Oktober 2014

Hoeveel zijn we opgeschoten na de crisis?

Tweede Nationaal Onderzoek Risicomanagement in Nederland 2014

Nederlandse Beroepsorganisatie van Accountants
NBA

NYENRODE BUSINESS UNIVERSITEIT

rijksuniversiteit groningen
faculteit economie en bedrijfskunde

pwc

De onderzoekers v.l.n.r.: Casper Ruizendaal, Remko Renes, Dirk Swagerman, Marcel Prinsenberg, Esra Aktas, Leen Paape, Johan Scheffe, Matthijs van de Belt. Gerben Posthumus ontbreekt op deze foto.

Titel:
Hoeveel zijn we opgeschoten na de crisis?

Subtitel:
Tweede nationaal onderzoek risicomanagement in Nederland 2014

Opdrachtgevers:
Rijksuniversiteit Groningen; Nyenrode School of Accountancy & Controlling; NBA; PwC

Beeldmateriaal:
Dreamstime, Nationale beeldbank

Eindredactie:
Margreeth Kloppenburg

ISBN/EAN: 978-90-75103-79-3

Voorwoord

Herkenbare resultaten, helaas. Maar ook lichtpuntjes

Met dit rapport leggen de auteurs helder bloot wat er helaas nog mis is met risicomanagement in Nederland. Dat is natuurlijk in de eerste plaats de eigen verantwoordelijkheid van de bestuurders. We zien gelukkig ook voorbeelden van organisaties die de verantwoordelijkheid voor adequaat risicomanagement wel nemen. Feit blijft dat niet alle bestuurders goed lijken te beseffen wat er mis kan gaan. De uitkomst dat bestuurders zelf denken dat zij het voor elkaar hebben, waar een objectieve meting vaststelt dat dat niet zo is. Dat kan als oorzaak hebben dat risicomanagement onvoldoende serieus genomen wordt, of doordat bestuurders het lastig vinden, bijvoorbeeld als hen gevraagd wordt ook niet kwantificeerbare risico's in kaart te brengen; reputatierisico's bijvoorbeeld, of de risicocultuur in de organisatie. Beide oorzaken wil ik graag nader toelichten.

Niet serieus?

Als het de eerste oorzaak is, en organisaties risicomanagement niet serieus nemen, dan is het zaak dat we laten zien - ook wij als DNB - hoe serieus aangepakt risicomanagement kan bijdragen aan een stabiele economie. Wettelijk zijn vele instellingen onder ons toezicht dat ook verplicht trouwens. Op grond van de Wft en de onderliggende regelgeving moeten de instellingen die onder ons toezicht staan op een systematische manier hun risico's analyseren en daarop gepaste maatregelen nemen. Dit betekent dat instellingen zelf moeten bepalen welke risico's voor hun organisatie het grootst zijn en hoe zij hun beleid en procedures hierop aanpassen. De huidige praktijk leert dat veel instellingen nu nog onvoldoende invulling geven aan de systematische analyse van de risico's en niet voldoende actie ondernemen naar aanleiding van een (soms onvoldoende) analyse. Het is belangrijk dat deze analyse een continue karakter heeft, omdat risico's ook niet statisch zijn. Zowel interne als externe factoren kunnen ervoor zorgen dat risico's voor een instelling veranderen. Met zo'n systematische risicoanalyse stelt de instelling vast of de huidige beheersmaatregelen effectief zijn. Als dat niet het geval is, dan past de instelling de beheersmaatregelen aan. Een systematische risicoanalyse houdt verder in dat de instelling zo'n analyse periodiek uitvoert volgens een vastgestelde methodiek én de uitkomsten schriftelijk vastlegt.

Risicomanagement lastig?

Jazeker is goed risicomanagement lastig. Dat is nou juist het hele idee: tegenspraak is niet leuk, grootse plannen afblazen vanwege te hoge risico's is niet leuk. Maar het is een noodzaak. Hoe onafhankelijker de risicofunctie belegd is in de organisatie, des te sterker het risicomanagement zich kan ontwikkelen en - natuurlijk ook - des te meer potentiële tegenspraak. Het is zaak dat de risicomanagers in Nederland (en daar draagt DNB graag aan bij) helder laten zien wat goed risicomanagement is en hoe dat juist ondernemersdoelen dichterbij kan helpen brengen. Een onafhankelijke Chief Risk Officer naast een Chief Financial Officer in het bestuur opnemen kan helpen om risicomanagement een vanzelfsprekend onderdeel van het bedrijfsproces te maken en zo waarborgen in te bouwen voor gezonde bedrijfsvoering, continuïteit en levensvatbaarheid van een onderneming.

Beide oorzaken zijn weg te nemen, dunkt mij. Wellicht kunnen we dus over vijf jaar - als het derde Nationaal Onderzoek Risicomanagement in Nederland is uitgevoerd - vaststellen dat in ieder geval de beleving van bestuurders en van de onderzoekers dichter bij elkaar gekomen is en liefst zien we dan flink hogere scores. Daar wens ik u veel sterkte bij.

Jan Sijbrand, Directie DNB

Open brief aan de bestuurders van Nederland

Bestuurders van Nederland,

In 2009 presenteerden wij ons eerste onderzoek naar de stand van zaken van risicomanagement in Nederland. Nu, vijf jaar later, bieden wij u met veel plezier het vervolg aan op ons onderzoek. In hoeverre zijn organisaties als de uwe in de weer geweest met het invoeren en verbeteren van hun risicomanagementsysteem?

Tot onze verrassing hebben we geconstateerd dat er nauwelijks verbetering is gerealiseerd; sterker nog, soms is er zelfs sprake van een lichte achteruitgang. Het vervelende is dat u zelf van mening bent dat u wel bent opgeschoten. Dat kan ertoe leiden dat u zichzelf zand in de ogen hebt laten strooien en daar op een onverwacht moment de rekening voor zult betalen. Heeft u inderdaad goed nagedacht over welke risico's u wenst te accepteren en welke niet? Is er een cultuur waarin slecht nieuws u op tijd bereikt? Wordt bij besluitvorming onder onzekerheid - uw schone taak - voldoende nagedacht over mogelijke scenario's, of komt u misschien ook niet veel verder dan een slecht en een goed scenario en met iets dat er tussenin zit?

Veel van uw collega-bestuurders meenden ook dat het wel goed zat. Diverse organisaties kwamen echter ernstig in problemen. Vestia, Imtech, Rabobank, BAM, Meavita, Douwe Egberts, Ballast Nedam, SNS Reaal, Amarantis zijn slechts een paar namen. Het bijzondere is dat in alle gevallen de organisaties zeperds te verduren kregen in de kern van hun bedrijf. Niet in buitenissige activiteiten, nee, in activiteiten waarin ze verondersteld werden goed te zijn! Zij werden vol geraakt in het hart van hun bedrijf. Iedere bestuurder, en waarschijnlijk ook u, vraagt zich dan af: *"Kan dat ook bij mij gebeuren?"* Ons antwoord luidt: *"Dat zou zo maar kunnen"*; als u net als veel van de respondenten in ons onderzoek veronderstelt dat u het beter doet dan die ongelukkige organisaties. Als u wilt nagaan of uw organisatie het werkelijk beter doet, dan nodigen we u graag uit kennis te nemen van dit rapport.

Leest u op zijn minst hoofdstuk 3 door en ga in gesprek met uw Chief Risk Officer, Compliance Officer, internal auditor of uw financiële verantwoordelijke met de vraag welke lessen u samen kunt trekken uit dit rapport. *"Welke conclusies en aanbevelingen gelden ook voor ons? Wat gaan wij doen om dit te verbeteren?"* Wij roepen u op om in ieder geval kritisch te kijken naar de volgende zes vragen:

- Is risicomanagement bij ons echt geïntegreerd in ons prestatiemanagement? En er is een directe link met de beoordeling en beloning van onze medewerkers?
- Zijn risicomanagement en interne controle verankerd in het DNA van onze organisatie?
- Hoe brengen wij structuur, kwaliteit en positie van onze risicomanagementafdeling naar een hoger plan?
- Hebben wij onze risicobereidheid wel uitgesproken? En consistent doorvertaald en gecommuniceerd naar de hele organisatie?
- Is ons risicomanagement daadwerkelijk integraal, dus dekt het alle risico's af inclusief de invloeden van buitenaf?
- Hoe kunnen wij ons strategisch risico-denken verder versterken?

Wij verzekeren u dat het u zal helpen te voorkomen dat u terechtkomt in het hierboven genoemde rijtje schandalen in ons volgende onderzoek over vijf jaar.

Wij wensen u daarbij alle succes.

Oktober 2014

Open brief aan de risicomanagers van Nederland

Risicomanagers van Nederland,

In 2009 presenteerden wij ons eerste onderzoek naar de stand van zaken van risicomanagement in Nederland. Nu vijf jaar later bieden wij u met veel plezier het vervolg aan op ons onderzoek. In hoeverre zijn organisaties als de uwe, in de weer geweest met het invoeren en verbeteren van hun risicomanagementsysteem?

Tot onze verrassing hebben we geconstateerd dat er nauwelijks verbetering is gerealiseerd; sterker nog, soms is er zelfs sprake van een lichte achteruitgang. Het vervelende is dat u zelf van mening bent dat u wel bent opgeschoten. Dat kan ertoe leiden dat u zichzelf zand in de ogen strooit en daar op een onverwacht moment de rekening voor zult betalen. Heeft u inderdaad goed nagedacht over welke risico's u wenst te accepteren en welke niet? Is er een cultuur waarin u slecht nieuws op tijd kan brengen? Bent u in staat om bij besluitvorming onder onzekerheid uw bestuurders in voldoende mate te informeren over de voor- en nadelen van de mogelijke scenario's, of komt u misschien ook niet veel verder dan een slecht en een goed scenario en met iets dat er tussenin zit?

Natuurlijk weet u ook dat er nog veel te verbeteren is. Vaak zal het niet meevallen uw omgeving daarvan te overtuigen. Risicomanagement is wel belangrijk, maar vaak wordt u gezien als 'tweede lijn', weliswaar noodzakelijk maar soms ook een sta in de weg. U heeft de afgelopen jaren de wind in de rug gehad, de financiële crisis en de bedrijfsschandalen die de krant haalden, maakten dat de belangstelling voor uw werk toenam, soms ook vereist door regelgeving. Er is echter nog steeds meer dan genoeg werk aan de winkel. De krant staat nog steeds rijkelijk vol met schandalen van flinke omvang.

Het zou goed zijn als u met dit rapport in de hand nog eens vaststelt waar uw organisatie staat en wat er beter kan. Bespreek het met uw bestuurders en stel aan hen de vraag wat u samen met het bestuur kan doen. Deze vragen kunnen u in dat gesprek wellicht helpen:

- Welke rol willen we dat ons risicomanagement speelt: van reactief naar proactief? Van technische skills naar business skills? En wat betekent dat voor ons team?
- Hoe kunnen we alle managementlagen beter betrekken en het lijnmanagement helpen de verantwoordelijkheid voor risicomanagement op te pakken?
- Is er technologie dat ons kan helpen ons risicomanagement effectiever en efficiënter te maken én het tegelijk aantrekkelijker en gemakkelijker te maken voor het lijnmanagement?
- Hoe kunnen we nieuwe technieken en methoden vinden en implementeren om ook in de toekomst alert te blijven op strategische en 'emerging risico's' en het managen ervan?

Met dit rapport in uw hand kunt u ook een onderbouwd pleidooi houden om als Chief Risk Officer voortaan in de Directie/Raad van Bestuur te komen zitten, omdat ons onderzoek vooralsnog aangeeft dat de CRO als 'dedicated risk champion' tot betere resultaten leidt dan in organisaties waar risicomanagement een van de vele taken is van een van de directieleden.

Over vijf jaar horen wij graag welke vorderingen u heeft gemaakt. Wij wensen u daarbij veel succes, wetend dat uw organisatie er wel bij zal varen.

Inhoud

1. Inleiding

Met trots presenteren wij u - gewaardeerde lezer, bestuurder van, risicomanager bij of geïnteresseerde in profit en non-profit organisaties in Nederland - de resultaten van het tweede nationale onderzoek naar de stand van zaken rondom risicomanagement. In 2009 hebben wij het eerste nationale onderzoek naar risicomanagement in Nederland gepresenteerd met toen ruim 900 deelnemers. In ons voorwoord schreven we dat over vijf jaar zou blijken hoeveel we zijn opgeschoten. Tijd dus voor een update.

De timing van het eerste nationale onderzoek had niet beter gekund: de grootste financiële crisis in mensenheugenis was net daarvoor uitgebroken. Pijnlijk duidelijk werd zichtbaar dat veel organisaties hun risicomanagement niet op orde hadden. Met name financiële instellingen, die toch vermeend over de beste systemen en methoden beschikten en zeker over het beste toezicht op hun handel en wandel, vielen door de mand. De wereld lijdt nog altijd onder de gevolgen. Er lijkt vooralsnog ook nog geen einde te komen aan de voortdurende stroom van nieuwe incidenten op het gebied van risicomanagement en interne beheersing, waarbij het woord incident de lading eigenlijk onvoldoende dekt, zoals recent bij Vestia, Imtech, Rabobank, Amarantis, BAM, Douwe Egberts, Ballast Nedam, SNS Reaal, etc.

Vergelijkbare vragen als 2009, maar nu met risicocultuur

Zou het vijf jaar, veel rapporten, onderzoeken en verbeterinitiatieven later, beter zijn gesteld, zo vroegen wij ons af. Hebben we geleerd van onze fouten? En welke vragen zouden ons helpen meer inzicht te verkrijgen in de ontwikkeling van risicomanagement in de afgelopen jaren? In wetenschappelijk opzicht was er niet veel kennis opgedaan op dit punt en natuurlijk, veranderingen hebben tijd nodig. Wel helder kwam naar voren dat zowel risicocultuur als toon aan de top dominante thema's zijn geworden. Want als het dan niet aan de instrumenten en methoden ligt, dan misschien toch aan de mensen en de cultuur waarbinnen zij moeten werken, zo is de gedachtegang. Wij hebben dan ook een poging gedaan dat begrip risicocultuur in onze vragenlijst een plaats te geven. Een poging met gebreken, want bruikbare resultaten van hoe risicocultuur te meten zijn nog niet of nauwelijks voorhanden. Bovendien vergt het in kaart brengen van cultuur grootschalig onderzoek en dit was praktisch gezien helaas onmogelijk. Desondanks bevat dit rapport genoeg interessante aanknopingspunten over risicocultuur. En nodigen wij u bij dezen ook graag uit een bijdrage te leveren aan het verder brengen van ons begrip van risicocultuur.

De vragen die we in dit tweede onderzoek hebben gesteld, zijn vaak onveranderd gebleven ten opzichte van ons eerste onderzoek in 2009 en daar waar relevant - licht - aangepast op basis van de laatste inzichten. Die ongewijzigde vragen stellen ons in staat een vergelijking te maken met de uitkomsten uit 2009. Is er nu progressie gemaakt? Is er soms zelfs een terugval te zien? Zo ja, op welke terreinen dan? De 727 respondenten - van de bijna 10.000 uitgezonden vragenlijsten - hebben ons informatie verstrekt over vele sectoren. Daardoor zijn wij in staat verschillende vergelijkingen voor u te maken. Een vergelijking tussen profit en non-profit had bijvoorbeeld onze belangstelling, maar ook de eventuele waterscheiding tussen bedrijven in de financiële sector en de rest. De eerste keer was er een flink verschil tussen die twee. En of het nu weer zo is, leest u verderop in dit rapport.

Verder wensten we u graag meer inzicht te bieden in het gebruik van tools, technieken en software ter ondersteuning van de risicomanagementactiviteiten. Er is het nodige op de markt gekomen in de afgelopen jaren en de markt van aanbieders zelf is ook veranderd. Aanbieders consolideerden, softwaretools verbeterden en er werd meer gebruik van gemaakt. Wij vroegen ons dan ook af in

hoeverre deze nieuwe instrumenten de organisaties bereikt hebben. Want goed gebruikt, geven tools en software een krachtige impuls aan het monitoren, analyseren en vroegtijdig signaleren van risico's. Bovendien helpen ze de feilbare mens uitstekend hem/haar bij de les te houden. Zijn die effecten zichtbaar?

Dit rapport

In het rapport vindt u eerst een kleine schets van de geschiedenis sinds ons vorige rapport, uit 2009. Daarna leest u ons eindoordeel, het antwoord op de vraag: *"Hoeveel zijn we opgeschoten in de crisis?"* Aan dat antwoord koppelen we een serie aanbevelingen, van concrete, makkelijk te implementeren verbeteringen tot aanzetten voor grootschaliger ingrepen.

Mocht u meer willen weten over een specifieke sector, of over een speciaal onderwerp, bladert u dan meteen naar hoofdstuk 4. Daarin onderbouwen we onze oordelen en aanbevelingen en laten we zien waar het soms goed en soms minder gaat; steeds opgezet aan de hand van de vragen uit onze survey. Opvallende cijfers, bijvoorbeeld een sector die eruit springt, of een onderdeel dat een aparte score heeft, lichten we er daar uit. Omdat risicocultuur zo'n grote rol speelt in de huidige discussie over het falen van organisaties en hun risicomanagement, hebben we de risicocultuur als nieuw onderdeel aan onze vragenlijst toegevoegd en er een afzonderlijk hoofdstuk aan gewijd in dit rapport: hoofdstuk 5.

In hoofdstuk 6 vindt u tot slot een toegift: we hebben de data die we verzameld hebben ook met een andere bril bekeken: ten eerste hebben we onderzocht welke voordelen risicomanagement kan bieden in de ogen van de respondenten. Ten tweede hebben we dankzij de onderzoeksdata op wetenschappelijk onderbouwde manier kunnen benoemen welke in- en externe factoren van invloed zijn op de volwassenheid van een risicomanagementsysteem. De uitgebreide verantwoording van de door ons gebruikte methodologie tot slot vindt u waar u die verwacht: achterin, vlak achter de literatuuropgave.

We wensen u veel leesplezier en hopen dat wij u verder helpen met de resultaten uit het onderzoek. Mist u bepaalde vragen, of mist u uw eigen bedrijf in de resultaten? Laat het ons weten, en nog mooier, meld u aan als deelnemende organisatie voor het derde onderzoek. In 2019!

Breukelen/Amsterdam/Groningen, 29 oktober 2014

2. Trends in risicomanagement 2009 - 2014

'Wat kan er veel veranderen in 5 jaar'... dat waren de beginwoorden van het rapport van 2009. We bevonden ons toen in het zwaartepunt van de crisis. Hoe had de crisis invloed op het denken over risicomanagement? Zou risicomanagement organisaties in staat stellen zich te wapenen tegen politieke of macro-economische stormen die buiten woedden? Het waren ineens wel heel urgente vragen.

Wie dacht dat de storm waar we toen over schreven na vijf jaar wel geluwd zou zijn, had het (helaas!) mis. De omgeving is nog altijd turbulent en de dreiging dat de economische 'double dip' een 'triple dip' wordt, is nog altijd aanwezig. In het zoeken naar 'schuldigen' is de tolerantie voor fouten van bestuurders en toezichthouders in de publieke opinie tot een minimum gedaald. Toezichthouders reageren door regelgeving stringenter te maken en zijn steeds meer voorschrijvend in de uitvoering van primaire processen.

De crisis en het moeizame herstel hebben ook duidelijk effect gehad op de ontwikkelingen binnen het vak van risicomanagement. Traditionele methoden van risico's beheersen blijken niet meer te voldoen in een omgeving die sneller en heftiger verandert. Dit zien we in toenemende aandacht voor een deugdelijke risicocultuur en een steeds verder gaande integratie van prestatie- en risicomanagement. Niet meer van hetzelfde, maar hetzelfde op een andere en betere manier. Hieronder leest u de belangrijkste vijf trends van de afgelopen vijf jaren.

2.1 Zero-tolerance

De voormalig bestuurders van onder meer Vestia, Imtech, Rabobank, Amarantis, BAM, Douwe Egberts, Ballast Nedam, SNS Reaal kunnen erover meepraten: klanten, aandeelhouders, de politiek, men kent geen tolerantie meer voor bestuurders of commissarissen die grote fouten maken. Al dan niet via de rechter wil de maatschappij hen laten boeten voor fouten die zij vanuit hun voormalige functies maakten. De aansprakelijkheid van topbestuurders en commissarissen neemt de laatste jaren toe, onder meer onder politieke druk. Waar er bij de rechter nog steeds sprake moet zijn van 'ernstig verwijtbaar handelen', zijn de politiek en publieke opinie stukken minder voorzichtig in het uiten van kritiek. Niet zelden voordat een eventueel strafrechtelijk onderzoek is afgerond.

De persoonlijke reputatie- en financiële risico's die bestuurders en commissarissen lopen zijn door bovenstaande ontwikkelingen en toenemend claimgedrag flink toegenomen. Dit betekent ook dat er veel meer gebeurd moet zijn voordat een bestuurder zijn handtekening zet onder een 'in-control' verklaring, waardoor het belang en de werking van de onderliggende methodieken veel meer gewicht hebben gekregen.

De vraag om transparantere bedrijfsvoering en het beheersen van risico's klinkt steeds luider: vanuit klanten, investeerders, toezichthouders en rating agencies.

2.2 Toenemende druk van wet- en regelgeving

Al op de eerste dag van de openbare hoorzittingen naar de oorzaken van de crisis van de onderzoekscommissie Financieel Herstel[1] gingen de beschuldigende vingers richting de toezichthou-

1 Commissie De Wit

ders. Het toezicht zou te veel gericht zijn op de naleving van regels in plaats van op de naleving van principes.

Welnu, meer regels zijn er de afgelopen jaren absoluut bijgekomen! Zoveel zelfs dat uit PwC onderzoek[2] onder ruim 1300 ceo's uit 68 landen bleek dat de toenemende regeldruk als grootste bedreiging wordt gezien voor economisch herstel (en het welzijn van hun organisaties). De tendens is dat er inderdaad meer aandacht komt voor naleving van principes. Maar dat moet dan wel aantoonbaar zijn, met als gevolg dat er alsnog meer regels bij komen. Voor internationaal opererende organisaties of organisaties met internationale klanten vormen de verschillen in regimes en filosofieën van toezicht nog eens een extra uitdaging.

2.3 Snelheid en impact van veranderingen

Het risicolandschap verandert in sneltreinvaart: demografische veranderingen, versnelde verstedelijking, verschuiving van de economische macht, klimaatverandering, technologische innovaties, de rol van sociale media, de veranderingen in de arbeidsmarkt en complexer wordende waardeketens met steeds meer afhankelijkheden. Hoe beheers je dat? Door de diversiteit in strategische risico's als gevolg van deze veranderingen en de onvoorspelbaarheid van de bijbehorende risico's volstaat een traditionele ad hoc (eendimensionale) aanpak voor het managen van risico's niet meer en is een andere aanpak vereist.

Het World Economic Forum[3] concludeerde in 2012 al dat de risico's waar organisaties vandaag de dag aan blootstaan alleen kunnen worden beheerst door middel van samenwerking van bedrijven, overheden en de maatschappij op basis van langetermijndenken.

Het vroegtijdig ontdekken van zogenaamde 'Black Swans[4]' vraagt om uitdaging van de status quo, om inbreng van externe en misschien wel vreemde denkbeelden in strategievorming en risicoidentificatie. Hierbij is samenwerking (over waardeketens heen, met consumenten, leveranciers, binnen sectoren, met overheid, NGO's, etc.) een basis voor succes.

2.4 Risicocultuur

Organisaties leggen graag het zwaartepunt op tastbare maatregelen bij het uitvoeren van risicomanagement. Bijvoorbeeld door alle risico's te beschrijven, een risicomanager aan te stellen of concrete beheersmaatregelen vast te leggen.

Alleen, risicomanagement gaat over veel meer dan risico's op managementniveau. Het zijn ook de medewerkers op de vloer die iedere dag afwegen of ze wel of geen risico nemen. Gewoon tijdens het werk. Veel van het succes van risicomanagement hangt dus af van het risico- en controlbewustzijn op alle lagen binnen een organisatie.

Er is dan ook toenemende aandacht voor soft controls. Deze zijn nodig om harde beheersmaatregelen te laten werken. Denk aan zaken als leiderschap, voorbeeldgedrag en communicatiestijlen.

2 PwC: 17th Annual Global CEO Survey: Fit for the future
3 World Economic Forum: Global Risks 2012
4 Nassim Nicholas Taleb behandelt in zijn boek 'The Black Swan' uitzonderlijke gebeurtenissen die een enorme invloed hebben, maar die niemand ziet aankomen.

2.5 Integratie van prestatie- en risicomanagement

Een indicatie voor de risicocultuur van een organisatie is in hoeverre er gestuurd wordt op een balans tussen prestaties en risico's. Is analyse en beheersing van risico's al een wezenlijk onderdeel van de bedrijfsvoering? Het eerder genoemde PwC-onderzoek toont aan dat 65 procent van de organisaties hun risico's en prestaties niet in samenhang analyseert en bestuurt. Onverstandig, als men zich realiseert dat de buitenwereld degene die verantwoordelijk is voor de resultaten, ook verantwoordelijk houdt voor de risico's.

Het startpunt van een succesvolle integratie is dan ook dat organisaties risicobereidheid gaan beschouwen als een belangrijk onderdeel van de strategische planvorming. De beste vervolgstap is het wanneer er vervolgens ook nog in samenhang op prestatie en risico gestuurd wordt. Immers, risico en rendement horen onlosmakelijk bij elkaar. Meer risico kan leiden tot meer rendement, maar uiteraard is de andere kant van de medaille dat de volatiliteit zal toenemen en daarmee de voorspelbaarheid van de resultaten afneemt.

Steeds meer organisaties erkennen - al dan niet geprikkeld door toezichthouders - dat het zinvol is risicobereidheid mee te nemen in de plannen. Nog niet veel organisaties zijn al zo ver dat ze de tweede stap hebben gezet en sturen op resultaten én op risicobeheersing. Dit is een kwestie van de lange adem, maar de omgeving vraagt er nu al om.

In ons volgende hoofdstuk leest u ons oordeel over de ontwikkeling van risicomanagement anno 2014.

"Risicomanagement blijft voor een groot deel mensenwerk. Het begint met risicobewust handelen, risico's systematisch in kaart brengen en dialoog over de toprisico's op elk niveau van de organisatie."

Siebe Riedstra, Secretaris-generaal bij het ministerie van Infrastructuur en Milieu

"De dialoog tussen bestuur en toezicht verbetert aanmerkelijk wanneer risicomanagement serieus genomen wordt en regelmatig op de agenda staat."

