2009). "ISO31000 Risk management — Principles and guidelines."

Jaafari, A. (2001). "Management of risks, uncertainties and opportunities on projects: time for a fundamental shift." International Journal of Project Management **19**(2): 89-101.

Kaplan, S. and B.J. Garrick (1981). “On the quantitative definition of risk.” Risk Analysis **1:** 11-27.

Kleffner, A.E., R.B. Lee, et al. (2003). “The effect of corporate governance on the use of enterprise risk management: Evidence from Canada.” Risk Management and Insurance Review **6:** 53-73.

Klinke, A. and O. Renn (2002). “A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies.” Risk Analysis **22:** 1071-1094.

Knechel, W.R. (2007). "The business risk audit: Origins, obstacles and opportunities." Accounting, Organizations and Society **32**(4-5): 383-408.

Liaqat Shah, A.S., François Vernadat (2009). “Maturity Assessment in Risk Management in Manufacturing Engineering.” 2009 IEEE International Systems Conference Proceedings p296.

March, J.G. and Z. Shapira (1987). ‘Managerial perspectives on risk and risk taking” Institute of Management Sciences **33:** 1404-1418.

Olson, D. D. W. (2007). “Optimizing Risk Management: Methods and Tools.” Human and Ecological Risk Assessment: An International Journal **15**(2) 220-226.

P.F. Claes and H.J.J.M. Meerman (1997). “Risk Management - inleiding tot het risicobeheersproces.” Educatieve Partners Nederland B.V., Houten

Paape, L., D.M. Swagerman, (2006). “Risicomanagement - De Praktijk In Nederland” rapport Rijks Universiteit Groningen.

PM&C. from http://www.dpmc.gov.au/implementation/policy.cfm (geraadpleegd juni 2012).

Power, M. (2001). “Organised uncertainty: designing a world of risk management.” ISBN 0199253943, Routledge.

Ren, Y. T. and K. T. Yeo (2004). Risk management capability maturity model for complex product systems (CoPS) projects, IEEE. **2:** 807-811 Vol. 2.

Sarbanes-Oxley (2002). "Sarbanes-Oxley Act 2002." Government Printing Public Office *Law No.107–204.*

Simkins, B. and S. A. Ramirez (2007). “Enterprise-Wide Risk Management and Corporate Governance.” Loyola University Chicago Law Journal **39:** 571.

Skjong, R. and B. H. Wentworth (2001). “Expert judgment and risk perception.” Proceedings of the Eleventh International Offshore and Polar Engineering Conference. ISBN 1-880653-51-6

Snider, W. (1991). “Risk management: A retrospective view.” Risk Management **34:** 47–54.

Software Engineering Institute – Carnegie Mellon University, website: http://www.sei.cmu.edu/cmmi/

Staveren, V. (2009). “Risk, Innovation & Change: Design Propositions for Implementing Risk Management in Organizations” PhD thesis, Universiteit Twente, Enschede

Ward, S. C. (1999). “Assessing and managing important risks.” International Journal of Project Management **17:** 331-336.

Williams, T. M. (1996). “The two-dimensionality of project risk.” International Journal of Project Management **14:** 185-186.

Bijlagen

Bijlage A: Enquêtevragenlijst

Enquête Risicomanagement

De naam van uw bedrijf:.....

Uw naam:.....

Uw functie binnen de organisatie:.....

Deze enquête bestaat uit 22 vragen, waaronder zowel open als gesloten vragen. De vragen zijn gerangschikt naar onderwerp en zijn verdeeld over tien pagina's. Het grootste deel van de gesloten vragen is geformuleerd als stelling welke in meer of mindere mate betrekking zullen hebben op uw organisatie. Door het desbetreffende cirkeltje van de vijfpuntsschaal in te vullen geeft u aan in welke mate u het eens dan wel oneens bent met de stelling, i.e. in welke mate u vindt dat de stelling van toepassing is op uw organisatie. Het is de bedoeling dat u één kruisje zet, tenzij anders aangegeven. In principe volstaat het selecteren van een antwoordalternatief, maar indien de stelling onduidelijk is of als u om een andere reden meer informatie wilt geven, kunt u gebruik maken van de vrijgelaten ruimte onder de regel met de antwoordopties. Daarnaast zult u enkele ja/nee-vragen en een aantal open vragen tegenkomen. Voor het invullen van de enquête zult u naar schatting 30 à 40 minuten nodig hebben.