Paul van Gelder, Lid Raad van Bestuur Royal Imtech NV

3. Samenvatting: ons oordeel over de ontwikkeling van risicomanagement

3.1 Op onderdelen verbetering - geen structurele stap gezet

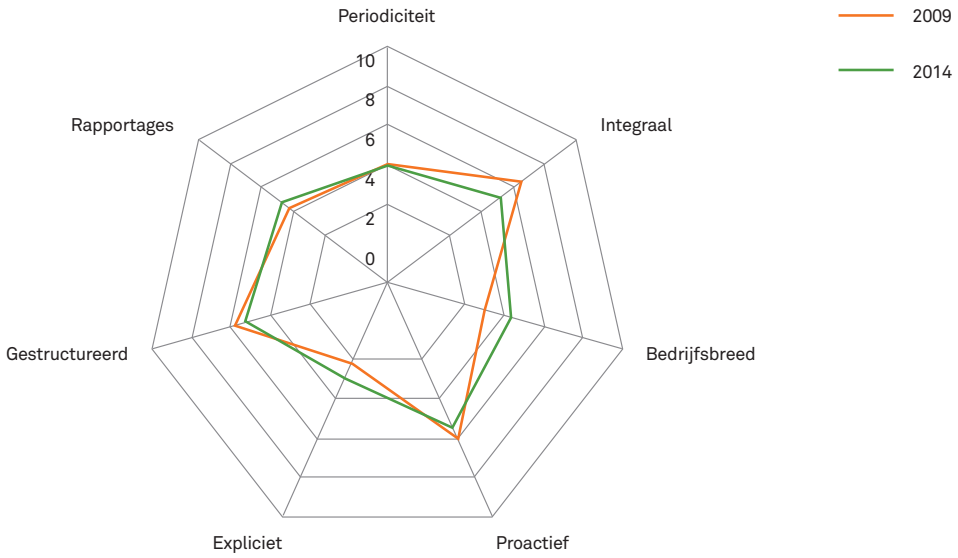
Hoeveel zijn we opgeschoten na de crisis?

De resultaten laten zien dat op sommige terreinen vooruitgang is geboekt, maar op andere zelfs een lichte achteruitgang te constateren valt. Verder zijn er opvallende verschillen te zien tussen de ontwikkelingen in de publieke versus de private sector. In de tekst hierna zullen we duiden welke factoren bijdragen aan beter risicomanagement en welke niet. Om u als risicomanager of als ondernemer in staat te stellen keuzes te maken bij het verder verbeteren van uw risicomanagementsysteem.

Ondanks crisis geen structurele verbetering in vijf jaar

Wij hebben op basis van een degelijk onderzoek, vergelijkbaar met vijf jaar geleden, niet kunnen vaststellen dat risicomanagement in Nederland significant of structureel is verbeterd, noch de totaalscore, noch de scores per sector of criterium.[5]

Figuur 1: Spiderdiagram vergelijking scores 2014 - 2009 per criterium



We vroegen de respondenten ook hun eigen risicomanagementsysteem te waarderen en de uitslag heeft ons verrast: Organisaties voelen zich blijkbaar vrij zeker over de kwaliteit van hun eigen risicomanagementsysteem. En dit vertrouwen is ook nog eens toegenomen afgezet tegen de resultaten van 2009. Op een schaal van 1 tot 10 vroegen wij hen zichzelf te scoren (1 = zeer slecht, 10 = uitstekend). Het gemiddelde zelf gegeven rapportcijfer is een 6,85 (+0,37 vergeleken met 2009). Bovendien vindt ongeveer 89 procent (+9 procent vergeleken met 2009) van de respondenten hun risicomanagementsysteem voldoende: een score van een 6 of hoger. Er is overigens een significante samenhang tussen hogere zelfscore en hogere score op onze criteria: respondenten die zichzelf een hoger rapportcijfer geven, scoren ook op onze scoreleidraad hoger.

5 Volgens scoreleidraad onderzoekers.

Dit neemt niet weg dat wij van mening zijn dat risicomanagement in Nederland nog steeds van onvoldoende niveau is.

Waarom is dit niet goed genoeg?

Een structurele verbetering is wel degelijk nodig, om drie redenen. Ten eerste blijkt uit vele onderzoeken[6] dat gebrekkig of kwalitatief minder risicomanagement een van de oorzaken is geweest van de financiële crisis. Ten tweede dreigt het gevaar dat bij uitblijven van betere zelfregulering (of betere eigen invulling van in dit geval risicomanagement), een overheid zal ingrijpen, met meer wet- en regelgeving op het terrein van risicomanagement. Zeker met de constatering dat er in de afgelopen vijf jaar nog steeds in alle sectoren incidenten met risicomanagement zijn geweest. Dat hebben we namelijk eerder zien gebeuren in sectoren als financiële dienstverlening, energie en handel. En ten derde zien we het gevaar levensgroot opdoemen dat organisaties die nu moeten besparen, juist zullen besparen op cruciale onderdelen van risicomanagement, wellicht door het vertrouwen dat ' we nu toch uit het dal aan het klimmen zijn'.

Wel verbetering, op onderdelen

Is er in onze ogen dan helemaal geen vooruitgang geboekt? Gemiddeld misschien niet, maar op onderdelen zien we wel interessante - en soms verontrustende - resultaten.

Van de scores van de verschillende respondenten viel ons vooral op dat grotere organisaties hoger scoren in ons onderzoek, dat geldt zowel voor 'groter in omzet' als 'groter in aantal fte's'. Verder is de functie van Chief Risk Officer (CRO) in opkomst, vooral in de financiële dienstverlening. Die sector heeft überhaupt het meest geïnvesteerd in risicomanagement sinds het vorige onderzoek, zo kunnen we vaststellen.

Opvallende scores bij **risico-inventarisatie en -analyse** zijn ten eerste dat iets meer dan twee derde van de respondenten niet vaker dan één keer per jaar in kaart brengt wat de relevante risico's zijn en dat iets meer dan 13 procent volgens eigen opgave helemaal geen risico's inventariseert noch analyseert. We vonden geen grote verschillen tussen sectoren bij deze vraag. Wel is er gelukkig sprake van een stijging ten opzichte van 2009: meer en meer organisaties inventariseren en analyseren de risico's voor hun bedrijfsvoering en dat geldt gelukkig ook voor alle soorten risico's. Winst is er nog te boeken als organisaties hun risico's meer integraal in kaart brengen en als die inventarisaties en analyses 'dieper' in de organisatie gebeuren: een bedrijfsbrede risicoanalyse is waardevoller dan die waarin alleen een directie of raad van bestuur die uitvoert.

Qua **rapportage en monitoring** van risico's zien we niet veel verschillen met 2009, helaas. Met één uitzondering: waar in 2009 nog 11 procent van de respondenten zei dat intern niet gerapporteerd werd over risico's, is deze categorie nu gedaald tot 5 procent. Bij de andere deelvragen over rapportage en monitoring zien we steeds vergelijkbare uitkomsten als in 2009, meestal met een lichte stijging.

Bij de vragen over **risicomanagement en organisatie** verheugden ons de antwoorden op de vraag naar de risicobereidheid. Het aantal respondenten dat überhaupt een risicobereidheid heeft geformuleerd is verbeterd ten opzichte van 2009. Wel bevreemdt het ons dat niet iedereen die risicobereidheid vastlegt en communiceert. Misschien hangt dat samen met een andere verras-

6 Onder meer **Huber, C. en Scheytt, T.** (2013): The dispositif of risk management: Reconstructing risk management after the financial crisis. *Management Accounting Research*, 24(2), pp 88 - 99
Mikes, A. (2009): Risk management and calculative cultures, *Management Accounting Research*, 20, pp 18 - 40
Power, M. (2009): The risk management of nothing, Accounting, *Organizations and Society*, 34, pp 849 - 855

sende uitkomst: een flinke meerderheid van de respondenten blijkt geen standaard te gebruiken bij de inrichting van risicomanagement en interne beheersing. Een standaard (denk aan ISO, Basel, COSO, INK, EFQM) biedt geen garantie, natuurlijk, maar het biedt wel de kans om te vergelijken en om aan te sluiten bij best practices. Het gebruik van een standaard introduceert namelijk een taal om onderling informatie uit te wisselen over risico's en beheersing.

Door de antwoorden op de (nieuwe) vragen over **risicocultuur** hebben wij de indruk gekregen dat risicomanagement in veel organisaties nog sterk compliance-gedreven is. *"Wij doen aan risicomanagement omdat men dat van ons vraagt"*, lijken de antwoorden te zeggen. En *"men"*, dat kan een accountant zijn, een (extern) toezichthouder of het publiek. De effectiviteit van risicomanagement is bijvoorbeeld bij maar 9 procent van de respondenten een factor bij de beloningssystemen. En de risicoparagraaf is bij de helft van de respondenten vooral of uitsluitend het werk van de financiële functie in de organisatie.

Een belangrijke conclusie uit ons onderzoek die ondersteunt dat risicomanagement met name compliance gedreven is blijkt uit het feit dat ondernemingen het voorkomen van reputatieschade en het verlagen van de vermogenskosten als significante drijfveren zien om hun risicomanagement met een goed rapportcijfer te beoordelen. Daarentegen leiden de mogelijkheden die risicomanagement in zich heeft in termen van hogere winstgevendheid en meer groeimogelijkheden niet tot een hogere waardering van het eigen risicomanagementsysteem.

Ook onze conclusie dat de volwassenheid van risicomanagement met name bepaald wordt door de invloed van externe partijen als een BIG4 accountant, de toezichthouder en normgevende governance codes (al dan niet vrijwillig) bevestigt dit beeld. Risicomanagement voor de buitenwacht of vanuit externe druk. Dit terwijl eigendomsstructuren, met uitzondering van beursfondsen, financiële instellingen en (semi) publieke instellingen, en audit commissies geen significante invloed uitoefenen op risicomanagement. De interne stimulans van risicomanagement berust met name bij de Chief Risk Officer, bij voorkeur met een specifiek toegewijde functie. Dit terwijl het in termen van cultuur niet gezien wordt als een versterking van je carrière en risicomanagement toch nog met name in de bovenste lagen van de organisatie wordt gebezigd.

Dat is opgeteld niet veel verbetering ten opzichte van vijf jaar geleden en het stelt ons dan ook niet gerust. Maar tegelijkertijd beseffen we terdege: het gaat ook niet vanzelf en vijf jaar ís ook kort. We kunnen niet verwachten dat in vijf jaar risicomanagement volledig geïntegreerd is geraakt in alle sectoren. Dat gaat niet vanzelf en bovendien: kúnnen we wel alle risico's managen? Instrumenteel kan dat, ja. Maar wat managen we dan precies? In een wereld die steeds complexer wordt, is het hoogste niveau van risicomanagementvolwassenheid nog niet realistisch en bovendien realiseren we ons dat alle management (dus ook risicomanagement) mensenwerk is. Dus blijven we last houden van menselijke eigenschappen als overschatting van het eigen kunnen, we zoeken vooral bevestiging van wat we al dachten, we laten ons in slaap sussen door vertrouwenwekkende anderen, we houden gebrekkige structuren in stand omdat dat in ieder geval geen onrustwekkende berichten oplevert, enzovoort. *"Nee hoor, de kans dat de rente nóg lager wordt is heel klein", "Het gaat toch al heel lang heel goed? Nou dan!"*

En daar komt nog bij: risicomanagement is zo rijk als de verbeeldingskracht van degene die het risicomanagement toepast.

Hoewel dat begrijpelijk is, is het ook gevaarlijk. Niet alles moeten we maar laten passeren omdat het begrijpelijk en menselijk is, daarvoor is de inzet te hoog. Bewust kiezen voor risicovolle in-

vesteringen als semipublieke instantie, in de kern van je beleid beslissingen nemen die na vijf jaar aan niemand meer uit te leggen zijn, of wél hedgen met swaps maar later in de krant stellen *"Ik weet niet eens wat een swap is"*, dat moeten we niet meer accepteren.

3.2 Hoe verder?

Uit onze uitslagen destilleren we adviezen voor organisaties die een slag willen maken, die een stap willen zetten op weg naar volwassen risicomanagement en die zo klaar zijn voor de volgende crisis of althans het net wat slimmer doen dan hun concurrenten en daarmee een competitief voordeel kunnen realiseren. Voor u dus die dit leest. Maar we zien ook kansen op een grotere schaal, kansen om risicomanagement een serieuzere rol te kunnen laten spelen. We hebben vastgesteld dat in de sectoren waar meer aandacht was voor risicomanagement, de scores hoger zijn geworden en ook sectoren die gereguleerd zijn (wat ook meer aandacht oplevert) hebben eveneens aantoonbaar beter en meer risicomanagement-volwassenheid. Dus accountants, investeerders, toezichthouders, analisten, blijf aandringen.

Risicomanagers van Nederland, u vindt in deze groepen een belangrijke bondgenoot. Ga het gesprek aan met uw bestuurder om risicomanagement op grotere hoogte te brengen.

En bestuurders zelf: u zou vaker dan nu de tijd kunnen nemen om risico's in kaart te brengen en te analyseren - niet alleen op het gebied van risicomanagement maar überhaupt - organiseer tegenspraak (ofwel *constructive dissent*): zorg voor tegenspraak die een bredere blik biedt. Vaak blijkt dat in een organisatie al lang bekend was dat er iets niet deugde, maar bereikten de signalen de top niet, omdat niemand het feestje durfde te bederven.

Neem risicoanalyse en risicomanagement serieus. Stuur niet alleen op compliance, maar stel liever vast wat voor organisatie u wilt zijn, welke risico's u nog wilt lopen en welke niet en bouw daarop zelf uw risicoprofiel. Dát profiel vastleggen en breed in de organisatie delen en daarop checks inbouwen, dat is risicomanagement. En dan natuurlijk vaak monitoren en up-daten.

Tot slot - het zal u niet verrassen - gaan wij verder met onderzoeken. En ook anderen nodigen wij van harte uit verder te onderzoeken hoe we risicomanagement effectiever kunnen maken, om te beginnen in Nederland.

> "'Control' is vitamine aan het begin van de groei en gif aan het einde van diezelfde groei."
>
> *Peter Robertson, Nyenrode en Monterey Institute (VS)*

> "Adequaat riskmanagement voorkomt verrassingen en leidt tot betere resultaten."
>
> *Erik van de Merwe, commissaris en jurylid FD Henri Sijthoff Prijs*

4. Onderzoeksresultaten: analyse en observaties

4.1 Introductie

Hieronder vindt u de resultaten van ons onderzoek, ingedeeld volgens de vijf hoofdgebieden van onze vragenlijst/survey:

1. algemene karakteristieken van de respondenten en hun organisaties (paragraaf 4.2);
2. risico-inventarisatie en -analyse (paragraaf 4.3);
3. risicomanagementrapportage en -monitoring (paragraaf 4.4);
4. risicomanagement en -organisatie (paragraaf 4.5);
5. risicocultuur (hoofdstuk 5).

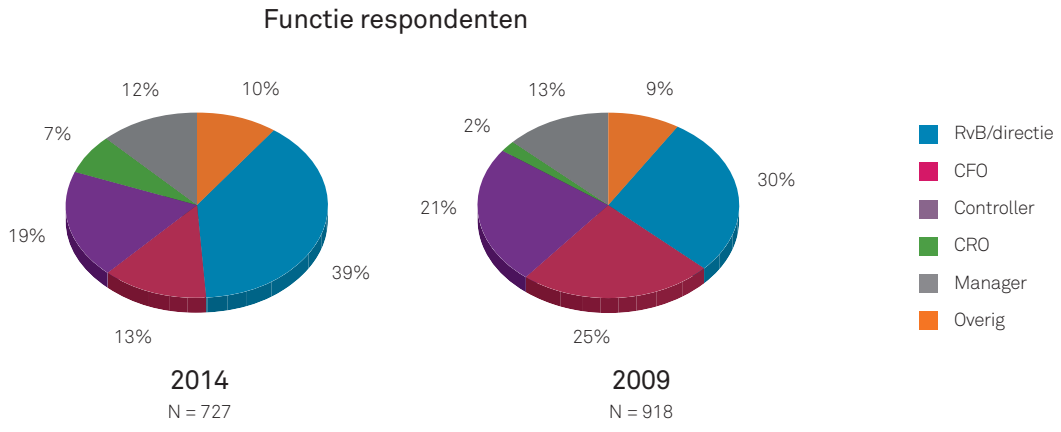
U leest hieronder de feiten en getallen, vergelijkingen, analyses en observaties op basis waarvan wij in hoofdstuk 3 tot ons oordeel en onze aanbevelingen zijn gekomen. De onderzoeksopzet, methodologie en kwaliteit van de verkregen en gebruikte data kunt u terugvinden in Bijlage 1.

De survey is in april 2014 uitgestuurd naar organisaties waarvan de adressen zijn verkregen uit het databestand van 'Company Info'. In totaal zijn er 9.582 surveys verstuurd naar organisaties met een budget of omzet groter dan 10 miljoen euro, waarvan er 20 retour zijn gekomen vanwege faillissement of foute adressering. Dit heeft uiteindelijk geleid tot 727 bruikbare surveys. De respons van 7,6 procent is vrij hoog voor een dergelijke survey.

Wij kunnen nu de vergelijking met 2009 gaan maken omdat de vragen van onze survey bijna integraal hetzelfde zijn als die uit ons onderzoek van toen (de verschillen vindt u in Bijlage 1). Hoe staan we er voor vijf jaar na het uitbreken van de crisis? Wat zijn we opgeschoten?

4.2 Profiel van de respondenten

Figuur 2: Verschuivingen in functie van respondenten 2014 - 2009



De meerderheid van de respondenten (52 procent tegen 55 in 2009) zijn directieleden. We hebben cfo's - zoals gebruikelijk - gerekend tot de categorie directieleden. Belangrijk, omdat risicomanagement uiteindelijk een verantwoordelijkheid is van de directie. Dit hebben we niet gedaan voor de CRO-functie, want het is (nog) geen gemeengoed dat de CRO altijd onderdeel is van de directie. De resultaten opgenomen in Figuur 7 ondersteunen vooralsnog die keuze (de helft van de CRO's is onderdeel van de directie).

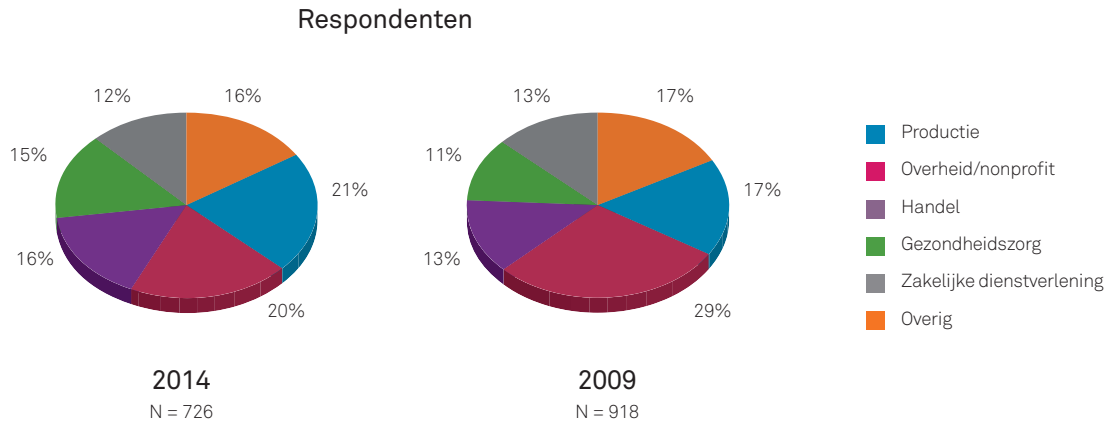
Van de respondenten zit 32 procent in een financiële functie (cfo en controller). Dit is een belangrijke kentering ten opzichte van 2009, waar sprake was van 46 procent, maar wel in lijn met de algemene gedachtegang dat risicomanagement vaak wordt gestuurd door de financiële functie. De verdeling van 2014 is op drie punten anders dan in 2009:

1. het belang van risicomanagement op RvB/directieniveau (bijna +10 procent);
2. de rol en het belang van de CRO (bijna +5 procent);
3. een verschuiving van de financiële/ondersteunende functie naar meer business functies.

Verdeling respondenten naar sector

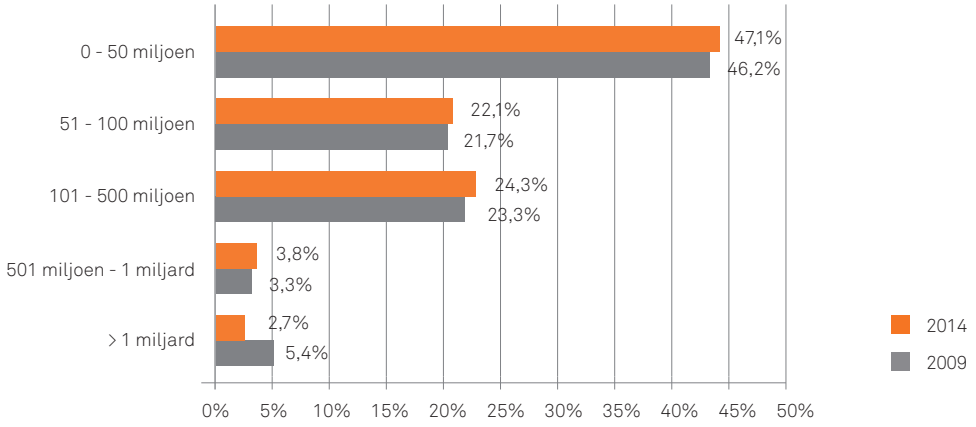
In totaal opereert 35 procent (2009: 40 procent) van de organisaties in de gezondheidszorg en de non-profitsector. Om een betere vergelijking te kunnen maken tussen profit en non-profit, hebben we gezondheidszorg ook onder non-profit geschaard. Wat opvalt is dat de categorie 'Overig' bestaande uit transport & logistiek, telecommunicatie, informatietechnologie en entertainment en energie & utilities een stevige terugval kent in aantal participanten. Wel zijn de aantallen nog steeds representatief om voor elke sector conclusies te kunnen trekken.

Figuur 3: Respondenten naar sector 2014 - 2009

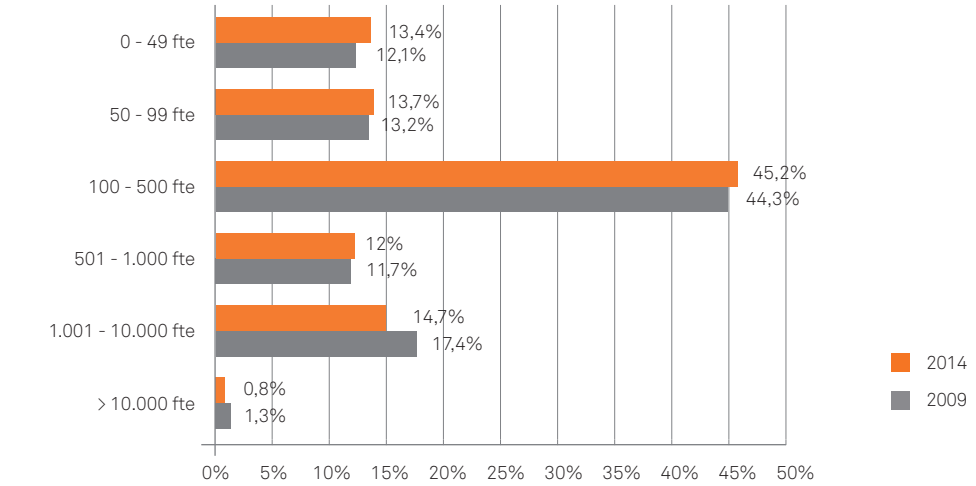


Figuur 4 en 5 geven een overzicht van de grootte van de organisaties in omzet of budget en full time equivalent (fte). Het enige verschil met vijf jaar geleden is dat dit jaar de grotere organisaties (omzet/budget > 1 miljard) minder geparticipeerd hebben.

Figuur 4: Respondenten naar omzetgroepen



Figuur 5: Respondenten naar FTE groepen



Karakteristieken van respondenten

In de aandeleneigendomsstructuren van de respondenten blijkt iets eigenaardigs: meer dan de helft van de organisaties is geen eigendom van één van de categorieën die we uitvroegen. Dit zijn in ieder geval vrijwel alle non-profitorganisaties (35 procent) en een aantal andere organisaties uit andere sectoren. Verder is 8 procent (2009: 9 procent) van de respondenten beursgenoteerd en is 29 procent (2009: 65 procent) actief in meer dan drie landen. Het verschil qua internationalisatie is opmerkelijk. Hiervoor is geen duidelijke verklaring.

Figuur 6: Eigendomsstructuur

Eigendom	Profit (N=475)	Non-profit (N=251)	2014 (in %)	2009 (in %)
Niet van toepassing	30,0	92,9	51,4	46,2
Anonieme aandeelhouder	6,2	-	4,1	4,5
Aantal institutionele beleggers	3,4	-	2,3	11,3
Eén of meerdere families	19,3	2,1	13,5	14,4
Administratiekantoor	2,4	-	1,6	2,5
(Directeur) grootaandeelhouder	18,7	2,9	13,3	15,4
Dochter van moedermaatschappij	7,3	-	4,8	5,7
Banken	0,9	0,4	0,7	-
Anders	11,8	1,7	8,4	-
Totaal	**100**	**100**	**100**	**100**

Chief Risk Officer

Uit het onderzoek komt naar voren dat 58,2 procent van de beursgenoteerde ondernemingen een CRO of een vergelijkbare functie hebben aangesteld. Gezien de grote aandacht voor risicomanagement en voor 'in control' zijn de afgelopen tien jaar, ondersteund door corporate-governance-codes , is dit in onze ogen een relatief laag percentage, dat niet overeenkomt met het beeld dat wij uit de praktijk kennen.

Figuur 7: Wel of geen Chief Risk Officer (CRO)

Opmerkelijk is dat 35,5 procent van de respondenten een CRO of een vergelijkbare functie heeft aangesteld die eindverantwoordelijk is voor het risicomanagement; in 2009 was dit nog maar 18,7 procent. Blijkbaar wordt binnen risicomanagement in toenemende mate belang gehecht aan een betrokken functionaris en is een dergelijke functie, in ieder geval in naam, hoger in de organisatie gepositioneerd.

De cijfers bevestigen verder dat het in de financiële dienstverlening relatief gemeengoed is een CRO of gelijkwaardige functie te hebben: twee derde van alle organisaties heeft er een. Opvallend zijn ook de resultaten bij transport & logistiek en zakelijke dienstverlening, waarbij bijna de helft

van alle respondenten in die sector een CRO of vergelijkbare functie heeft. Hieronder ziet u verder dat de omvang van een organisatie naar omzet/budget sterk bepalend is voor het hebben van een CRO of vergelijkbare functie. En ook opvallend: bijna een derde van de kleinste organisaties is al zo ver dat zij een CRO of vergelijkbare functie hebben aangesteld.

Figuur 8: CRO naar sector (in percentages)

Aanstelling CRO naar sector	Wel CRO of vergelijkbare functie
Handel	33,1
Transport & logistiek	48,0
Productie	27,5
Financiële dienstverlening	68,4
Zakelijke dienstverlening	44,4
Telecommunicatie, informatietechnologie en entertainment	27,8
Energie & utilities	27,8
Gezondheidszorg	33,6
Overheid/Non-profit	27,8

Figuur 9: CRO naar omzet/budget (in percentages)

Aanstelling CRO naar omzet	Wel CRO of vergelijkbare functie
0 - 50 miljoen	32,5
51 - 100 miljoen	26,8
101 - 500 miljoen	40,5
501 miljoen - 1 miljard	55,6
> 1 miljard	68,4

Naar sector uitgesplitst levert dit het volgende beeld op:

Figuur 10: Aanstelling CRO of anders, per sector (in percentages)

Aanstelling CRO naar sector	CRO op RVB/Directie Niveau	CRO niet op RVB/Directie niveau	Geen CRO, vergelijkbare functie	Geen CRO geen vergelijk-bare functie
Handel	3,4	14,5	15	66,7
Transport & logistiek	8,0	20,0	20,0	52,0
Productie	10,1	4,1	17,6	68,2
Financiële dienstverlening	42,1	7,0	21,1	29,8
Zakelijke dienstverlening	11,2	10,1	15,7	62,9
Telecommunicatie, informatietechnologie en entertainment	11,1	11,1	5,6	72,2
Energie & utilities	5,9	11,8	11,8	70,6
Gezondheidszorg	7,5	9,3	16,8	66,4
Overheid/Non-profit	6,9	8,3	12,5	72,2

Figuur 11: Aanstelling CRO of anders, naar omzet/budget (in percentages)

Aanstelling CRO naar omzet/budget	CRO op RVB/Directie Niveau	CRO niet op RVB/Directie niveau	Geen CRO, vergelijkbare functie	Geen CRO, geen vergelijk-bare functie
0 - 50 miljoen	11,4	7,8	13,5	67,3
51 - 100 miljoen	3,2	9,0	14,7	73,1
101 - 500 miljoen	10,4	8,7	21,4	59,6
501 miljoen - 1 miljard	18,5	14,8	22,2	44,5
> 1 miljard	36,8	21,1	10,5	31,6

Extra toezichthoudende functie

Naast de Chief Risk Officer blijken met name de externe governance mechanismen zoals de rol van de externe toezichthouder, alsmede de Big4 accountant belangrijke drivers voor een volwassener risicomanagementsysteem. Toezichthouders, zoals de DNB, benadrukken in hun toezicht het belang van risicomanagement en geven risicomanagement daarmee een kwaliteitsimpuls. Maar ook Big4 accountants en accountants die de organisatie, na een accountantswissel, met frisse ogen bekijken dragen bij aan een volwassener risicomanagement. De discussie maakt uw risicomanagement rijker en zorgt klaarblijkelijk voor de door ons gepropagandeerde 'constructive descent', het kritische tegengeluid.

42,2 procent van de respondenten heeft te maken met een externe toezichthouder, bijvoorbeeld AFM, DNB of ACM. 72,1 procent heeft een Raad van Commissarissen/Raad van Toezicht en 49,5 procent (2009: 47,8 procent) heeft een Auditcommissie en/of Risicocommissie geïnstalleerd. Ruim 76,2 procent van de organisaties (2009: 77,1 procent) wordt tot slot door een Big4-accountantsorganisatie gecontroleerd. In de afgelopen 3 jaar heeft 24,4 procent van de onderzochte organisaties een nieuwe externe accountantsorganisatie aangesteld.

Hogere zelfscore versus onze lagere score

Gemiddeld scoren alle respondenten hun risicomanagement in de eigen organisatie flink veel hoger dan de score die uit de survey rolt volgens onze scoreleidraad (zie bijlage 2). De non-profitsector scoort in beide gevallen relatief laag, de gezondheidszorg bevindt zich daar net boven.

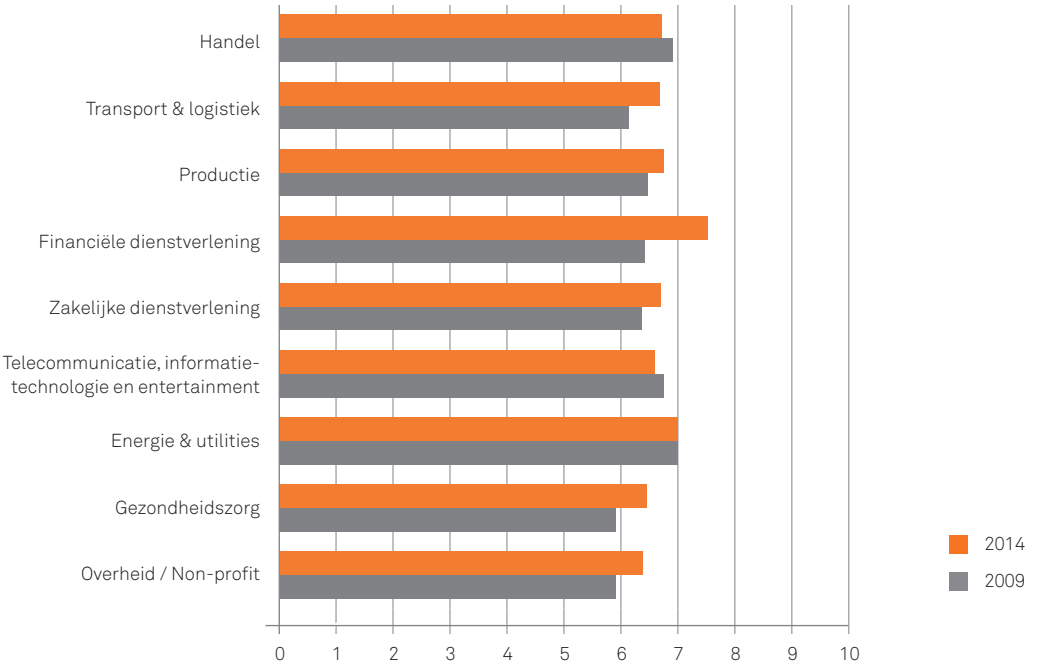
Figuur 12: Verschil tussen zelfevaluatie en survey-score per sector

Sector	Aantal	Gemiddelde rapportcijfer (zelfevaluatie)	Gemiddelde survey-score	Verschil
Handel	117	6,86	4,27	2,59
Transport & logistiek	25	6,76	4,70	2,06
Productie	147	6,90	4,21	2,69
Financiële dienstverlening	55	7,55	6,26	1,29
Zakelijke dienstverlening	89	6,82	4,65	2,17
Telecommunicatie, informatietechnologie en entertainment	18	6,67	4,03	2,64
Energie & utilities	18	7,11	5,24	1,87
Gezondheidszorg	107	6,75	4,61	2,14
Overheid/Non-profit	144	6,59	4,53	2,06
Totaal	**720**	**6,85**	**4,60**	**2,25**

Vergelijken we de resultaten uit 2009 met die van 2014 (zie figuur 13 en 14) dan is een positieve tendens waar te nemen. Zowel de non-profitsector als de gezondheidssector laat een significante stijging zien volgens eigen zeggen en beide zijn ingelopen op de profit-sector. Het verschil is nu miniem, behalve bij financiële dienstverlening en energie & utilities. Met uitzondering van telecommunicatie, informatietechnologie en entertainment en handel (alleen eigen rapportcijfer) zijn alle sectoren erop vooruit gegaan in hun risicomanagement, in de eigen score én in de surveyscore.

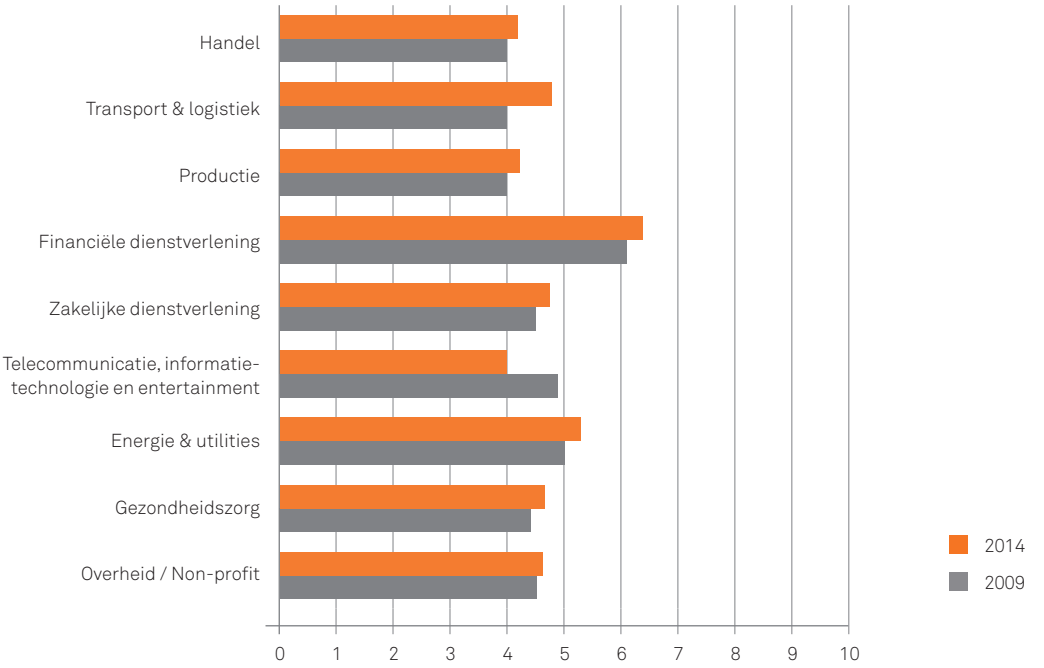
De achteruitgang van telecommunicatie, informatietechnologie en entertainment volgens eigen zeggen wordt zelfs versterkt door onze surveyscore. De financiële dienstverlening lijkt verder geïnvesteerd te hebben in risicomanagement gezien de relatief forste stijging ten opzichte van 2009.

Figuur 13: Vergelijking rapportcijfers (zelfevaluatie) 2014 versus 2009



Gebaseerd op onze scoreleidraad scoort financiële dienstverlening het hoogst en telecommunicatie, informatietechnologie en entertainment het laagst. Het grootste beoordelingsverschil tussen het eigen cijfer en onze score treffen we bij productie aan, terwijl de kleinste verschillen in de financiële dienstverlening en transport & logistiek zitten. De non-profitsector scoort niet significant lager ten opzichte van de andere sectoren, alleen nog wel lager dan de financiële dienstverlening en energie & utilities.

Figuur 14: Vergelijking surveyscore (volgens scoreleidraad) 2014 versus 2009



De scores uit onze survey hebben we ook gesplitst naar omzet en naar omvang. Dan is goed te zien dat hoe groter de organisatie is, in omzet/budget of in aantal fte, des te hoger de score op risicomanagement. Er is één uitzondering op die regel, en dat is de kleinste categorie, met een score van 4,52 (2009: 4,42). Zij scoren hoger dan de volgende twee categorieën.

Figuur 15a: Surveyscore naar omzet

Omzetgroep in €	2014		2009	
	Aantal	Gemiddeld	Aantal	Gemiddeld
0 - 50 miljoen	335	4,22	418	4,16
51 - 100 miljoen	157	4,48	198	4,22
101 - 500 miljoen	173	4,99	215	4,81
501 miljoen - 1 miljard	27	5,48	29	6,09
> 1 miljard	19	6,73	50	6,92
Totaal	**711**	**4,60**	**910**	**4,54**

Figuur 15b: Surveyscore naar omvang

Fte-groep	2014		2009	
	Aantal	Gemiddeld	Aantal	Gemiddeld
0 - 49 fte	96	4,52	110	4,42
50 - 99 fte	98	4,26	120	4,15
100 - 500 fte	323	4,36	404	4,22
501 - 1.000 fte	86	4,79	107	4,75
1.001 - 10.000 fte	103	5,42	159	5,37
> 10.000 fte	6	6,72	12	7,06
Totaal	**714**	**4,60**	**912**	**4,54**

Samenhang tussen eigen scores en surveyscores?

We hebben gekeken of er een significante samenhang bestaat tussen onze scores en de eigen scores van de respondenten en die blijkt er te zijn. Dit betekent dat als respondenten zichzelf hoger beoordelen, wij ook uitkomen op een hogere (survey-) score. Deze samenhang wordt bewezen in 25 procent van de gevallen. Hoewel dat percentage misschien laag lijkt, is dat toch respectabel voor een dergelijk onderzoek. Uit dezelfde vergelijking met het volwassenheidsmodel (zie hieronder) blijkt minder sterke samenhang. Hier komt bijna 19 procent van de rapportcijfers die respondenten zichzelf geven en de mate van volwassenheid die zij zichzelf op basis van de vijf stadia van Beasley

geven overeen. Hieruit concluderen we dat het rapportcijfer van de respondenten niet afhankelijk is van het stadium van volwassenheid van hun risicomanagement. De samenhang tussen eigen rapportcijfer en de surveyscore op basis van onze scoreleidraad bevestigt dat respondenten hun cijfer minder baseren op de harde aspecten van hun risicomanagement dan wij hebben gedaan.

De voordelen van risicomanagement die respondenten zelf zien

Een nieuwe vraag in ons onderzoek van 2014 was om expliciet de voordelen voor een organisatie van een risicomanagementsysteem in kaart te brengen volgens de beleving van de respondenten. De meer generieke, kwalitatieve kenmerken als minder verrassingen, meer vertrouwen in doelrealisatie en betere reputatie springen er positief uit. De meer kwantitatieve voordelen, met een directe impact op de balans of winst- en verliesrekening, zoals lagere vermogenskosten, minder boetes, hogere marge, hogere omzet en/of meer marktaandeel, scoren juist laag. Dit is jammer voor de kwantitatieve onderbouwing van de business case voor risicomanagement, maar bevestigt wel dat er nog beperkt onderzoek is gedaan naar goed risicomanagement en de direct financiële bijdrage aan het succes van de organisatie.

Figuur 16: Voordelen van risicomanagement

Voordelen	Gemiddelde Score (schaal 1-5)	Standaard Deviatie
Minder verrassingen	3,6	0,88
Meer vertrouwen in het realiseren van de begroting/doelstellingen	3,5	0,86
Minder afwijkingen t.o.v. de begroting/planning	3,2	0,88
Lagere vermogenskosten	2,5	1,06
Betrouwbaarder geschatte voorzieningen	3,1	1,02
Minder klachten van klanten/medewerkers	2,9	1,04
Minder en kleinere bedrijfsincidenten	3,0	1,07
Minder claims en rechtszaken	2,9	1,11
Minder aanwijzingen en/of minder boetes van toezichthouders	2,7	1,21
Minder negatieve media aandacht	2,9	1,16
Hogere klantentevredenheid	3,1	1,02
Hogere medewerkerstevredenheid	2,9	0,98
Hogere marge	2,6	1,03
Hogere omzet/ winstgevendheid	2,6	1,04
Betere reputatie	3,4	0,98
Meer groei/marktaandeel	2,5	1,02

(Kwantitatieve voordelen zijn oranje)

Op basis van de waardering van het risicomanagementsysteem en de behaalde voordelen gebaseerd op eigen oordeel van de respondenten, hebben wij onderzocht of het risicomanagementsysteem invloed heeft op de ondernemingsprestaties. Uit ons empirisch onderzoek is naar voren gekomen dat de organisaties risicomanagement niet zien als een zinvol instrument voor het beheersen van groei. Het gebruik van risicomanagement leidt volgens gebruikers tot verlaging van kapitaalkosten en draagt bij aan de reputatie.

Risicovolwassenheid

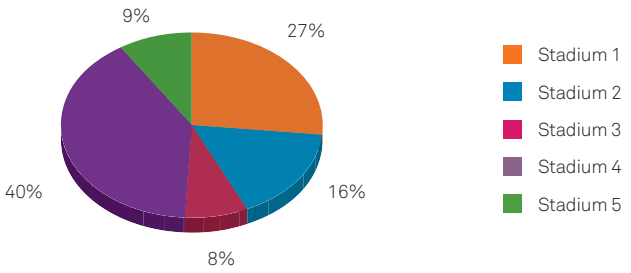
We vroegen ook aan de respondenten hun eigen organisatie in te delen aan de hand van een risicovolwassenheidsmodel. Die antwoorden zijn minder goed te vergelijken met de antwoorden uit 2009. Dat komt doordat we bij de definiëring van de stadia aansluiten bij de recente literatuur. Vijf jaar geleden definieerden wij de stadia iets ruimer.[7]

Het model gebruikt vijf stadia van ontwikkeling (zie vraag 35 in de vragenlijst, bijlage 3). Hoe hoger het getal hoe volwassener risicomanagement:

- **Stadium 1:** er bestaan op dit moment geen plannen om een risicomanagementsysteem in te voeren;
- **Stadium 2:** wij onderzoeken de mogelijkheid om een risicomanagementsysteem in te voeren, maar hebben nog geen definitieve beslissing genomen;
- **Stadium 3:** wij plannen nu de implementatie van een risicomanagementsysteem;
- **Stadium 4:** op dit moment is een risicomanagementsysteem gedeeltelijk aanwezig en geïmplementeerd;
- **Stadium 5:** een volledig risicomanagementsysteem is aanwezig en geïmplementeerd;

Gegeven hun eigen volwassenheidsscore voelen organisaties zich blijkbaar vrij zeker over hun risicomanagement. Bijna 49 procent kwam uit op het volwassenheidsstadium 4 of 5, en als we ook stadium 3 meetellen als 'voldoende', stijgt het percentage dat zichzelf een voldoende geeft tot 57. Bijna de helft van de respondenten (43 procent) heeft geen risicomanagementsysteem, heeft geen plannen daartoe of onderzoekt slechts de wenselijkheid van zo'n systeem. De andere helft (49 procent) heeft een gedeeltelijk risicomanagementsysteem geïmplementeerd. Slechts 8 procent heeft concrete plannen voor invoering van een systeem. De keuze voor wel of geen risicomanagementsysteem lijkt anno 2014 gemaakt te zijn.

Figuur 17: Risicovolwassenheidsmodel



7 Dit type 'maturity'-model is eerder toegepast in studies van Beasley e.a. (2005) en Ward (2003). In 2009 zijn de stadia van volwassenheid ruimer gedefinieerd dan die volgens Beasley et al. Op die manier wordt er meer ruimte gelaten voor interpretabele vraagstelling waarbij het onderscheid tussen stadia iets diffuser is dan de oorspronkelijke stadia-indeling van Beasley et al. Hoewel dit uiteindelijk niet heeft geleid tot verwarring bij de respondenten gezien de wijze waarop ze deze vraag hebben beantwoord, zijn de stadia in 2014 geherformuleerd om weer dichter bij de oorspronkelijke basisindeling van Beasley et al te komen. Daarom zijn de resultaten van 2014 niet of zeer beperkt vergelijkbaar met die uit 2009.

Zoomen we in op de sectoren, dan blijkt de spreiding relatief groot te zijn in de gezondheidszorg, overheid/non-profit en productie.

Figuur 18: Volwassenheidsstadia per sector

Volwassenheidsscore								
Sector	**1**	**2**	**3**	**4**	**5**	**Aantal**	**Gemiddeld**	**Mediaan**
Energie en utilities	3	3	1	7	2	16	3,1	4
Financiële dienstverlening	4	3	2	27	17	53	3,9	4
Gezondheidszorg	18	19	13	47	6	103	3,0	4
Handel	32	17	6	53	5	113	2,8	4
Overheid/non-profit	40	19	14	52	9	134	2,8	3
Productie	46	28	9	47	10	140	2,6	2
Telecom, IT enz.	7	7	1	2	1	18	2,1	2
Transport & logistiek	8	3	1	9	2	23	2,7	3
Zakelijke dienstverlening	25	16	7	31	5	84	2,7	3
Totaal	**183**	**115**	**54**	**275**	**57**	**684**	**2,9**	**3**
Procentueel	**27%**	**16%**	**8%**	**40%**	**9%**	**100,0%**		

Ook hier treffen we de bevestiging aan van eerdere rapportcijfers: de hoge score voor financiële dienstverlening en voor energie & utilities. Ook de lagere rapportcijfers worden bevestigd: zie telecommunicatie, informatietechnologie en entertainment. Handel, productie en overheid vormen het grootste deel, zo'n 60 procent, van stadium 1 organisaties. Overheid en gezondheidszorg verkeren nog het meest in het derde stadium, de planningsfase.

Er is een significant verband tussen de surveyscore en de volwassenheidsscore op basis van de vijf stadia van Beasley, een mooie indicatie dat onze scoreleidraad een goede maatstaf is om de volwassenheid te meten van het risicomanagementsysteem.

4.3 Risico-inventarisatie en -analyse

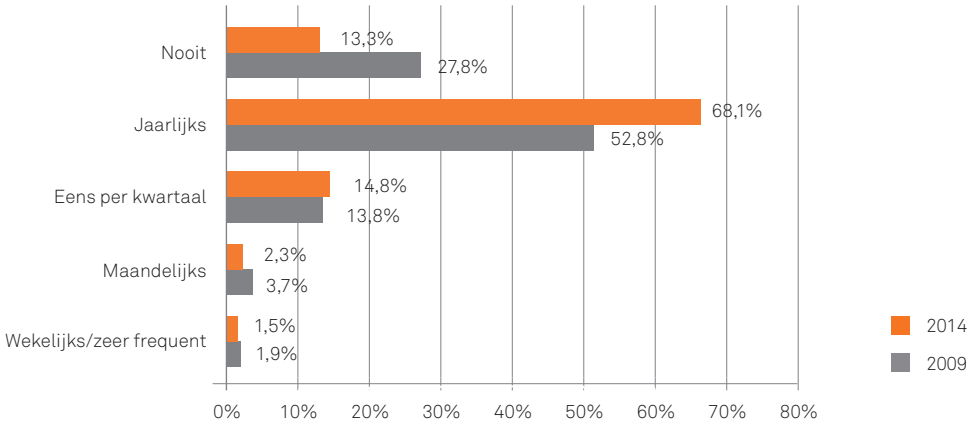
Hoe vaak wordt in de organisatie een integrale en bedrijfsbrede risico- inventarisatie en -analyse uitgevoerd?

Risicomanagement staat of valt met een helder en gemeenschappelijk beeld van de relevante risico's voor de organisatie, hun karakteristieken en hun prioriteiten. Een risicoanalyse biedt precies dat. Het spreekt voor zich dat in een snel veranderende omgeving organisaties hun risicoprofiel regelmatig toetsen op actualiteit en relevantie en eventueel bijstellen om tijdig en effectief te kunnen inspelen op veranderingen.

Het is daarom des te opvallender dat 68,1 procent (2009: 52,8 procent) van de respondenten niet meer dan eenmaal per jaar een dergelijke analyse uitvoert en toch nog 13,3 procent (2009: 27,8 procent) helemaal géén inventarisatie en analyse uitvoert. Het voert te ver om te zeggen dat er helemaal niet aan risicomanagement wordt gedaan in deze organisaties, maar het doet wel vraagtekens rijzen. Het is positief dat we wel een verbetering kunnen vaststellen ten opzichte van 2009: het gebeurt nu tenminste in ieder geval eenmaal per jaar.

Managers geven vaak aan dat het managen van risico's hun dagelijkse werk is. Dit gebeurt vaak impliciet. Is dat toereikend? Het sluit aan bij het beeld dat we hebben vanuit de praktijk: als men aan risico-inventarisatie en -analyse doet, is dat vrij instrumenteel, vaak eenmaal per jaar, vlak voor of na het begin van een nieuw planjaar.

Figuur 19: Frequentie van risico-inventarisatie en -analyse



Profit- en non-profitorganisaties blijken ongeveer evenveel tijd en energie te steken in de analyse van risico's en ook per sector is geen groot verschil te zien. Hoewel dat op zichzelf acceptabel lijkt, is het wel opvallend. We verwachtten immers dat in sterk gereguleerde sectoren als financiële dienstverlening risicomanagement meer gemeengoed zou zijn en dat er dus vaker een dergelijke analyse wordt uitgevoerd. Ook van profit-ondernemingen zou mogen worden verwacht dat vanwege de competitieve omgeving zij vaker een analyse uitvoeren dan in de non-profitsector.

Een andere veronderstelling hebben we wel kunnen bevestigen. We verwachtten dat de grootte van de organisatie invloed heeft op het institutionele karakter van risicomanagement en daarmee ook de frequentie van risicoanalyses. En inderdaad: alle organisaties met een omzet/budget groter dan € 1 miljard blijken inderdaad significant vaker een risico-inventarisatie uit te voeren.

Wanneer wordt de risico-inventarisatie en -analyse uitgevoerd?

Wij vinden het belangrijk dat organisaties regelmatig risico's inventariseren in relatie met de strategie en doelen van die organisatie en dat risicomanagementactiviteiten zoveel mogelijk geïntegreerd worden met bestaande managementactiviteiten. Je zou daarom verwachten dat een risico-inventarisatie of -analyse ten minste is opgenomen in de Planning & Control (P&C) cyclus. Het logische ritme en karakter van die cyclus combineert immers goed met een gedegen risico-inventarisatie en -analyse.

Uit de resultaten blijkt dat in 78,4 procent (2009: 60,1 procent) van de gevallen de P&C-cyclus

wordt gebruikt om de risico-inventarisatie en -analyse uit te voeren, daar waar je tegen de 100 procent zou verwachten. Het valt ons op dat non-profitorganisaties dit meer doen dan profitorganisaties (87,6 versus 73,7 procent). Deze percentages zijn hoger ten opzichte van het onderzoek uit 2009, waarbij de significante stijging in de non-profit eruit springt. In 2009 bleek dat slechts circa 60 procent van de geënquêteerden het proces van risicomanagement in de P&C-cyclus incorporeert.

Figuur 20: Moment van risico-inventarisatie en -analyse (in %)

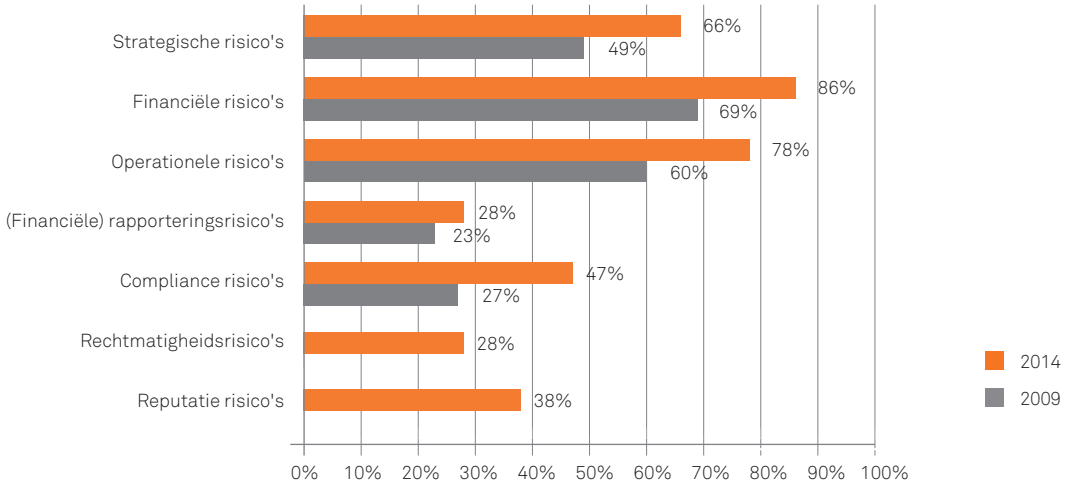
Wanneer?	2014			2009		
	Gemiddeld	Profit (N=475)	Non-profit (N=251)	Gemiddeld	Profit (N=548)	Non-profit (N=368)
Planning & Control cyclus	78,4	73,7	87,6	60,1	56,9	65,5
Acquisities/ (des)investeringen	20,1	23,8	13,1	15,9	19,9	10,3
Belangrijke projecten/ ontwikkelingen	33,3	33,9	32,3	24,3	24,3	24,7
Strategische beslissingen	30,9	31,6	29,9	22,5	27,0	16,0
Belangrijke incidenten	16,1	15,6	17,1	11,7	13,1	9,8

Maar omdat risico's zich doorgaans niet laten dicteren door het ritme van de cyclus, is het ook wenselijk bij belangrijke veranderingen, intern en extern, het risicoprofiel weer te evalueren. De survey laat alleen zien dat organisaties die wens niet vertalen in concrete actie. De hoogste score op deze vraag is 31,6 procent voor de profitsector. Dit vinden wij een erg laag percentage. Immers, strategische beslissingen zijn van groot belang voor elke organisatie en een risico-inventarisatie zou daar op zijn plaats zijn. In alle andere gevallen houdt men een vergelijkbaar niveau van risicoanalyse aan of zelfs nog minder: dat is verontrustend te noemen.