---

1) *In het topmanagement is mandaat en toewijding aanwezig om risicomanagement te implementeren en blijvend van de benodigde resources te voorzien.*

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

---

2) *Risicomanagement wordt vanuit het topmanagement gecoördineerd.*

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

---

3) *Is er in uw organisatie een Chief Risk Officer (CRO) of iemand met een vergelijkbare functie?*

Ja	Nee
○	○

Zo ja, ga verder met de delen a, b, c en d van deze vraag. Zo nee, ga verder met vraag 4.

a. *Op welk niveau in de organisatie bevindt deze CRO zich?(Raad van Bestuur (RvB), tweede of derde managementlaag, of lager?)*

.....

.....

.....

.....

b. *Als de CRO geen lid van de RvB is – heeft de CRO directe of indirecte toegang tot de RvB?En zo ja, hoe?*

.....

.....

.....

.....

c. *Is er voor risicomanagement een speciale afdeling ingericht, of is het wellicht ondergebracht bij finance & control of een andere afdeling?*

.....

.....

.....

.....

d. *Is de CRO gemachtigd om afdelingshoofden/plantmanagers voorschriften te geven?*

.....

.....

.....

.....

4) *Er is door het topmanagement een risicomanagementbeleid[8] geformuleerd en gecommuniceerd.*

Ja	Nee
○	○

Zo ja, ga verder met de delen a, b en c van deze vraag. Zo nee, ga verder met vraag 5.

a. Het risicomanagementbeleid omvat een visie of langetermijnperspectief voor risicomanagement.

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

b. Het is duidelijk vastgelegd wie verantwoordelijk zijn voor risicomanagement en wat deze verantwoordelijkheden inhouden.

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

c. De mate van risk appetite (risicobereidheid) is duidelijk vastgelegd.

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

5) *Er wordt gebruik gemaakt van een risicomanagemenraamwerk[9] dat aansluit bij de eigen specifieke situatie van de organisatie.*

Ja	Nee
○	○

Zo ja, welk raamwerk is dit?

.....

.....

.....

[8] *Typische elementen die in een risicomanagementbeleid worden opgenomen zijn de visie en doelstellingen, taken, verantwoordelijkheden, de risicobereidheid (ook wel 'risk appetite' genoemd) en een korte beschrijving van het risicomanagementraamwerk.*

[9] *Bijvoorbeeld Enterprise Risk Management van COSO.*

6) Er zijn concrete risicocriteria[10] geformuleerd.

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

7) Er wordt een risicobestand (riskfile) bijgehouden.

Ja	Nee
○	○

Zo ja, ga verder met de delen a, b en c van deze vraag. Zo nee, ga verder met vraag 8.

a. Hoe is het risicobestand samengesteld? (Meerdere antwoorden mogelijk)

- ○ Checklists
- ○ Incidentenregister
- ○ Incidentenregister, aangevuld met schadebedragen
- ○ Bestand met niet-gerealiseerde bedreigingen
- ○ Meningen van experts
- ○ Brainstormsessies
- ○ Anders, namelijk:

.....

.....

.....

b. Het risicobestand is volledig.

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

[10] *Risicocriteria zijn beoordelingscriteria die samen een referentiekader vormen op basis waarvan een risico op zijn belang getoetst kan worden. De risicocriteria vloeien voort uit het risicobeleid van de organisatie en geven de grenzen van de 'risk appetite' aan. De criteria dienen aan te sluiten bij de waarden, doelstellingen en middelen van de organisatie.*

c. *Het risicobestand is up-to-date.*

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

8) *Hoe worden risico's geselecteerd voor behandeling? Wordt daarbij gebruik gemaakt van een risicomatrix?*

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

9) *De risico's waaraan de organisatie wordt blootgesteld, zijn geïdentificeerd, geanalyseerd en geëvalueerd op basis van de risicocriteria.*

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

10) *Het bepalen en in kaart brengen van de prestaties van het risicomanagement is een integraal onderdeel van het meten en in kaart brengen van de prestaties van de organisatie.*

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

11) Er wordt nadrukkelijk gepoogd risicomanagement continu te verbeteren door het formuleren van organisationele prestatiedoelstellingen, metingen, beoordelingen en het vervolgens aanpassen van processen, systemen, middelen, bekwaamheid en vaardigheden.