Gelukkig lijkt er wel sprake van een positieve tendens, omdat in ieder geval op alle genoemde momenten er sprake is van een stijging ten opzichte van 2009. Een paar zaken vallen daarbij op: in de non-profitsector is nu bijna twee keer zo vaak een risicoanalyse gedaan bij strategische beslissingen (van 16,0 naar 29,9 procent). Dit geldt evenzo voor belangrijke incidenten (van 9,8 procent naar 17,1 procent). Mogelijke verklaringen zijn: de terugtrekkende overheid, de druk op budgetten, verschuiving van taken en budgetten naar lagere overheden, het grote aantal incidenten en kwetsbaarheid van de samenleving en daardoor steeds scherper aan de wind moeten varen. Ruimte om verrassingen op te vangen is er steeds minder.

Welke risico's worden in kaart gebracht?

Figuur 21: Risico's in kaart gebracht 2014 - 2009



In het beste geval neemt u in uw risicoanalyses alle mogelijke risico's mee. Een primaire focus op (financiële) rapporteringsrisico's lijkt daarbij logisch, gezien de aandacht hiervoor van met name corporate governance-regelgeving . Maar uit onderzoek[8] blijkt dat juist operationele risico's en meer nog strategische risico's uiteindelijk de grootste bedreigingen vormen en ook de grootste consequenties met zich meebrengen. Positief is dat alle risico's vaker in kaart gebracht worden dan in 2009, vooral strategische, operationele en financiële risico's. Waar in 2009 nog relatief laag werd gescoord op compliance risico's, worden die nu bijna dubbel zo vaak in kaart gebracht. Dit past in de herkenbare trend van het toenemen van wet- en regelgeving en de afnemende tolerantie van het maatschappelijk verkeer voor slecht risicomanagement. Wij constateren verder dat financiële rapporteringsrisico's en rechtmatigheidsrisico's laag scoren. Hieronder ziet u een overzicht van alle in kaart gebrachte risico's, verdeeld naar profit en non-profit, vergeleken tussen 2014 en 2009.

Figuur 22: In kaart gebrachte risico's[9] profit - non-profit (in percentages)

Risico	2014			2009		
	Gemiddeld	Profit (N=475)	Non-profit (N=251)	Gemiddeld	Profit (N=548)	Non-profit (N=368)
Strategische risico's	66,2	64,8	68,9	49,4	49,8	49,2
Financiële risico's	86,4	85,1	89,2	69,1	67,6	71,5
Operationele risico's	77,6	79,2	74,9	59,9	62,7	56,5
(Financiële) rapporteringrisico's	27,9	30,9	22,3	23,2	26,1	15,9
Rechtmatigheidsrisico's	27,5	21,7	38,6	-	-	-
Compliance risico's	47,0	50,9	39,8	26,8	29,2	20,5
Reputatie risico's	38,0	34,3	45,0	-	-	-

8 PricewaterhouseCoopers Advisory, Internal Audit, "An opportunity for transformation", 2008
9 De indeling is aangepast ten opzichte van 2009, rechtmatigheidsrisico's en reputatierisico's zijn toegevoegd

De non-profitsector inventariseert en analyseert meer dan de profitsector hun strategische-, financiële risico's en reputatierisico's. Gezien het publieke en maatschappelijke karakter is dit wel te verklaren. De hogere score op financiële risico's is mogelijk te verklaren uit de druk op budgetten, minder ruimte voor tegenvallers, terugtrekkende overheid en verschuiving van kerntaken naar lagere overheden. In die zin zou je echter ook verwachten dat operationele risico's (kwaliteit, geen ruimte voor fouten, in 1 keer goed, etc.) een grotere rol zou spelen bij profit-organisaties. Dit wordt niet bevestigd door de uitkomsten van ons onderzoek. De lagere score op compliance voor non-profit is wellicht te verklaren doordat de non-profit-respondenten geen duidelijk verschil zien tussen 'compliance-risico's' en 'rechtmatigheidsrisico's'. Tot slot is het interessant om te zien dat ook in profit die rechtmatigheidsrisico's een rol spelen. Dat risico scoort met 21,7 procent namelijk onverwacht hoog en dat zou alleen maar te verklaren kunnen zijn door mogelijke inbreng van commercieel georiënteerde semi-overheidsorganisaties.

Het integrale karakter van risico's - of het gebrek daaraan - blijkt vooral uit figuur 23. Hierin wordt zichtbaar hoeveel verschillende typen risico's respondenten meenemen. We maken daarbij een onderscheid tussen profit en non-profit. Alle zeven typen risico's worden in profitorganisaties maar in 20,8 procent van de gevallen in ogenschouw genomen (2009: 16,5 procent). Non-profit-organisaties doen dit zelfs iets meer, namelijk in 21,9 procent van de gevallen.

Een paar zaken vallen op vergeleken met 2009. Meer respondenten brengen risico's integraal in kaart, vooral voor non-profit is de stijging fors: van 7,9 procent voor maximaal 5 naar 21,9 procent voor 7 risico's. Hiermee loopt non-profit inmiddels voor op profit, wat past in het eerdere beeld van meer aandacht voor en stijging van kwaliteit van risicomanagement binnen de overheid/non-profit organisaties.

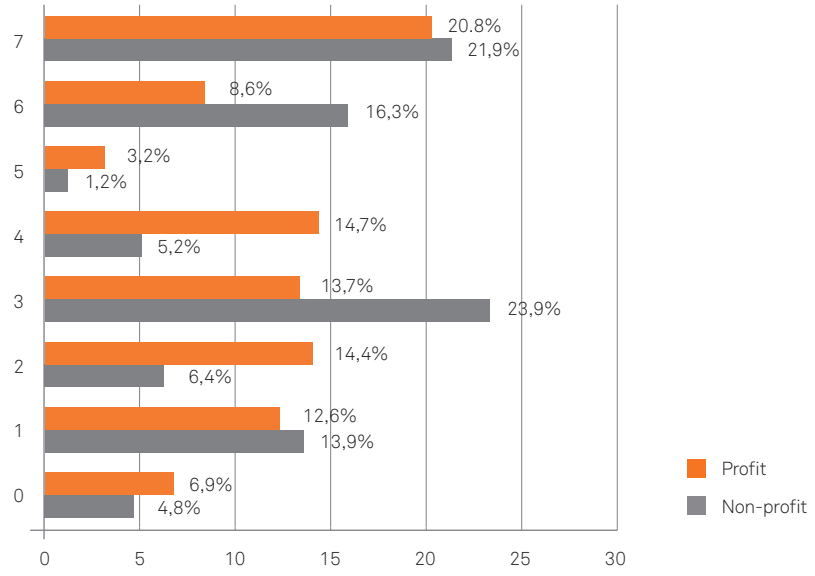
Hetzelfde beeld - maar extremer - is zichtbaar bij '6 risico's in kaart brengen' (versus 4 in 2009) typen risico's. Hier is het grote verschil tussen profit en non-profit echt opvallend, maar moeilijk te verklaren.

Dit geldt evenzo voor '3 typen risico's in kaart brengen', wat het hoogst scoort in non-profit en daarmee samen met '7 typen' gemeengoed lijkt te zijn in bijna 45 procent van de gevallen. Daarentegen is het beeld voor '4 typen risico's' precies tegengesteld.

De spreiding in aantal typen is voor non-profit relatief groot, terwijl voor profit het aantal typen risicocategorieën zich evenredig lijkt te concentreren op 1 t/m 4 met een uitschieter naar integraal (is 7).

Bijna verheugend is dat nog slechts 6,9 procent (profit) versus 4,8 procent (non-profit) van de ondervraagden geen enkele risicocategorie in overweging neemt, waarbij het opmerkelijk is dat die voor profit groter is dan voor non-profit. Dat strookt uiteraard met de 13,3 procent die niet aan risico-inventarisatie doet (zie figuur 19).

Figuur 23: Aantal typen risico's in kaart gebracht



Uit hoeveel managementlagen bestaat uw organisatie en op welke managementniveaus worden de risico's in kaart gebracht?

Het aantal managementniveaus dat betrokken is bij risico-inventarisatie en -analyse representeert het bedrijfsbrede karakter van risicomanagement. In het ideale geval zijn zelfs alle lagen van de organisatie betrokken bij het opstellen van een risico-inventarisatie en -analyse. Zo bezien zijn de resultaten op het eerste gezicht niet hoopvol: in 75 procent van de gevallen is slechts de RvB/Directie/1e managementniveau betrokken. De resultaten van 2014 en 2009 zijn niet 1 op 1 met elkaar te vergelijken (zie tekst onder figuur 24), maar wat opvalt is dat er in 2014 een tendens lijkt ingezet om de inventarisatie op een hoger en beperkt aantal niveaus te doen.

Figuur 24: Risico-inventarisatie managementniveau

	2014	2009*
Risico-inventarisatie managementniveau	Percentage	Percentage
Uitsluitend Raad van Bestuur/Directie	20,6	54,5
Raad van Bestuur/Directie en 1e managementniveau	54,5	41,0
Raad van Bestuur/Directie en 1e en 2e managementniveau	19,3	23,2
Raad van Bestuur/Directie en 1e, 2e en 3e managementniveau	3,7	14,0
Raad van Bestuur/Directie en meer dan drie managementniveaus	1,8	2,3

* De vraagstelling in 2009 was anders door per managementlaag de participatie te vragen; hierdoor waren er meerdere antwoorden mogelijk en de antwoorden niet elkaar uitsluitend. Dit verklaart ook een totaal van meer dan 100%

Het voorgaande vergt wel enige nuance en moet afgezet worden tegen het aantal managementlagen dat aanwezig is in de organisatie. Als er een groot verschil is tussen het aantal aanwezige lagen en de lagen waarop de inventarisatie wordt uitgevoerd , dan is het voorgaande in onze ogen

echt verontrustend. Figuur 25 geeft hierover uitsluitsel en bevestigt het voorgaande in grote lijnen. De discrepantie tussen RvB/directie en RvB/directie, 1e en 2e managementlaag valt daarbij op. Het aantal managementlagen van 2 of meer beslaat bijna 45 procent terwijl slechts 25 procent van risico-inventarisaties op deze niveaus worden gehouden. Gezien het gewenste bedrijfsbrede karakter toch wel opvallend. Daarmee is de 'diepte' waarmee risicomanagement in organisaties wordt uitgevoerd gering.

We hebben tot slot ook nog de organisatielaag waarop een 'in control'-statement wordt gevraagd afgezet tegen het aantal lagen en de risico-inventarisaties. We zien dan een vergelijkbare tendens, namelijk die van een in de hiërarchie opgaande activiteit/verantwoordelijkheid. Dit is wat ons betreft ook een belangrijke indicator voor de risicocultuur en het control-bewustzijn van de organisatie. Zolang die verantwoordelijkheid niet zichtbaar breed gedragen is en er geen verantwoording over wordt afgelegd, zal risicomanagement niet echt deel worden van het DNA van de organisatie, is onze ervaring .

We hebben vastgesteld (zie figuur 25 hieronder) dat er een significant verband bestaat tussen omzet en het aantal managementlagen, maar zelfs bij organisaties met een omzet groter dan 1 miljard euro is de participatie van de derde managementlaag nog steeds beperkt (10,5 procent).

Figuur 25: Risico-inventarisatie managementniveau afgezet tegen het aantal managementlagen (in percentages)

Aantal managementlagen	Uit hoeveel management-lagen bestaat de onderneming?	Op welke niveau worden de risico's in kaart gebracht?	Voor welke organisatielaag wordt in control statement gevraagd?
Niet van toepassing	-	7,2	45,5
RvB/Directie	7,3	20,6	29,3
RvB/Directie en 1e laag	49,9	54,5	11,4
RvB/Directie en 2e laag	33,3	19,3	3,6
RvB/Directie en 3e laag	6,5	3,7	1,5
RvB/Directie en > 3e lagen	3,0	1,9	-

Welke technieken worden gebruikt bij risico-inventarisatie en -analyse?

Voor alle uitkomsten geldt dat de resultaten nauwelijks verschil geven tussen profit- en non-profit. Meer gereguleerde sectoren zoals financiële dienstverlening en de energiesector onderscheiden zich in positieve zin ten opzichte van het gemiddelde. De kwaliteit van een risico-inventarisatie en -analyse hangt af van de keuze van technieken, de mensen en de gebruikte bronnen. De kwaliteit verbetert wanneer er veel mensen betrokken zijn en er verschillende technieken gelijktijdig worden ingezet om zoveel mogelijke bronnen van informatie te ontsluiten. Daarnaast is een aantal technieken specifiek voor bepaalde sectoren; zo worden de meer kwantitatieve technieken vooral gebruikt in de financiële sector. Uit de resultaten blijkt dat 68,8 procent van de respondenten kwantitatieve technieken gebruikt en 87,1 procent van de respondenten kwalitatieve technieken. Het eerste vinden wij relatief opvallend hoog en het bevestigt bovendien de in de praktijk toenemende tendens om risicomanagement meer tastbaar te maken door het te kwantificeren.

Op vrijwel alle technieken zijn er forse stijgingen waar te nemen ten opzichte van 2009, met incidentregistraties als koploper (zie figuur 26). Dit geeft aan dat het vakgebied verder professionaliseert. In veel gevallen zijn de verschillen tussen profit en non-profit beperkt voor de kwalitatieve technieken en is de stijging navenant. Documentstudie (2014: 1 versus 2 in 2009) en interviews (2014: 2 versus 1 in 2009) hebben stuivertje gewisseld waar het de populairste techniek betreft. Alle nieuw toegevoegde technieken (niet te verwarren met nieuwe technieken) lijken toch vooral een specialistisch karakter te hebben, met scores rond de 10 procent. Dissonant hierbij is de techniek van serious gaming/war gaming, te classificeren als relatief nieuwe techniek, met een score van nog slechts 2,1 procent.

Figuur 26: Technieken van risicomanagement, 2014 tegenover 2009, financiële dienstverlening, profit en non-profit (in percentages)

Techniek	Gemiddeld		Financiële dienstverlening (N=64)		Profit (N=475)		Non-profit (N=251)	
	2014*	2009	2014*	2009	2014*	2009	2014*	2009
Documentenstudie	73,7	38,6	71,9	39,1	73,5	34,3	74,1	44,3
Interviews	70,0	42,2	80,7	57,8	68,4	42,1	72,9	42,4
Workshop	40,6	17,4	68,4	34,4	41,1	17,2	39,8	17,9
Vragenlijsten/Checklist	69,7	36,8	82,5	56,3	70,9	37,7	67,3	35,3
Incidentenregistraties	69,7	24,7	89,5	42,2	72,6	27,3	63,7	20,9
Scenario-analyses	57,3	31,0	82,5	48,4	60,0	33,6	52,2	27,7
Gevoeligheidsanalyses	33,3	19,3	57,9	34,4	38,7	22,4	23,1	14,9
Simulaties	28,1	9,6	49,1	15,6	30,7	10,9	23,1	7,6
Stress testing	22,9	5,4	73,7	31,3	26,7	8,2	15,5	1,1
Value at Risk	23,1	8,7	59,6	32,8	28,8	11,1	12,4	5,2
Economic capital	16,1	5,7	47,4	29,7	21,1	7,5	6,8	3,3
Back testing	8,3	-	36,8	-	11,6	-	2,0	-
Serious gaming/war gaming	2,1	-	7,0	-	2,3	-	1,6	-
Fault tree analysis/foutenboom	11,7	-	7,0	-	12,8	-	9,6	-
Visgraat-methode	11,3	-	8,9	-	12,2	-	9,6	-
Hazard and operability study (HAZOP)	8,0	-	5,3	-	11,4	-	1,6	-
Failure Method and Effects Analysis (FMEA)	10,5	-	8,8	-	12,8	-	6,0	-

* In 2014 zijn zes technieken toegevoegd aan het instrumentarium (zie tabel voor die technieken waarvoor in 2009 geen registraties waren)

Interviews, documentenstudie, vragenlijsten en incidentenregistratie blijken de meest gebruikte technieken te zijn, schommelend rond de 70 procent. Een goede dialoog faciliteren over (de achtergronden van) risico's en hoe ermee om te gaan is nog belangrijker dan het vaststellen van een risicoprofiel. Het proces is belangrijker dan de uitkomst. In dat opzicht verrast ons de uitkomst. Het aantal workshops is sinds 2009 significant toegenomen van 17,4 procent tot 40,6 procent, maar is nog steeds relatief laag in onze ogen. Een andere opvallende uitkomst is dat meer dan de helft van de respondenten gebruik maakt van scenarioanalyse, waarmee deze techniek de vijfde plaats inneemt van meest gebruikt.

4.4 Risicomanagementrapportage en risicomonitoring

Hoe vaak wordt intern gerapporteerd over risico's?

Een belangrijk element van risicomanagement is het intern rapporteren over risico's. Voor het hogere management van een organisatie is het zinvol om goed inzicht te hebben in de aard en de omvang van de risico's die verschillende organisatieonderdelen lopen. Pas wanneer dat inzicht bestaat, kan een bestuur de (financiële) prestaties van een organisatiedeel werkelijk op waarde schatten. Een goed uitgevoerde risicomanagementrapportage geeft een duidelijk antwoord op de vraag hoeveel risico men loopt om de gerapporteerde (financiële) resultaten te realiseren. Ook biedt zo'n rapportage het hogere management inzicht in de zaken die lager in de organisatie spelen en hoe de verantwoordelijke managers ermee omgaan. Dat heeft natuurlijk vooral zin als de interne rapportage periodiek is (bij voorkeur maandelijks, maar in elk geval in het ritme van de P&C-cyclus) én op ad-hoc basis, zodra een specifieke situatie dit vereist.

Onze eerste indruk is dat er nauwelijks verschuivingen/veranderingen zijn ten opzichte van 2009, kortom een stabiel beeld, met één zeer gunstige uitzondering. Nog maar 5 procent (2009: 11 procent) van de respondenten geeft aan dat intern niet gerapporteerd wordt over risico's. Dit is een aanmerkelijke verbetering sinds 2009. Bij deze vijf procent is risicomanagement waarschijnlijk nog nauwelijks aan de orde. En risicoanalyses uitvoeren zonder intern daarover te rapporteren is weinig zinvol. Zonder die rapportages kun je risico's niet monitoren en dus niet managen.

Figuur 27: Frequentie interne rapportage over risico's

Frequentie	2014 (in %)	2009 (in %)
Niet van toepassing	5	11
Wekelijks	3	4
Maandelijks	22	23
Per kwartaal	42	38
Jaarlijks	33	31
Incidenteel/ ad hoc	20	29

Bij de 95 procent (2009: 89 procent) van de respondenten die wel intern rapporteren, valt op dat 33 procent (2009: 31 procent) dat niet vaker dan een keer paar jaar doet. Met de snelle wijzigingen in risico's door de huidige dynamiek, is dat veel te laag. Differentiëren wij de uitkomsten naar omvang, dan blijkt dit percentage tot onze verassing nog hoger uit te vallen bij organisaties met een jaaromzet/budget groter dan € 1 miljard. Deze zelfde tendens wordt, helaas, niet gecompenseerd door incidentele/ad hoc-rapportages. Ook hier blijven we een lage score zien en verdere achteruitgang ten opzichte van 2009.

Van de respondenten rapporteert 42 procent (2009: 38 procent) intern elk kwartaal en 22 procent (2009: 23 procent) elke maand over risico's. Met name in de financiële sector rapporteert bijna de helft van de respondenten maandelijks. Dit is conform onze verwachtingen, gelet op de rapportagevereisten vanuit toezichthouders als De Nederlandsche Bank. Ook de energiesector blijkt veelvuldig op maandelijkse basis te rapporteren over risico's. De antwoordmogelijkheid "wekelijks" is slechts door een kleine groep (3 procent) gekozen. Bovendien heeft 20 procent (2009: 29 procent) aangegeven dat zij (ook) incidenteel/ad hoc intern rapporteren over risico's.

Wat staat er in een interne risicorapportage?

Rapporteren over risico's heeft slechts zin als het rapport toegesneden is op de doelgroep. Het stelt de ontvanger in het beste geval in staat zijn taken en verantwoordelijkheden uit te voeren en besluiten te nemen, actie te nemen en waar nodig bij te sturen. Daarom verwachten wij minimaal de belangrijkste risico's, de status van de belangrijkste beheersmaatregelen, de ontwikkeling van risico's en de status van verbeteracties in de rapportage terug te vinden.

Over het algemeen lijkt ook hier een stabiel beeld te ontdekken ten opzichte van 2009, met vrijwel overal (lichte) stijgingen. Slechts de status van de belangrijkste beheersingsmaatregelen springt er enigszins uit. Alleen 'belangrijke externe veranderingen' laat een kleine daling zien vergeleken met 2009. Ongeveer 71 procent (2009: 66 procent) rapporteert intern over de belangrijkste risico's. Over incidenten rapporteert men ook vaak. Dat is begrijpelijk en verstandig: je leert van fouten en je scherpt het risicoprofiel verder aan. De andere scores laten zien dat er nog veel kan worden verbeterd. Kritieke risico-indicatoren gebruikt men bijvoorbeeld nog nauwelijks.

Figuur 28: Interne rapportage-onderwerpen

Rapportage over	2014 (in %)	2009 (in %)
Belangrijkste risico's	70,8	65,8
De status van de belangrijkste beheersingsmaatregelen	46,7	37,4
Kritieke risico-indicatoren	22,9	16,4
De ontwikkeling/wijziging van risico's	45,6	41,0
Incidenten die zich hebben voorgedaan	50,0	46,5
Belangrijke interne veranderingen en gevolgen	29,9	29,9
Belangrijke externe veranderingen en gevolgen	30,6	31,8
De status van verbeteracties	41,0	37,9

Wanneer worden de risico's besproken?

Risicomanagement is bij voorkeur ingebed in de reguliere managementactiviteiten en dan vooral in de voor de hand liggende combinatie met de P&C-cyclus. Management en risicomanagement vallen dan op natuurlijke wijze samen.Het moment om risico's te bespreken is tijdens het regulier intern overleg van Raad van Bestuur/directie/management. En er wordt op ad-hoc basis frequent over risico's gesproken. Schommelend tussen de 40 en 45 procent bespreekt risico's als onderdeel van interne en externe audit-rapportagebesprekingen en AC/RvC/RvT vergaderingen. Dit is in onze ogen veel te weinig en is zelfs minder geworden ten opzichte van 2009. Opvallend is ook de lage(re) score op businessreviews/voortgang businessplannen (slechts 26,2 procent). Misschien doordat dit nu onderdeel uitmaakt van de planning & control-cyclus die eerder veel hoger scoorde daar waar het risico-inventarisatie en -analyse betrof en de frequentie van monitoring/rapportage op kwartaalbasis. Een andere mogelijkheid is dat dit deels te niet wordt gedaan/opgevangen door de hogere score op budget/begrotingsbesprekingen. De rol van risicomanagement in projectvoortgangsbesprekingen is ook nog laag, zij het met een lichte verbetering vergeleken met 2009.

Figuur 29: Wanneer bespreekt u risico's?

Bespreking	2014 (in %)*	2009 (in %)
Als onderdeel van Raad van Bestuur/Directie/Management Team meetings	75,6	66,0
Als onderdeel van Business Reviews/bespreking voortgang businessplannen	26,2	28,4
Als onderdeel van interne en externe audit rapportagebesprekingen	43,0	43,7
Als onderdeel van Audit Commissie/Raad van Commissarissen/Raad van Toezicht vergaderingen	44,1	45,9
Als onderdeel van budget/begrotingsbesprekingen	41,2	46,1
Ad hoc/ bij incidenten/bij grote veranderingen	43,5	48,2
Als onderdeel van project (voortgangs) besprekingen	36,5	31,2
Als onderdeel van de Algemene vergadering van Aandeelhouders (AVA)	10,7	-
Als onderdeel van overleg met externe partijen	20,7	-
Als onderdeel van de Risicocommissievergaderingen	9,8	-

* Ook hier zijn in de vraagstelling van 2014 een aantal mogelijkheden toegevoegd (zie elementen die geen score hadden in 2009)

In organisaties met een Auditcommissie bespreekt men in 70 procent van de gevallen de risico's in vergaderingen[10]. Wij vinden dit een laag percentage, ook omdat in veel corporate governance-codes het bespreken van risico's als best practice is opgenomen. Blijkbaar is dit nog niet overal doorgedrongen.

Tot slot lijkt de lage score van 9,8 procent voor risicocommissievergaderingen erg laag. Dit hangt misschien samen met het feit dat nog maar weinig organisaties - behalve in de financiële sector[11] - verbijzonderde risicocommissies hebben.

10 356 respondenten hebben een Auditcommissie, maar slecht 248 organisaties bespreekt de risico's met de Auditcommissie. (248/356 = 70%)

11 In de door de Nederlandse Vereniging van Banken gepubliceerde Code Banken (2009) wordt de risicocommissie geïntroduceerd als subcommissie van de RvC. Dergelijke commissies besteden aandacht aan het risicobeheer van de banken maar komen in Nederland nog niet veel voor.

Werkt u met een verklaring van het verantwoordelijke management dat hun organisatiedeel 'in control' is?

Het expliciete karakter van risicomanagement vindt zijn bevestiging door de zogenaamde 'in control'-verklaring. Het stimulerende karakter van zo'n verklaring bevordert in het beste geval de kwaliteit van de onderliggende informatie en risicomanagement. Het verdient aanbeveling dat wanneer het hoogste management zo'n verklaring afgeeft, zij dit baseren op 'in-control' -verklaringen van mangementlagen onder hen. Dit neemt toe doordat meer organisaties, al dan niet onder invloed van Corporate Governance Codes zoals de Nederlandse Corporate Governance Code, extern een 'in control'- verklaring af moeten geven. Bijna 63 procent van de respondenten maakt geen gebruik van een interne verklaring.

In figuur 30 hieronder ziet u waarop de interne verklaring bij de resterende 37 procent van de respondenten betrekking heeft. Hierbij waren meerdere antwoorden mogelijk.

Figuur 30: 'In-control' risico's

Risico's*	Percentage (N=271)
Op het gebied van strategische risico's	27,3
Op het gebied van financiële risico's	77,1
Op het gebied van operationele risico's	54,2
Op het gebied van (financiële) rapporteringsrisico's	50,2
Op het gebied van rechtmatigheidsrisico's	33,6
Op het gebied van compliance risico's	46,9

* In 2009 waren er slechts 3 mogelijke antwoorden op deze vraag: nee, ja voor financiële verslaglegging of ja voor alle risicogebieden. In 2014 is een meer genuanceerd beeld mogelijk van de risicogebieden.