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

12) Welke concrete maatregelen zijn de afgelopen twee jaar zoal ondernomen om het risicomanagement van uw organisatie te verbeteren?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

13) Risicomanagement omvat uitvoerig en volledig gedefinieerde, toegewezen en geaccepteerde verantwoordelijkheid voor risico's en risicobeheers- en behandelingstaken.

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

14) *De organisatie zet zich in om er voor te zorgen dat alle leden van de organisatie zich volledig bewust zijn van de risico's, de beheersmiddelen en de taken waarvoor zij verantwoordelijk zijn*[11].

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

15) *Er zijn aangewezen individuen verantwoordelijk gemaakt om risico's in de gaten te houden, te beheersen en om de beheersmaatregelen te verbeteren.*

Ja	Nee
○	○

Zo ja, ga verder met de delen a en b van deze vraag. Zo nee, ga verder met vraag 16.

a. *Deze aangewezen individuen beschikken over de autoriteit, tijd, training, middelen en competenties die nodig zijn om hun verantwoordelijkheden te kunnen nakomen.*

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

b. *Deze aangewezen individuen zijn in staat om effectief met interne en externe betrokkenen te communiceren over risico's en het management daarvan.*

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

16) *De definities van taken en verantwoordelijkheden met betrekking tot risicomanagement zijn onderdeel van alle introductieprogramma's*[12] *van de organisatie.*

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

[11] *Doorgaans worden deze zaken opgenomen in taak- of functieomschrijvingen, databases of informatiesystemen.*
[12] *Een programma dat nieuwe werknemers moeten doorlopen, waarin zij kennis maken met de organisatie en worden voorbereid op hun nieuwe rol en taken.*

17) *Bij alle beslissingen die binnen de organisatie genomen worden, wordt – onafhankelijk van het niveau of de mate van belangrijkheid – in gepaste mate expliciet rekening gehouden met risico's en de toepassing van risicomanagement.*

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

18) *Bij belangrijke processen en beslissingen binnen de organisatie zijn alle componenten van het risicomanagementproces[13] vertegenwoordigd; e.g. voor beslissingen met betrekking tot grote projecten, de toewijzing van budgetten, herstructurering en organisatieveranderingen.*

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

Hebt u 'Volledig oneens' ingevuld, ga verder met vraag 19. Hebt u één van de andere antwoordalternatieven ingevuld, ga verder met deel a van deze vraag.

a. *Dit kan worden aangetoond met behulp van notulen van vergaderingen en documentatie van beslissingen waarbij risico's expliciet aan de orde gekomen zijn.*

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

19) *Communicatie met interne en externe belanghebbenden wordt beschouwd als een integraal en essentieel component van risicomanagement.*

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

[13] *I.e. risico-identificatie, risico-analyse, riciso-evaluatie, risico-behandeling, terugkoppeling, duidelijke toekenning van verantwoordelijkheden en de volgorde en timing van de verschillende activiteiten.*

20) Als onderdeel van goede governance is er sprake van uitvoerige rapportage met betrekking tot het functioneren van het risicomanagement.

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

Indien er sprake is van een dergelijke rapportage – hoe vaak wordt het functioneren van het risicomanagement in kaart gebracht en gerapporteerd?

.....

.....

.....

.....

.....

.....

.....

.....

.....

21) Risicomanagement wordt binnen de gehele organisatie algemeen beschouwd als een centraal en integraal onderdeel van het managementproces.

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

22) *Effectief risicomanagement wordt door managers beschouwd als essentieel voor het behalen van de doelstellingen van de organisatie. Dit blijkt uit het taalgebruik van managers en uit belangrijk geschreven materiaal in de organisatie, waarin de termen onzekerheid en risico worden genoemd in relatie tot doelstellingen.*

Volledig oneens	Oneens	Neutraal	Eens	Volledig eens
○	○	○	○	○

Bedankt voor het invullen van de enquête!

Bijlage B: Resultaten enquête

Vraag	Onderwerp	A	B	C	D	E
1	Mandaat & Toewijding	4,0	3,0	2,0	3,0	3,0
2	Coördinatie topmanagement	4,0	3,0	3,0	3,0	3,0
3	CRO of vergelijkbare functie	7,5	7,0	6,8		7,8
3a	Zo ja, welk niveau	open	open	open	open	open
3b	Toegang RvB	open	open	open	open	open
3c	Separate RM-afdeling	open	open	open	open	open
4	RM-beleid	4,0	3,3	4,0	3,8	0,0
4a	Visie of langetermijnperspectief	open	open	open	open	open
4b	Verantwoordelijkheden vastgelegd	open	open	open	open	open
4c	Risk Appetite vastgelegd	open	open	open	open	open
5	RM-Raamwerk	4,0	4,0	4,0	4,0	4,0
5a	Zo ja, welke	open	open	open	open	open
6	Risicocriteria	4,0	4,0	4,0	3,0	1,0
7	Risicobestand	3,3	3,3	3,3	2,7	2,3
7a	Hoe samengesteld	open	open	open	open	open
7b	Volledigheid	open	open	open	open	open
7c	Up-to-date	open	open	open	open	open
8	Hoe risico's geselecteerd	open	open	open	open	open
9	Identificatie, analyse en evaluatie risico's	4,0	4,0	3,0	2,0	3,0
10	Meten RM onderdeel organisatie	2,0	3,0	1,0	3,0	3,0
11	Continue verbetering RM	4,0	3,0	2,0	3,0	2,0
12	Welke concrete maatregelen	open	open	open	open	open
13	Verantwoordelijkheden RM	4,0	4,0	2,0	3,0	4,0
14	Organisatie zorgt voor kennis m.b.t. RM	4,0	3,0	2,0	3,0	3,0
15	Aangewezen individuen controle RM	2,3	3,3	3,3	2,7	3,3
15a	Autoriteit, middelen, training etc.	open	open	open	open	open
15b	Communicatie	open	open	open	open	open
16	RM introductieprogramma's	1,0	3,0	3,0	1,0	1,0
17	Expliciet rekening houden risico	3,0	2,0	3,0	1,0	3,0
18	RM vertegenwoordigd bij belangrijke processen	3,0	3,0	3,0	1,0	3,0
18a	Aangetoond met notulen en documenten	3,0	3,0	0,0	1,0	2,0
19	Communicatie essentieel	3,0	2,0	3,0	1,0	2,0
20	Rapportage RM voor governance	2,0	4,0	3,0	3,0	3,0
20a	Frequentie rapportage	2,0	4,0	2,0	2,0	3,0
21	RM beschouwd als belangrijk	3,0	3,0	2,0	1,0	3,0
22	RM beschouwd als belangrijk door managers	3,0	3,0	2,0	1,0	2,0
	Score	74,2	74,9	61,4	48,1	65,4
	Niveau	4	5	4	3	4

Aken, v. (2004). Management research based on the paradigm of the design sciences: The quest for field-tested and grounded technological rules, John Wiley & Sons. **41:** 219-246.