18,5 procent (50 procent van de ja stemmers; 2009: 21 procent) van de respondenten die aangeven een dergelijke verklaring te gebruiken voor enkel de financiële verslaggeving-risico's, zijn voornamelijk organisaties in de profitsector. Strategische risico's en rechtmatigheidsrisico's spelen blijkbaar een geringe rol. Gezien het belang van strategische risico's is dit vreemd. Voor wat betreft rechtmatigheidsrisico's is dit te verklaren aangezien dit primair binnen overheid/non-profit organisaties speelt. Deze mono matige aanpak lijkt deels ook te stroken als we kijken naar het integrale karakter van de verklaringen. Er is nog steeds een grote groep die slechts over 1 risicotype een verklaring aflegt (22,9 procent). Hoewel de vraag in 2009 anders is gesteld (keuze: geen, alleen financiële rapportage risico, integraal) is de toen 21procent score op alleen financiële rapportage risico's vergelijkbaar. Er is echter sprake van een forse stijging daar waar het het integrale karakter betreft van de verklaring: 27,3 procent in 2014 afgezet tegen 10 procent in 2009. Focus ligt dus vooral op de meer traditionele risicogroepen.

Vergelijking met 2009 is beperkt mogelijk. In 2009 waren er drie antwoordmogelijkheden, namelijk:

- Nee, geen 'in control' verklaring
- Ja, op het gebied van financiële verslaglegging
- Ja, op alle risicogebieden (strategisch, operationeel, financiële verslaglegging, wet en regelgeving)

Als er met een 'in control'-verklaring wordt gewerkt, voor welke organisatielagen geldt dit dan?

Hoe meer managementlagen betrokken zijn bij een 'in-control'-verklaring, hoe beter een organisatie erin slaagt risicomanagement goed uit te voeren. Want hoe diep, liefst tot in de haarvaten van de organisatie, men zich bewust is van de risico's en het belang van 'in control' zijn, des te beter de mogelijkheden van risicomanagement tot hun recht komen.

Zoals viel te verwachten, neemt het percentage af naarmate we dieper in de organisatie afdalen. Opvallend genoeg geeft maar 29 procent (2009: 22 procent) van de respondenten een verklaring af aan de hoogste managementlaag. Bij de vorige vraag zagen we dat bij 37 procent (2009: 31 procent) wordt gewerkt met een 'in control'-verklaring. Mogelijk heeft een deel van de respondenten gemeend deze vraag niet met 'ja' te kunnen beantwoorden, omdat zij alleen een externe verklaring afgeven. Wat verrassend en tevens verontrustend is, is dat de penetratiegraad in de organisatie op alle andere niveaus lager is dan 2009 en dus de 'in control' verklaring steeds meer alleen bij de RvB/directie komt te liggen. Dit bevordert in onze ogen niet een risico/control-bewuste cultuur waarover actief en zichtbaar verantwoording wordt afgelegd. Dit wordt nog eens versterkt doordat het totaal percentage van organisaties dat een verklaring afgeeft ook is afgenomen vergeleken met 2009 (van 49,2 procent in 2009 naar 46, procent in 2014).

Figuur 31: 'In control-verklaringen' per organisatielaag

In control- verklaring per organisatielaag	2014 (in %)	2009 (in %)
In control verklaring van de Raad van Bestuur/Directie	29,3	22,1
In control verklaring van de 1e management laag	11,4	14,4
In control verklaring van de 2e management laag	3,6	8,1
In control verklaring van de 3e management laag	1,5	3,2
In control verklaring van meer dan 3 managementlagen onder de Raad van Bestuur/Directie	0,8	1,4

4.5 Risicomanagement en -organisatie

Is binnen uw organisatie de risicobereidheid bepaald en/of vastgelegd?

Om risico's goed te managen is het belangrijk om helder te zijn over de mate van risicobereidheid. Die geeft een beeld van wat als een groot een wat als een klein risico gezien wordt. Daarnaast geeft die risicobereidheid informatie over wanneer actie vereist is en misschien zelfs op welke manier. Daarom is het zonder een eenduidige en expliciete risicobereidheid lastig om te kunnen spreken van geïntegreerd en bedrijfsbreed risicomanagement.

Op de vraag of überhaupt de risicobereidheid was bepaald, gaf 42 procent aan dat dit gebeurd was. Dit percentage is een behoorlijke verbetering van het resultaat in 2009 (31,8 procent). Dit is bemoedigend, gezien het belang, en ook omdat veel organisaties nog worstelen om het concept van risicobereidheid praktisch te vertalen in hun bedrijfsvoering.

Figuur 32: Bepaling risicobereidheid

Risicobereidheid karakteristieken*	Percentage (N=305)
Kwalitatief bepaald	77,0
Kwantitatief bepaald	68,2
Specifiek bepaald voor één of meerdere risicogroepen	48,2
Risicobereidheid vastgelegd	66,2
Risicobereidheid gecommuniceerd	61,0

* Deze aspecten zijn in 2014 toegevoegd aan de vraag over risicotolerantie/-bereidheid

De kwaliteit van het risicobereidheidsconcept in een organisatie (toepassing, effect, etc.) wordt bepaald door een aantal kenmerken, zoals opgenomen in figuur 32. Alle kenmerken scoren hoger dan 60 procent, uitgezonderd de specifieke invulling voor bepaalde risicogroepen. Hoewel wij in de praktijk zien dat risicobereidheid vaak uitgedrukt wordt in kwalitatieve termen, is de score voor kwantitatieve bepaling nog steeds bijna 70 procent. Het bevreemdt dat vastlegging en communicatie relatief laag scoren en niet dicht tegen de 100 procent liggen, want dit is de kern en de kracht van het concept. Het werkt als een eenduidig beeld mits toegepast. Alleen in kleine, 'eenvoudige organisaties' kan men volstaan dit na te laten en toch effect te sorteren.

De uitkomsten laten zich niet vergelijken met 2009, omdat de vraagstelling is aangepast (*"Is risicotolerantie gekwantificeerd?"*). Wel kunnen we natuurlijk bekijken of er verschillen zijn per sector. En jawel, die zijn er. In de non-profit communiceert men beduidend meer en bepaalt men ook iets vaker de risicobereidheid kwalitatief .

Figuur 33: Bepaling risicobereidheid profit - non-profit (in percentages)

Risicobereidheid karakteristieken*	Profit (N=226)	Non-profit (N=79)
Kwalitatief bepaald	75,7	81,0
Kwantitatief bepaald	68,1	68,4
Specifiek bepaald voor één of meerdere risicogroepen	51,3	39,2
Risicobereidheid vastgelegd	67,3	63,3
Risicobereidheid gecommuniceerd	63,3	54,4

* N = 305 (42,0%) is gesplitst in 226 (74,1%) profit en 79 (25,9%) non-profit.

Wie coördineren de activiteiten in het kader van risicomanagement?

Er kan er maar een zijn die eindverantwoordelijk is voor risicomanagement in een organisatie: dat is uiteraard het management zelf. Wel zien wij een rol weggelegd voor een coördinator, veelal een staffunctionaris die faciliterend optreedt. Wij verwachtten dan ook een rol voor, bij voorkeur, een stafafdeling.

Hoezo dan? Verschillende afdelingen en functies kunnen coördineren. Het woord coördinatie werkt soms verwarrend, omdat het ruimte geeft voor verschil in interpretatie. Sommigen stellen dat een situatie met meerdere coördinerende functies problemen veroorzaakt. Anderen stellen dat hoe meer functies betrokken zijn bij risico's, des te beter risico's worden gemanaged.

Er zijn een paar opvallende zaken te vinden in de antwoorden van de respondenten. Allereerst de toename van een verbijzonderde risicomanagement functie/afdeling. Dit wordt verder ondersteund door een verlaging van het aantal respondenten zonder georganiseerde functie en een lichte toename van de rol van de kwaliteitsafdeling. De aansluiting met figuur 7 over de CRO-functie is lastig te maken, omdat op basis van deze figuur juist nog een hogere score zou mogen worden verwacht. Hetzelfde geldt voor de verbijzonderde commissie (zie aansluiting met figuur 34).

Figuur 34: Coördinatie risicomanagement

Functie	2014 (in %)	2009 (in %)
Een verbijzonderde risicomanagement functie/afdeling	19,9	12,8
Een verbijzonderde commissie	7,3	6,0
Het lijnmanagement	30,4	33,9
De financiële functie	47,7	64,1
De verzekeringsafdeling	3,3	5,0
Internal audit/interne accountantsdienst	15,0	17,7
De compliance afdeling	9,8	7,4
De kwaliteitsafdeling	20,5	18,7
Niet georganiseerd	5,2	6,7

De afname van de rol van de eerste lijn laat zich op twee manieren uitleggen. Óf respondenten passen het 'three lines of defence' concept strikter toe (zie ook de volgende vraag), wat de afnemende rol verklaart, óf risicomanagement is primair een lijnactiviteit en onderdeel van de reguliere bedrijfsvoering; zo opgevat is een afname ongelukkig.

Niet verassend is dat de financiële functie nog steeds koploper is, met 47,7 procent, maar wel is die sterk gedaald vergeleken met 2009 (64,1 procent).

Omdat sommigen van mening waren dat meer dan één coördinerende functie of afdeling moet worden vermeden, hebben wij ook het aantal coördinatoren berekend. De meeste organisaties, 48 procent, hebben slechts één coördinerende functie, 17 procent heeft er twee en 30 procent heeft drie of meer coördinerende functies.

148 (22,5 procent) organisaties hanteren het 'three lines of defence' principe. Dit is vanuit de praktijk gezien toch nog verrassend laag. Er wordt namelijk de laatste tijd veel geschreven en gesproken over de 'lines of defence' als concept voor governance-ordening in het risico-, compliance- en control-veld. Overigens is daarvan de theoretische en wetenschappelijke onderbouwing gering.

We hebben daarom in onze analyse in kaart gebracht wat de verschillen zijn per sector en per omzetcategorie. Niet geheel verrassend is dat het 'three lines of defence' principe vooral gemeengoed is in de financiële sector. Dat telecommunicatie, informatietechnologie en entertainment second best is, is juist verrassend, gezien de lage score op de volwassenheidsgraad en rapportcijfer/surveyscore. Alle andere sectoren zitten op een niveau van 24 procent of lager met productie als sector waarin het begrip nauwelijks is doorgedrongen. Ook de omzetgrootte geeft een bevestigend beeld van wat zou mogen worden verwacht, namelijk dat vooral grote bedrijven het principe kennen en toepassen. Pas vanaf 500 miljoen en hoger is sprake van 42 procent of meer. Figuur 35 en 36 hieronder laten een nadere verbijzondering zien van het concept naar sector en omzetgrootte.

Figuur 35: Three lines of defence naar sector

Three Lines of Defence naar sector	Toepassing Three Lines of Defence (in %)*
Handel	23,7
Transport & logistiek	24,0
Productie	8,7
Financiële dienstverlening	66,67
Zakelijke dienstverlening	13,3
Telecommunicatie, informatietechnologie en entertainment	33,3
Energie & utilities	22,2
Gezondheidszorg	12,1
Overheid/Non- profit	14,6

* N = Aantal organisaties per sector.

Figuur 36: Three lines of defence naar omzet

Three Lines of Defence naar omzet	Toepassing Three Lines of Defence (in %)*
0 - 50 miljoen	9,9
51 - 100 miljoen	18,6
101 - 500 miljoen	27,9
501 miljoen - 1 miljard	42,3
> 1 miljard	73,7

* N = Aantal organisaties per sector.

Welke standaarden hanteren organisaties bij de inrichting van risicomanagement en interne beheersing?

Het gebruik van een breed erkende standaard is een best practice. Soms kunnen er ook specifieke standaarden bestaan voor functionele deelgebieden zoals bijvoorbeeld voor IT, dan wel sectoren zoals de financiële sector.

De uitkomst op de vraag welke standaarden organisaties hanteren, kwam wederom als een verassing. We hadden niet verwacht dat nog steeds een duizelingwekkende 51,3 procent geen standaard gebruikt, alhoewel het een betere score is vergeleken met 2009. Hoewel er geen garantie bestaat dat het gebruik van een model noodzakelijk is om risico's te managen, is enige vorm van referentie behulpzaam. Het is geen verassing dat COSO deze lijst nog steeds aanvoert, maar dit ook weer niet met overtuiging doet, ondanks dat men vaak naar COSO verwijst. INK is runner-up en loopt in op COSO. Ook opvallend is opkomst van ISO, uit het niets op plek nummer drie met 12 procent bescheiden, maar met potentie. In alle gevallen is er sprake van een stijging vergeleken met 2009, maar het is nog steeds weinig overtuigend. De vorige survey uit 2009 onthulde dat 63,2 procent geen gebruik maakt van een standaard/model.

Figuur 37: Overzicht van gebruikte standaarden (in percentages)

Standaard	Financiële dienstverlening (N=57)	Profit sector (N=475)	Non-profit sector (N=251)	2014	2009
Geen standaard	10,5	49,1	47,8	48,6	63,2
COSO	64,9	29,5	20,3	26,3	21,2
INK/EFQM model	10,5	14,5	31,5	20,4	14,4
ISO 31000*	17,5	12,0	12,0	12,0	-
6Sigma	5,3	10,3	3,6	8,0	3,7
Basel/Solvency	63,2	11,2	1,2	7,7	4,7
Management of Risk (M_o_R)*	3,5	4,6	4,4	4,6	-
Australian/New Zealand	1,8	0,4	1,2	0,7	0,3
OCEG	1,8	0,4	0,4	0,4	0
AIRMIC	1,8	0,2	0,4	0,3	0
Anders	19,3	10,9	13,1	11,7	7,5

* In 2009 was dit geen antwoordcategorie, omdat ISO 31000 nog niet was gepubliceerd. Zelfde geldt voor Management of Risk, maar toen vanwege de onbekendheid.

De volgende sectorverschillen zijn verder nog de moeite van het vermelden waard:

- INK/EFQM wordt, zoals verwacht, voornamelijk toegepast in non-profit.
- ISO31000 past men relatief weinig toe in de profit-sector. Hiervoor kennen wij geen logische verklaring, juist omdat ISO-richtlijnen veel in industriële omgevingen worden toegepast.
- 6Sigma heeft een hogere penetratie in de profit-sector. Dit laat zich wel verklaren: het is van oorsprong een productie-concept.
- Basel/Solvency is alleen in de financiële sector (hoeft geen verklaring), maar verrast toch met een score van 63 procent, aangezien dit verplicht is voor verzekeraars en banken; men zou een score in het laatste kwartiel verwachten, tenzij er sprake is van financiële instellingen anders dan banken en verzekeraars.
- Management of Risk en OCEG vinden we vooral binnen de profit.

Welke software wordt gebruikt?

Het gebruik van software is niet per se noodzakelijk, maar draagt wel bij aan een efficiëntere manier van werken en aan de verdere professionalisering van risicomanagement. Er zijn vele mogelijkheden om het risicomanagementproces te ondersteunen. Zeker grotere en/of meer ontwikkelde organisaties op het gebied van risicomanagement gebruiken software. De wijze van beantwoording laat zien dat men mogelijk niet helemaal op de hoogte is van de mogelijkheden van de pakketten die men in huis heeft gehaald. Zo heeft elk Enterprise Resources Planning (ERP-) pakket tegenwoordig standaard 'segregation of duties (SoD)' ingebouwd. Deze categorie had in de onderstaande tabel (figuur 38) dan ook een veel hoger percentage moeten krijgen indien de respondenten zich daarvan bewust waren geweest. Waarschijnlijk is het topmanagement onvoldoende thuis in de IT-materie voor de beantwoording van deze vraag, of - maar dat is minder waarschijnlijk - het classificeert SoD niet als een risicomanagement-instrument.

We vroegen welke software organisaties gebruiken om het uitvoeren van risicomanagement te ondersteunen. De uitkomsten zijn een stuk rooskleuriger dan in 2009 en in lijn met de tendens van het toenemen van het belang van technologie in het managen van risico's. Die tendens zien we ook in de professionalisering en sterke consolidering van GRC-software bedrijven de afgelopen jaren. Er wordt geen software gebruikt in 32,3 procent van de gevallen. Vergeleken met de survey uit 2009 (73,8 procent) is dit percentage sterk afgenomen en daarmee dus het gebruik van software toegenomen. In aanvulling op de vraag uit 2009 hebben we ook de volgens Gartner/Forrester meest bekende, toegepaste en ontwikkelde integrale (GRC) software-oplossingen opgenomen (zogenaamde vendors). De scores op die oplossingen zijn zeer laag in de Nederlandse markt. Alleen SAP/GRC kan enige aanwezigheid claimen. De diversiteit van oplossingen inclusief het zelf bouwen in bijvoorbeeld Excel of Lotus Notes lijken nog de overhand te hebben. Hier is duidelijk nog een wereld te winnen en groei te verwachten in de toekomst.

Figuur 38: Risicomanagementsoftware toepassing en vendors

Risicomanagementsoftware	Percentage
Geen (ondersteunend) software	32,2
Nasdaq OMX Bwise	0,8
EMC (RSA Archer)	0,1
Thomson Reuters (Accelus)	0,4
SAP (GRC)	3,3
IBM (OpenPages)	0,3
Software AG (Aris)	0,7
Wynyard (Methodware)	0,1
Zelfontwikkelde software	10,9
Andere software	15,6

De resultaten op het gebied van functionaliteiten voor risicomanagement-ondersteuning zijn ook in 2014 nog bedroevend laag. Er is ook geen duidelijke tendens van verbetering en eerder sprake van een lichte verslechtering tussen 2009 en 2014 (zie figuur 39).

Slechts 1,4 procent claimt het gebruik van 'segregation of duties' SoD-software. We concluderen hieruit dat veel van de respondenten de standaardsoftware niet begrijpen - bijvoorbeeld ERP-systemen zoals die worden geleverd door SAP en andere softwareorganisaties - maar deze wel in gebruik hebben. Het percentage gebruikers van deze soort standaardsoftware is naar verwachting veel hoger en daarmee zou het percentage van 1,4 procent (2009: 1,5 procent) ook veel hoger moeten zijn.

Figuur 39: Gebruik software ten behoeve van en ondersteunend aan risicomanagement

Overige ondersteunende software	2014 (in %)	2009 (in %)
Brainstorm software	1,2	1,3
Voting software	2,1	2,7
SoD (segregation of duties) software	1,4	1,5
Data-analyzing software	6,8	6,4
Procesmanagement software	8,0	10,2
Internal audit management software	5,8	7,7
Monitoring software	6,9	5,6
Performance management software	6,1	7,1
Andere ondersteunende software	4,0	5,8

Hoe ziet de externe rapportage over risicomanagement eruit?

Voor externe rapportages geldt grotendeels hetzelfde als voor interne rapportages. Relevant om op te nemen zijn: helderheid over het integrale risicoprofiel, de veranderingen daarin, de manier waarop deze gemanaged worden en de belangrijkste acties. Bovendien wordt dankzij corporate governance codes extern rapporteren over risico's ook steeds meer gemeengoed. Ook veronderstellen wij dat externe rapportages een positieve invloed hebben op de mate van risicomanagement. Immers, om te kunnen rapporteren, zul je ook data moeten gaan verzamelen.

De resultaten uit 2014 afgezet tegen 2009 laten zien dat er over het algemeen meer en beter wordt gerapporteerd: 25,4 procent zei in 2009 'niets' te rapporteren en dat is gedaald naar 16,7 procent; vrijwel alle andere rubrieken scoren hoger dan 2009. Iets meer dan de helft van de respondenten rapporteren financiële risico's. Hoewel ongeveer alle corporate governance regels eisen dat organisaties ten minste rapporteren over financiële rapportage of financiële risico's, komen de uitkomsten niet in de buurt van de 100 procent. Onze conclusie: er is veel ruimte voor verbetering.

Figuur 40: Inrichting externe rapportage risicomanagement (in %)

Rapportage	2014 (in %)	2009 (in %)
De wijze waarop risicomanagement is opgezet	37,2	30,5
Effectiviteit van risicomanagement/interne beheersing (alle risico's)	14,8	12,0
Effectiviteit van risicomanagement/interne beheersing (financiële risico's)	20,0	13,1
De risicotolerantie in kwalitatieve zin	11,6	5,3
De risicotolerantie in kwantitatieve zin	7,2	5,2
De belangrijkste strategische risico's	41,4	36,8
De belangrijkste financiële risico's	53,0	53,8
De belangrijkste (financiële) verslaggevingsrisico's	14,9	10,6
De belangrijkste operationele risico's	31,7	33,7
De belangrijkste compliance risico's	17,9	11,3
De belangrijkste verbeterpunten/getroffen maatregelen	25,8	27,1
De belangrijkste incidenten die zich hebben voorgedaan	18,2	19,2
De materiële gevolgen van incidenten	9,0	9,5
De belangrijkste wijzigingen in ons risicoprofiel/interne beheersingssysteem	15,0	12,4
Niets	16,7	25,4

Opmerkelijk is de lichte daling van operationele risico's (van 33,7 procent naar 31,7 procent). Daarentegen is de relatief significante stijging van compliancerisico's weer goed te verklaren in het huidige tijdsgewricht.

Ook de (weliswaar lichte) daling van belangrijkste verbeterpunten/getroffen maatregelen is contra-intuïtief, gezien de eisen vanuit het maatschappelijk verkeer en pogingen de informatie toegankelijker te maken voor de lezer/gebruiker ervan. Uit de figuur 'Inrichting externe rapportage' is verder duidelijk te zien dat de risicotolerantie doorgaans noch in kwalitatieve (dan wel beperkte mate) noch in kwantitatieve zin wordt vermeld in externe rapportages.

Externe rapportage-elementen naar omzetcategorie (figuur 41) laat zien dat hoe groter de organisatie hoe meer en beter er over risicomanagement wordt gerapporteerd. De omzetcategorie 101 - 500 miljoen wijkt daar opvallenderwijs enkele keren van af. Hiervoor hebben wij geen verklaring kunnen vinden.

Er zijn tot slot nog een paar bijzondere dissonanten in het geschetste beeld van lineaire verbetering naar omzet:

- de spreiding over omzetcategorieën voor effectiviteit van risicomanagement/interne beheersing voor financiële risico's (geen eenduidig en verklaarbaar beeld);
- een uitschieter in de omzetcategorie 501 - 1000 miljoen voor belangrijkste wijzigingen in ons risicoprofiel;
- het voorgaande geldt in iets mindere mate voor (financiële) verslaggevingsrisico's.

Figuur 41: Inrichting externe rapportage risicomanagement per omzetcategorie (in percentages)

Rapportage naar omzet (in miljoenen)	0 - 50	51 - 100	101 - 500	501 - 1000	>1000
Wijze waarop risicomanagement is opgezet	29,8	33,3	44,8	65,4	73,7
Effectiviteit van risicomanagement/ interne beheersing (alle risico's)	11,4	10,9	18,6	26,9	52,6
Effectiviteit van risicomanagement/ interne beheersing (financiële risico's)	20,2	17,3	23,3	15,4	31,6
Risicotolerantie in kwalitatieve zin	8,4	11,5	10,5	23,1	52,6
Risicotolerantie in kwantitatieve zin	6,0	6,4	5,2	15,4	21,1
Belangrijkste strategische risico's	35,8	42,3	42,4	61,5	84,2
Belangrijkste financiële risico's	48,5	57,1	52,3	69,2	84,2
Belangrijkste (financiële) verslaggevingsrisico's	12,7	13,5	13,4	42,3	31,6
Belangrijkste operationele risico's	26,2	35,3	34,3	50,0	57,9
Belangrijkste compliancerisico's	13,6	17,3	19,8	46,2	63,2
Belangrijkste verbeterpunten/getroffen maatregelen	23,5	30,1	25,0	38,5	42,1
Belangrijkste incidenten die zich hebben voorgedaan	17,8	19,9	18,0	15,4	26,3
Materiële gevolgen van incidenten	9,4	8,3	7,0	11,5	15,8
Belangrijkste wijzigingen in ons risicoprofiel/interne beheersingssysteem	11,4	16,7	14,5	66,7	47,4
Niets	18,1	18,6	14,5	11,5	-

5. Risicocultuur

In de aanloop naar ons onderzoek van 2009 en als resultaat van de uitkomsten van 2009 hebben we vaak en diepgaand gediscussieerd over de rol van cultuur in de kwaliteit van het risicomanagement en of en zo ja hoe je dit kan vangen in een vragenlijst. Die moet namelijk een balans vinden tussen voldoende relevant/diepgaand en tegelijk aantrekkelijk/makkelijk en snel in te vullen. We hebben destijds gemeend dat dit lastig, zo niet ondoenlijk, is en hebben een andere insteek gekozen. We moeten kijken naar de manier waarop organisaties risicomanagement invullen; die is - zeiden we toen - een reflectie van de risicocultuur/control-omgeving en het belang dat organisaties hechten aan risicomanagement. Wie is betrokken, hoe vaak, is er een verbijzonderde functie, een heldere risicoscope, hoe wordt verantwoording afgelegd, etc.

Dit is misschien niet helemaal waterdicht, maar wij zijn die mening nog steeds toegedaan. Toch hebben we bij dit nieuwe onderzoek gemeend, mede ook gezien de discussie de afgelopen jaren en de feitelijke herbevestiging van de rol en het belang van risicocultuur, dit onderwerp nadrukkelijker in de vragenlijst te adresseren. De risicocultuur/control-omgeving vormt namelijk het fundament voor de opzet en vooral de werking van het risicomanagementsysteem. Dit is helaas wederom bevestigd in alle bedrijfsschandalen (ook in de non-profit sector!) van de afgelopen jaren in Nederland en daarbuiten. Naast het fundamenteel ontbreken van effectieve beheersingsmaatregelen, schortte het ook altijd aan de cultuur.

We hebben ervoor gekozen om een indicatie over risicocultuur te krijgen door te vragen naar managementbetrokkenheid, de relatie met beoordeling en beloning (prikkels) en een aantal stellingen die de control-omgeving duiden. We hebben niet de pretentie met onderstaande vragen volledig te zijn en het onderwerp adequaat af te dekken (als dit überhaupt mogelijk is met alleen een vragenlijst/zelfbeoordeling). Hieronder vindt u de resultaten met een korte analyse.

Wie schrijft de risicoparagraaf in uw jaarverslag

Het jaarverslag vormt het unieke formele middel om verslag te doen en verantwoording af te leggen naar alle externe stakeholders inclusief het maatschappelijk verkeer. De risicoparagraaf is al een groot aantal jaren gemeengoed als onderdeel van het jaarverslag en is de afgelopen jaren geëvolueerd in omvang, diepgang en relevantie. In onze ogen kunnen we het belang dat wordt gehecht aan risicomanagement, gereflecteerd zien in de managementfunctie en -positie die materieel het verslag schrijft en samenstelt.

Hoewel er geen vergelijking mogelijk is met 2009, valt op dat de financiële functie met meer dan 50 procent van de respons degene is die de risicoparagraaf schrijft. Dit is deels te verklaren vanuit een traditioneel standpunt over de rol die de financiële discipline inneemt over risicomanagement en interne beheersing, en anderzijds dat het nog niet gemeengoed is dat er een verbijzonderde risicomanagement-functionaris in elke organisatie is (zie hiervoor de vraag en analyse over de CRO en coördinatie van risicomanagement).