Aven, T. and O. Renn (2009). "On risk defined as an event where the outcome is uncertain." Journal of Risk Research **12**(1): 1-11.
Barateiro, J. and J. Borbinha (2011). "Integrated management of risk information." Proceedings of the Federated Conference on
Computer Science and Information Systems pp. 799–806.
Beasley, M. S., R. Clune, et al. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation, Elsevier. **24:** 521-531.
Bowling, D. M. and L. A. Rieger (2005). 'Making sense of COSO's new Framework for Enterprise Risk Management'. **18:** 29-34.
Chapman, C. and S. Ward (2004). Why risk efficiency is a key aspect of best practice projects, Elsevier. **22:** 619-632.
Chopra, S. and M. M. S. Sodhi (2004). "Supply-Chain Breakdown." MITSLOAN Management Review **45**(1).
Christensen, F. M., O. Andersen, et al. (2003). "Risk terminology--a platform for common understanding and better communication." Journal of Hazardous Materials **103**(3): 181-203.
Claes P.F. , M. H. J. J. M. (1997). Risk Management - inleiding tot het risicobeheersproces. Houten, Stenfert Kroese/Educatieve Partners Nederland B.V.
COSO (1992). Internal Control – Integrated Framework (Executive Summary).
COSO (2004). "Enterprise Risk
Management —
Integrated Framework
Executive Summary."
Cox Jr, A. T. (2008). What's wrong with risk matrices?, Wiley Online Library. **28:** 497-512.
Cozijnsen, A. J., W. J. Vrakking, et al. (2000). Success and failure of 50 innovation projects in Dutch companies, MCB UP Ltd. **3:** 150-159.
Denenberg, H. S. and J. R. Ferrari (1966). New perspectives on risk management: The search for principles, JSTOR. **33:** 647-661.
Dickinson, G. (2001). "Enterprise Risk Management: Its Origins and Conceptual Foundation." The Geneva Papers on Risk and Insurance **26**: 360 - 366.
Haimes, Y. Y. (2009). Risk Modeling, Assessment, and Management. Virginia, Wiley.
Hedges, B. A. (1965). A Methodology for a Course in Risk Management, JSTOR. **32:** 609-615.
Heijden, W. v. d. (2006). "Risicomanagement in de aderen?!, Een onderzoek naar het invoeren en inbedden van
projectrisicomanagement binnen NS Project Consult."
Hillson, D. A. (1997). "Toward a Risk Maturity Model." The International Journal of Project & Business Risk Management **1**(1): 35-43.
Hillson, D. A. (2002). "Extending the risk process to manage opportunities." International Journal of Project Management **20** (3): 235-240.
Hubert, P., M. H. Barny, et al. (1991). Elicitation of Decisionâ€Makersâ€™ Preferences for Management of Major Hazards, Wiley Online Library. **11:** 199-206.
Humphrey, W. (1989). Managing the Software Process, Addison-Wesley.
ISO (2002). "Guide 73: Risk management — Vocabulary."
ISO (2009). "ISO31000 Risk management — Principles and
guidelines."
ISO/FDIS (2009). "ISO/FDIS31000 Risk management — Principles and
guidelines."
ISO/IEC (2002). Guide73, Risk management - Vocabulary.
ISO/IEC (2002). "Guide 73: Risk management — Vocabulary."
Jaafari, A. (2001). "Management of risks, uncertainties and opportunities on projects: time for a fundamental shift." International Journal of Project Management **19**(2): 89-101.
Kaplan, S. and B. J. Garrick (1981). On the quantitative definition of risk, Blackwell Publishing Ltd. **1:** 11-27.

Kleffner, A. E., R. B. Lee, et al. (2003). The effect of corporate governance on the use of enterprise risk management: Evidence from Canada, Wiley Online Library. **6:** 53-73.
Klinke, A. and O. Renn (2002). A New Approach to Risk Evaluation and Management: Riskâ€Based, Precautionâ€Based, and Discourseâ€Based Strategies1, Wiley Online Library. **22:** 1071-1094.
Knechel, W. R. (2007). "The business risk audit: Origins, obstacles and opportunities." Accounting, Organizations and Society **32**(4-5): 383-408.
March, J. G. and Z. Shapira (1987). Managerial perspectives on risk and risk taking, Institute of Management Sciences. **33:** 1404-1418.
Olson, D. D. W. (2007). Enterprise Risk Management. Singapore, World Scientific Publishing Co. .
P.F. Claes, H. J. J. M. M. (1997). Risk Management - inleiding tot het risicobeheersproces. Houten, Stenfert Kroese/Educatieve Partners Nederland B.V.
Paape, L., D.M. Swagerman, (2006). Risicomanagement - De Praktijk In Nederland. . Amsterdam, PriceWaterhouseCoopers, Rijks Universiteit Groningen

Paulk, M. C., C. V. Weber, et al. (1993). Key Practices of the Capability Maturity Model SM, Version 1.1, Citeseer.
PM&C. from http://www.dpmc.gov.au/implementation/policy.cfm.
Power, M. (2001). Organised uncertainty: designing a world of risk management, Routledge. **14:** 33-34.
Sarbanes-Oxley (2002). "Sarbanes-Oxley Act 2002." Government Printing Public Office **Law No.107–204**.
Simkins, B. and S. A. Ramirez (2007). Enterprise-Wide Risk Management and Corporate Governance, HeinOnline. **39:** 571.
Skjong, R. and B. H. Wentworth (2001). Expert judgment and risk perception.
Snider, W. (1991). Risk management: A retrospective view, Risk Management Society Publishing, Inc. **34:** 47–54.
Software and Engineering Institute, C. M. U., http://www.sei.cmu.edu/cmmi/. Retrieved 2012-07-29.
Staveren, V. (2009). RISK, INNOVATION & CHANGE, Design Propositions for Implementing Risk Management
in Organizations, Universiteit Twente, Enschede, Nederland. **PhD.**
Ward, S. C. (1999). Assessing and managing important risks, Elsevier. **17:** 331-336.
Williams, T. M. (1996). The two-dimensionality of project risk, Elsevier. **14:** 185-186.