Figuur 42: Functionaris die risicoparagraaf schrijft

Functie	Aantal	Percentage
Niet van toepassing	128	17,7
Algemeen directeur	168	23,2
De financiële functie	383	52,8
De risicomanager/IC functionaris/GRC functionaris	130	17,9
De bestuurssecretaris/ secretariële functie	40	5,5
Juridische afdeling	14	1,9
Anders	55	7,6

De lage score van de juridische afdeling is opvallend omdat onze indruk is dat de juridische afdeling wel degelijk soms een grote rol speelt in de samenstelling van de rapportage, bijvoorbeeld bij de vraag welke informatie naar buiten wordt gebracht. Hetzelfde geldt in mindere mate voor de bestuurssecretaris, het blijft toch een specialistische functie. Een score van 23,2 procent voor de algemeen directeur vinden wij niet slecht, maar kan zeker beter, gezien de rol die wij toedichten aan het lijnmanagement op het gebied van risicomanagement én omdat respondenten meerdere antwoorden konden geven en de algemeen directeur vaak in coproductie een rol zal spelen. Uit de cultuurvraag blijkt verder dat de risicomanager eigenlijk maar in zeer beperkte gevallen meeschrijft aan de risicoparagraaf, terwijl hij toch de coördinator van risicomanagement is. Slechts in 36 procent van de gevallen dat er een CRO (210) is aangesteld, is deze betrokken op directieniveau (76 van de 210).

Hoe wordt de belonings- en waarderingssystemen afgestemd op de effectiviteit van risicomanagement?

In het handelen van mensen en de keuzes die zij maken staan (positieve) prikkels centraal. Dit is niet anders bij risicomanagement. De aandacht die mensen geven en het belang dat zij hechten aan risicomanagement worden gestimuleerd door de waardering die zij daarvoor krijgen en de eventuele beloning, materieel of immaterieel, die zij daarvoor ontvangen. Die waardering en beloning moeten verankerd zijn in functie- en rolbeschrijvingen en vervolgens in persoonlijke (jaar-) plannen.

Gegeven het beschreven verband is het verontrustend te zien dat er slechts in 9 procent van de gevallen een dergelijke formele en directe relatie bestaat tussen de effectiviteit van het risicomanagement en de belonings- en waarderingssystemen. In 66 procent van de gevallen is er zelfs geen enkele relatie.

Dit draagt in onze ogen niet bij aan het duurzaam verankeren van risicomanagement in de organisatie (in 'het DNA van de organisatie') en het onderdeel te maken van de dagelijkse werkzaamheden. Wij hebben hiervoor geen eenduidige verklaring, anders dat voor de respondenten die relatie niet zo duidelijk is als wij die zien, wat we bevestigd zien door een relatief lage score van 1,9 respectievelijk 2,1 op de laatste 2 stellingen op de volgende pagina's. Wij durven wel te stellen dat er vrij eenvoudig nog een wereld te winnen valt op dit vlak.

Figuur 43: Relatie beloning/waardering en risicomanagement

Functie	Aantal	Percentage
Er is een directe formele relatie tussen de effectiviteit van risicomanagement en de belonings- en waarderingssystemen.	65	9,0
Er is geen directe relatie, maar informeel wordt risicomanagement wel meegenomen in de belonings- en waarderingssystemen.	181	25,1
Er is geen enkele relatie tussen de effectiviteit van risicomanagement en de belonings- en waarderingssystemen.	475	65,9
Totaal	721	100

Elf stellingen over risicomanagement in relatie tot cultuur

Om een beeld te krijgen van de risicocultuur hebben we aan de respondenten 11 stellingen voorgelegd, over diverse onderwerpen in relatie tot risicomanagement[12] die in onze ogen iets zeggen over de rol, het belang en de verankering van risicomanagement in de onderzochte organisaties. De vragen zijn gesteld langs een schaal van 1, helemaal oneens, tot 5, volledig eens. Vanwege het karakter van de survey, een zelfbeoordeling, is de vraag gerechtvaardigd of we hier sociaal-wenselijke antwoorden hebben gekregen of een benadering van de realiteit vanuit het perspectief/achtergrond van de respondent. We hebben geen cross-checks kunnen uitvoeren om dit uit te sluiten.

Gegeven deze beperkingen valt de hoge score op over het inherente belang van risicomanagement voor een goede bedrijfsvoering. In de praktijk, maar zeker ook gezien de overige scores, bestaat bij ons het beeld dat risicomanagement nog steeds een sterk compliance-gedreven activiteit is, die dus wordt opgedragen of uitgelokt door een prikkel van buiten. Deze score verbaast ons en lijkt een sociaal wenselijk antwoord te bevestigen.Hetzelfde geldt voor de stelling: *"fouten maken mag, als je er maar van leert"*.

Maar dit kunnen we niet rijmen met de antwoorden op een van de eerdere vragen. De positionering van risicomanagement en het bekleden van een functie daarin lijkt te bevestigen wat we al wisten, inclusief de klachten vanuit de business over de kwaliteit van het risicomanagement of de risicomanagers. Nu mogen we natuurlijk niet iedereen over een kam scheren, maar hier ligt wel een fundamenteel probleem, zeker als we weten dat meer dan 50 procent van de respondenten bestuurders waren. Zij kunnen dit doorbreken door de statuur van risicomanagement en de mensen die daarin werken naar een hoger plan te tillen en kwaliteit (waaronder businesskennis) de overhand te geven in het vullen van posities op dit vlak.

De nadruk op korte termijn resultaten scoort ook relatief laag en lijkt in discrepantie met in ieder geval de beleving van veel mensen zowel in als buiten organisaties. Ook hier komt wellicht het sociaal-wenselijk karakter naar boven drijven, wat wij niet kunnen wegnemen op basis van andere feiten/inzichten.

Veel antwoorden lijken verder het veilige midden te kiezen met een score rondom 3,5 met in alle gevallen een acceptabele en in ieder geval niet opvallende standaarddeviatie.

12 Gebaseerd op Institute of International Finance, 2012

Figuur 44: Score op stellingen

Stellingen	Gemiddelde score (schaal 1-5)	Standaard-deviatie
1. Risicomanagement wordt uitgevoerd omdat dat bijdraagt aan een betere bedrijfsvoering en wordt niet gezien als een kostenpost.	3,9	0,92
2. Medewerkers worden gemotiveerd om als ze risico's nemen, dit weloverwogen te doen.	3,6	0,95
3. Een positie binnen risicomanagement wordt gezien als versterking van je carrière.	2,5	0,96
4. Fouten maken mag, als je er maar van leert.	4,0	0,80
5. De cultuur in onze organisatie bevordert risicomanagement.	3,2	0,98
6. Overtredingen van interne regels worden zeer serieus genomen en bestraft.	3,2	1,00
7. De Raad van Bestuur/Directie is zeer gecommitteerd aan risico-management en ondersteunt dat actief.	3,5	1,01
8. Medewerkers voelen zich vrij om risico's aan te kaarten bij hun leidinggevenden.	3,7	0,81
9. In onze organisatie ligt de nadruk vooral op korte termijn resultaten.	2,5	1,11
10. De beloningsstructuur bevordert het nemen van risico's.	1,9	0,99
11. Er wordt een duidelijke relatie gelegd tussen te behalen doelen, risico's en de beloning.	2,1	1,08

Figuur 45: Score op stellingen naar sector

Stellingen naar sector	1	2	3	4	5	6	7	8	9	10	11
Handel	3,88	3,61	2,43	3,96	3,21	3,35	3,41	3,70	2,43	1,94	2,03
Transport & logistiek	3,76	3,36	2,48	3,88	3,28	3,32	3,32	3,72	2,44	2,00	2,56
Productie	3,79	3,51	2,54	4,07	3,16	3,23	3,31	3,71	2,56	2,25	2,46
Financiële dienstverlening	4,04	3,74	3,09	3,84	3,70	3,67	3,93	3,89	2,28	1,91	2,91
Zakelijke dienstverlening	3,95	3,59	2,40	3,98	3,13	3,28	3,50	3,78	2,85	2,02	2,17
Telecommunicatie, informatietechnologie en entertainment	3,41	3,59	2,29	4,11	2,94	3,12	3,35	3,59	3,00	2,59	3,06
Energie & utilities	4,17	3,67	2,83	3,89	3,22	3,67	3,72	3,50	2,83	1,40	2,50
Gezondheidszorg	3,96	3,57	2,33	4,14	3,12	2,97	3,55	3,56	2,56	1,68	1,69
Overheid/Non-profit	3,99	3,42	2,21	3,35	2,85	2,88	3,35	3,55	2,35	1,49	1,62

Figuur 46: Score op stellingen naar omzet

Stellingen naar omzet	1	2	3	4	5	6	7	8	9	10	11
0 - 50 miljoen	3,87	3,54	2,42	4,03	3,15	3,06	3,42	3,67	2,45	1,74	2,05
51 - 100 miljoen	3,90	3,45	2,36	4,02	3,03	3,16	3,37	3,69	2,50	1,95	2,06
101 - 500 miljoen	3,95	3,60	3,50	3,96	3,18	3,38	3,50	3,66	2,67	2,10	2,19
501 miljoen - 1 miljard	3,92	3,65	2,58	3,69	3,08	3,45	3,50	3,58	2,27	2,12	2,54
> 1 miljard	3,95	3,79	3,32	3,69	3,63	3,84	4,00	3,53	3,05	2,26	2,63

Rapportcijfers voor risicomanagement herzien

Ondanks alle voorbehouden over risicocultuur-scores, zijn we benieuwd wat de uitkomsten van het risicocultuur-gedeelte betekenen voor de totaalscore. In de scoreleidraad zijn we uitgegaan van zeven kwaliteitsaspecten (zie Bijlage 2) waaraan we 'Risicocultuur in het DNA' als element toevoegen, maar dan wel met andere weging. Zonder een redelijke 'Risicocultuur in het DNA' van een organisatie kán risicomanagement niet goed zijn; het is dan hoogstens window-dressing. Hoe we dit extra kwaliteitsaspect ook wegen, de totale score van kwaliteit van het risicomanagement neemt flink af. Hieronder hebben we twee varianten opgenomen wat DNA doet met de surveyscore:

1. DNA weegt even zwaar als de andere zeven aspecten (15 procent bijdrage);
2. DNA weegt zwaarder, ongeveer een derde van het totaal (30 procent bijdrage).

De resultaten spreken voor zich: de verschillen tussen de eigen score en onze scores worden alleen maar groter. Wij willen nogmaals aantekenen dat dit een bijdrage levert aan de discussie van de rol van risicocultuur in organisaties, maar dat de diepgang en reikwijdte van onze vragen nog niet voldoende zijn om goed onderbouwde conclusies te trekken op dit vlak.

Figuur 47: Totaalscore met weging, afgezet tegen zelfevaluatie

Sector	Gemiddelde rapportcijfer (zelfevaluatie)	Surveyscore Weging 85% - 15%	Surveyscore Weging 70% - 30%
Handel	6,86	4,21	3,95
Transport & logistiek	6,76	4,58	4,38
Productie	6,90	3,94	3,72
Financiële dienstverlening	7,55	6,01	5,74
Zakelijke dienstverlening	6,82	4,29	4,03
Telecommunicatie, informatietechnologie en entertainment	6,67	3,78	3,53
Energie & utilities	7,11	4,95	4,67
Gezondheidszorg	6,75	4,36	4,06
Overheid/Non-profit	6,59	4,10	3,81
Totaal	**6,85**	**4,32**	**4,06**

6. Twee andere invalshoeken

6.1 De dataset opnieuw bekeken, twee keer met andere vraag

Op grond van de onderzoeksdata die we voor dit onderzoek vergaarden, hebben we ook twee andere vragen gesteld. Ten eerste: Doen organisaties die aangeven Enterprise Risk Management te gebruiken, het ook beter? In paragraaf 6.2 vindt u het antwoord.

En ten tweede: Welke factoren dragen positief bij aan een meer volwassen risicomanagement-systeem? Daarop geven we het antwoord in paragraaf 6.3, dat u kunt lezen als een serie heel concrete aanbevelingen voor uw eigen organisatie.

6.2 Enterprise Risk Management, vanzelf een hogere score?

In de afgelopen jaren hebben steeds meer organisaties Enterprise Risk Management (ERM) ingezet om risico's te beheersen. In tegenstelling tot de traditionele risicomanagementbenadering, waarin risico's vanuit diverse organisatieonderdelen of perspectieven wordt bezien, veronderstelt ERM dat het hele spectrum aan risico's op een meer integrale wijze wordt bezien. Binnen ERM worden zo strategische, operationele, rapportage- en compliancerisico's gelijktijdig behandeld. Een dergelijke aanpak moet de bedrijven helpen effectief om te gaan met kansen en risico's. De veronderstelling is dat dit bijdraagt aan het beter beheersen van risico's en benutten van kansen. Tot op heden is dat overigens voor veel organisaties zeker geen sinecure gebleken, er gaat nog vaak van alles mis. De boodschap is ook dat het niet reëel is te veronderstellen dat incidenten zich na het implementeren van zo'n systeem zich nooit meer zullen voordoen.

De voor- en nadelen van het implementeren van ERM kunnen niet eenduidig worden geschetst. Sommige onderzoeken tonen aan dat het goedkoper wordt om in hun kapitaalbehoefte te voorzien en dat de toewijzing en benutting van kapitaal worden verbeterd (COSO 2004). Er wordt veel tijd, kennis en middelen geïnvesteerd in het ontwikkelen en implementeren van een ERM-systeem. De vraag is of de voordelen de gemaakte kosten overschrijden. ERM gaat uiteraard gepaard met kosten en als het geen waarneembare resultaten oplevert, kan de invoering ervan in twijfel worden getrokken.

Om een antwoord op die laatste vraag te geven hebben wij onderzoek gedaan. Op basis van statistische analyses is er onderzocht of een ERM systeem invloed heeft op de ondernemingsprestaties. De verwachting daarbij is dat hoe hoger de waardering van het ERM is, hoe groter de voordelen zijn die organisaties kunnen behalen. Hieronder vatten wij de belangrijkste uitkomsten samen.

Groeimogelijkheden

We vroegen de respondenten in welke mate het ERM voordeel heeft opgeleverd voor de groeimogelijkheden van de organisatie. Ondernemingen met groeipotentie hebben te maken met onzekerheid inzake toekomstige kasstromen en zouden derhalve eerder geneigd zijn om een ERM te implementeren (Liebenberg en Hoyt, 2003). Groei dient te leiden tot een toename van de waarde van een onderneming en dat vergt uiteraard een afweging van risico's en te behalen rendement. In dit traject worden de risico's opgespoord, consequenties beoordeeld en worden aanvullende maatregelen getroffen om risico's te beheersen. ERM kan daarbij helpen.

Helaas is uit ons onderzoek niet gebleken dat ERM die positieve invloed heeft. Kennelijk zien snel groeiende organisaties niet het nut van ERM.

Winstgevendheid

Voorts hebben wij de respondenten gevraagd in welke mate ERM een positieve bijdrage heeft opgeleverd voor de winstgevendheid. De veronderstelling is hoe beter de respondenten hun ERM-systeem waarderen, hoe meer dat bij zal dragen aan de winstgevendheid.

Immers, het integraal bezien van risico's maakt het mogelijk om de volatiliteit van de winst in te perken en daarmee de voorspelbaarheid van de resultaten. In ons onderzoek hebben we helaas ook op dit punt geen positieve relatie gevonden.

Vermogenskosten

Vervolgens hebben de respondenten aangegeven in welke mate het ERM voordeel heeft opgeleverd voor de vermogenskosten. Leidt het tot lagere vermogenskosten?

Kosten van kapitaal worden direct beïnvloed door het risicoprofiel. Beleggers eisen een hoger rendement bij een meer risicovolle onderneming. Als ERM volledig geïmplementeerd is, beschikt de onderneming over meer en betere informatie over haar risicoprofiel. Deze informatie kan worden gedeeld met investeerders, wat leidt tot meer transparantie over de (toekomstige) risico's. Dergelijke informatie zou vooral belangrijk kunnen zijn voor ondernemingen met complexe activiteiten, omdat dergelijke bedrijven van buitenaf moeilijk te beoordelen zijn. Het beheersen van de risico's verbetert ook de risicoperceptie van het bedrijf zelf. Deze verbeterde perceptie zou op haar beurt ertoe kunnen leiden dat de financiële markt lagere risicopremies op aandelen en leningen eist en een lagere solvabiliteit (meer vreemd vermogen ten opzichte van het eigen vermogen) toestaat. Uiteindelijk zou dit moeten leiden tot een verlaging van de kapitaalkosten. Dit blijkt inderdaad het geval te zijn.

Reputatie

Tot slot hebben wij onderzocht in welke mate ERM de reputatie vergroot. De veronderstelling is dat hoe hoger de respondenten hun ERM hebben gewaardeerd, hoe meer ERM bijdraagt aan de reputatie. De paragrafen over risicomanagement in de jaarverslagen impliceren dat bedrijven zich meer bewust zijn van de noodzaak om een breed scala van risico's te analyseren en te kijken welke maatregelen zijn genomen om deze risico's te beperken. Het bewustzijn van de risico's en het managen van deze risico's, leiden tot bescherming van het imago en dragen bij aan de reputatie.

Ook hier zien we dat dit het geval is.

6.3 Risicomanagementvolwassenheid, hoe komt u vooruit?

Het onderzoek heeft een schat aan waardevolle informatie opgeleverd inzake de vraag welke factoren bijdragen aan een hogere waardering voor het risicomanagementsysteem van een organisatie. Hiermee kunt u dus direct uw voordeel doen.

Uw Chief Risk Officer helpt u verder, betrokkenheid van het bestuur is cruciaal

Omdat het managen van risico's meer en meer een strategische aangelegenheid wordt, benoemen bedrijven vaker een Chief Risk Officer (CRO) als eindverantwoordelijke voor risicomanagement. Die CRO is enerzijds verantwoordelijk voor de coördinatie van risicomanagement en communica-

tie van de doelstelling en resultaten richting de Raad van Bestuur en beleggers. Zo kan een organisatie de kans op asymmetrische informatie tussen de vertegenwoordigers van de onderneming en de aandeelhouders reduceren. Anderzijds heeft de CRO een voortrekkersrol als het gaat om promotie van risicomanagement richting managers. Bovendien dient de CRO ervoor te zorgen dat het risicomanagementsysteem is afgestemd op de strategie van de organisatie.

In de publieke managementletter van de NBA (2013) wordt er niet expliciet gesproken over een CRO als bekleder van de risicomanagementfunctie, maar in de praktijk is vastgesteld dat slechts een derde van de respondenten een CRO heeft aangesteld, waarbij een kwart die eindverantwoordelijkheid voor risico's heeft belegd in de top van de onderneming. Ons onderzoek toont aan dat het benoemen van een CRO inderdaad aan te raden is, het leidt tot een hogere waardering voor het risicomanagementsysteem. Bijzonder is dat de CRO die niet op directieniveau acteert aanzienlijk beter scoort dan een CRO die wel lid is van de directie. De CRO als 'risk champion' heeft in de praktijk hiermee zijn toegevoegde waarde op het gebied van risicomanagement bewezen. Aanstellen dus zo'n functionaris!

Auditcommissies: Meer zichtbaarheid en relevantie gewenst, minder techniek

De auditcommissie (AC) is in het leven geroepen om toezicht te houden op het bestuur en met name diens plicht om te zorgen voor een betrouwbare financiële verslaggeving. Sinds 2008 is het wettelijk vastgesteld dat een 'Organisatie van Openbaar Belang' een AC dient in te stellen. Dit is het gevolg van de verplichte implementatie van de Europese Richtlijn 2006/43/EG inzake de wettelijke accountantscontrole in Nederland.

Een van de aandachtsgebieden van zo'n AC bij het uitvoeren van haar rol als toezichthouder is risicobeheersing en interne controle. De belangrijkste risico's en de wijze waarop de organisatie deze risico's beheerst, moet de AC in een periodiek overleg bespreken met de Raad van Bestuur/directie en in dat gesprek kan de AC invloed uitoefenen. Zo kan de AC het management aansporen om voldoende aandacht te besteden aan het risicomanagementsysteem en het vrijmaken van budgetten om het risicomanagementsysteem door te ontwikkelen (Paape en Speklé, 2012).

Maar een AC moet wel aan eisen voldoen: een goede AC moet expertise, tijd en betrokkenheid bij de dagelijkse gang van zaken hebben om risico's in zijn geheel goed te kunnen beoordelen. De AC blijkt wel een positieve invloed te hebben op risicomanagement. Een AC kijkt met name instrumenteel naar risicomanagement, maar is op grond van ons onderzoek in de perceptie van de respondenten nog onvoldoende relevant . Respondenten geven aan dat een AC niet bijdraagt aan een hogere waardering voor het risicomanagementsysteem. Hier is dus voor de AC's nog winst te halen.

Internationale diversificatie als natuurlijk risicomanagementmechanisme

Nederland is van oudsher een exportland en is in 2013 zelfs voor het zesde jaar op rij het tweede exportland in de Europese Unie (CBS, 2014). Hiermee zijn internationaal gediversifieerde organisaties een belangrijke pijler voor de Nederlandse economie. Maar een internationaal opererende organisatie krijgt te maken met een grotere complexiteit van risico's (Wagner, 2010) en de daarmee tegelijk toegenomen complexiteit in de organisatiestructuur maakt het gedrag van organisaties voor investeerders minder voorspelbaar en daardoor lastiger te monitoren. Leaven en Levine (2007) stellen dat er hierdoor ruimte ontstaat voor opportunistisch gedrag. Aan de andere kant zorgt internationale diversificatie volgens de portfolio-theorie ervoor dat risico's worden gereduceerd. Dit wordt bereikt door de imperfecte samenhang tussen verschillende gebieden en markten (Carson et al, 2008; Song en Cummins, 2008). Diversificatie heeft dan ook tot gevolg dat er behoefte is aan een meer geavanceerde organisatiestructuur om kennis over te dragen, het coör-

dineren van taken en het effectief toewijzen van middelen (Lang en Stulz, 1994). Internationale diversificatie is hiermee een nieuwe variabele die aan het onderzoek naar risicomanagement in Nederland is toegevoegd. Uit ons onderzoek kan worden geconcludeerd dat internationale diversificatie ertoe leidt dat er een meer volwassen risicomanagementsysteem is.

Toch hebben lang niet alle internationaal opererende organisaties een zelfde mate van volwassenheid ten aanzien van hun ERM. Een derde heeft geen plannen om een risicomanagementsysteem te implementeren en een vijfde denkt er nog over na. Een verklaring kan zijn dat deze organisaties op andere wijze hun risico's in kaart brengen en beheersen.

Risicomanagement steeds meer onder de aandacht van accountants

Accountants zijn ook niet ongeschonden door de crisis gekomen in hun rol als controlerend accountant, zoals al pijnlijk werd aangetoond in het artikel *'Financial Crisis and the silence of the auditor'* (Sikka, 2009) gericht aan de Big4 accountantsfirma's. Ook de Autoriteit Financiële Markten heeft de nodige kritiek geuit op de audit kwaliteit van de accountantskantoren. Dit heeft onder andere geleid tot nieuwe wetgeving op het gebied van verplichte roulatie van accountants bij beursfondsen, nieuwe onafhankelijkheidseisen (ViO) en herziene gedrags- en beroepsregels (VGBA), maar ook de recente, vanuit de sector gepresenteerde hervormingsvoorstellen 'In het publiek belang'.

Big4 accountantsfirma's zijn hierbij primair aangesproken en uit ons onderzoek blijkt dat zij nu primair het voortouw nemen in de discussie. Ondernemingen die gecontroleerd worden door een Big4 accountantsfirma hebben een hogere mate van risicomanagementvolwassenheid dan ondernemingen die door niet-Big4-accountantsfirma's worden gecontroleerd. Een bevinding die in lijn is met Beasley et al. (2005).

Een andere belangrijke ontwikkeling die zal bijdragen aan meer aandacht voor risicomanagement is de klantspecifieke controleverklaring van de accountant. Hiermee hebben Big4-accountanskantoren over het boekjaar 2013 voor het eerst geëxperimenteerd, wat mogelijk een deel van het Big4-effect verklaart. In deze verklaring geeft de accountant uitleg over de belangrijkste door haar geïdentificeerde controlerisico's, gehanteerde toleranties, de continuïteitsveronderstelling en eventueel de reikwijdte van de groepscontrole. Het doel van deze nieuwe verklaring is om de gebruiker van de jaarrekening beter te informeren over wat de accountant nu precies heeft gedaan. De gebruiker wil immers weten welke (risico)gebieden de accountant heeft gesignaleerd en wat hij hieraan heeft gedaan (PwC, 2014).

Een frisse blik doet wonderen

Een voortvloeisel uit de nieuwe regelgeving voor accountants is dat ondernemingen van openbaar belang (oob's) vaker verplicht van accountant dienen te wisselen. Hoewel de wetenschap er nog niet uit is of dit de audit kwaliteit goed doet en er meer bewijs is dat dit de kwaliteit, zeker in de eerste drie jaar na aanstelling, negatief beïnvloedt, is de nieuwe regelgeving wel een feit. Van de accountants mag verwacht worden dat in de planningsfase (klantacceptatie en risico-analyse) aandacht aan risicomanagement wordt besteed. De accountant gebruikt daarvoor de risico-analyse van de klant zelf. Het interne risicomanagementsysteem van de onderneming en de discussie als accountant hierover met de klant zou ondernemingen kunnen uitdagen te reflecteren op hun risicomanagementsysteem en de nieuwe accountant zou een frisse blik hierop kunnen geven. Dit beeld lijkt bevestigd te worden door dit deelonderzoek, dat een statische significante relatie vindt tussen een wisseling van accountantsfirma in de afgelopen drie jaar en een hogere risicomanagementvolwassenheidsscore. Daarnaast lijken (hoewel statistisch niet significant) ondernemingen

die van accountant zijn gewisseld iets negatiever over hun risicomanagementsystemen te zijn, wat enerzijds zou kunnen betekenen dat een frisse blik van een nieuwe accountant leidt tot het inzicht dat er mogelijk nog tekortkomingen in de interne beheersing- en risicomanagementsfeer zitten. Anderzijds leidt een accountantswissel mogelijk tot een realistischer oordeel over het eigen risicomanagement, dus tot minder ruimte tussen eigen waarneming en die van de accountant. Maar omdat de uitkomsten niet significant zijn, bestaat hier nog ruimte voor nader vervolgonderzoek. Als de invloed van een accountantswissel wordt gemeten op basis van de scoreleidraad, blijkt dat de frisse blik van een nieuw aangestelde accountant niet statistisch waarneembaar is.

Risicomanagement als antwoord op toezicht

De eisen van toezichthouders worden door ondernemingen gepercipieerd als de minimale eisen waaraan de onderneming moet voldoen als vorm van compliance, maar ook een vorm van 'license to operate'. Risicomanagement is één van de instrumenten die daarvoor gebruikt wordt (bijvoorbeeld in de vorm van incidentmanagement). Risicomanagement als instrument kan zo fungeren als een vorm van legitimatie richting toezichthouders, om te laten zien dat de aspecten van toezicht in voldoende mate beheerst worden. Op basis van de institutionele theorie, geïntroduceerd door Powell en DiMaggio in 1983, kan aan de hand van isomorfismen (spiegelgedrag) verklaard worden dat risicomanagement gezien gaat worden als een geaccepteerde methode van compliance binnen een sector.

Financiële instellingen kennen ten opzichte van andere sectoren specifieke vereisten ten aanzien van risicomanagement en verplichting tot het hanteren van het 'three lines of defence' principe. De specifieke aandacht voor risicomanagement door DNB (onder andere in de vorm van het themaonderzoek risicomanagement) vindt daarom ook logischerwijs haar uiting in de governance codes van financiële instellingen. Dit ondersteunt ook de theorie van het normatief isomorfisme, risicomanagement als vorm van compliance. Toezicht als vorm van dwang dus tot risicomanagement, dan wel als best practice voor organisaties ter legitimatie.

Governance codes zijn een relevante stimulans, ook bij zelfregulering

Governance codes in zijn geheel dragen positief bij aan de volwassenheid van risicomanagement ten opzichte van sectoren waar geen code geldt. Opvallend hierbij is ook dat de (niet-beursgenoteerde) financiële instellingen een hogere volwassenheidsscore kennen dan beursgenoteerde ondernemingen, wat verklaard kan worden door de explicietere aandacht die aan risicomanagement wordt geschonken in de codes van financiële sector.

Het meest opvallende resultaat uit dit onderzoek is dat de (semi)publieke sector, waar met behulp van gedragscodes wordt gewerkt, in vijf jaar tijd een duidelijke positieve ontwikkeling heeft doorgemaakt in de volwassenheid van haar risicomanagementsysteem. Dit levert bewijs dat zelfregulering door middel van codes positief kan bijdragen aan de volwassenheid van risicomanagement. Governance codes als stimulans voor risicomanagement door de publieke sector werken!

Institutionele beleggers laat van u horen!

Ondernemingen waarbij het eigendom in handen is van institutionele beleggers zijn, evenals in 2009, terughoudend om zich openlijk uit te spreken over hun risicomanagement; zij participeren niet in groten getale in dit onderzoek. Bij de ondernemingen die wel geparticipeerd hebben in dit onderzoek lijkt het effect van institutioneel eigendom niet significant, maar er zijn onvoldoende waarnemingen om een relevante conclusie te kunnen trekken.

Literatuurlijst

Journals

Beasley, M.S., Clune, R., Hermanson, D.R. (2005): Enterprise Risk Management: An Empirical Analysis of Factors Associated with the Extent of Implementation. *Journal of Accounting and Public Policy*, Vol.24, pp 521 - 531.

Busco, C., Frigo, M.L., Giovanni, E., Riccaboni, A., Scapens, R.W. (2005): Beyond compliance, why integrated governance matters today, *Strategic Finance*, 87 (2), pp 35 - 43.

Bushman, R., Chen, Q., Engel, E., Smith, A. (2004): Financial accounting information complexity and corporate governance systems, *Journal of Accounting and Economics*, 37, pp 167 - 201.

Deephouse, D.L. (1996): Does isomorphism legitimate?, *Academy of Management Journal*, 29 (4), pp 1024 - 1039.

DiMaggio, P.J., Powell, W.W. (1983): The iron cage revisited: institutional isomorphism and collective rationality in organization fields, *American Sociological Review*, 48 (2), pp 147 - 160.

Frumkin, P., Galaskiewizc, J. (2004): Institutional isomorphism and public sector organizations, *Journal of public administration research and theory*, 14 (3), pp 283 - 307.

Gates, S., Nicolas, J.L., Walker, P.L. (2012): Enterprise Risk Management: A Process for Enhanced Management and Improved Performance. *Management Accounting Quarterly*, 13 (3), 28 - 38.

Golshan, N.M., Rasid, S.Z.A. (2012): Determinants of Enterprise Risk Management Adoption: An Empirical Analysis of Malaysian Public Listed Firms. *International Journal of Social and Human Sciences vol. 6* pp 119 - 126.

Hillson, D.A. (1997): Towards a risk maturity model, *International Journal of project and business risk management, vol 1, no 1*, pp 35 - 45.

Huber, C., Scheytt, T. (2013): The Dispositif Of Risk Management: Reconstructing Risk Management After The Financial Crisis. *Management Accounting Research*, 24(2), pp 88 - 99.

Jackson, A.B., Moldrich, M., Roebuck, P. (2008): Mandatory audit firm rotation and audit quality, *Managerial Auditing Journal, 23 (5),* pp 420 - 437.

Jensen, M.C., Meckling, W.H. (1976): Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure, *Journal of Financial Economics, 3 (4),* pp 305 - 360.

Johnsen V., Khurana, I., Reynold, J.K. (2002): Audit firm tenure and the quality of financial reports, *Contemporary Accounting Research (winter),* pp 637 - 660.

Johnstone, K.M. (2000): Client acceptance descisions: simultaneous effects of client business risk, audit risk, auditor business risk and risk adaption, *Auditing: A journal of practice and theory*, 19 (1), pp 1 - 25.

Kleffner, A.E., Lee, R.B., McGannon, B. (2003): The effect of corporate governance on the use of enterprise risk management: evidence from Canada, *Risk Management and Insurance Review, 6 (1)*, pp. 53 - 73.

Liebenberg, A.P., Hoyt, R.E. (2003): The determinants of enterprise risk management: evidence from the appointment of chief risk officers, *Risk Management and Insurance Review, 6*, pp. 37 - 52.

Hoyt, R.E., Liebenberg, A. (2011): The value of Enterprise Risk Management, *The Journal of Risk and Insurance, Vol. 78, No. 4*, pp. 795 - 822.

Majone, G. (1997): From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance, *Journal of Public Policy, 17(2)*, pp 139 - 167.

Mikes, A. (2009): Risk management and calculative cultures, *Management Accounting Research*, *20,* pp. 18 - 40.

Paape, L., Speklé, R.F. (2012): The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study, *European Accounting Review, 21 (3)*, pp 533 - 564, DOI: 10.1080/09638180.2012.661937.

Pagach, D., Warr, R. (2011): The Characteristics Of Firms That Hire Chief Risk Officers. *Journal of Risk and Insurance, 78(1),* pp 185 - 211.

Power, M. (2009): The risk management of nothing, Accounting, *Organizations and Society*, 34, pp 849 - 855.

Sikka, P. (2009): Financial crisis and the silence of the auditors, Accounting, *Organizations and society*, 34, pp 868 - 873.

Sobel, P.F., Reding, K.J. (2004): Aligning corporate governance with enterprise risk management, *Management Accounting Quarterly, 5 (2)*, pp 29 - 37.

Spira, L.F., Page, M. (2003): Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing and Accountability Journal, 16*, pp 640 - 661.

Ward, S., (2003): Approaches to integrated risk management: a multi-dimensional framework, Risk management: an international journal, pp 7 - 23.

Wan Daud, W.N., Haron, H., Ibrahim, D.N. (2011): The Role of Quality Board of Directors in Enterprise Risk Management (ERM) Practices: Evidence from Binary Logistic Regression, *International Journal of Business and Management*, 6(12), pp 205 - 211.

Wan Daud, W.N., Yazid, A.S., Hussin, M.R. (2010): The Effect Of Chief Risk Officer (CRO) On Enterprise Risk Management (ERM) Practices: Evidence From Malaysia. *The International Business and Economics Research Journal, 9(11)*, pp 55 - 64.

Woods, M. (2009): A contingency perspective on the risk management control system within Birmingham City Council, *Management Accounting Research, 20*, pp 69 - 81.

Yazid, A.S., Razali, A.R., Hussin, M.R. (2012): Determinants of Enterprise Risk Management (ERM): A Pro-posed Framework for Malysian Public Listed Companies, *International Business Research, 5 (1)*, pp 80 - 86.

Boeken /rapporten/publicaties/scripties

Aktas, E. (2014): Invloed van risicomanagement op de ondernemingsprestaties - perceptie op risicomanagement, *Master thesis Accountancy en Controlling*, Rijksuniversiteit Groningen

Belt, M. van de. (2014): Risicomanagement in Nederland - Hoe accountants, externe toezichthouders, de wetgever en verschillende eigendomsstructuren het volwassenheidsniveau van risicomanagement beïnvloeden, *Master thesis Accountancy en Controlling*, Rijksuniversiteit Groningen

Berry- Stölzle, T.R., Xu, J. (2013): Enterprise Risk Management and the Cost of Capital

Collier, P. M., Berry, A. J., Burke, G. T. (2007): Risk and Management Accounting: Best Practice Guidelines for Enterprise-Wide Internal Control Procedures, *Oxford: CIMA/Elsevier*, ISBN: 978-0-7506-8040-0.

COSO. (2010): Coso's 2010 report on ERM: Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework, *The Committee of Sponsoring Organizations of the Treadway Commission (CO-SO)*.

DeLoach, J.W. (2000): Enterprise Wide Risk Management: Strategies for Linking Risk with Opportunity, *London: Financial Times/Prentice Hall*.

Desender, K. (2007): On the Determinants of Enterprise Risk Management Implementation. Information Resources Management Association Annual Meeting Paper. Electronic copy available at: http://ssrn.com/abstract=1025982.

DNB. (2010): In het spoor van de crisis - achtergronden bij de financiële crisis, De Nederlandse Bank N.V., ISBN 9789 080 478 466.

European Commission. (2010): Audit Policy: Lessons from the crisis, Green Paper, *Brussel*.

EY. (2013): Wie had dit kunnen zien aankomen, white paper december 2013.

Gatzert, N., Martin, M. (2013): Determinants and Value of Enterprise Risk Management: Empirical Evidence from the literature, Working Paper, *Department for Insurance Economics and Risk Management Friedrich-Alexander-University (FAU) of Erlangen-Nurnberg*.

Koninklijke NIVRA Amsterdam, PricewaterhouseCoopers Amsterdam, Nyenrode Breukelen, Rijksuniversiteit Groningen (2009): Risicomanagement in tijden van crisis (en voor en na).

Mertens, F. (2009): De regulerende staat - ontwikkeling in toezicht door inspecties, *Nederlandse School voor Openbaar Bestuur*, ISBN: 978-90-75297-08-9.

Monda, B., Giorgino, M. (2013): An Enterprise Risk Management Maturity model, paper submitted for the Enterprise Risk Management Symposium, April 22 - 24, 2013, Chicago Illinois.

NBA, Nederlandse Beroepsorganisatie van Accountants (2013): Risico's managen is mensenwerk: Risicomanagement en -verslaggeving bij grote ondernemingen.

OECD. (2010): Corporate Governance and the financial crisis: conclusions and emerging good practices to enhance implementation of the principles.

Pagach, D., Warr, R. (2007): An Empirical Investigation Of The Characteristics Of Firms Adopting Enterprise Risk Management. *North Carolina State University working paper*.

Pagach, D., Warr, R. (2010): The effects of Enterprise Risk Management on Firm Performance, Working Paper, *North Carolina State University, Raleigh*

Pooser, D.M. (2012): An Empirical Examination Of The Interrelations Of Risks And The Firm's Relation With Enterprise Risk Management. (3539604 Ph.D.), The Florida State University, Ann Arbor. Retrieved from http://search.proquest.com/docview/1095535349 ProQuest Dissertations en Theses Full Text database.

Posthumus, G.J. (2014): Risicomanagement in Nederland - Een onderzoek naar het effect van de Chief Risk Officer, Audit Commissie en Internationale diversificatie op het volwassenheidsniveau van risicomanagement anno 2014, Master thesis Accountancy en Controlling, *Rijksuniversiteit Groningen*

PwC. (2014): Klare taal! Benchmark controleverklaringen 'nieuwe stijl' onder Nederlandse beursfondsen.

Weick, K.E., Sutcliffe, K.M. (2007): Managing the Unexpected, 2nd ed. *John Wiley en Sons, San Francisco*

Bijlage 1: Methodologische verantwoording

Surveyonderzoek

Om de stand van het huidige risicomanagement in kaart te kunnen brengen is gebruik gemaakt van survey-onderzoek. Dit type onderzoek wordt in de wetenschappelijke literatuur veelvuldig gebruikt om de stand van risicomanagement in kaart te brengen (o.a. Kleffner et al. 2003, Beasley et al., 2005; Gates et al., 2012). In het vorige onderzoek is een conceptueel model ontwikkeld (zie voor een schematisch weergave bijlage 4). Het conceptueel model is ons raamwerk. Dit is mede richtinggevend voor de vragenlijst. Als onderdeel van dit onderzoek is op basis van statistische analyses het conceptueel model geëvalueerd tegen de uitkomsten van de enquête. Daarnaast hebben wij de scoreleidraad die ook tijdens het vorige onderzoek is gehanteerd, opnieuw geëvalueerd en toegepast om zelfstandig een uniforme standaard te hebben om de volwassenheid van het risicomanagementsysteem te meten.

De vragenlijst

Als startpunt om te komen tot een enquête is eerst het uitgangspunt gekozen om de vragenlijst behorend bij het in 2009 gehouden onderzoek te gebruiken. In diverse groepsoverleggen is die vragenlijst geëvalueerd tegen de uitkomsten van het onderzoek. Hierbij is gekeken welke vragen in de praktijk in de interpretatie dan wel de analyse van uitkomsten minder goed werkten. Daarnaast zijn er vragen toegevoegd over cultuur. In de vragen in de sectie algemeen zijn de volgende elementen van interesse toegevoegd: 'extern toezicht' en 'wisseling van accountantsfirma'. Beide vragen zijn vertaald in ja/nee-vragen waardoor dit qua interpretatie duidelijk is. Bij vraag 6 zijn de categorieën toegevoegd voor het aantal landen om een betere gradatie te kunnen geven in de complexiteit die gepaard gaat met internationaal opereren. Vraag 12 over de Chief Risk Officer is aangepast om onderscheid te kunnen maken tussen de functie sec en de betrokkenheid van het management anderzijds in een vergelijkbare functie. Met betrekking tot intern toezicht is in de nieuwe enquête een extra vraag toegevoegd (vraag 10), waarin gevraagd wordt naar de aanwezigheid van een Raad van Commissarissen en/of Raad van Toezicht. Met behulp van deze vraag kan het functioneren van het intern toezichthoudend orgaan beter worden geduid dan door alleen te vragen naar de aanwezigheid van een auditcommissie. Daarnaast zijn de sectoren waarbinnen respondenten opereren geordend naar de CBS-indeling. In het kader van vergelijkbaarheid met 2009 is echter wel een 'omnummertabel' gemaakt om vergelijking mogelijk te maken. Daarnaast is vraag 35, mede in verband met de kritieken vanwege vergelijkbaarheid vanuit het onderzoek van Paape en Speklé (2012), geherformuleerd. Hierop wordt in de onderzoeksresultaten verder ingegaan.

De pilotfase

Voorwaarde voor een goede enquête is dat de vraagstelling duidelijk is en niet tot interpretatiediscussies leidt, wat een eventueel vooroordeel of diversiteit aan interpretaties bij het invullen zou kunnen veroorzaken. Daarnaast moet het invullen niet te veel tijd kosten omdat dit ook verlagend werkt op de response. Nadat de definitieve vragenlijst is opgesteld, is deze vragenlijst vervolgens via het netwerk van de onderzoeksgroep uitgezet naar professionals uit de praktijk van enkele bekende toonaangevende bedrijven (ca. 5 - 10). Opmerkingen die hieruit naar voren zijn gekomen zijn geëvalueerd en qua formulering en/of volgorde van vraagstelling aangepast. Vervolgens is de aangepaste vragenlijst als geheel opnieuw individueel door de onderzoeksgroep beoordeeld. Hieruit is vervolgens de definitieve enquête en begeleidend schrijven vastgesteld.

Onderzoekspopulatie

Evenals in 2009 is het onderzoek gehouden onder alle ondernemingen in Nederland met meer dan € 10 miljoen omzet/budget (overheid/non-profit). Deze grens is gekozen omdat de verwachting is dat bedrijven met minder dan € 10 miljoen omzet geen risicomanagementsystemen hebben (althans niet geformaliseerd). Het onderzoek richt zich op alle organisaties in Nederland, dus geen specifieke sector of deel-groepen. Basis voor de dataset is een export uit de database Company.info (die onder andere gekoppeld is aan de registratie van de Nederlandse Kamer van Koophandel) met sortering naar omzetgegevens. In deze database zijn alle in Nederland geregistreerde organisaties opgenomen. Na analyse van het adressenbestand inclusief aanvullende analyses heeft dit in totaal geleid tot een adressenbestand van 9.582 organisaties.

Verzenden van de enquête

Bij het verzenden van de enquête is bewust nagedacht over de timing. We hebben rekening gehouden met vakantieperiodes en piekperioden qua rapportages/jaarrekeningcontrole van bijvoorbeeld beursfondsen die mogelijk tot ongewenste non-response kan leiden. Binnen de onderzoeksgroep is daarnaast gediscussieerd over de wijze van distribueren (via online survey tools of papieren enquête). Uiteindelijk is gekozen om een papieren enquête uit te zenden. Hiervoor is gekozen omdat de verwachting is dat een uitnodiging per e-mail eerder leidt tot non-response, omdat qua databestand de uitnodiging dan naar een algemeen mailadres van de organisatie wordt verstuurd en het risico bestaat dat de uitnodiging in de spamfilter van de organisatie komt. Hoewel de papieren versie ook redelijk algemeen 'Aan de Raad van Bestuur/Directie van' is verstuurd, die inherent toch een vergelijkbaar risico kennen, blijkt het aandeel van respondenten op directieniveau hoog (52 procent van alle reacties). Daarnaast is via diverse social media de enquête onder de aandacht gebracht om de response te verhogen. Evenals in 2009 wordt enerzijds de mogelijkheid geboden om de enquête anoniem in te vullen (om de response te verhogen). Daarnaast wordt de mogelijkheid geboden om een kopie van het onderzoeksrapport toegezonden te krijgen met vergelijking van de eigen resultaten (op basis van de scoreleidraad) gebenchmarkt ten opzichte van de populatie als geheel om ook deze manier interesse te wekken bij de respondenten.

Respons en non-respons

Van de totaal uitgezonden 9.582 enquêtes zijn er circa. 20 retour gekomen in verband met faillissementen en verkeerde adressering. Dit heeft geleid tot in totaal 727 bruikbare enquêtes, een response van 7,6 procent. Dit ligt daarmee iets lager dan de in 2009 verstuurde enquête, toen 9,9 procent reageerde en de dataset 929 bruikbare reacties op leverde. De response toon echter een representatieve verdeling over profit en non-profit en publiek versus private ondernemingen. Daarnaast zijn ook organisaties van verschillende omvang vertegenwoordigd.

Scoreleidraad

Voor de scoreleidraad hebben we uitgangspunten geformuleerd waaraan een adequaat risicomanagementsysteem volgens ons zou moeten voldoen. Deze uitgangspunten zijn net zoals in 2009 ontleend aan een aantal breed geaccepteerde standaarden van risicomanagement zoals COSO ERM, AS/NZS 4360 2004 en ISO 31000. Ook spelen inzichten opgedaan op grond van praktijkervaringen, onderzoek en interviews een rol.

De scoreleidraad kent daarmee diverse subjectieve elementen die voor discussie vatbaar zijn. Wij juichen discussie toe; wij menen dat dit de ontwikkeling van het risicomanagement ten goede zal komen.

Wij zijn uitgegaan van de volgende zeven principes voor adequaat risicomanagement:

- de periodiciteit/frequentie waarmee risicomanagement wordt toegepast;
- het integrale karakter ervan (reikwijdte, type risico's);
- bedrijfsbrede toepassing (tot op welk niveau in de organisatie doorgevoerd)
- de mate van proactiviteit;
- het expliciete karakter;
- de mate van gestructureerdheid (methodische karakter);
- het periodiek intern dan wel extern rapporteren over risico's en risicomanagement.

Deze uitgangspunten zijn uitgewerkt in 16 vragen verdeeld over de 7 principes. Vervolgens is per principe en daarbinnen per vraag een aantal punten toegekend. Wij verwijzen voor de verdere detaillering van deze puntentoekenning naar de bijgevoegde scoreleidraad (Bijlage 2) waarin per principe de bijbehorende vragen en het maximaal aantal te behalen punten is weergegeven. De vragenlijst en de puntentoekenning is in 2014 ten opzichte van 2009 verder verfijnd. Deze aanpassingen hebben een verwaarloosbaar effect op de scores.

Statistische analyses op het conceptueel model en toevoegde waarde risicomanagement

Aanvullend op de presentatie van de platte onderzoeksresultaten zijn aanvullend ook statistische analyses uitgevoerd om conclusies te trekken over de geldigheid van het conceptueel model in de context van dit onderzoek. Ook zijn er statistische analyses uitgevoerd om een uitspraak te kunnen doen over de door respondenten gepercipieerde toegevoegde waarde van risicomanagement. De conclusies uit deze analyses worden gepresenteerd in hoofdstuk 6. Bij de statistische analyses, uitgevoerd in SPSS, zijn alle noodzakelijke veronderstellingen voor het legitiem gebruik maken van meervoudige lineaire regressie en ordinale regressie getoetst en toereikend bevonden (waaronder multicollinariteit, normaal verdeelde residuen, test op gelijk verdeelde kansen). Daarnaast is er gebruik gemaakt van correlatiematrices en beschrijvende statistiek.

Risicomanagementvolwassenheid

In lijn met wetenschappelijke onderzoeken Beasley et al. (2005) en Paape en Speklé (2012) is ervoor gekozen om volwassenheid te definiëren op basis van de vijf stadia zoals door Beasley et al. voor het eerst geïntroduceerd en uitgevraagd in vraag 35. De uitkomsten zijn daarnaast (deels) geconfronteerd met de uitkomsten zoals deze uit de eigen scoreleidraad zouden komen. Dit leidt echter (met uitzondering van de rol van de auditcommissie) niet tot andere statistisch significante uitkomsten. Hoewel op beide methoden de nodige tekortkoming te benoemen zijn, is de consistentie in uitkomsten tussen beide een bevestiging dat de uitkomsten wetenschappelijk houdbaar zijn.

Definitieverschillen ten opzichte van onderzoekresultaten in hoofdstuk 4

Belangrijk om te benoemen is dat er definitieverschillen kunnen bestaan in de gegevens zoals deze in de onderzoeksresultaten worden gepresenteerd en zoals deze in de statistische analyses zijn gehanteerd. Zo zijn er 43 respondenten uitgesloten in de statistische analyses omdat zij één of meerdere relevante vragen niet hebben beantwoord en alleen volledig ingevulde enquêtes zijn gebruikt. Daarnaast zijn er in definitie van (semi)publieke sector keuzes gemaakt om woningbouwcorporaties die op basis van CBS-indeling in de sector handel terecht komen mee te rekenen als publieke sector, en zijn charitatieve instellingen die in de resultaten als non-profit gelijk gesteld worden met overheid in de statistische analyses niet als (semi)overheid beschouwd. Dit beïnvloedt deels de uitkomsten van de analyse. Hierdoor wordt de conclusie dat de (semi)publieke sector belangrijke stappen heeft gemaakt minder expliciet zichtbaar in de kale onderzoeksresul-

taten. Als laatste merken wij op dat wij de statistische analyses vooral gericht hebben op interne en externe organen, governance-regelgeving en toezicht en minder hebben gekeken naar factoren die min of meer gegeven zijn en minder beïnvloedbaar zijn door managementreacties of die interactie met management tot gevolg hebben. Dus factoren als verhouding vreemd-eigen vermogen (leverage), organisatiegrootte en volatiliteit van resultaten zijn buiten beschouwing gelaten.

Bijlage 2: Scoreleidraad Nationaal Onderzoek Risicomanagement in Nederland 2014

Inleiding

De meting van de kwaliteit van risicomanagement is gebaseerd op 7 kwaliteitsfactoren, identiek aan het onderzoek uitgevoerd in 2009. Het gaat om meetbare factoren. Het maximaal aantal te behalen punten bedraagt 100, onderverdeeld als volgt:

1.	Periodiciteit/frequentie RM	14 punten
2.	Integraal	14 punten
3.	Bedrijfsbreed (en -diep)	14 punten
4.	Pro actief	14 punten
5.	Expliciet	15 punten
6.	Gestructureerd/methodisch	15 punten
7.	Rapportages (intern en extern)	14 punten
	Totaal	100 punten

Deze punten zijn toebedeeld aan een groot aantal vragen in de vragenlijst. Hierna volgt per kwaliteitsfactor een nadere uitleg.

1. Periodiciteit/ frequentie RM, 14 punten maximaal

Vraag 17 (8 punten maximaal)

Hoe vaak wordt in uw organisatie een bedrijfsbrede (voor alle organisatie delen) risico-inventarisatie en risicoanalyse uitgevoerd? *(kies één antwoord)*

- Nooit 0 punten
- Jaarlijks 2 punt
- Eens per kwartaal 4 punten
- Maandelijks 8 punten
- Wekelijks/zeer frequent 8 punten

Vraag 24 (6 punten maximaal)

Hoe vaak wordt intern gerapporteerd naar de Raad van Bestuur/Directie in uw organisatie over risico's en de beheersing daarvan? *(meerdere antwoorden mogelijk)*

- Niet van toepassing 0 punten
- Wekelijks 6 punten
- Maandelijks 6 punten
- Per kwartaal 4 punten
- Jaarlijks 2 punt
- Incidenteel/ad hoc 1 punt
- Anders, namelijk. 1 punt

2. Integraal, 14 punten maximaal

Vraag 19 (14 punten maximaal)
Welke risico's worden daarbij in kaart gebracht? *(meerdere antwoorden mogelijk)*

- Niet van toepassing 0 punten
- Strategische risico's 2 punten
- Financiële risico's 2 punten
- Operationele risico's 2 punten
- (Financiële) rapporteringrisico's 2 punten
- Rechtmatigheidsrisico's 2 punten
- Compliance risico's 2 punten
- Reputatieschade risico's 2 punten

3. Bedrijfsbreed (en -diep), 14 punten maximaal

Vraag 21 (10 punten maximaal)
Op welke managementniveaus worden de risico's uit vraag 19 in kaart gebracht?
(meerdere antwoorden mogelijk)

- Niet van toepassing 0 punten
- Raad van Bestuur/Directie 3 punten
- RvB/Directie en 1e managementniveau 6 punten
- RvB/Directie en 1e en 2e managementniveau 8 punten
- RvB/Directie en 1e, 2e en 3e managementniveau 10 punten
- RvB/Directie en meer dan drie managementniveaus 10 punten

Vraag 28 (4 punten maximaal)
Voor welke organisatielagen word een "in control statement" gevraagd?
(meerdere antwoorden mogelijk)

- Niet van toepassing 0 punten
- In control verklaring van de Raad van Bestuur/Directie 1 punt
- In control verklaring van de 1e management laag (bijvoorbeeld de divisieleiding) 1 punt
- In control verklaring van de 2e management laag (bijvoorbeeld business unit management) 1 punt
- In control verklaring van de 3e management laag (bijvoorbeeld afdelingsmanagement) 1 punt
- In control verklaring van meer dan 3 managementlagen onder de Raad van Bestuur/Directie 1 punt

4. Pro actief, 14 punten maximaal

Vraag 18 (7 punten maximaal)
Wanneer wordt de risico-inventarisatie en risicoanalyse uitgevoerd?
(meerdere antwoorden mogelijk)

- Nooit/niet van toepassing 0 punten
- Als onderdeel van de (jaarlijkse) P&C cyclus 3 punten
- Bij acquisities/investeringen/desinvesteringen 2 punten
- Bij belangrijke projecten/ontwikkelingen 2 punten
- Bij strategische beslissingen 2 punten
- Na belangrijke incidenten 2 punten
- Anders, namelijk: 2 punten

Vraag 26 (7 punten maximaal, 1 punt per antwoord)
Wanneer bespreekt u uw risico's? *(meerdere antwoorden mogelijk)*

- Als onderdeel van de Algemene vergadering van Aandeelhouders (AvA)
- Als onderdeel van overleg met externe partijen, zoals bijvoorbeeld overleg met externe toezichthouders of andere stakeholders
- Als onderdeel van Raad van Bestuur/Directie/Management Team meetings
- Als onderdeel van Business Reviews/bespreking voortgang businessplannen
- Als onderdeel van interne en externe audit rapportagebesprekingen
- Als onderdeel van de Risico Commissie vergaderingen
- Als onderdeel van Audit Commissie/Raad van Commissarissen/Raad van Toezicht vergaderingen
- Als onderdeel van budget/begrotingsbesprekingen
- Ad hoc/bij incidenten/bij grote veranderingen
- Als onderdeel van project(voortgangs)besprekingen
- Anders, namelijk:

5. Expliciet, 15 punten maximaal

Vraag 27 (5 punten maximaal)
Wordt er binnen uw organisatie (intern) gewerkt met een verklaring van het verantwoordelijke management dat hun organisatiedeel 'in control' is zoals bijvoorbeeld door middel van een interne Letter of Representation (LOR) of een ander vergelijkbaar document? *(meerdere antwoorden mogelijk)*

- Nee, geen 'in control' verklaring 0 punten
- Ja, te weten:
- Op het gebied van strategische risico's 1 punt
- Op het gebied van financiële risico's 1 punt
- Op het gebied van operationele risico's 1 punt
- Op het gebied van (financ.) rapporteringsrisico's 1 punt
- Op het gebied van rechtmatigheid risico's 1 punt
- Op het gebied van compliance risico's 1 punt

Vraag 29 (10 punten maximaal)

Is binnen uw organisatie de risicobereidheid bepaald en/of vastgelegd? Dat wil zeggen hoeveel risico de organisatie bereid is te accepteren bij de uitvoering van de strategie of de uitvoering van de activiteiten. *(meerdere antwoorden mogelijk)*

Is de risicobereidheid binnen uw organisatie bepaald? Indien ja:

- Is de risicobereidheid vooral kwalitatief bepaald? 3 punten
- Is de risicobereidheid vooral kwantitatief bepaald 4 punten
- Is de risicobereidheid specifiek bepaald vooréén of meerdere risicogroepen? 1 punt
- Is de risicobereidheid binnen uw organisatie vastgelegd? 2 punten
- Is de risicobereidheid binnen uw organisatie gecommuniceerd? 3 punten

6. Gestructureerd/methodisch, 15 punten maximaal

Vraag 23 (4 punten maximaal, 1 punt per antwoord)

Wilt u aangeven welke van de onderstaande technieken worden gebruikt bij risico-inventarisatie en risicoanalyse? *(meerdere antwoorden mogelijk)*

- Documentenstudie
- Interviews
- Workshops
- Vragenlijsten/checklists
- Incidentenregistraties
- Scenarioanalyses
- Gevoeligheidsanalyses
- Simulaties
- Stress testing
- Value at Risk
- Economic capital
- Back testing
- Serious gaming/war gaming
- Fault tree analysis/foutenboom
- Visgraatmethode
- Hazard and operability study (HAZOP)
- Failure Method and Effects Analysis (FMEA)
- Andere, namelijk

Vraag 30 (3 punten maximaal als één afdeling coördineert. Bij twee afdelingen 2 punten, bij drie afdelingen slechts 1 punt en bij nog meer afdelingen geen punten)

Wie coördineert de activiteiten in het kader van risicomanagement in uw organisatie? *(meerdere antwoorden mogelijk)*

- Een 'dedicated' risicomanagement functie/afdeling
- Een 'dedicated' commissie (risicomanagement comité, etc.)
- Het lijnmanagement
- De financiële functie
- De verzekeringsafdeling
- Internal audit/interne accountantsdienst
- De compliance afdeling
- De kwaliteitsafdeling
- Niet georganiseerd
- Anders, namelijk:

Vraag 31 (2 punten maximaal bij antwoord Ja)

Hanteert u in uw organisatie het (three) 'Lines of Defence' principe?

Vraag 32 (3 punten maximaal)

Heeft u zich bij het inrichten van risicomanagement en interne beheersing in uw organisatie laten beïnvloeden door één van de onderstaande standaarden? *(meerdere antwoorden mogelijk)*

• COSO/COSO ERM	3 punten
• ISO 31000	3 punten
• Management of Risk (M_0_R)	3 punten
• Basel/Solvency	1 punt
• Australian/New Zealand Framework	2 punten
• INK/EFQM model	2 punten
• OCEG	1 punt
• 6Sigma	1 punt
• AIRMIC	2 punten
• Anders, namelijk:	1 punt

Vraag 33 (3 punten maximaal, 1 punt per antwoord)

Welke software gebruikt uw organisatie om risicomanagement te ondersteunen? *(meerdere antwoorden mogelijk)*

- Brainstorm software
- Voting software
- SoD (Segregation of Duties) software
- Data analyzing software
- Procesmanagement software
- Internal audit management software
- Monitoring software
- Performance management software
- Andere, namelijk:

7. Rapportages (intern en extern), 14 punten maximaal

Vraag 25 (7 punten maximaal, 1 punt per antwoord)
Waarover wordt in de interne risicorapportages gerapporteerd?
(meerdere antwoorden mogelijk)

- Niet van toepassing/er zijn geen interne risicorapportages
- De belangrijkste risico's
- De status van de belangrijkste beheersmaatregelen
- Kritieke risico indicatoren (KRI's)
- De ontwikkeling/wijzigingen van risico's
- Incidenten die zich hebben voorgedaan
- Belangrijke interne veranderingen en de gevolgen daarvan voor uw organisatie
- Belangrijke externe veranderingen en de gevolgen daarvan voor uw organisatie
- De status van verbeteracties
- Anders, namelijk:

Vraag 34 (7 punten maximaal, 1 punt per antwoord)
Wat rapporteert uw organisatie extern over risicomanagement, bijvoorbeeld in uw jaarverslag?
(meerdere antwoorden mogelijk)

- De wijze waarop risicomanagement is opgezet
- Brede 'in control' verklaring
  Effectiviteit van risicomanagement/interne beheersing in volle omvang (rapportage heeft betrekking op alle risico's)
- Beperkte 'in control' verklaring
  Effectiviteit van risicomanagement/interne beheersing inzake financiële verslagleggings-risico's (rapportage heeft alleen betrekking op financiële verslagleggingsrisico's)
- De risicobereidheid in kwalitatieve zin
- De risicobereidheid in kwantitatieve zin
- De belangrijkste strategische risico's
- De belangrijkste financiële risico's
- De belangrijkste (financiële) verslagleggingsrisico's
- De belangrijkste operationele risico's
- De belangrijkste compliance risico's
- De belangrijkste verbeterpunten/getroffen maatregelen
- De belangrijkste incidenten die zich hebben voorgedaan
- De materiële gevolgen van incidenten
- De belangrijkste wijzigingen in ons risicoprofiel/interne beheersingssysteem.

Bijlage 3: Vragenlijst onderzoek Risicomanagement in Nederland 2014

Algemene vragen

1. Mijn functie is: _____

2. In welke branche is uw organisatie voornamelijk actief?
   (Kies één antwoord uit onderstaande CBS indeling)

   - o Landbouw, bosbouw en visserij
   - o Winning van delfstoffen
   - o Industrie
   - o Productie en distributie van en handel in elektriciteit, aardgas, stoom en gekoelde lucht
   - o Winning en distributie van water; afval- en afvalwaterbeheer en sanering
   - o Bouwnijverheid
   - o Groot- en detailhandel; reparatie van auto's
   - o Vervoer en opslag
   - o Logies-, maaltijd- en drankverstrekking
   - o Informatie en communicatie
   - o Financiële instellingen
   - o Verhuur van en handel in onroerend goed
   - o Advisering, onderzoek en overige specialistische zakelijke dienstverlening
   - o Verhuur van roerende goederen en overige zakelijke dienstverlening
   - o Beveiliging en opsporing
   - o Openbaar bestuur, overheidsdiensten en verplichte sociale verzekeringen
   - o Onderwijs
   - o Gezondheids- en welzijnszorg
   - o Cultuur, sport en recreatie
   - o Overige dienstverlening
   - o Huishoudens als werkgever; niet-gedifferentieerde productie van goederen en diensten door huishoudens voor eigen gebruik
   - o Extraterritoriale organisaties en lichamen

3. Wat is de jaaromzet van uw onderneming/organisatie per einde laatste boekjaar?
   (Indien omzet bij u niet wordt gebruikt, graag het jaarbudget noemen)

   € _____

4. Wat is het totale aantal medewerkers in 'full time equivalents' werkzaam in uw organisatie per einde laatste boekjaar?

   _____ Fte

5. Geef aan per einde van het laatste boekjaar welke ratio voor uw organisatie van toepassing is voor de verhouding Eigen Vermogen/Vreemd Vermogen (EV/VV).

   o 10% of minder EV/VV
   o 11 tot 20% EV/VV
   o 21 tot 30% EV/VV
   o 31 tot 40% EV/VV
   o meer dan 40% EV/VV

6. In hoeveel landen is uw organisatie actief?

   o 1 land
   o 2 landen
   o 3 landen
   o Meer dan 3 landen

7. Is uw organisatie beursgenoteerd?

   J - N

8. Uw aandelen zijn vooral in het bezit van:
   (kies één antwoord)

   o Niet van toepassing
   o Anonieme aandeelhouders
   o Een aantal institutionele beleggers
   o Één of meerdere families
   o Administratiekantoor (certificaten van aandelen)
   o Banken
   o (Directeur) Grootaandeelhouder
   o Anders, namelijk:

9. Zijn de activiteiten van uw organisatie onderhevig aan toezicht van een externe toezichthouder, zoals bijv. AFM, DNB, ACM (OPTA)?

   J - N

10. Heeft uw organisatie een Raad van Commissarissen/Raad van Toezicht?

    J - N

11. Is er binnen dit toezichthoudende orgaan een Audit Commissie en/of Risico Commissie (bij financiële instellingen) geïnstalleerd?

J - N

12. Is binnen uw organisatie op het niveau van Raad van Bestuur/Directie een afzonderlijke 'Chief Risk Officer' (of vergelijkbare functionaris of functie als "Risico Commisie") aangesteld die eindverantwoordelijk is voor risicomanagement? *(kies één antwoord)*

o Ja, er is een CRO op Raad van Bestuur/Directie niveau
o Ja, er is een CRO, maar niet op Raad van Bestuur/Directie niveau
o Nee, er is geen CRO, maar wel een vergelijkbare functie op Raad van Bestuur/Directie niveau
o Nee, er is geen CRO en ook geen vergelijkbare functie op Raad van Bestuur/Directie niveau

13. Door welke accountantsorganisatie wordt uw jaarverslag gecontroleerd?

---

14. Heeft uw organisatie in de afgelopen 3 jaar een nieuwe externe accountantsorganisatie aangesteld?

J - N

15. Welk rapportcijfer geeft u aan het risicomanagementsysteem van uw organisatie:
(schaal 1 - 10, waarbij 1 de laagste score is en 10 de hoogste)

1 2 3 4 5 6 7 8 9 10

16. In welke mate heeft uw organisatie voordeel van het risicomanagementsysteem?
(schaal 1 - 5, waarbij 1 'geen voordeel' en 5 'heel veel voordeel' aangeeft)

Minder onzekerheid/variatie van resultaten

a. Minder verrassingen	1 - 2 - 3 - 4 - 5
b. Meer vertrouwen in het realiseren van de begroting/doelstellingen	1 - 2 - 3 - 4 - 5
c. Minder afwijkingen ten opzichte van de begroting/planning	1 - 2 - 3 - 4 - 5
d. Lagere vermogenskosten ('lower cost of capital')	1 - 2 - 3 - 4 - 5
e. Meer betrouwbaarder geschatte voorzieningen	1 - 2 - 3 - 4 - 5

Minder schade

f. Minder klachten van klanten/medewerkers	1 - 2 - 3 - 4 - 5
g. Minder en kleinere bedrijfsincidenten	1 - 2 - 3 - 4 - 5
h. Minder claims en rechtszaken	1 - 2 - 3 - 4 - 5
i. Minder aanwijzingen en/of minder boetes van toezichthouders	1 - 2 - 3 - 4 - 5
j. Minder negatieve media aandacht	1 - 2 - 3 - 4 - 5

Betere resultaten

k. Hogere klantentevredenheid	1 - 2 - 3 - 4 - 5
l. Hogere medewerkerstevredenheid	1 - 2 - 3 - 4 - 5
m. Hogere marge	1 - 2 - 3 - 4 - 5
n. Hogere omzet/winstgevendheid	1 - 2 - 3 - 4 - 5
o. Betere reputatie	1 - 2 - 3 - 4 - 5
p. Meer groei/marktaandeel	1 - 2 - 3 - 4 - 5

Vragen inzake risico-inventarisatie en -analyse

17. Hoe vaak wordt in uw organisatie een bedrijfsbrede (voor alle organisatie delen) risico-inventarisatie en risicoanalyse uitgevoerd?
(kies één antwoord)

- o Nooit
- o Jaarlijks
- o Eens per kwartaal
- o Maandelijks
- o Wekelijks/zeer frequent

18. Wanneer wordt de risico-inventarisatie en risicoanalyse uitgevoerd?
(meerdere antwoorden mogelijk)

- o Nooit/niet van toepassing
- o Als onderdeel van de (jaarlijkse) planning & control cyclus
- o Bij acquisities/investeringen/desinvesteringen
- o Bij belangrijke projecten/ontwikkelingen
- o Bij strategische beslissingen
- o Na belangrijke incidenten
- o Anders, namelijk:

19. Welke risico's worden daarbij in kaart gebracht?
(meerdere antwoorden mogelijk)

- o Niet van toepassing
- o Strategische risico's
- o Financiële risico's
- o Operationele risico's
- o (Financiële) rapporteringrisico's
- o Rechtmatigheidsrisico's
- o Compliance risico's
- o Reputatieschade risico's

20. Uit hoeveel managementlagen bestaat uw organisatie?
(kies één antwoord)

- o Uitsluitend Raad van Bestuur/Directie
- o Raad van Bestuur/Directie en één managementniveau daaronder
- o Raad van Bestuur/Directie en twee managementniveaus daaronder
- o Raad van Bestuur/Directie en drie managementniveaus daaronder
- o Raad van Bestuur/Directie en meer dan drie managementniveaus daaronder

21. Op welke managementniveaus worden de risico's uit vraag 19 in kaart gebracht?
(meerdere antwoorden mogelijk)

- o Niet van toepassing
- o Raad van Bestuur/Directie
- o Raad van Bestuur/Directie en 1e managementniveau
- o Raad van Bestuur/Directie en 1e en 2e managementniveau
- o Raad van Bestuur/Directie en 1e, 2e en 3e managementniveau
- o Raad van Bestuur/Directie en meer dan drie managementniveaus

22. Welke technieken worden in uw organisatie gebruikt bij risico-inventarisatie en risicoanalyse?
(meerdere antwoorden mogelijk)

- o Kwantitatieve technieken
- o Kwalitatieve technieken

23. Wilt u aangeven welke van de onderstaande technieken worden gebruikt bij risico-inventarisatie en risicoanalyse?
(meerdere antwoorden mogelijk)

	Ja	Nee	Weet niet
a. Documentenstudie			
b. Interviews			
c. Workshops			
d. Vragenlijsten/checklists			
e. Incidentenregistraties			
f. Scenarioanalyses			
g. Gevoeligheidsanalyses			
h. Simulaties			
i. Stress testing			
j. Value at Risk			
k. Economic capital			
l. Back testing			
m. Serious gaming/war gaming			

	Ja	Nee	Weet niet
n. Fault tree analysis/foutenboom o. Visgraatmethode p. Hazard and operability study (HAZOP) q. Failure Method and Effects Analysis (FMEA) r. Andere, namelijk:			

Vragen inzake risicomanagementrapportage en -monitoring

24. Hoe vaak wordt intern gerapporteerd naar de Raad van Bestuur/Directie in uw organisatie over risico's en de beheersing daarvan?
(meerdere antwoorden mogelijk)

- o Niet van toepassing
- o Wekelijks
- o Maandelijks
- o Per kwartaal
- o Jaarlijks
- o Incidenteel/ad hoc
- o Anders, namelijk:

25. Waarover wordt in de interne risicorapportages gerapporteerd?
(meerdere antwoorden mogelijk)

- o Niet van toepassing/er zijn geen interne risicorapportages
- o De belangrijkste risico's
- o De status van de belangrijkste beheersmaatregelen
- o Kritieke risico indicatoren (KRI's)
- o De ontwikkeling/wijzigingen van risico's
- o Incidenten die zich hebben voorgedaan
- o Belangrijke interne veranderingen en de gevolgen daarvan voor uw organisatie
- o Belangrijke externe veranderingen en de gevolgen daarvan voor uw organisatie
- o De status van verbeteracties
- o Anders, namelijk:

26. Wanneer bespreekt u uw risico's?
(meerdere antwoorden mogelijk)

- o Als onderdeel van de Algemene vergadering van Aandeelhouders (AvA)
- o Als onderdeel van overleg met externe partijen, zoals bijvoorbeeld overleg met externe toezichthouders of andere stakeholders
- o Als onderdeel van Raad van Bestuur/Directie/Management Team meetings
- o Als onderdeel van Business Reviews/bespreking voortgang businessplannen
- o Als onderdeel van interne en externe audit rapportagebesprekingen

- o Als onderdeel van de Risico Commissie vergaderingen
- o Als onderdeel van Audit Commissie/Raad van Commissarissen/Raad van Toezicht vergaderingen
- o Als onderdeel van budget/begrotingsbesprekingen
- o Ad hoc/bij incidenten/bij grote veranderingen
- o Als onderdeel van project(voortgangs)besprekingen
- o Anders, namelijk:

27. Wordt er binnen uw organisatie (intern) gewerkt met een verklaring van het verantwoordelijke management dat hun organisatiedeel 'in control' is zoals bijvoorbeeld door middel van een interne Letter of Representation (LOR) of een ander vergelijkbaar document?
(meerdere antwoorden mogelijk)

- o Nee, geen 'in control' verklaring
- o Ja, te weten:
- o Op het gebied van strategische risico's
- o Op het gebied van financiële risico's
- o Op het gebied van operationele risico's
- o Op het gebied van (financiële) rapporteringsrisico's
- o Op het gebied van rechtmatigheid risico's
- o Op het gebied van compliance risico's

28. Voor welke organisatielagen word een "in control statement" gevraagd?
(meerdere antwoorden mogelijk)

- o Niet van toepassing
- o In control verklaring van de Raad van Bestuur/Directie
- o In control verklaring van de 1e management laag (bijvoorbeeld de divisieleiding)
- o In control verklaring van de 2e management laag (bijvoorbeeld business unit management)
- o In control verklaring van de 3e management laag (bijvoorbeeld afdelingsmanagement)
- o In control verklaring van meer dan 3 managementlagen onder de Raad van Bestuur/ Directie

Vragen inzake risicomanagement en -organisatie

29. Is binnen uw organisatie de risicobereidheid bepaald en/of vastgelegd? Dat wil zeggen hoeveel risico de organisatie bereid is te accepteren bij de uitvoering van de strategie of de uitvoering van de activiteiten.
(meerdere antwoorden mogelijk)

	Ja	Nee	Weet niet
a. Is de risicobereidheid binnen uw organisatie bepaald? Indien ja: b. Is de risicobereidheid vooral kwalitatief bepaald? c. Is de risicobereidheid vooral kwantitatief bepaald d. Is de risicobereidheid specifiek bepaald voor één of meerdere risicogroepen? e. Is de risicobereidheid binnen uw organisatie vastgelegd? f. Is de risicobereidheid binnen uw organisatie gecommuniceerd?			

30. Wie coördineert de activiteiten in het kader van risicomanagement in uw organisatie?
(meerdere antwoorden mogelijk)

- o Een verbijzonderde risicomanagement functie/afdeling
- o Een verbijzonderde commissie (risicomanagement comité, etc.)
- o Het lijnmanagement
- o De financiële functie
- o De verzekeringsafdeling
- o Internal audit/interne accountantsdienst
- o De compliance afdeling
- o De kwaliteitsafdeling
- o Niet georganiseerd
- o Anders, namelijk:

31. Hanteert u in uw organisatie het (three) 'Lines of Defence' principe?

J - N

32. Heeft u zich bij het inrichten van risicomanagement en interne beheersing in uw organisatie laten beïnvloeden door één van de onderstaande standaarden?
(meerdere antwoorden mogelijk)

- o Niet van toepassing/Wij hebben ons niet door een standaard laten beïnvloeden

	Ja	Nee	Weet niet
a. COSO/COSO ERM b. ISO 31000 c. Management of Risk (M_o_R) d. Basel/Solvency e. Australian/New Zealand Framework f. INK/EFQM model g. OCEG h. 6Sigma i. AIRMIC j. Andere, namelijk:			

33. Welke software gebruikt uw organisatie om risicomanagement te ondersteunen?
(meerdere antwoorden mogelijk)

o Niet van toepassing/Wij gebruiken geen software voor risicomanagement

Brede zogenaamde GRC platforms (risicodata management software)	Ja	Nee	Weet niet
a. Metricstream b. Nasdaq OMX Bwise c. EMC (RSA Archer) d. Thomson Reuters (Accelus) e. SAP (GRC) f. IBM (OpenPages) g. Enablon h. Software AG (Aris) i. Wynyard (Methodware) j. Zelfontwikkelde software k. Andere, namelijk:			
Overige ondersteunende software (enkelvoudige functionaliteit) (eventueel aanvullend op hierboven genoemde software)	**Ja**	**Nee**	**Weet niet**
l. Brainstorm software m. Voting software n. SoD (Segregation of Duties) software o. Data-analyzing software p. Procesmanagement software q. Internal audit management software r. Monitoring software s. Performance management software t. Andere, namelijk:			

34. Wat rapporteert uw organisatie extern over risicomanagement, bijvoorbeeld in uw jaarverslag?
(meerdere antwoorden mogelijk)

- o De wijze waarop risicomanagement is opgezet
- o Brede 'in control' verklaring
  Effectiviteit van risicomanagement/interne beheersing in volle omvang (rapportage heeft betrekking op alle risico's)
- o Beperkte 'in control' verklaring
  Effectiviteit van risicomanagement/interne beheersing inzake financiële verslagleggings-risico's (rapportage heeft alleen betrekking op financiële verslagleggingsrisico's)
- o De risicobereidheid in kwalitatieve zin
- o De risicobereidheid in kwantitatieve zin
- o De belangrijkste strategische risico's
- o De belangrijkste financiële risico's
- o De belangrijkste (financiële) verslagleggingsrisico's
- o De belangrijkste operationele risico's
- o De belangrijkste compliance risico's
- o De belangrijkste verbeterpunten/getroffen maatregelen
- o De belangrijkste incidenten die zich hebben voorgedaan
- o De materiële gevolgen van incidenten
- o De belangrijkste wijzigingen in ons risicoprofiel/interne beheersingssysteem
- o Niets

35. Wilt u aangeven in welk van de opeenvolgende stadia van volwassenheid van het risico-managementsysteem uw organisatie is in te delen?
(kies één antwoord)

- o Stadium 1: Er bestaan op dit moment geen plannen om een risicomanagementsysteem te implementeren.
- o Stadium 2: Wij onderzoeken de mogelijkheid om een risicomanagementsysteem te implementeren, maar hebben nog geen definitieve beslissing genomen.
- o Stadium 3: Wij plannen op dit moment de implementatie van een risicomanagement-systeem.
- o Stadium 4: Op dit moment is een risicomanagementsysteem gedeeltelijk aanwezig en geïmplementeerd.
- o Stadium 5: Een volledig risicomanagementsysteem voor Enterprise Risk Management is aanwezig en geïmplementeerd.

Vragen inzake risicocultuur

36. Wie schrijft de risicoparagraaf in uw jaarverslag?
(meerdere antwoorden mogelijk)

- o Niet van toepassing
- o Algemeen directeur
- o De financiële functie (cfo, Hoofd financiële administratie, treasury afdeling)

- o De risicomanager/IC functionaris/GRC functionaris
- o De bestuurssecretaris/secretariële functie
- o De juridische afdeling
- o Anders, namelijk:

37. In welke mate wordt in het belonings- en waarderingssystemen van uw bestuur en lijn managers rekening gehouden met de effectiviteit van risicomanagement?
(kies één antwoord)

- o Er is een directe formele relatie tussen de effectiviteit van risicomanagement en de belonings- en waarderingssystemen.
- o Er is geen directe relatie, maar informeel wordt risicomanagement wel meegenomen in de belonings- en waarderingssystemen.
- o Er is geen enkele relatie tussen de effectiviteit van risicomanagement en de belonings- en waarderingssystemen.

38. In welke mate bent u het eens met de volgende stellingen over risicomanagement?
(schaal 1 - 5, waarbij 1 'oneens' en 5 'eens' aangeeft)

Stellingen over risicomanagement

a. Risicomanagement wordt uitgevoerd omdat dat bijdraagt aan een betere bedrijfsvoering en wordt niet gezien als een kostenpost.	1 - 2 - 3 - 4 - 5
b. Medewerkers worden gemotiveerd om als ze risico's nemen, dit weloverwogen te doen.	1 - 2 - 3 - 4 - 5
c. Een positie binnen risico management wordt gezien als versterking van je carrière.	1 - 2 - 3 - 4 - 5
d. Fouten maken mag, als je er maar van leert (lerende organisatie).	1 - 2 - 3 - 4 - 5
e. De cultuur in onze organisatie bevordert risicomanagement.	1 - 2 - 3 - 4 - 5
f. Overtredingen van interne regels worden zeer serieus genomen en bestraft.	1 - 2 - 3 - 4 - 5
g. De Raad van Bestuur/Directie is zeer gecommitteerd aan risicomanagement en ondersteunt dat actief.	1 - 2 - 3 - 4 - 5
h. Medewerkers voelen zich vrij om risico's aan te kaarten bij hun leidinggevenden.	1 - 2 - 3 - 4 - 5
i. In onze organisatie ligt de nadruk vooral op korte termijn resultaten.	1 - 2 - 3 - 4 - 5
j. De beloningsstructuur bevordert het nemen van risico's.	1 - 2 - 3 - 4 - 5
k. Er wordt een duidelijke relatie gelegd tussen te behalen doelen, risico's en de beloning.	1 - 2 - 3 - 4 - 5

39. Heeft u nog opmerkingen naar aanleiding van deze enquête?

Organisatie: _____

Uw naam: _____

Uw functie: _____

Adres: _____

Postcode/woonplaats: _____

Uw e-mailadres: _____

Bijlage 4: Conceptueel model